International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

An Efficient Radical Image Encryption Based on 3-D Lorenz Chaotic System

V. Sangavi , P. Thangavel

Abstract*: We propose a new encryption strategy based on the Lorenz chaotic system. Scrambling and diffusion techniques are carried out availing the chaotic sequences rendered by Lorenz system. The chaotic sequences tactically clutter the pixel positions and curtail the relationship between the original image and the encrypted image.Wittingly a high-dimensional system delivers a well robust cryptosystem bearing good efficiency and resistivity. Here we demonstrate through dilated measures and statistical analyses that the proposed system prominently improves security scales and is also potential in withstanding to various sort of attacks. Securing images in cyber space became vital in communication for instance, military affairs, national security, diplomatic affairs, medical database and so on expanding its attention broadly.

Keywords* : Cryptosystem, Diffusion, Lorenz Chaotic system, Scrambling.

I. INTRODUCTION

A. Background

The mass spectrum of internet activities and network communication includes data transfer in the form of image, audio, video etc., and enormous growth of information has given rise to unlawful venture. This phenomena ignited researchers to oversupply secureness over the data during transmission. Cryptography tackles this challenge in a fertile manner with the aid of chaos. Cryptographic algorithms are used to devise the cryptosystems comprising mathematical formula, numeric, expression and word to carry out the encryption and decryption process in a fruitful way.

Hence multiple encryption approaches have been suggested all along over the decades. Well-known image encryption method is notably chaotic image encryption [1, 2]. Encryption approaches based on permutation and substitution network using chaotic maps are studied in [4, 5]. Self-adaptive permutation and diffusion are accomplished in image encryption [11]. Though too many methods are proposed less key space weakens the cryptosystem, to overrule this aspect new chaotic maps and high dimensional systems are used to posses colossal secureness over the Cryptosystem.

B. Related work

Several researchers have exploited the logistic map for enciphering and deciphering the multimedia content, notably Zahmoul et al. [3] proposed new chaotic maps to enlarge bifurcation parameters and also to strengthen the chaotic system. In recent years, hyper chaotic image encryption schemes are formulated to provide much complexity to the dynamical systems [6, 22] as they highly reactive to the initial condition and non-convergence in nature. Wang et al. [7] proposed an algorithm based on chaos using random growth technique. Guodong Ye [8] presented a pixel bit based scrambling for image encryption. Zhou et al. [9] presented image block encryption schemes using S-box computation and chaotic map to get rid of the limitation in dimension of the image. Kandar et al. [10] proposed an image encryption model structured using the sequences generated from the cyclic group followed by bit-level permutation and transformation techniques.

Tang et al. [12] presented multiple image encryptions using bit-plane decomposition method. Hsiao and Lee [13] proposed a chaotic encryption model based on non-linear adaptive filters for specialized images. Zhang and Wei [14] presented a color image encryption method based on DNA sub-sequence operation and chaos. Change's Dong [15] proposed a model using one time key based image encryption with coupled chaotic systems. Buncha and Banlue [16] described the ability of the Lorenz system and identified the hidden attractors in system. The two dimensional chaotic maps are employed [17, 18] combining sine logistic map and chaotic generators to enhance its nonlinearity and randomness. Diab and El-semary [19] presented cryptanalysis and shown improvement in the cryptosystem by reusing the permutation matrix in a dynamical way. Zhang et.al [20] presented an encryption model based on the chaotic sequences. Furthermore, to increase the robustness of the system in the medical field Smita and Bellamkonda [21] proposed the medical image encryption using chaos.

C. Our contribution

To increase the protection of image encryption methods, we use Lorenz chaotic system incorporating Runge-Kutta method of order N=4 introducing significant scrambling and diffusion technique to enhance the performance of the encryption process. Under this structure the pixel positions are trans-positioned during scrambling process to avoid correlation relation between the neighbouring pixels. Diffusion is carried out to overture the avalanche effect in the kernel. Sequences are generated from Lorenz system and employed for key generation process.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
V. Sangavi*, Department of Computer Science, University of Madras, Chennai, India. Email: vkansanny.comet@gmail.com
P. Thangavel, Department of Computer Science, University of Madras, Chennai, India. Email: pthang.cs@unom.ac.in

Therefore high resistances to the vulnerabilities are noticed.

The rest of the paper is organized as follows: Second section concisely describes the preliminaries to create the encryption model, third section briefly explains the proposed scheme, fourth section demonstrates the experimental results and statistical analysis of the obtained results. At last, we conclude the proposed work in the fifth section.

II. PRELIMINARIES

A. The Lorenz system

During the year 1963, Edward Norton Lorenz an American mathematician and meteorologist numerically integrated an elementary system of three coupled nonlinear equations bearing first-order on behalf of fluid convection model depicting the atmospheric weather conditions. Lorenz equation has opened up the study of chaos and sensitiveness to initial conditions. The Lorenz model takes up the initial conditions $x_0 = 0$, $y_0 = 0$ and $z_0 = 0$ and parameters $\sigma = 10$, $\beta = 8/3$ and $\rho = 28$. σ is the Prandtl number, β is the Biot number, ρ is the Rayleigh number. The Lorenz system of equations is mentioned below:

$$x'(t) = \sigma(y - x) \quad (1)$$

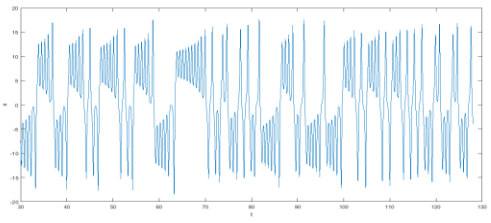
$$y'(t) = x(\rho - z) - y \quad (2)$$

$$z'(t) = (xy - \beta z) \quad (3)$$

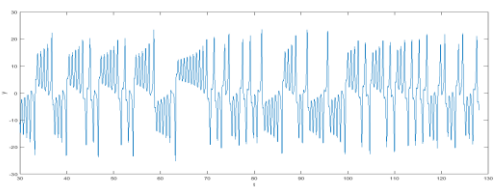
In the above trio Eqs. (1-3), $x(t)$ represents the magnitude of the convection motion and $y(t)$, $z(t)$ represents the horizontal and vertical alterations. Lorenz system has complex inner structure that exhibits Ergodic properties in the nonlinear systems.

The standard Lorenz system consists of seven parameters namely x, y, z, t,σ, β and ρ. Since x, y, z and t are scaled between 0 - 1 among the seven coefficients. The three canonical parametersσ, β and ρ are left behind to completely takeover the chaotic system. Basically all studies have inferred the parameters to be positive considering the energy needed to maintain the oscillations are equipped by the positive response. The protrusion of the axes on various planes and their magnitude with respect to the spatial domain are shown in Fig. 1 and 2.

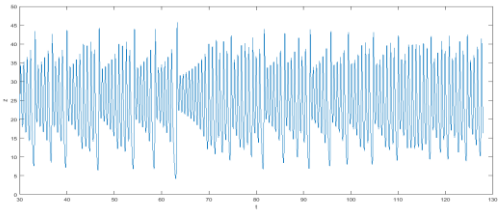
The attributes of the Lorenz chaotic system are as follows: Aperiodic long-term behavior, Sensitivity to initial values and Chaos attractors. The Lorenz system is integrated using Runge-Kutta fourth order method.



(a)

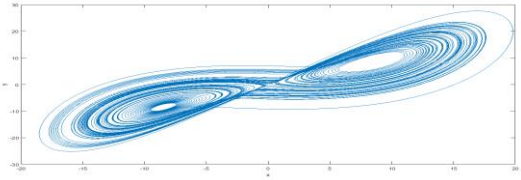


(b)

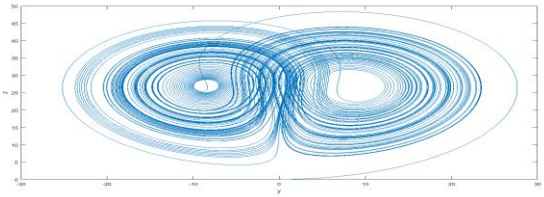


(c)

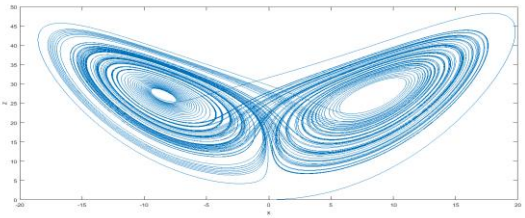
Fig. 1.Time series of the chaotic attractors. (a) *x* axis, (b) *y* axis, and (C) *z* axis.



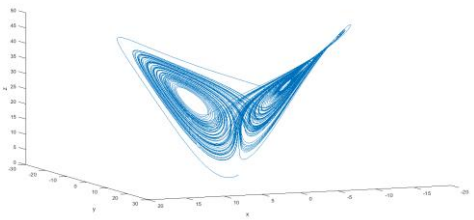
(a)



(b)



(c)



(d)

Fig. 2.Projection of the attractors. (a) *xy* plane, (b) *yz* plane, (c) *xz* plane and (d) *xyz* space

III. PROPOSED CHAOTIC SYSTEM

A. Quantization of the generated sequence

The triplet sequence generated by the Lorenz chaotic system, may possess the auto correlation property between the sequences and in order to eliminate the numeric relation between them quantization approach is obtained.

In this process of quantization for the classical logistic chaotic sequence, we choose a method to take average value of the output sequence, whereas the mean value quantization method make the sequence period serious. So we obtain the following quantization approach.

- Determine the sequence value, and multiply the sequence by a constant value δ.
- Add the resultant sequence with $\alpha(\pi)$, where α is sin, cos and tan for the respective *x*, *y* and *z* sequence.
- Modulus is taken for the sequence with respect to the image dimension.
- Ceiling function is used to eliminate the fractional part of all the sequence values.

$$X = ceil\left[\left(|X(i)|.\delta + \alpha(\pi)\right) \bmod N\right] \quad (4)$$

where i=1, 2, 3,..,N. For instance the quantization of chaotic sequence for x is shown in Eq. 4 where δ is the multiplicative constant and *N* is the maximum allowed pixel intensity value of the test image. The quantization processes of *y* and *z* chaotic sequence are similar. The histogram representation shown in Fig. 3 and 4 depicts the sequences before and after quantization.

B. Key distribution

The secure and secret key value *K* is generated to determine the pixel location to begin the scrambling and diffusion process in the matrix. This is done based on the key produced and though a minuscule change takes place in the initial conditions of Lorenz system it can flood a cascading reflection in the image encryption scheme. The sequences *x, y* and *z* are sliced to $N \times N$ square matrices and every column is processed combining the plain image A. It is defined as:

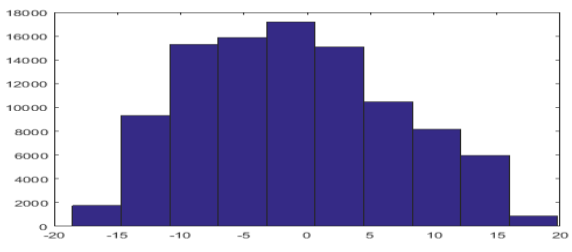
$$K_i = \left[\sum_{k=1}^{N*N} A_k \bmod 7\right] + (i*(j+1)) * [L \bmod N] \quad (5)$$

$$L = floor\left(\left|\frac{1}{N^2}\left(\sum_{p=1}^{N*N} \psi_{ip}\right)\right|\right) \quad \text{where} \quad \psi_i = X, Y, Z \quad (6)$$

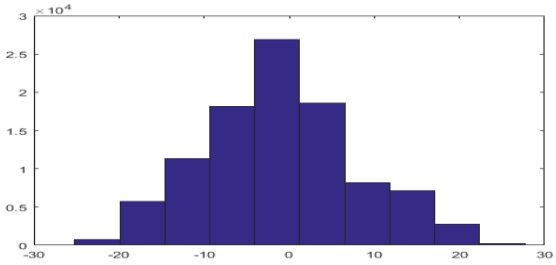
where i = 1, 2, 3 and j = 0, 1, 2 here *j* is the control parameter and *i* is the iteration variable and the above Eq. 5 and 6 produce keys K_1, K_2 and K_3 with respect to *x, y* and *z* sequence. The key value *K* is used to generate the initial state of two rounds of the encryption. Assuming the initial state is a determined pseudo random number. The initial states for the two encryption rounds can be derived as follows:

$$SK_j(i) = \phi(i + K_j) \quad (7)$$

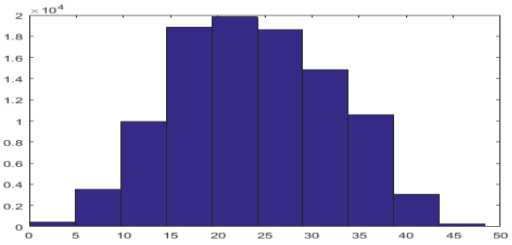
Where i = 1, 2, 3,…,N * N, j = 1, 2, 3 and ϕ = X, Y, Z. Using the Eq. 7 SK_1, SK_2 and SK_3 are generated for the two rounds of encryption such as column and row pixel scrambling and combined pixel diffusion. Here the sequences *x, y* and *z* are supplemented with the key values.



(a)

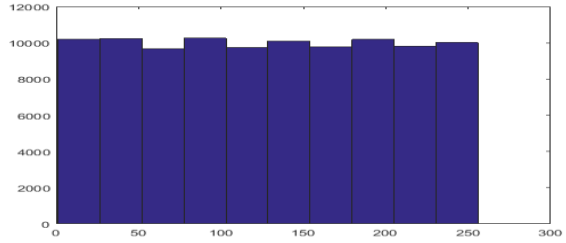


(b)

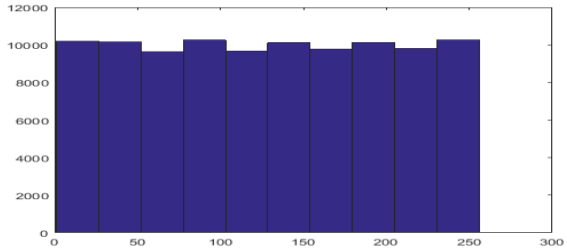


(c)

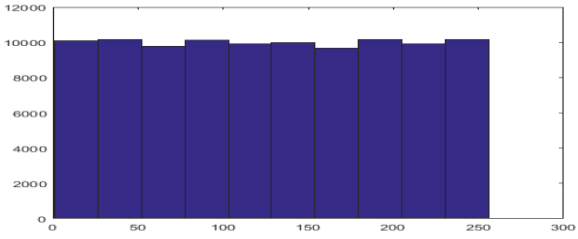
Fig. 3.The histogram of the sequences of x, y, z (a, b, c) before quantization.



(a)



(b)



(c)

Fig. 4.The histogram of the sequences of x, y, z (a, b, c) after quantization.

C. Pixel Scrambling algorithm

Scrambling is a confusion process carried out within the image to eradicate the correlation between the adjacent pixels, here the pixel intensity values are not changed but the position of the pixel intensity values are altered. Several rounds of encryption can only accomplish a tiny change in the confusion process but using the above Eq. 5 and 7 pave way for an effective confusion among the pixel position in the scrambling process during encryption. Here the pixels are shuffled in the forward basis and reverse basis with the cell value fetched from the initial state SK_1 and SK_2 based on the odd even parity of the elements. The steps are explained below:

- The initial key value K_1 and K_2 are obtained using Eq. 5 and 6 to pinpoint the pixel location to initiate the scrambling procedure.
- The sequence of numeric values of the chaotic sequence extracted from x and y sequence are subjected to odd and even parity check.
- If the element of the sequence value satisfies the even parity check then the plain image pixel matrix value is shifted in forward basis else the pixel matrix value gets shifted in reverse order.

By repeating the above steps in row and column order completely scramble and results in a scrambled image.

D. Pixel Diffusion algorithm

An algorithm that holds a good diffusion property should be capable of resisting the chosen plain text attack. Like the scrambling algorithm, first we produce a key stream by using the formula in Eq. 7. In this process the current pixel intensity value is modified and a new pixel value is replaced by processing the current pixel element with the pixel element obtained from the scrambling process. Here a continuous diffusion is proposed to overcome the usual disadvantages in this process. The diffusion is done sequentially using the equation:

$$D(i) = [S(i) + 2/N] \bmod N \oplus SK_3(i) \qquad (8)$$

where, N is the maximum allowed pixel intensity value in the image, S is the scrambled matrix and i ranges from *1 to N*N*. After this process the matrix is entirely changed and this provides ambiguity to the attackers to fetch information using any type of metrics.

E. Proposed image encryption scheme

The encryption scheme is outlined below:

Step 1 Consider an image of size $M * N$ and convert the image into a gray scale image. We consider a square image A.

Step 2 Generate three chaotic sequences X, Y and Z using the Lorenz system of equations.

Step 3 The unordered sequences are discretized and quantized using Eq. 4.

Step 4 Calculate the key stream for the pixel values using Eq. 7. The sub keys are generated for the key stream along with sum of intensity values of every pixel in the plain image using Eq. 5 and 6 to locate the pixel position to be processed.

Step 5 Scrambling algorithm is applied in both row and column directions to provide good amount of confusion and results in matrix B.

Step 6 Take a transpose of the scrambled matrix to alter the row and column position of the current matrix pixels and the matrix B is changed to C [$C=B^T$].

Step 7 Obtain the processed matrix C and apply the diffusion process as stated in the pixel diffusion algorithm using Eq.8 to entirely change the current matrix C to matrix D.

Step 8 The number of iterations can be increased accordingly to obtain a very good cryptosystem.

Step 9 The encryption process is complete and a gray scale ciphered image is generated.

F. Decryption process

Since the proposed encryption algorithm is a symmetric cryptosystem, it is easy to implement the decryption in reverse procedure based on the image encryption process as illustrated above. Here we obtain the chaotic sequence with the same initial condition as they are reactive to tiny changes in the condition. Then, inverse operation of diffusion is implemented and the transpose is applied to the matrix followed by scrambling operation. Finally the plain image is obtained by the inversion procedure with the same key.

IV. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

In this section we analyze and evaluate the metrics of the proposed system including histogram, correlation coefficients, differential analysis, key sensitive analysis, information entropy analysis, error computation, peak-signal-noise-ratio and noise resistance. Number of images are used from USC-SIPI Image Database as plain images and utilized for the testing purpose. Here an elaborated comparison is done with the existing algorithms [3, 4, 7, 17 and 18]. Our scheme has shown good amount of efficiency that overcomes all kinds of statistical attacks compared to conventional schemes.

A. Histogram

Histogram is the image information earned from the frequency of the grey level dispersed within an image. The highly secure cryptosystem shows the uniform distribution of the intensity values. If the histogram pattern leads to uneven distribution then the system is error-prone to statistical attacks. Seeing the histogram in Fig. 5 one can see the self-explanatory gray value distribution in the original image and the encrypted image. This proves that the proposed encryption system using Lorenz chaotic attractors has very good effect on image encryption.

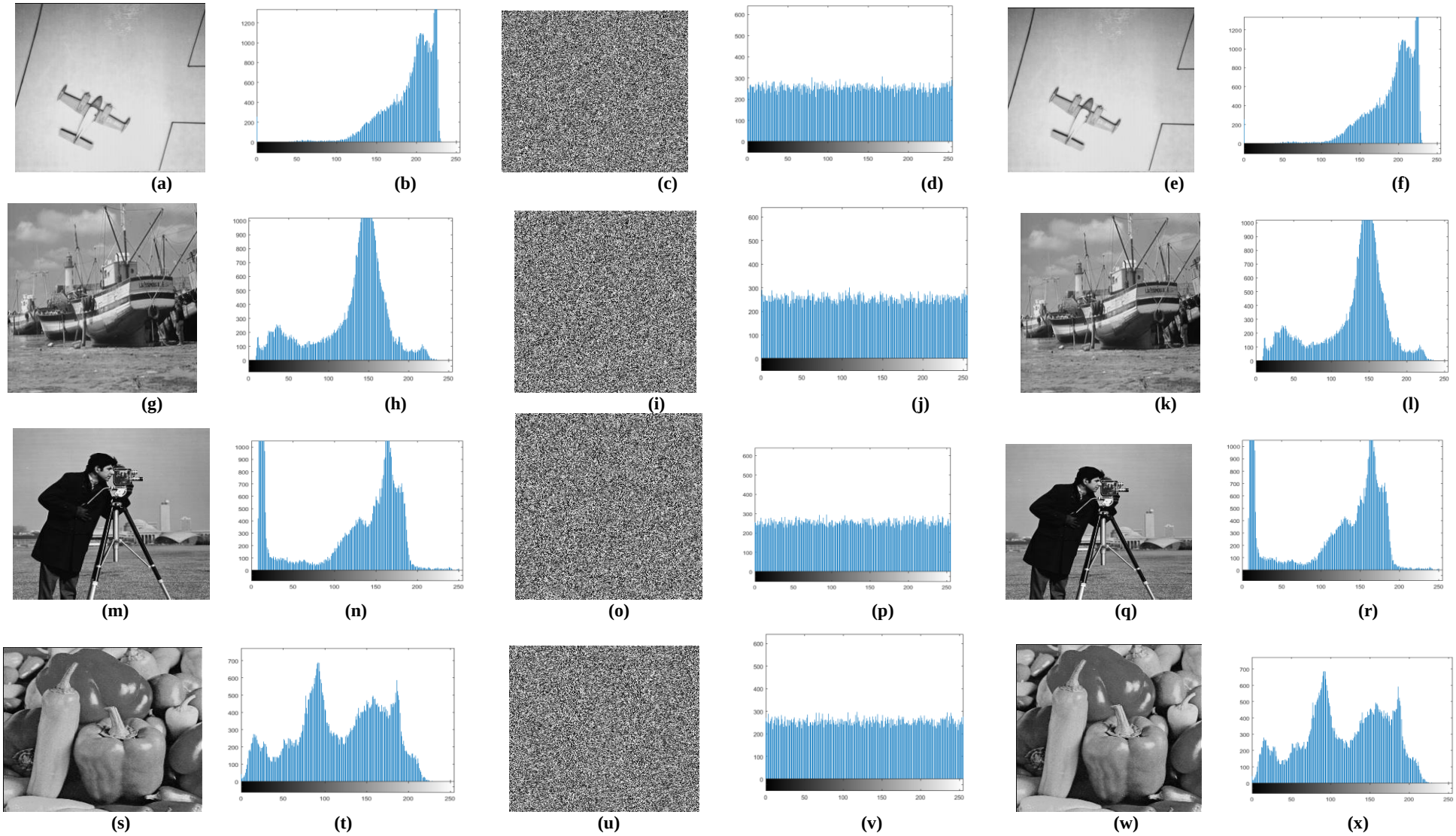


Fig. 5.Histogram of the images. (a), (g), (m) and (s) show the plain image, (b), (h), (n) and (t) show the histogram of the plain image, (c), (i), (o) and (u) show the encrypted image, (d), (j), (p) and (v) show the histogram of the encrypted image, (e), (k), (q) and (w) show the decrypted image and (f), (l), (r) and (x) show the histogram of the decrypted image.

B. Key space analysis

Higher dimensional system has larger key space compared to the lower dimensional systems. Here we acquire a non-linear three dimensional system that enlarges the key space and makes the computation complex. The key space should be large enough to resist the attacks such as brute force attack as much as possible. Here we determine the initial conditions and canonical parameters x_0, y_0, z_0, σ, β, ρ, SK_1, SK_2 and SK_3 as keys. The computational precision of the floating point number is about 10^{14}, so the key space can grow up to 10^{126} this is large enough to beat out the attacks.

C. Key sensitive analysis

Key sensitiveness of the cryptosystem conquers the major part, since a tiny variation in a key can result in different cipher images. To test the robustness of an ideal cryptosystem key sensitive analysis is carried out. Our proposed system has high efficiency where a bit change in the original key produce a different cipher image as shown in Fig. 6.

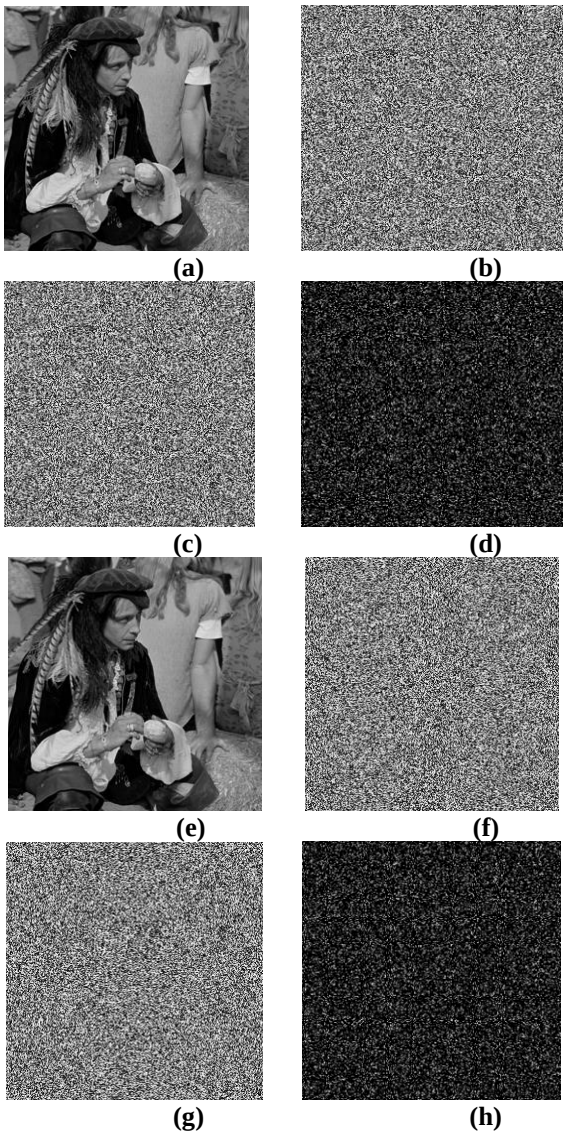


Fig. 6.Key sensitive analysis. (a) Plain image, (b) Encrypted image with key K1, (c) Encrypted image with duplicate key K2, (d) Difference between the encrypted images b and c, (e) Decrypted image with key K1, (f) Decrypted image with key K2, (g) Decrypted image with another duplicate key K3 and (h) Difference between the decrypted images f and g.

D. Information entropy

Information entropy is used to measure the randomness of information in the encrypted image. We can obtain the information entropy by using the following formula.

$$E(m) = \sum_{i=0}^{N-1} p(m_i) \log_2 \frac{1}{p(m_i)} \quad (9)$$

Here N is the total number of allowed pixel intensity value, $p(m_i)$ indicates the probability of the symbols m_i. The entropy value closer to 8 proves the system to be ideal and much more random holding the randomness property in a fair way. The encrypted image entropy values are recorded in Tables. 1 and 2. The tabulated values show the results of our scheme and the comparisons with existing algorithms in [3, 4, 7 and 17].

Table- I: The Information entropy results

Image name	Our scheme
Airport	7.9977
Airplane	7.9971
Boat	7.9979
Cameraman	7.9974
Chemical plant	7.9972
Clock	7.9971
Couple	7.9974
Elaine	7.9973
House	7.9978
Lena	7.9982
Man	7.9977
Moon surface	7.9973
Peppers	7.9972
Tank	7.9974

Table- II: The comparison of average Information entropy results with other schemes

Method	Our scheme	Zahmoul et.al [3]	Belazi et.al [4]	Wang et.al [7]	Hua et.al [17]
Average	7.9975	7.9986	7.9976	7.9959	7.9965

E. Correlation analysis

Correlation analysis analyzes the existing relationship present in between the pixels within an image. A good cryptosystem should posses a very minimal amount or null correlation between the encrypted images to get rid of the relation present in the adjacent pixels. We measure the horizontal and vertical correlations spread across the encrypted image. We derive the correlation coefficients by the following formula.

$$Corr(r,s) = \frac{E[(r-\mu_r)(s-\mu_s)]}{\sigma_r \sigma_s} \quad (11)$$

where r, s are the gray scale values of the randomized pair of the images. Fig. 7 shows the horizontal and vertical correlation coefficients of the plain and encrypted images. From Table. 3 and 4 we infer the correlation values of the proposed method with the compared algorithms are much smaller than the original image ensuring the encrypted correlation values are entirely randomized.

Table- III: Simulation results of Correlation analysis

Image name	Direction	Our scheme
Airport	Horizontal	-0.0086
	Vertical	-0.0027
Airplane	Horizontal	-0.0130
	Vertical	-0.0079

Boat	Horizontal	-0.0018
	Vertical	-0.0029
Cameraman	Horizontal	-0.0104
	Vertical	-0.0015
Chemical plant	Horizontal	0.0078
	Vertical	0.0009
Clock	Horizontal	-0.0049
	Vertical	-0.0028
Couple	Horizontal	0.0008
	Vertical	-0.0001
Elaine	Horizontal	0.0039
	Vertical	-0.0043
House	Horizontal	-0.0045
	Vertical	-0.0055
Lena	Horizontal	0.0104
	Vertical	-0.0055
Man	Horizontal	0.0033
	Vertical	-0.0025
Moon surface	Horizontal	0.0003
	Vertical	-0.0072
Peppers	Horizontal	0.0003
	Vertical	-0.0047
Tank	Horizontal	-0.0042
	Vertical	0.0025

Table- IV: The comparison of average Correlation values with the existing schemes

Direction	Our scheme	Zahmoul et.al [3]	Belazi et.al [4]	Wang et.al [7]	Hua et.al [17]
Horizontal	-0.0014	-0.0574	-0.0120	-0.0083	-0.0102
Vertical	**-0.0024**	**-0.0383**	**-0.0179**	**-0.0081**	**-0.0070**

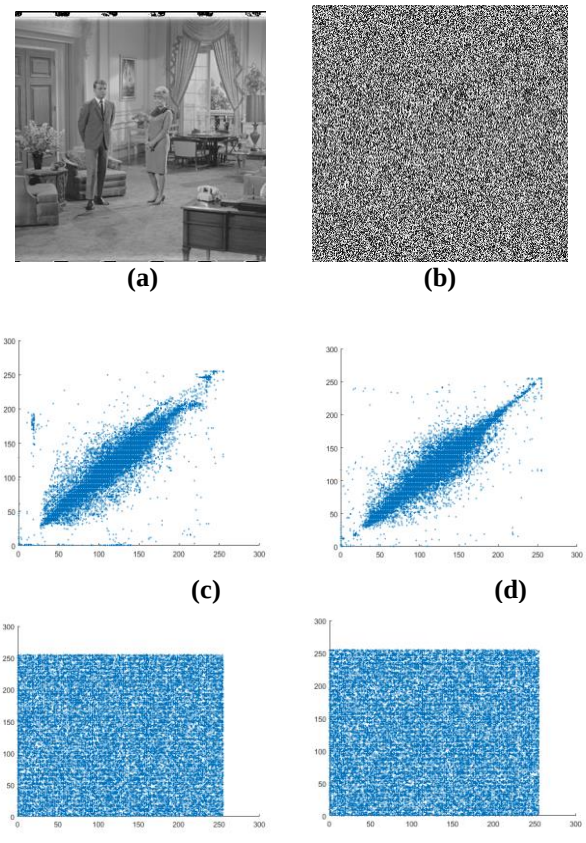


Fig. 7.Correlation analysis. (a) Plain image, (b) Encrypted image, (c) Horizontal correlation of the plain image, (d) Vertical correlation of the plain image, (e) Horizontal correlation of the encrypted image, (f) Vertical correlation of the encrypted image.

F. NPCR and UACI test

The number of pixel change rate (NPCR) and unified average changing intensity (UACI) are the two metrics used to test the consequence of the changed pixels between two encrypted images. The number of pixel change rate measures the number of distinct pixels between two encrypted images, while the unified average changing intensity measures the average intensity of the two images. We obtain the differential analysis by the following formula.

$$NPCR = \frac{1}{M * M} \sum_{i=1}^{M} \sum_{j=1}^{M} P(i, j) * 100 \quad (11)$$

$$UACI = \frac{1}{M * M} \sum_{i=1}^{M} \sum_{j=1}^{M} \frac{\left| C_1'(i, j) - C_2'(i, j) \right|}{255} * 100 \quad (12)$$

$$P(i, j) = \begin{cases} 0, & if\ C_1'(i, j) = C_2'(i, j) \\ 1, & if\ C_1'(i, j) \neq C_2'(i, j) \end{cases} \quad (13)$$

where *C1'* and *C2'* are the two encrypted images obtained by changing their plain images by one bit. *M* represent the dimension of the image.

After evaluation we get the average NPCR 99.6 and UACI 33.5 which are compared with the values of the existing algorithms [3, 4, 7 and 17]. Here first the comparison is made for the number of pixel change rate of our proposed scheme with other algorithms and secondly the unified average changing intensity of the proposed scheme is compared to the existing algorithms and the values are tabulated in the Tables 5, 6 and 7. Experimented results show that our method achieves notable diffusion property showing robustness and resistant to attacks.

Table- V: Simulation results of NPCR and UACI tests

Image name	NPCR	UACI
Airport	99.6063	33.3998
Airplane	99.6017	33.6138
Boat	99.6002	33.6690
Cameraman	99.6216	33.4849
Chemical plant	99.6078	33.2264
Clock	99.5895	33.4335
Couple	99.6384	33.5494
Elaine	99.6353	33.5203
House	99.6231	33.5061
Lena	99.6170	33.4305
Man	99.6063	33.3824
Moon surface	99.6094	33.5690
Peppers	99.6315	33.6049
Tank	99.6469	33.6405

Table- VI: The comparison of NPCR results with other schemes

Method	Our scheme	Zahmoul et.al [3]	Belazi et.al [4]	Wang et.al [7]	Hua et.al [17]
Average	99.6168	99.6170	99.6182	99.5600	99.6235

Table- VII: The comparison of UACI results with other schemes

Method	Our scheme	Zahmoul et.al [3]	Belazi et.al [4]	Wang et.al [7]	Hua et.al[17]
Average	33.5022	33.5000	33.6500	33.3831	33.6133

G. MSE analysis

Mean square error (MSE) is used to delimit the difference between the original image and the encrypted image. We derive MSE by the following formula.

$$MSE = \frac{1}{MN}\sum_{i=1}^{N}\sum_{j=1}^{M}[C(i,j) - E(i,j)] \qquad (14)$$

where C and E represents the original image and the encrypted image of size M and N. In the cryptosystem the mean square error values should range low to symbolize invulnerability. Tables. 8 and 9 shows the proposed scheme comprised of less mean square error value than the existing methods in Ref. [3, 18].

Table- VII: Mean Square Error results

Image name	Our scheme
Airport	8401.02
Airplane	10923.78
Boat	7572.43
Cameraman	9368.63
Chemical plant	7726.76
Clock	12244.39
Couple	6948.85
Elaine	7609.46
House	7722.20
Lena	7824.94
Man	10152.49
Moon surface	6213.42
Peppers	8409.44
Tank	6169.79

Table- IX: The comparison of MSE results with other schemes

Method	Our scheme	Zahmoul et.al [3]	Wua et.al [18]
Average	8377.68	8498.28	8456.06

H. PSNR analysis

The PSNR is the ratio to calculate the error occurrence between the original image and encrypted image. Qualitative measurement is used to scale the quality of the reconstructed image. We derive the Peak-signal-to-noise ratio by the following formula.

$$PSNR = 10 \times \log_{10}\left[\frac{N^2}{MSE}\right] \qquad (15)$$

where N is the maximum possible pixel intensity value of the image, MSE is the error introduced. To verify the quality of an encrypted image, the PSNR is calculated for several gray scale images and the corresponding results are tabulated in Tables 10 and 11. Therefore we conclude the proposed method bearing good quality and resistivity to attacks.

Table- X: The comparison of Psnr results with other schemes

Image name	Our scheme
Airport	8.92
Airplane	7.78
Boat	9.37
Cameraman	8.45
Chemical plant	9.28
Clock	7.29
Couple	9.75
Elaine	9.35
House	9.29
Lena	9.23
Man	8.10
Moon surface	10.23
Peppers	8.92
Tank	10.26

Table- XI: The comparison of Psnr results with other schemes

Method	Our scheme	Zahmoul et.al [3]	Wua et.al [18]
Average	9.02	8.95	8.97

I. Robustness to noise

Noise is a needless factor that distorts and degrades the images in an undesired way. Though an encrypted image is blurred or subjected to data loss a pertinent amount of information should be retrieved using a standard algorithm of the ideal cryptosystem. Here we experimented several encrypted images contaminated with Salt and Pepper noise, Speckle noise and Gaussian noise at various density levels and the corresponding decrypted results are analyzed and the results are shown in Fig. 8, 9 and 10.

(a) 0.01 **(b) 0.05**

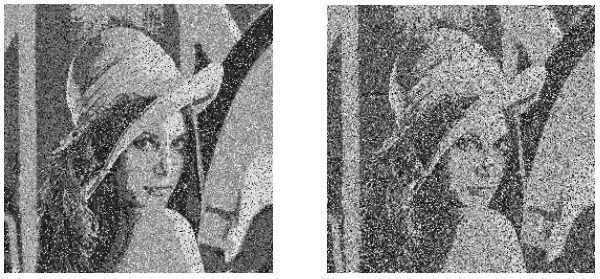
(c) 0.1 **(d) 0.2**

Fig. 8. Salt and Pepper noise with varied densities

(a) 0.01 **(b) 0.05**

(c) 0.1 **(d) 0.2**

Fig. 9.Speckle noise with varied densities



(c) 0.01 **(d) 0.05**

(c) 0.1 **(d) 0.2**

Fig. 10. Gaussian noise with varied densities

V. CONCLUSION

Our work has led us to conclude the proposed cryptosystem that exhibit endurance of three dimensional Lorenz system in a finite time. The scrambling and diffusion are accomplished using the persuasive chaotic sequences. The proposed system assures the trailing aspects: statistical attack, differential attack and noise attack. In addition, the key space is large and their sequences are moreover significant. Security measures exemplify the dependence of this method which is highly reactive to a light adjustment in the key unit. Numerical calculation and comparison of results have affirmed best dynamical characteristics, effectiveness and credibility of this proposed method. Conclusively based on this approach forthcoming conceptions can be boosted in signal encryption and video encryption.

REFERENCES

1. Ruisong Ye. 2011, “A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism”. Optics Communications, vol. 284, pp.5290-5298.
2. Ahmed G. Radwan, Sherif H. AbdElHaleem, Salwa K. Abd-El-Hafiz. 2016, “Symmetric encryption algorithms using chaotic and non-chaotic generators: A review”, Journal of Advanced Research, vol. 7, pp. 193-208.
3. Rim Zahmoul, Ridha Ejbali, Mourad Zaied. 2017, “Image encryption based on new Beta chaotic maps. Optics and Lasers in Engineering”, vol. 96, pp. 39-49.
4. Akram Belazi, Ahmed A. Abd El-Latif, Safya Belghith. 2016, “A novel image encryption scheme based on substitution-permutation network and chaos”, Signal Processing, vol. 128, pp. 155-170.
5. Ping Ping, Feng Xu, Yingchi Mao, Zhijian Wang. 2018, “Designing permutation-substitution image encryption networks with Henon map”, Neurocomputing, vol. 283, pp. 53-63.
6. Hayder Natiq, N.M.G. Al-Saidi, M.R.M. Said, Adem Kilicman. 2018, “A new hyperchaotic map and its application for image Encryption”, The European Physical Journal Plus, vol. 133, no. 6, pp. 1-14.
7. Xingyuan Wang, Lintao Liu, Yingqian Zhang. 2015, “A novel chaotic block image encryption algorithm based on dynamic random growth technique”, Optics and Lasers in Engineering, vol.66, pp. 10-18.
8. Guodong Ye. 2010, ”Image scrambling encryption algorithm of pixel bit based on chaos map”, Pattern Recognition Letters, vol.31, no.5, pp. 347-354.
9. Guomin Zhou, Daxing Zhang, Yanjian Liu, Ying Yuan, Qiang Liu. 2015, “A novel image encryption algorithm based on chaos and Line map”, Neurocomputing, vol. 169, pp. 50-157.
10. Shyamalendu Kandar, Dhaibat Chaudhuri, Apurbaa Bhattacharjee, Bibhas Chandra Dhara. 2019, “A novel image encryption using sequence generated by cyclic group”, Journal of Information Security and Applications, vol. 44, pp. 117-129.
11. Junxin Chen, Zhi-liang Zhu, Li-bo Zhang, Yushu Zhang, Ben-qiang Yang. 2018, “Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption”, Signal Processing, vol. 142, pp.340-353.
12. Zhenjun Tang, Juan Song, Xianquan Zhang, Ronghai Sun. 2016, “Multiple-image encryption with bit-plane decomposition and chaotic maps”, Optics and Lasers in Engineering, vol. 80, pp.1-11.
13. Hung-I Hsiao, Junghsi Lee. 2015, “Color image encryption using chaotic nonlinear adaptive filter”, Signal Processing, vol. 117, pp.281-309.
14. Qiang Zhang, Xiaopeng Wei. 2013, “A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system”, Optik, vol. 124, no. 23, pp. 6276-6281.
15. Chang'e Dong. 2014,”Color image encryption using one-time keys and coupled chaotic systems”, Signal Processing:Image Communication, vol. 29, no. 5, pp. 628-640.
16. Buncha Munmuangsaen, Banlue Srisuchinwong. 2018, “A hidden chaotic attractor in the classical Lorenz system”, Chaos, Solitons and Fractals, vol. 107, pp. 61-66.
17. Zhongyun Hua, Yicong Zhou, Chi-Man Pun, C.L. Philip Chen. 2015, “2D sine logistic modulation map for image encryption”, Information Sciences, vol. 297, pp. 80-94.
18. Yue Wua, Gelan Yangb, Huixia Jinb, Joseph P. Noonana. 2012, “Image encryption using the two dimensional logistic chaotic map”, Journal of Electron Imaging, vol. 21 no. 1, pp. 1-15.
19. Hossam Diab, Aly M. El-semary. 2018, “Cryptanalysis and improvement of the image cryptosystem reusing permutation matrix dynamically”, Signal Processing, vol. 148, pp. 172-192.
20. Qi Zhang, Yuchao Guo, Wangshu Li and Qun Ding. 2016, “Image encryption method based on discrete Lorenz chaotic sequences”, Journal of Information Hiding and Multimedia Signal Processing, vol. 7 no. 3, pp. 576-586.
21. Smita Khond, Bellamkonda Vijayakumar. 2019, “Secure Medical Image Processing Using Chaos And Dna Encryption Enhanced Using Reversible Data Hiding”, International Journal of Engineering and Advanced Technology, vol. 8, no. 6S, pp. 1062-1067.
22. Hong-Mei Yuan, Ye Liu, Tao Lin, Ting Hu, Li-Hua Gong. 2017, “A new parallel image cryptosystem based on 5D hyper-chaotic system”, Signal Processing: Image Communication, vol. 52, pp. 87-96.

AUTHORS PROFILE

V. Sangavi, Research scholar, Department of Computer Science, University of Madras, Chennai, India. She received the B.Sc. degree in Computer Science from University of Madras in 2014 and M.Sc. degree in Computer Science from University of Madras in 2016 respectively. Currently she is pursuing PhD in University of Madras. She has secured Best paper award in the 7th International conference on Contemporary Engineering and Technology 2019. Her research interests include Algorithms, Image processing, Nonlinear Dynamics and Cryptography.

P. Thangavel, Professor, Department of Computer Science, University of Madras, Chennai, India. He is a distinguished Professor and the Chairperson of computer science department at University of Madras. He served as an Adjunct Professor of Computer Science, at Liverpool Hope University, UK from August 2007 to July 2009. He served as referee for the Journals: Information Processing Letters, Parallel Processing Letters, and Information and Software Technology, Neurocomputing, IEEE Transactions on Neural Networks. His specialization includes Algorithms and Artificial Systems, Image Processing and Neural Networks and so on.