Proceedings of the 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA 2018)
IEEE Conference Record # 42487; IEEE Xplore ISBN:978-1-5386-0965-1

Image Encryption based on Neural Network Architecture and Chaotic Systems

Gollapudi Venkata Sai Eswar Bharadwaj
gvseswar1995@gmail.com
Vellore Institute of Technology
Vellore, Tamil Nadu, India

Katikem Vijaya
vijaya14920914@gmail.com
Vellore Institute of Technology
Vellore, Tamil Nadu, India

Sandeep Kumar Balaga
san.kumar423@gmail.com
Vellore Institute of Technology
Vellore, Tamil Nadu, India

Thanikaiselvan V
thanikaiselvan@vit.ac.in
Vellore Institute of Technology
Vellore, Tamil Nadu, India

***Abstract*— In this digital era security is an issue that is to be addressed. For this purpose, a variety of encryption techniques are being developed. This paper looks into a technique of image encryption/decryption that utilizes 3 layers of mapping of pixels on different levels of the RGB planes. Two of them are intraplanar processes and one is an interplanar process to ensure security on all levels. The first layer is a 2 Dimensional logistic mapping that happens on all the 3 RGB planes but only in the plane. The second layer, inspired by Neural Network architecture, adds weights to the individual pixels and shuffling takes place between the 3 RGB planes. In this layer, 3 chaotic functions are used to generate respective weights for the pixels. These functions are Newton-Leipnik chaotic system, Rossler attractor equations, Volta chaotic system. The third layer is again a 2 Dimensional mapping using Duffing map that shuffles the pixels in the planes. This technique has three layers which further have sub-layers make it a more secure technique.**

Keywords*— *encryption; Rossler chaotic system; Newton-Leipnik chaotic system; Volta chaotic system; Duffing chaotic system; Neural Networks

I. INTRODUCTION

The advanced technology of this Digital age made our store and communicate terabytes of information with ease. With the advent of affordable capturing devices such as smartphones, ubiquitous network connection, and free social networking service images are generated and shared online at a staggering rate of 300 million pictures per day on Facebook itself. Free cloud storage services for the encouraged users to store personal images for the ease of access.

But in these latest years, it's also critical to keep the statistics securely. So researchers have developed an eager interest in a number of private conversation methods. The most common structure used is the permutation-diffusion structure for information encryption. It encrypts the data in iterative stages in this type of photo cryptosystems. The permutation layer adjusts the placement of the photo pixels but not the values of it and the diffusion stage takes care of the changes inside the values in one of these manner that a minor change inside the values impacts on nearly all the pixels of the photo.

There exist various methods that are used extensively in securing data.These employ standard methods of ciphering to achieve encryption. Some of these are
a) Steganography: it is the hiding of a secret message, which could be data/image within an ordinary data (text/image) and the Retrieval of data at its destination.
b) Watermarking: it is the process of hiding digital data in another signal (voice/text/image); the digital data should, but doesn't need to contain a relation with that signal (voice/text/image). It may be used to check the authenticity of the signal (voice/text/image) or to show the identity of its owners
c) Encryption: the modification of data (voice/text/image), such that a 3rd party cannot interfere with the data

[1] talks about compressive sensing, in which the data is compressed first that offers a layer of protection and later a chaos-based encryption is performed.[2]talks about cellular neural networks integrated with fuzzy logic(FCNN)[3] utilizes chaotic functions in a neural network architecture for encryption [4]discusses utilizing two rounds of high seed scrambling and pixel adaptive diffusion to randomly shuffle pixels.[5]utilizes cosine number transform that avoids rounding off errors to retrieve an unscathed image.[6]proposes a scheme where the image is combined with first with a random phase mask at the object plane and then is transformed using fractional Fourier transform.[7] discusses an approach which combines a substitute watermarking algorithm, the quantization index modulation, with an encryption algorithm such as the RC4.in [8] an encryption algorithm using a secret key of 128 bits is proposed and processed through key dependant diffusion and substitution processes.[9] deals with synchronization scheme for two fractional chaotic systems and is encoded by a nonlinear function of the fractional chaotic state.[10] is based on the integration of encryption in a compression process based on DCT(Discrete Cosine Transform).

II. RELATED SYSTEMS

As stated earlier, chaotic systems, as well as neural networks, are required to produce the desired chaotic neural network for the image encryption. The details of implementing this network will be described in Section 3. Beforehand, a short introduction to the employed chaotic systems, the logistic map, the duffing map permutation algorithms are presented below as follows:

2.1 *Logistic map*

This mapping is used for the polynomial mapping (equivalently, recurrence relation) of degree 2, which is the archetypal example of how complex, chaotic behavior is taken from the very simple non-linear dynamical equations.

$$x_{n+1} = r x_n (1 - x_n)$$

2.2 *Rössler attractor system*

A system with non-linear ordinary differential equations where we are using its continuous-time dynamical system which exhibits chaotic dynamics and factual properties. In the time domain, it becomes apparent that although each variable is oscillating within a fixed range of values, the oscillations are chaotic, which is clearly presented by its spiral graph.

$$\frac{dx}{dt} = -y - z$$
$$\frac{dy}{dt} = x + ay$$
$$\frac{dz}{dt} = b + z(x - c)$$

2.3 *Volta system*

A fractional chaotic system with the same structure and different orders is changed to the chaotic systems with identical orders and different structures according to the property of fractional differentiation. It displays double scroll attractor

$$\dot{x}(t) = -x(t) - 5y(t) - z(t)y(t),$$
$$\dot{y}(t) = -y(t) - 85x(t) - x(t)z(t),$$
$$\dot{z}(t) = 0.5z(t) + x(t)y(t) + 1.$$

2.4 *Newton-Leipnik system*

A chaotic system working on the synchronization and effective linear feedback controllers are proposed for stabilizing chaos to unstable equilibria to activation of the control scheme.

$$\dot{x} = -ax + y + 10\,yz$$
$$\dot{y} = -x - 0.4y + 5\,xz,$$
$$\dot{z} = bz - 5\,xy$$

2.4 *Duffing map*

The Duffing map is a discrete time dynamical system that exhibits chaotic behavior. It takes the point (x_n, y_n) in the plane and maps it to a new point given by these are usually set to a = 2.75 and b = 0.2 to produce chaotic behavior

$$x_{n+1} = y_n$$
$$y_{n+1} = -bx_n + ay_n - y_n^3.$$

III. PROPOSED SCHEME

3.1.1 Block Diagram Encryption

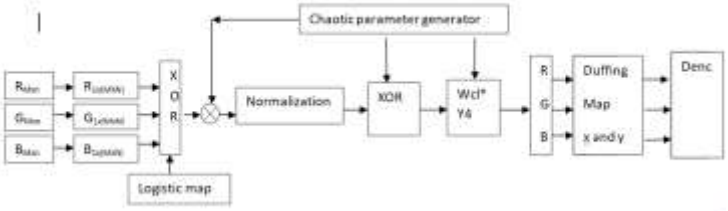

Fig. 1. Block Diagram of Encryption

3.1.2 Block Diagram Decryption

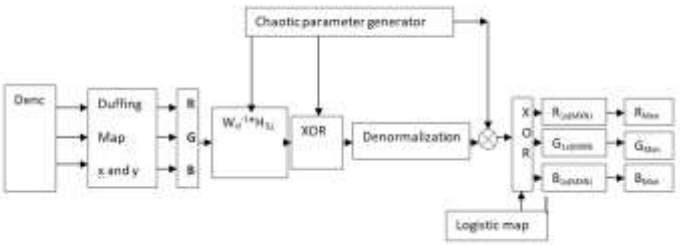

Fig. 2. Block Diagram of Decryption

3.2 *Encryption Algorithm*

Step 1: Read the 3D color image(X) and split it into its respective planes i.e., R, G, B as Xl_R, Xl_G, Xl_B and then linearize them into a 1D array.

Step 2: Iterate the Logistic map system to obtain 3 different chaotic sequence with parameter γ = 3.999, 0.3, 0.33,0.333 as initial values of 3 different cases to generate logi(j,i) j=1, 2, 3

Step 3: Perform the bitXOR operation

$$Xk = (\text{floor}(\text{mod}(\text{logi}(j,i) * 10^{14}, 256)) \oplus (Xl_j)$$

i.e.

j =1, 2, 3 (R, G, B) respectively.

Step4: Selective initial values are given and then split into 9 nine initial parameters

i.e. x1 x2 x3 ; y1 y2 y3 ; z1 z2 z3 ;
Step 5: Iterate the systems Rössler attractor, Volta system, Newton-Leipnik with the above initial conditions using Range-Kutta method of order 4 to generate 3 different sequences of chaotic values.
Step 6: For an image of size NxN pixels, i=1.....NxN, for each i^{th} iteration. Compute W_{dl}, $B_{dl,}$ and W_{cl} as follow:

$$W_{dl}=\begin{bmatrix} x1(i) & x2(i) & x3(i) \\ y1(i) & y2(i) & y3(i) \\ z1(i) & z2(i) & z3(i) \end{bmatrix}$$

$$B(j,i)=(\mathrm{mod}(|y_j(i)|)-\mathrm{floor}(y_j(i))*10^{14},255)+1 \quad ;j=1,2,3$$

Where $W_{dl,i}$ is the weigh matrix ; $B_{dl,i}$ is the bias matrix

mod(x,y) returns the remainder after division; floor(x) rounds the elements of x to the nearest integer less than or equal to x

Step 7: the next matrix to be calculated is W_{cl}. This would be used in the linear shifting of the 3 color components of the image. To determine W_{cl}, we take:

$$D_i=[x_1(i), y_2(i), z_3(i)]$$

$$w_{1,i}=\arg(\max(D_i))$$

$w_{2,i}=\arg(\max(D_i))$; where $\arg(\max(D_i))$ means the index of the maximum value in the sequence D_i.Then the non zero term in the first and second rows of the matrix $W_{cl,\,i}$ is determined as

$$W_{cl,i}(1,w_{1,i})= W_{cl,i}(2,w_{2,i})=1$$

And the non-zero term of the third row is determined such that there exists just one 1 in each column of the matrix $W_{cl,\,k}$.
Step 8: $E_{1,i} = W_{dl,i} * X_{k,i}$ i=1, 2, 3
Step 9: normalization: this is to map the values of the processed image which may exceed the boundaries to a range of [1,255].This is achieved as follows

$$E_{2,i}=N(E_{1,i}) ; \qquad N(x)=255*[\tanh\frac{x}{\max(\max(x))}]+1$$

Step 10: $E_{3,i}=\mathrm{floor}(E_{2,i})+\mathrm{mod}(E_{2,i},\mathrm{floor}(E_{2,i}))$
$E_{31,i}= \mathrm{floor}(E_{2,i})$; $E_{32,i}= \mathrm{mod}(E_{2,i},\mathrm{floor}(E_{2,i}))$

Step 11: XOR Operation
$E_{4,i}=(\mathrm{floor}(E_{31}(j,i))\oplus\mathrm{floor}(B_{dl}(j,i))$; j=1,2,3

Step 12:$E_{5,i}=W_{cl,i}*E_{4,i}$

Step 13: Generate a chaotic sequence using Duffing map Algorithm, specifically sequences Duffing $X(D_x)$ and Duffing $Y(D_y)$ with initial condition as x=0,y=0.3,toensure there are two layers of encryption here
Step 14: XOR operation
the two layers of encryption are: e1, e2

$$e1_{j,i}=E_{5,i}\oplus D_x(i)$$
$$e2_{j,i}=e1_{j,i}\oplus D_y(i)$$

At last we delineraize the array into a NxN matrix with 3 layers to represent a Color image

Decryption algorithm

Step 1: take the encrypted image as the input, split the planes and linearize them into an 1-D array
DE_1 = en; H_1(j,i)=(split planes linearized)

Step 2: Generate a chaotic sequence using Duffing map Algorithm, specifically sequences Duffing X(D_x) and Duffing Y(D_y) with the initial condition as x=0,y=0.3.
Step 3: XOR Operation

$$DE_{2,i}=DE_{1,i}\oplus D_y(i)$$
$$DE_{3,i}=DE_{2,i}\oplus D_x(i)$$

Step 4: we have the initial values declared earlier
i.e. x1 x2 x3 ; y1 y2 y3 ; z1 z2 z3 ;
Iterate the systems: Rossler attractor, Volta system, Newton-Leipnik with the above initial conditions using Range-Kutta method of order 4 to generate different sequences of chaotic values.
Compute:W_{dl},B_{dl} and W_{cl}.

Step 5: $DE_{4,i}={W_{cl,i}}^{-1} * DE_{3,i}$
$DE_{5,i}=\mathrm{floor}(DE_{4,i})$
$DE_{52,i}=DE_{5,i}$

Step 6:XOR operation
$DE_{6,i}=|DE_{5,i}|\oplus|\mathrm{floor}(B_{dl}(j,i)|$;j=1,2,3
$DE_{7,i}=DE_{6,i}+DE_{52,i}$

Step 6: denormalization

$DE_{8,i}=N^{-1}(DE_{7,i})$
$N^{-1}(x)=\mathrm{atanh}[\frac{x-1}{255}]*\max(\max(x))$

Step 7: $DE_{9,i}={W_{dl,i}}^{-1}*DE_{8,i}$

Step 8: Iterate the Logistic map system to obtain 3 different chaotic sequence with parameter γ = 3.999, 0.3, 0.33, 0.333 as initial values of 3 different cases to generate logi(j,i) j=1, 2, 3
Step 9: Perform the bitXOR operation

i.e. $Dec=(floor(mod(logi(j,i)*10^{14},256) \oplus (DE_{9,i}),$

where j =1,2,3 (R,G,B)respectively.

The obtained "Dec" is the final decrypted image.

IV. RESULTS AND DISCUSSIONS

Fig. 3. (Lena) Real image- Encrypted image- Decrypted image

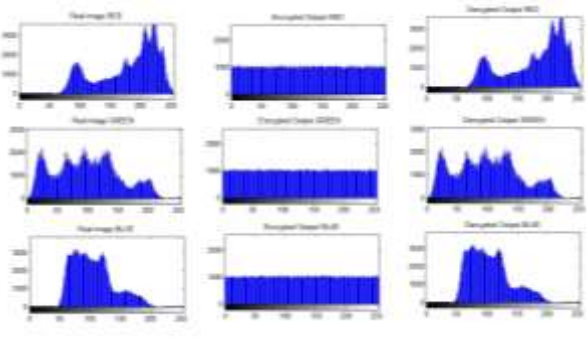

Fig. 4. Histogram analysis of real, encrypted, decrypted images on all 3 planes Red Green Blue respectively

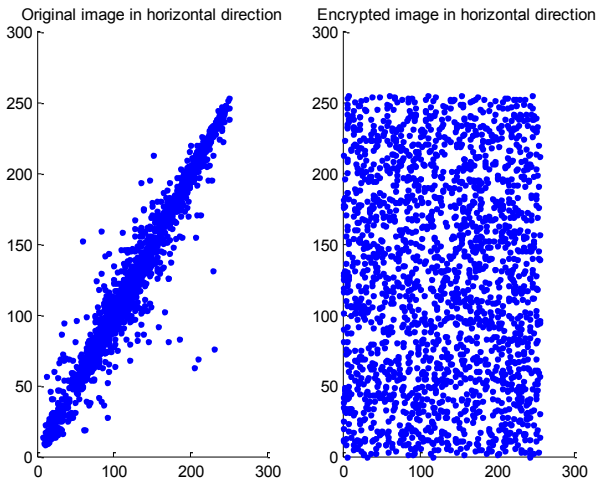

Fig. 5. Scatter plot of original and encrypted images in horizontal direction

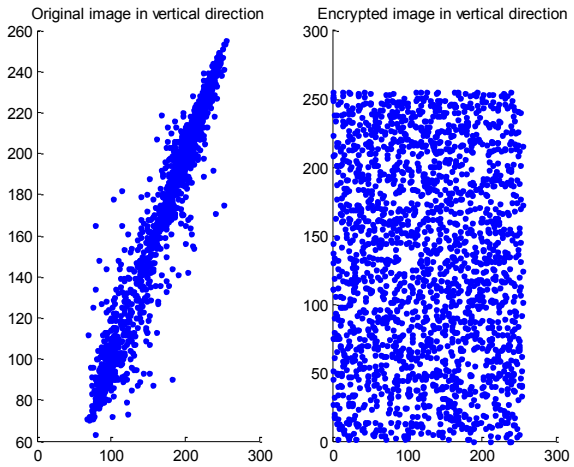

Fig. 6. Scatter plot of original and encrypted images in vertical direction

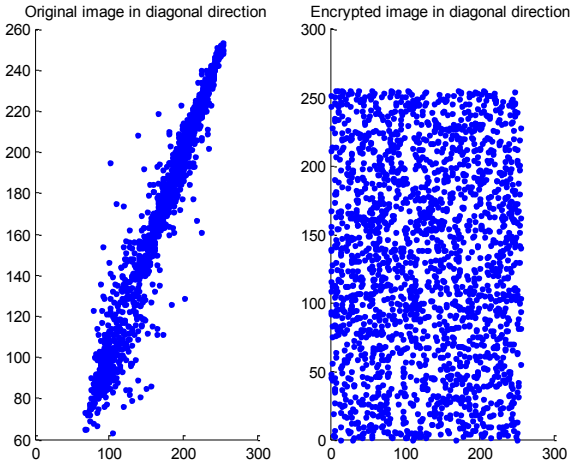

Fig. 7. Scatter plot of original and encrypted images in diagonal direction

Correlation Coefficient	Original Image	Encrypted Image
Horizontal	0.9784	-0.0076
Vertical	0.9661	-0.0041
Diagonal	0.9728	0.0366

Table. 1. Correlation coefficient analysis of Lena image

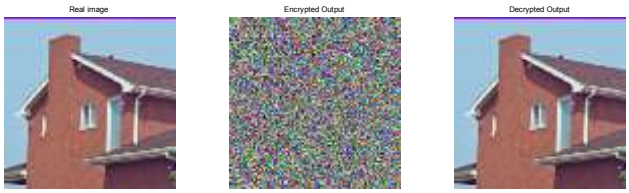

Fig. 8. (home) Real image- Encrypted image- Decrypted image

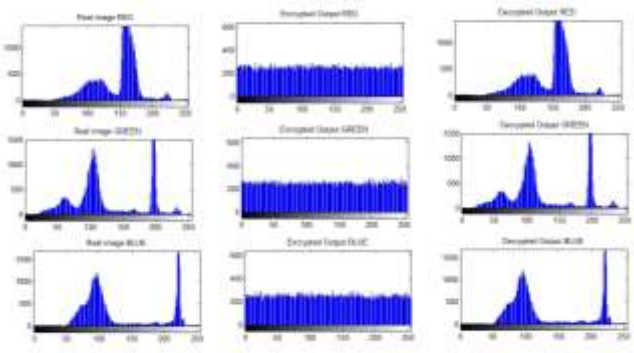

Fig. 9. Histogram analysis of real, encrypted, decrypted images on all 3 planes Red Green Blue respectively

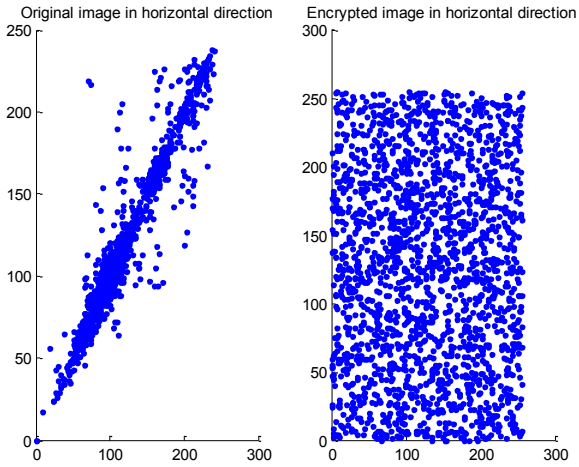

Fig. 10. Scatter plot of original and encrypted images in horizontal direction

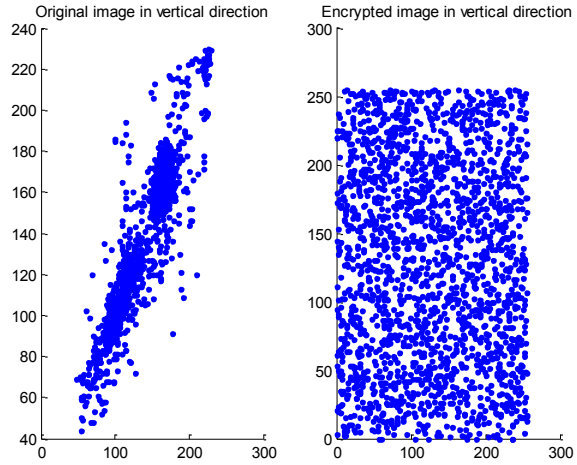

Fig. 11. Scatter plot of original and encrypted images in vertical direction

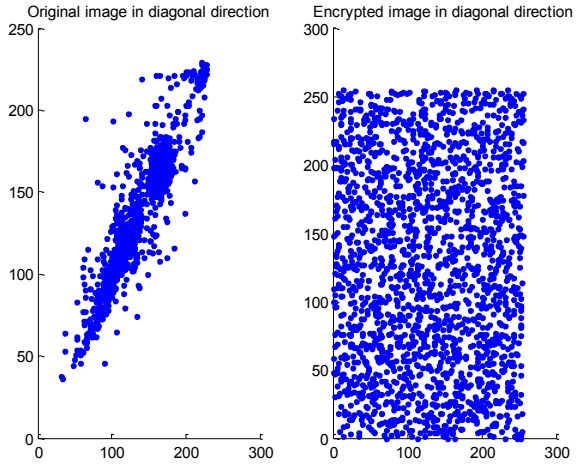

Fig. 12. Scatter plot of original and encrypted images in diagonal direction

Correlation Coefficient	Original Image	Encrypted Image
Horizontal	0.9733	-0.0140
Vertical	0.9154	-0.0234
Diagonal	0.9204	-0.0150

Table. 2. Correlation coefficient analysis of home image

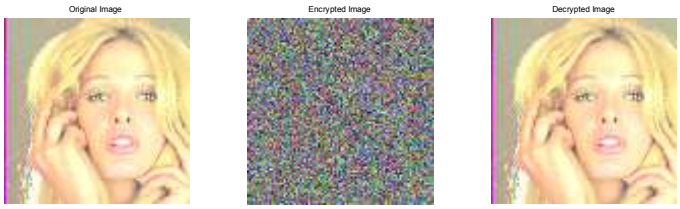

Fig. 13. (lady) Real image- Encrypted image- Decrypted image

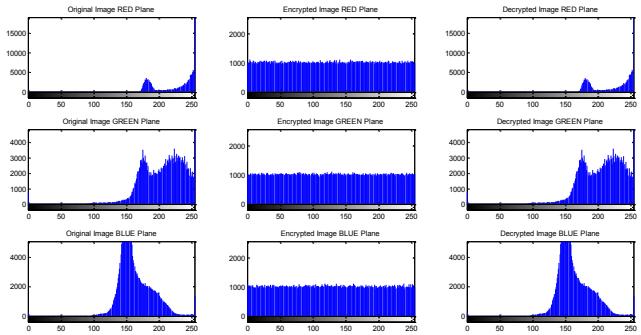

Fig. 14. Histogram analysis of real, encrypted, decrypted images on all 3 planes Red Green Blue respectively

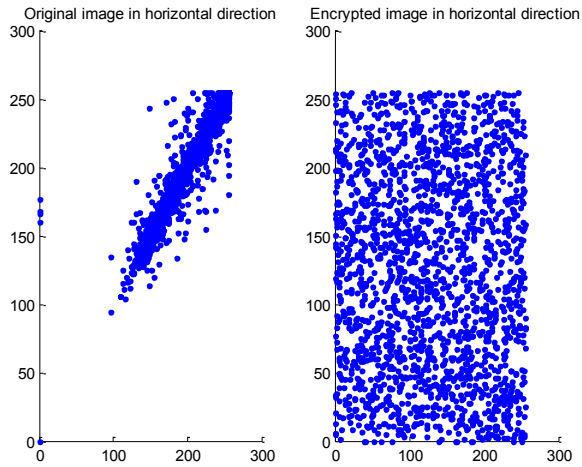

Fig. 15. Scatter plot of original and encrypted images in horizontal direction

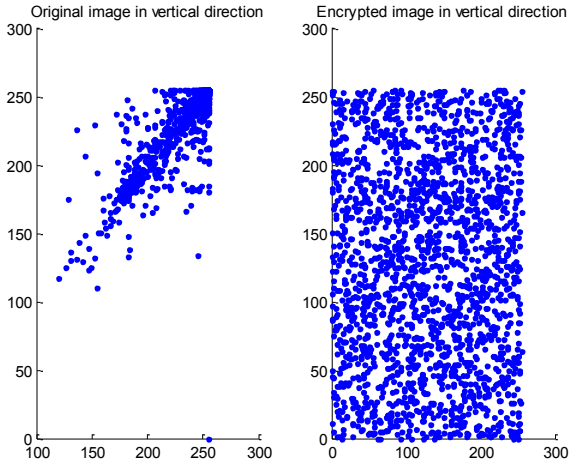

Fig. 16. Scatter plot of original and encrypted images in vertical direction

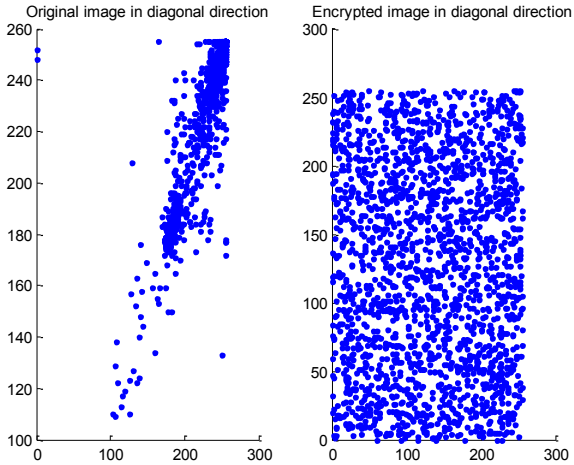

Fig. 17. Scatter plot of original and encrypted images in Diagonal direction

Correlation Coefficient	Original Image	Encrypted Image
Horizontal	0.9543	-0.0422
Vertical	0.9141	-0.0066
Diagonal	0.9197	-0.0205

Table. 3. Correlation coefficient analysis of lady image

Fig. 18. (tree) Real image- Encrypted image- Decrypted image

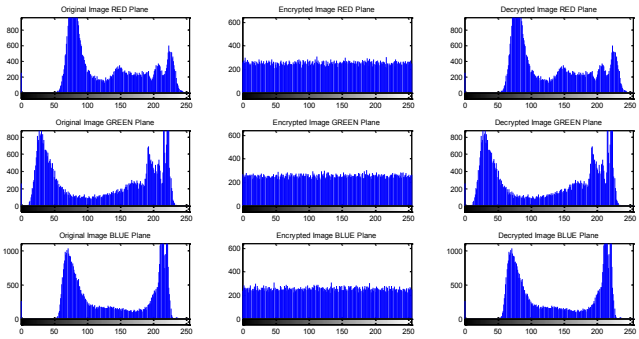

Fig. 19. Histogram analysis of real, encrypted, decrypted images on all 3 planes Red Green Blue respectively

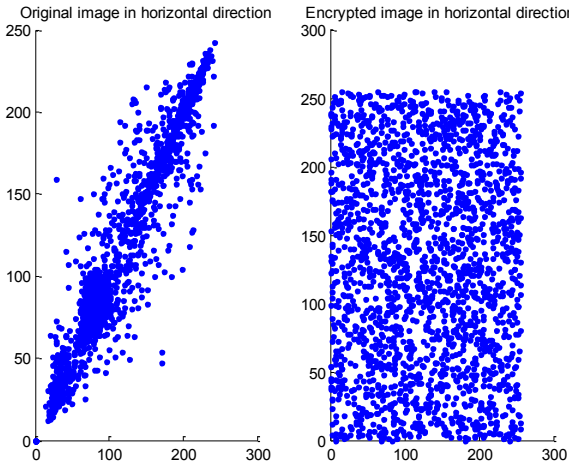

Fig. 20. Scatter plot of original and encrypted images in horizontal direction

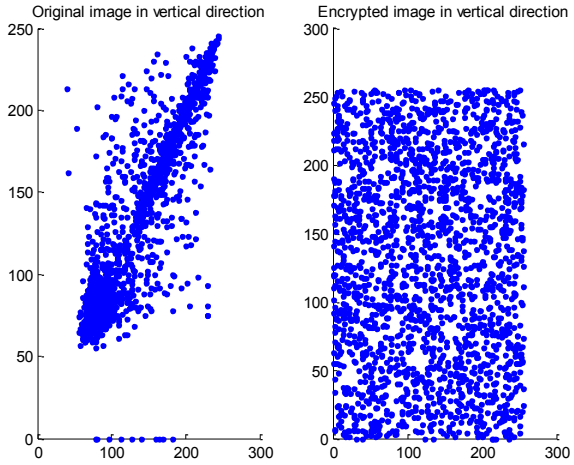

Fig. 21. Scatter plot of original and encrypted images in vertical direction

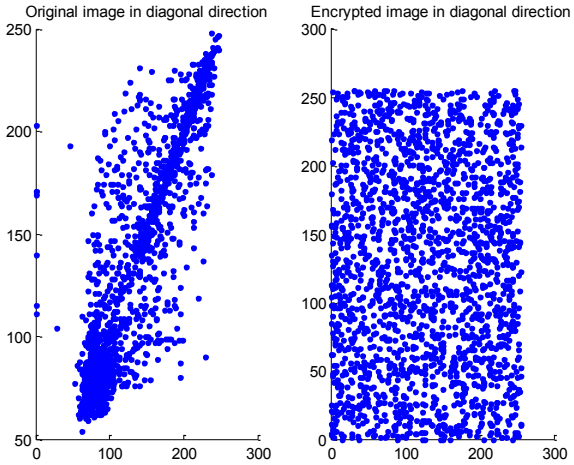

Fig. 22. Scatter plot of original and encrypted images in Diagonal direction

Correlation Coefficient	Original Image	Encrypted Image
Horizontal	0.9610	-0.0306
Vertical	0.9143	-0.0054
Diagonal	0.9106	-0.0307

Table. 4. Correlation coefficient analysis of tree image

As we can see, from Table.1, Table.2, Table.3, Table.4 the image after getting encrypted became totally unrecognizable from the original image which is the result of the shuffling of pixels in the planes and among the planes. Also the decrypted image same as the real image.

Also when we look at the histogram analysis the colors are distributed in a pattern in the real image. When we look at the histogram of the encrypted image they are spread over the entire range making the intensity of all colors the same. Also at the decrypted image, the patterns are brought to their positions as of that of the real image.

As we observe the scatter plots of the original and encrypted images original image tend to form a linear structure, but the encrypted image the entire pixels are scattered.

As we observe the Correlation coefficients of the original images and the encrypted images original image adjacent pixels are correlated in all directions. Whereas for the encrypted image we have pixels that are correlated not even in one direction.

IMAGE	NPCR	UACI
Lena	99.6076	33.4576
home	99.6150	33.3965
lady	99.6071	33.4276
Tree	99.6414	33.4231

Table. 5. NPCR and UACI analysis of test images

On observation, from table 5 we can say that Number of Pixel Change Rate is high and in the required range.

Also Averaged changing intensity is in the permissible range which ensure the Encryption algorithm.

CONCLUSION

In this paper an encryption scheme that comprises 3 stages of which the first stage has a Logistic mapping that is done on all 3 planes of the image. This image is then sent into a neural network architecture of which these outputs are sent as inputs to the final layer of encryption which uses Duffing map. Also, the histogram analysis of the real image deforming its histogram into the almost flat histogram and also reconstructing it back. This implies that the encryption scheme is perfect and is totally reversible.

REFERENCES

[1] Li-bo Zhang, Zhi-Liang Zhu, Ben-Qiang Yang, Wen-yuan Liu, Hong-Feng Zhu, and Ming-yu Zou, “Medical Image Encryption and Compression Scheme Using Compressive Sensing and Pixel Swapping Based Permutation Approach”, Mathematical Problems in Engineering Volume 2015 (2015), Article ID 940638, 9 pages

[2] K.Ratnavelu, M.Kalpana, P.Balasubramaniam, K.Wong, P.Raveendran, “Image encryption method based on chaotic fuzzy cellular neural networks”, Signal Processing, Volume 140, November 2017, Pages 87-96

[3] Nooshin Bigdeli, Yousef Farid, Karim Afshar, “A novel image encryption/decryption scheme based on chaotic neural networks” Engineering Applications of Artificial Intelligence, Volume 25, Issue 4, June 2012, Pages 753-765

[4] J.B Lima, F. Maderio, F.J.R.Sales,"Encryption of medical image based on cosine number transform", Signal Processing: Image Communication, 35,

[5] Narendra Singh; Aloka Sinha,"Optical image encryption using fractional Fourier transform and chaos",Optics and Lasers in Engineering, Volume 46 issue 2,2008 [doi 10.1016%2Fj.optlaseng.2007.09.001]

[6] Bouslimi, D.; Coatrieux, G.; Cozic, M.; Roux, C.,"A Joint Encryption/Watermarking System for verifying the reliability of the medical images", IEEE Transactions on Information Technology in Biomedicine, Volume 16 issue 5,2012 [doi 10.1109%2Ftitb.2012.2207730]

[7] Pareek, Narendra K.; Patidar, Vinod; Sud, Krishan K.," Diffusion–substitution based gray image encryption scheme", Digital Signal Processing Volume 23 issue 3, 2013 [doi 10.1016%2Fj.dsp.2013.01.005]

[8] Xu, Yong; Wang, Hua; Li, Yongge; Pei, Bin,"Image encryption based on synchronization of fractional chaotic systems", Communications in Nonlinear Science and Numerical Simulation Volume 19 issue 10,2014 [doi 10.1016%2Fj.cnsns.2014.02.029]

[9] Med Karim Abdmouleha,∗, Ali Khalfallaha, Med Salim Bouhlela,"A Novel Selective Encryption Scheme for Medical Images Transmission based-on jpeg Compression Algorithm ", Procedia Computer Science 112 (2017) 369–376, International Conference on Knowledge-Based and Intelligent Information and Engineering Systems, KES2017,6-8September2017

[10] Dolendro Singh Laiphrakpam, Manglem Singh Khumanthem, "Medical image encryption based on improved ElGamal encryption technique", Optik - International Journal for Light and Electron Optics, Volume 147, October 2017, Pages 88-102

[11] Zhongyun Hua, Shuang Yi, Yicong Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion", Signal Processing, Volume 144, March 2018, Pages 134-144

[12] A.M. Vengadapurvaja, G. Nisha, R. Aarthy, N. Sasikaladevi, "An Efficient Homomorphic Medical Image Encryption Algorithm For Cloud Storage Security", Procedia Computer Science, Volume 115, 2017, Pages 643-650

[13] Med Karim Abdmouleha, Ali Khalfallaha, Med Salim Bouhle, "A Novel Selective Encryption Scheme for Medical Images Transmission based-on JPEG Compression Algorithm", Procedia Computer Science, Volume 112, 2017, Pages 369-376

[14] Sachin Kailas Bhopi, Nilima M. Dongre, Reshma R. Gulwani, "Binary Key Based Permutation For Medical Image Encryption", 2016 International Conference on Inventive Computation Technologies (ICICT), Volume 3, 26-27 August 2016

[15] Iman Ranaee, Mahdi Majidi Nia, Reza J ahantigh, Amirhossein Gharib, "Introducing a new algorithm for medical image encryption based on chaotic feature of Cellular Automata", The 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)

[16] Amarit Nambutdee, Surapan Airphaiboon, "Medical Image Encryption based on DCT-DWT Domain Combining 2D-DataMatrix Barcode", The 2015 Biomedical Engineering International Conference (BMEiCON-2015)

[17] Prema T. Akkasaligar, Sumangala Biradar, "Secure Medical Image Encryption based on Intensity level using Chao’s theory and DNA Cryptography", 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 15-17 Dec. 2016