International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-9 Issue-1, May 2020

Chaos based Encryption of Image for Secure Communication

Mamatha.L.Japate, S.S.Navalgund

Abstract*: *The 20th century is known as the Information age. Development of technology led to the storing and communication of information in the digital form. Digital technology provides easy access to the information through internet and other forms of technology. Transmission of information is also become easy using digital technology. The information stored or communicated may be vulnerable to attacks from the adversaries. All the organizations and individuals are facing the threat of the insecurity of the information of data over the internet. Development of communication media and insecure media emphasizes the requirement to secure the data. The method of securing the information so that it is not stolen by the hackers is known as encryption. The development of multimedia technology has increased the images as the carriers of information. The conventional encryption algorithms are not well suited for the image encryption. Image encryption has developed in the past recent years as an important field. In the image encryption, the substitution and transposition techniques are performed on the pixel values of the image based on the key. One of the mechanisms for image encryption is based on chaos theory. Chaos sequence is used as a key for encryption because of its properties. This method of encryption is more secure and robust.

Keywords*: *Chaos theory, Lorenz attractor, Rossler attractor, Linear Feedback Shift Register (LFSR), Discrete wavelet transform (DWT), Confusion, Diffusion.

I. INTRODUCTION

The development of Digital technology led to the huge amount of digital data to be stored and communicated. The information stored or transmitted over the internet is subjected to security issues. The method to secure the information from the adversaries is encryption. It is a process of converting the data into non legible form so that no unauthorized person is able to read the data.

The conventional encryption method used is the symmetric encryption method. Symmetric encryption uses a single key for both encryption and decryption. The original data is also called as plaintext which is converted into illegible form (known as ciphertext) by using a key. The process of converting the plaintext to ciphertext is called encryption and the process of restoring the original data from the ciphertext is called decryption. The encryption algorithm performs various transpositions and substitutions on the plaintext to make it illegible. These transformations depend on the key used. The output of the algorithm is the ciphertext that is scrambled and illegible. The decryption algorithm is the reverse process of the encryption which takes ciphertext and the key as inputs and generates the estimate of the original data. The two important requirements of encryption are that the encryption algorithm should be strong and the key should be shared secretly between the sender and the receiver. If the key is discovered by someone else and if they know the algorithm, then the communication becomes readable. The several symmetrical encryption algorithms available that are suitable for text data. When images are used as the carriers of information, conventional encryption algorithms cannot be used. Image encryption has been developed as an important field in recent years. One of the mechanisms for image encryption is based on chaos theory [1].

Lorenz and Rossler chaotic models are more commonly used to study the chaotic systems. Both are three dimensional models. Linear Feedback shift register (LSFR) is used to increase the security of the image.

Manuscript received on April 02, 2020.
Revised Manuscript received on April 15, 2020.
Manuscript published on May 30, 2020.
* Correspondence Author
Mamatha L Japate, M.Tech student, Department of Electronics and Communication Engineering at SDM College of Engineering and Technology, Dharwad, Karnataka, India. Email: mamathalj@gmail.com
Dr.S.S.Navalgund, Assistant Professor, Department of Electronics and Communication Engineering at SDM College of Engineering and Technology, Dharwad, Karnataka, India.. Email: siddunavalgund@yahoo.com

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

II. PRELIMINARIES

Chaos systems are deterministic and random, that is used to study the behavior of non-linear, non-periodic dynamical systems. These chaotic systems are sensitive to initial conditions and system parameters. Because of its pseudo-randomness, ergodicity and sensitive nature, these chaotic systems provide good security and high efficiency,

A. Lorenz Attractor

The system of ordinary differential equations having chaotic solutions for some system parameters and some initial values is known as Lorenz system. Lorenz system is deterministic [2].

In 1960s Edward Lorenz developed a simplified mathematical model consisting of three ordinary differential equations. These equations are known as Lorenz equations [2].

$$\frac{dx}{dt} = \sigma(y - x) \quad (1)$$

$$\frac{dy}{dt} = x(\rho - z) - y \quad (2)$$

$$\frac{dz}{dt} = xy - \beta z \quad (3)$$

These equations determine the rate of change of the quantities with respect to time.

The constants σ, ρ and β are the system parameters. The constant σ is called the Prandtl number and ρ is called Rayleigh number. All the three constants take a positive value. The constants taken by Lorenz were σ=10, β=8/3 and ρ=28. With these system parameters the systems exhibit chaotic behavior.

To determine the behavior of the system for the given parameter values, the initial values x, y and z are set and the equations are solved [2].

B. Rossler Attractor

The Rossler systems or attractor is a system consisting of three nonlinear ordinary differential equations that describe the behavior of continuous time dynamical system exhibiting chaotic dynamics.

Rossler model is characterized by three ordinary differential equations given below [3],

$$\frac{dx}{dt} = -(y + z) \quad (4)$$

$$\frac{dy}{dt} = x + ay \quad (5)$$

$$\frac{dz}{dt} = b + xz - cz \quad (6)$$

Where a, b, c are the system parameters and x, y z are the variables depending on time. The values first studied by Rossler are a=b=0.2 and c=5.7. The equations (4) and (5) are linear and equation (6) is the only equation having the non-linear term (product of x and z).

C. Linear Feedback shift register

Linear Feedback Shift register (LFSR) is a register whose input is the function of its previous states. The output bit is xored with some of the bits of the previous states and fed back to the input. This register is used to generate a random sequence. At every clock pulse the output bit is generated and all the bits are shifted by one bit. The initial value of the shift register is called seed. The bit positions that affect the next state are called as taps. The output sequence generated depends on the taps used. In the proposed project work 17-bit LFSR is used as shown in the figure.1 [4].

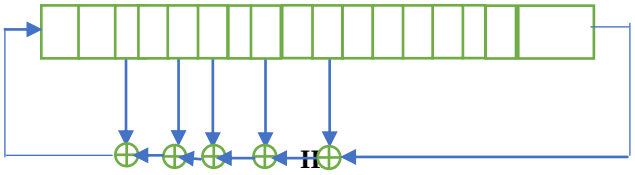

Fig. 1 Block diagram of 17-bit LFSR

The feedback function of the LFSR is expressed as finite field arithmetic or polynomial which is the arrangement of taps. The polynomial used for the 17-bit LFSR is,

$$P = x^{12} + x^8 + x^6 + x^5 + x^3 + 1 \quad (7)$$

IV. METHODOLOGY

In the proposed project, the Lorenz attractor and Rossler attractor both are used for the generation of the key sequence which is used for the confusion and diffusion operations done on the image.

The two encryption algorithms are tested, one without using the wavelet decomposition and another using wavelet decomposition.

First the encryption algorithm without using the wavelet decomposition is studied. The block diagram of the proposed work for encryption of image is shown in fig 2.

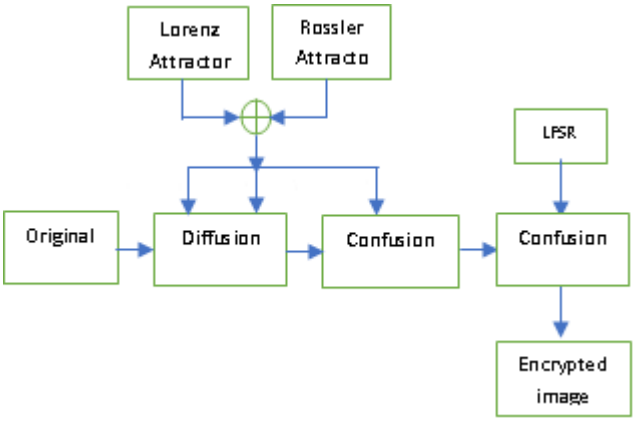

Fig.2. Block diagram of proposed work without dwt decomposition

The encryption algorithm of the proposed work is as follows:

1. Let I be the original gray scale image having the size of 256x256.

2.The initial parameters of the Lorentz attractor and Rossler attractors are set. These two attractors solve the ordinary differential equations at different instants of time. Both the sequences are combined.to generate three sequences x, y and z [5]

. Diffusion and confusion are performed on the original image using x, y and z series. Diffusion is performed by permutating the pixel values of the original image. The permutation is done to change the positions of the pixels and this is done by scrambling.

3. Image scrambling algorithm scrambles the position of pixels of image using the two sequences x and y sequences. These chaos sequence has no repeat values. Chaos sequence is of the length 256 without repetitions. The x and y sequence are sorted according to their indices [6].

Let x= {x1, x2, x3, …… ,xM} be the sorted x sequence and Ind1={i1, i2, i3, ….. iM } be the indices of the sorted x sequence. The key generation that is the generation of indices Ind1 is shown in fig 3.

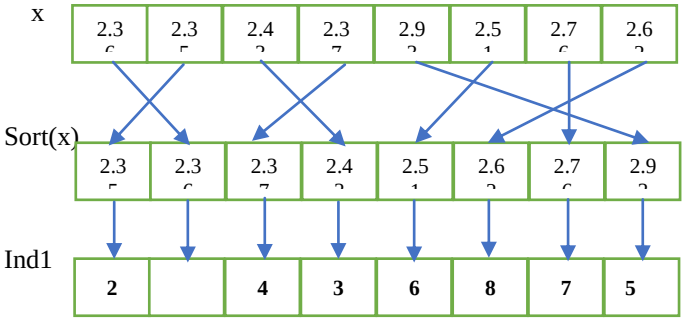

Fig 3 Key generation (i.e. index Ind1)

Retrieval Number: A2615059120/2020©BEIESP
DOI:10.35940/ijrte.A2615.059120
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Let y = {y1, y2, y3, ……yM } be the y sequence that is sorted and Ind2={ii1, ii2, ii3 …. } be the indices of the sorted y sequences. These indices of the sorted x and y series are used as key. The indices of sorted x and y sequence is used for scrambling of the image pixels. The image pixel at first position of the first row is shifted to the position [Ind1(1), ind2(1)] of the scrambled image.

The next image pixel of the first row is shifted to the position [Ind1(1), Ind2(2)] of the scrambled image. The same procedure is repeated for the other pixels for the first row. Then the first image pixel of the second row is shifted to the position [Ind1(2), Ind2(1)]. The second image pixel of the second row is shifted to the position [Ind1(2), Ind2(2)] and so on. This process is repeated for the rows of the image.

4. Once the scrambling of the image rows is over, the same process is repeated for all the pixels again changing the positions of the image by reversing the index values. The first pixel of the first row is now shifted to the new position [Ind1(1), Ind2(1)]. The second pixel of the first row is now shifted to the new position [Ind1(2), Ind1(1)], this is continued to all the pixels of the first row. Then the first pixel of the second row is shifted to the new position [Ind1(1), Ind2(2)]. The pixel of the second row is shifted to new position [Ind1(2). Ind2(2)] and so on. This process is repeated for all the rows.

5. Confusion is now performed on the scrambled image. The third series of the attractor (z series) is used as the initial vector for confusion process. The confusion process is performed as follows:

Each of the pixels of the initial column vector is xored with the corresponding pixels of the first column of the scrambled image. The first column is now replaced by the resultant values. Then the resultant first column is xored with the initial second column and the second column is replaced by the resultant of the xor operation. This process is continued with all the columns of the scrambled image as shown in figure 4 [7].

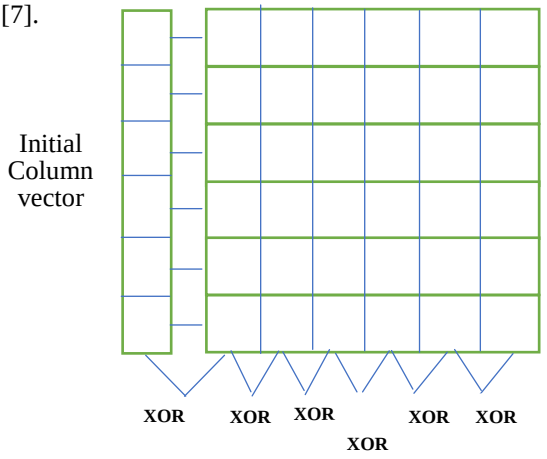

Fig 4 Generation of key (Ind1)

6. Then the confusion process is done on the rows of the resultant image. Each of the pixels of the initial row vector is xored with the corresponding pixels of the first row of the image. The first row is now replaced with the result of the xor operation. The second row is now replaced with the result of the xor of the resultant first row and the initial values of the second row. This process is continued as shown in the Fig.5.

7. In order to increase the security of the image encryption, confusion process is again performed using a series generated using Linear shift feedback register (LFSR). 17-bit LFSR is used in the process. This second confusion process further decreases the correlation between the pixel values of the image. Performing the confusion twice using the chaotic sequence and the sequence generated by LFSR improves the security of the encryption algorithm. The final encrypted image is thus more secure.

8. Decryption of the image is the reverse process of encryption. The same initial parameters and the initial values are used for decryption. The same algorithm is used for both the encryption and decryption process and hence have the same algorithmic complexity. The result of the decryption process gives the original image.

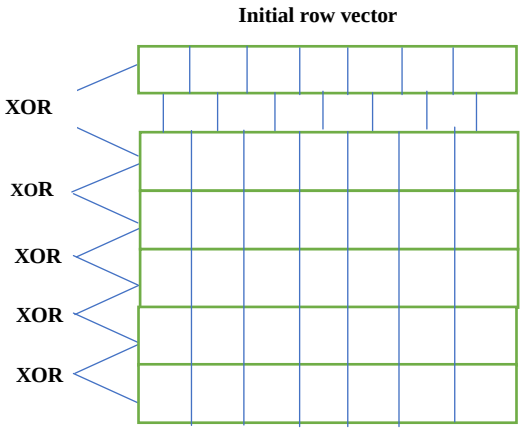

Fig 5. Confusion process on the rows of the scrambled image.

9. Secondly, the same encryption algorithm is used along with the wavelet decomposition of the image. The haar wavelet is used to decompose the image into four sub bands, approximation coefficients (LL), and the detailed coefficients as vertical, horizontal and the diagonal coefficients. The approximation coefficients contain most of the image information. Hence the encryption algorithm is performed only on the approximation coefficients. The process from step 3 to step 8 are performed on the approximation coefficients for encryption. This results in the encryption of the approximation coefficients which is transmitted to the receiver.

The block diagram of the proposed work with wavelet decomposition is shown in fig 6.

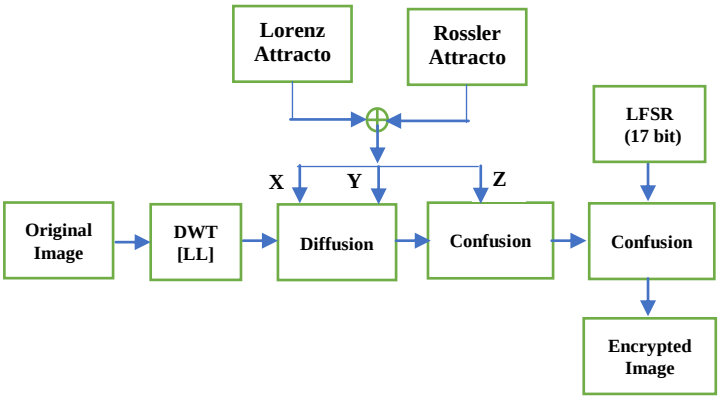

Fig 6. Block diagram of the proposed work with wavelet decomposition.

The inverse transform is performed and the image is recovered with a small amount of loss in this process. The data that is transmitted is only the approximation coefficients that is 1/4th the size of the original data. Hence this results in the compression of the transmitted data.

V. RESULTS AND ANALYSIS

The parameter values for the Lorenz attractor are set as σ=10, β=8/3 and ρ=28 and the initial values are set as x=1.3604, y=1.2052 and z=1.5062. The parameter values for the Rossler attractor are a=0.2, b=0.2 and c=5.7 and the initial values used are x=1.8923, y=1.7583, and z=0.6423. The standard Lena gray scale image of size 256x256 is used. The results obtained by the MATLAB simulation are as follows. The following fig 7 shows the original image (a), Encrypted image (b) and the decrypted image (c).

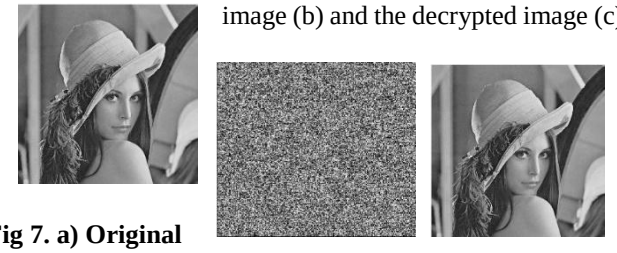

Fig 7. a) Original image, b) Encrypted image, c) Decrypted image

The performance and analysis are done by the following parameters.

A. Key Analysis

The Lorenz chaotic sequence has three initial conditions and three parameters and Rossler chaotic sequence also has three initial conditions and three parameters. These chaotic sequences are very sensitive to these initial parameters. For the encryption algorithm to be more secure, the secret key should be very sensitive to the small changes in the keys [8].

B. Statistical Analysis

- Histogram [9]

The histogram of the original image and the histogram of the encrypted images are studied. The pixel distribution in the original image is uneven. It is seen that the histogram of the encrypted image is uniformly distributed shown in the Fig. 8.

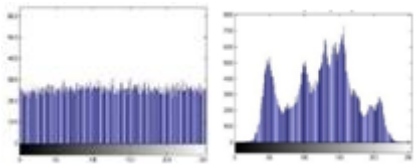

Fig 8. Histogram of Original and encrypted image

Table I Correlation Coefficients of Original and Encrypted image.

Correlation	Algorithm without using dwt			Algorithm with dwt		
(Lena Image)	Horizontal	Diagonal	Vertical	Horizontal	Diagonal	Vertical
Original image	0.9014	0.8888	0.9488	0.9049	0.8831	0.9323
Encrypted image	-0.0272	0.0176	0.0106	-0.0111	-0.0162	-0.0071

- Correlation Coefficient Analysis

Correlation defines the dependency among the pixels in the image. The correlation coefficient for highly correlated image is almost equal to 1 and for encrypted image, its value is nearly 0.

The formula used to calculate the correlation coefficient is [10],

$$R_{xy}=\frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (8)$$

Where x and y are the adjacent pixels or pixels at the same indices of the original or encrypted images and L is the number of pixels.

$$E(x)=\frac{1}{L}\sum_{i=1}^{L} x_i \quad (9)$$

$$D(x)=\frac{1}{L}\sum_{i=1}^{L}\left(x_i - E(x_i)\right)^2 \quad (10)$$

$$Cov(x,y)=\frac{1}{L}\sum_{i=1}^{L}\left(x_i - E(x_i)\right)\left(y_i - E(y_i)\right) \quad (11)$$

E(x) represents the mean value of x, D(x) is the variance with respect of x, cov(x,y) is the covariance between the adjacent pixels x and y, Rxy is the correlation coefficient.

For the original image or the plain images correlation coefficients is nearly equal to 1 and correlation coefficient for encrypted images is nearly 0, indicating that there is less correlation among the pixels.

The graph for the correlation of original and encrypted images for different images are shown in fig, 9 and Fig 10.

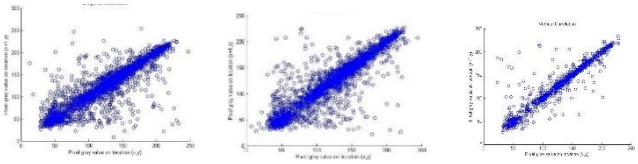

Fig 9. Horizontal, Diagonal and Vertical Correlation graph of original image

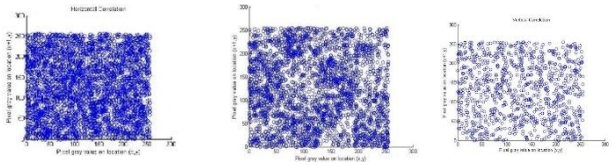

Fig 10. Horizontal, Diagonal and vertical Correlation graph of encrypted image.

The table I shows the distribution of adjacent pixels of original and encrypted images for lena image, horizontally, vertically and diagonally. Correlation coefficient between the original and encrypted image for the algorithms without dwt and with dwt is given in Table II.

Table II. Correlation between Original and Encrypted images

Correlation between original and Encrypted images	
Algorithm without dwt	Algorithm with dwt
0.001242	0.015659

C. Differential Analysis

Number of pixel Change rate (NPCR) and Unified Average Changing Intensity (UACI) are the measure of sensitivity of the encrypted image to small change in the original image.

NPCR is used to measure the number of pixels change rate of the encrypted image when one bit of one pixel of the original image is changed. UACI measure the difference between the average intensities between the original and the encrypted images. The formula are as follows [5],

$$NPCR=\frac{\sum_{i,j} D(i,j)}{MxN} \quad (12)$$

$$D(i,j)=0, \quad \text{if } C_1(i,j)= C_2(i,j)$$
$$=1, \quad \text{if } C_1(i,j) \neq C_2(i,j)$$

$$UACI=\frac{1}{MxN}\sum_{i,j}\frac{|C_1(i,j)-C_2(i,j)|}{255} x\ 100\ \% \quad (13)$$

Where $C_1(i,j)$ is the encrypted image of the original image of size MxN and $C_2(i,j)$ is the encrypted image with one bit change in one pixel in the original image. Table III shows the NPCR and UACI values of the encryption algorithm with and without dwt.

The results of NPCR and UACI are near to the optimum values. Even if there is a small change made by the attacker, this results in a large change in the encrypted image, and hence this encryption algorithm is resistant to the differential attacks.

Table III. NPCR and UCAI values

(Lena image)	Without DWT	With DWT
NPCR	99.9923	99.5494
UACI	33.5293	16.4603

D. Entropy Analysis

Information entropy is the measure of indeterminateness and defines the degree of uncertainty of the system. It is defined as [11],

$$H(m)= -\sum_{i=0}^{2N-1} P(m_i) log_2[P(m_i)] \quad (14)$$

$P(m_i)$ is the probability of the symbol m_i. If all the symbols have equal probability with i=0,1,….. .. 255, for gray scale image, then $P(m_i)$ will be equal to 8. Hence a good image encryption algorithm produces an encrypted image with the entropy near to 8. Table IV. shows the entropy values of the encrypted image

Table IV. Entropy values

(Lena image)	Without Dwt	With Dwt
Entropy	7.997051	7.084656

E. Error metric analysis

MSE and PSNR

The quality of measurement of encryption is calculated by the two parameters mean square error (MSE) and peak signal to noise ratio (PSNR). These metrics are used to compare the quality of the original and encrypted images. The MSE between two images is given as [5],

$$MSE=\frac{1}{MxN}\sum_{i=0}^{M-1}\sum_{i=0}^{N-1}|C(i,j) - P(i,j)|^2 \quad (15)$$

And the equation for PSNR is given as,

$$PSNR=10*\log_{10}(\frac{255}{sqrt(MSE)}) \quad (16)$$

The lower the PSNR values there is more difficulty in retrieving the original image from the encrypted image without the knowledge of the secret key. Table V shows the MSE and PSNR values of original and encrypted images.

Table V. MSE and PSNR values

	MSE		PSNR	
	Between Original & Encrypted images	Between Original & Decrypted image	Between Original & Encrypted images	Between Original & Decrypted image
Without Dwt	113.44386	0.000024	27.582994	94.241399
With Dwt	198.98026	0.01614	25.142704	66.051874

F) Chosen Plaintext attack analysis

The process of diffusion can be done using Xor operation which is validated by chosen plaintext analysis. To perform this analysis, two images are xored and their corresponding cipher images are xored, and this algorithm is secure against chosen plaintext attacks if it satisfies the condition [4],

$$Xor(O1,O2)\neq xor(C1,C2) \quad (17)$$

O1 and O2 are the two images and C1 and C2 are their corresponding encrypted images. Fig 11 shows the xor of two original images and xor of their corresponding encrypted images.

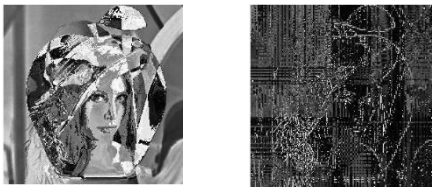

Fig 11. a) Xor of two original images, b) xor of encrypted images

G) SSIM

SSIM is the structural similarity index which is used to measure the similarity between the two images. Here the similarity between the original and decrypted images is tested. Structural information indicates that there are strong dependencies among the pixels when they are placed closely in space. The resultant SSIM value is in between -1 and 1. For the encryption algorithm, the value of SSIM should be close to 1 [12]. Table VI shows the SSIM vales of the proposed algorithm

Table VI. SSIM values of the proposed algorithm

(Lena image)	Without DWT	Haar DWT
SSIM	0.9964	0.7014

VI. CONCLUSION

The image is encrypted with the algorithm of diffusion and confusion. And the same algorithm is used to encrypt the image after applying the discrete wavelet transform (here Haar DWT is used). The image is first transformed which results in the formation of four sub bands. Then the encryption algorithm is applied on the approximation sub band which has maximum amount of information. The encrypted approximation sub band is transmitted which results in the compression ratio of the transmitted data by the factor of 4. But the drawback of using the transform is that some amount of information is lost and hence the decrypted image is a bit degraded.

The image encryption done without using the transform requires more amount of processing since the diffusion and confusion is to be done on the entire image. This does not result in the compression of the data that is transmitted. But the quality of the decrypted image is better than that of the decrypted image obtained after encrypting the transformed image. Hence this algorithm can be used with or without the DWT as per the applications and is more secure, robust and effective in both the cases.

REFERENCES

1. Cryptography and network security, principle and practice by William Stallings.
2. "The Lorenz Equations: Bifurcations, Chaos, and Strange Attractors", by Colin Sparrow published by Springer-Verlag New York Heidelberg Berlin
3. K M Ibrahim, R K Jamal and F H Ali," Chaotic behaviour of the Rossler model and its analysis by using bifurcations of limit cycles and chaotic attractors", Journal of Journal of Physics: Conference Series 1003 (2018) 012099, DOI:10.1088/1742-6596/1003/1/012099
4. V. Moorthi Paramasivam et al," Reciprocal Time Domain Disruption of Image for Secured Communication", Proceedings of International Conference on Computer Communication and Informatics, ICCCI,2019, DOI:10.1109/ICCCI.2019.8822167
5. Anish Batra, Siddarth Gorey, Ms Reena Singh, "Image Encryption based on chaotic systems and Shuffling Algorithm", International Journal of New Technology and Research (IJNTR), April 2018, ISSN:2454-4115, Volume-4, Issue-4, pages 86-90 **combination**
6. M.Essaida, I.Akharraza, A.Saaidia,b , A.Mouhiba, "A New Image Encryption Scheme Based on Confusion-Diffusion Using an Enhanced Skew Tent Map", Proceedings of The First International Conference On Intelligent Computing in Data Sciences, Procedia Computer Science 127 (2018) 539–548, published by ELSEVIER
7. Kayhan Celik, Erol Kurt, "A new image encryption algorithm based on Lorenz system", Proceedings of 5th European Conference on Renewable energy systems, ECRES 2017, DOI:10.1109/ECAI.2016.7861097
8. Jishuang Li, Yubo Xing, Chunyi Qu Junxing Zhang," An image encryption method based on Tent and Lorenz chaotic systems", Proceedings of 6th IEEE International conference on software engineering and service science, ICSESS,2015, DOI:10.1109/ICSESS.2015.7339125
9. Wang Zhen, Huang Xia, Li Yu-Xia, Song Xiao-Na, "A new image encryption algorithm based on the fractional order hyperchaotic Lorenz system", Journal of IOPScience, vol22, no1(2013) Chinese phys.,DOI:10.1088/1674-1956/22/1/010504
10. MU Xiu-chun, SONG E-Nuo,"A new color image encryption algorithm based on 3D Lorenz Chaos sequences", Proceedings of First International conference on Pervasive Computing, Signal Processing and Applications, 2010,DOI:10.1109/PCSPA.2010.72
11. Hailan Pan, Yongmei Lei and Chen Jian," Research on digital image encryption algorithm based on double logistic chaotic map", EURASIP Journal on Image and Video Processing, 2018, DOI:10.1186/s13640-018-0386-3, 2018:142
12. Mamy Alain Rakotomalalala. Et.al., "Image Ciphering Based on chaotic ANN and Fibonacci Transfomr improved by using the wavelet transform", International journal of Computer Trends and Technology (IJCTT), Volume 61, Number 3-July 2018

AUTHORS PROFILE

Miss Mamatha L Japate, is M.Tech student in the department of Electronics and Communication Engineering at SDM College of Engineering and Technology, Dharwad, Karnataka, India. She obtained her Bachelor of Engineering & Communication Engineering from U.B.D.T College of Engineering, Davangere, Karnataka. She is pursuing Masters in Digital Electronics from SDMCET and she has scored 10 CGPA till third semester. She has 11 years of teaching experience as lecturer at Government Polytechnic for women, Hubballi, Karnataka

Dr. S.S. Navalgund is a Assistant Professor in the department of Electronics and Communication Engineering at SDM College of Engineering and Technology, Dharwad, Karnataka, INDIA. He obtained his Bachelor of Engineering from S.D.M.C.E.T, Dharwad, Karnataka. Master degree in Microelectronics and Control Systems from N.M.A.M.I.T, Nitte, Karnataka. Submitted thesis for the award of Ph.D. from VTU, Belagavi, Karnataka, India. Guided 40+ U.G. and 10+ PG students. Conducted 01 Conference and 10+ Workshop on Pointers in C, MATLAB & Simulink and achieved 02 awards. Published 04 no. of papers at International Journal and 10 at conferences and life member of ISTE, IE and IETE