Available online at www.elixirpublishers.com (Elixir International Journal)

Electrical Engineering

Elixir Elec. Engg. 97 (2016) 41904-41909

ISSN: 2229-712X

Image Encryption using Four-Dimensional Hyper Chaotic Lorenz System

A. Kumar[1], M. Kar[1], M. K. Mandal[1*] and D. Nandi[2]

[1]Department of Physics, National Institute of Technology, Durgapur 713209, India.

[2]Department of Information Technology, National Institute of Technology, Durgapur 713209, India.

ARTICLE INFO

Article history:

Received: 15 June 2016;

Received in revised form: 24 July 2016;

Accepted: 30 July 2016;

Keywords

Lorenz system,
Chaos,
Encryption,
Decryption,
Information entropy,
NPCR,
UACI,
PSNR.

ABSTRACT

The paper proposed the application of a new four-dimensional hyper chaotic map based on the Lorenz chaotic system to realize chaotic encryption for improved security. Hyper chaotic systems are more complex and difficult to predict. An image encryption algorithm is designed by utilizing the basic operations like permutation, confusion and diffusion. The combination of the user defined 256 bits secret key and the plain image are used as initial conditions for the 4D hyper-chaotic system to generate the key matrix. Several test images are used for inspecting the validity of the proposed work. The security analyses and computer simulations on the basis of key space analysis, statistical analysis, histogram analysis, information entropy analysis, correlation analysis and differential analysis is done. The NPCR and UACI values of encrypted images are also calculated. The result shows that a single bit change in the pixel value of the input plain images will cause a significant changed in the ciphered images. Total key space for the proposed method is 2^{256}, which is good enough to protect the encrypted image against brute-force attack.

1.Introduction

With the advent of internet, computer communication techniques both wired and wireless, play a major role in data transmission and reception. The amount of information exchange per second in a dedicated network is far beyond imagination. The data may consist of a text, image, audio or video. A data may carry sensitive information and hence it's confidentiality, integrity and authenticity needs to be ensured. Therefore ensuring its security is a major concern. Keeping this in mind, work started on techniques of secure data communication. In the present age, Images have become very popular because of its visual information and flexibility to carry a variety of information. Hence image security has become an important topic in the current world of computers. The term cryptography got coined to the work related to encryption and decryption. Many encryption methods have been proposed in the literature. Conventional encryption methods both private key cryptosystems [1,2] and public key cryptosystems [3,4] had gained a lot of importance. But at a certain stage these methods fail in certain security analysis or are too complex in nature. Using these conventional methods information content stands vulnerable. Keeping these in mind work started on chaos theory. A chaotic behaviour is unpredictable. We use its unpredictability to generate randomness. Chaotic maps offer many desirable cryptographic properties and are simple to understand, execute, showing excellent security.

A lot of work on chaos based encryption techniques has been done in the recent times. Shannon [5] has successfully explained the implementation of chaos in communications. He suggested diffusion and confusion as the fundamental aspect of a good data encryption system. In its simplest form permutation and substitution are the fundamental aspects of cryptography. In reference [6] two chaotic logistic maps are used whose initial conditions are derived from the secret external key, eight different methods are being suggested for encrypting a pixel, the outcome of the logistic map will govern a particular encryption method for a particular pixel. In reference [7], Zhang et al. proposed a method which used both chaotic and conventional cryptographic methods using discrete exponential chaotic map. The proposed algorithm showed good resistance to attacks such as differential, statistic, grey code, and entropy. In reference [8], a secure image encryption technique is presented using two dimensional baker map. In reference [9], image encryption is done using multiple chaotic circular mapping. Step by step sub keys are being generated using chaotic maps and the sub key obtained in the last step is used for encryption. Dynamic sequences generated by one dimensional multiple chaotic systems are used in block encryption as proposed by Wang [10]. A new image encryption scheme using three different chaotic maps are presented in [11]. The plain image is broken into blocks of size (8×8) and cat map is used for block based shuffling and its control parameters are generated by 2D coupled logistic maps. Finally the shuffled image is encrypted using a chaotic logistic map. In reference [12], three step image encryption algorithm is proposed. First step constitutes of encrypting the whole image using logistic map, second step constitutes dividing the image into random number of blocks, and random permutation of these blocks is performed in the third step. Steps two and three are repeated for a fixed number of iterations. In reference [13], Dynamic substitution and diffusion based image encryption using modified logistic map ispresented. In the algorithm a new substitution box is proposed whose value changes dynamically after every iteration of the chaotic maps. However, some noteworthy

Tele:
E-mail address: mrinalkanti.mandal@phy.nitdgp.ac.in

encryption algorithms [14-18] are either easy to crack, insufficient in terms of security, or are too complex to develop.

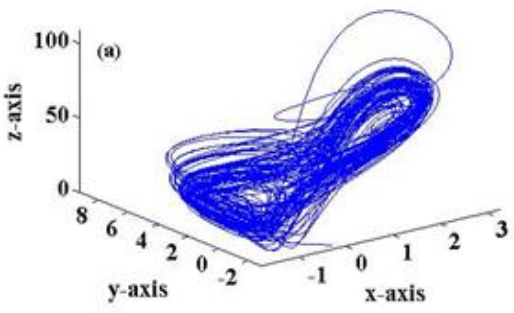
In this paper a novel image encryption scheme is proposed. A 4D Lorenz system is being used to generate key matrix which is sensitive to the plane image and secret key. This feature confirmed the self-diffusion of plane image information and as well as secret key in the encrypted image. The plain image and the secret key are used as initial conditions to the 4D Lorenz system. A single-step encryption process is used in the proposed algorithm by considering key shuffling, pixel permutation, pixel confusion, and diffusion. The rest of the paper is organized as follows: in section 2 the nature of the chaotic system is described. Section 3 presents the image encryption and decryption algorithm. Section 4 presents the security analysis. Relevant conclusion is presented in section 5.

2. 4D chaotic Lorenz system

The proposal of chaos based encryption came in the literature in 1989 [19]. Till date a lot of people have shifted their focus on chaotic maps and obtained a lot of achievements. The chaotic systems possess pseudo randomness, ergodicity, and are sensitive to initial values and parameters. A slight change in the initial values or parameters produce a great change in the resultant chaotic sequence. In this paper the application of 4D Lorenz system is presented. The first 3D chaotic attractor was found by Lorenz in 1963 [20]. The 3D Lorenz chaotic system has only one positive lyapunov exponent. But a hyper chaotic system is more complex and secure and it must satisfy the following two necessary conditions: (1) it should be at least four dimensional autonomous system, and; (2) two or more positive lyapunov exponents should be present and the sum of all the lyapunov exponents should be less than zero. Therefore the 3D Lorenz system can be modified as a 4D hyper chaotic system [21] as stated below to achieve better result in image encryption.

$$\left.\begin{aligned} \dot{x} &= a(y-x) \\ \dot{y} &= cx - xz - y + ew \\ \dot{z} &= x^4 + y^4 - bz \\ \dot{w} &= -dy \end{aligned}\right\} \quad (1)$$

Where *a*, *b*, *c*, *d*, *e* are the five parameters and *x*, *y*, *z*, *w* are the state variables of the hyper chaotic system. To solve equation (1) we have taken $a = 10$, $b = 8/3$, $c = 46$, $d = 2$ and $e = 12$ as the parameter values. The four lyapunov exponents of the system are $\lambda_1 = 0.60613$, $\lambda_2 = 0.28066$, $\lambda_3 = 0$ and $\lambda_4 = -11.489$. Figures 1 (a) and (b) represent the chaotic attractor in (x, y, z) space and (y, z, w) space respectively for the 4D Lorenz system.



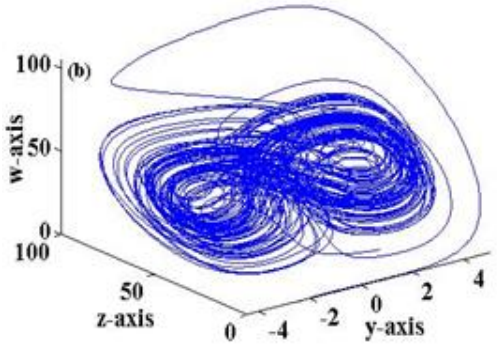


Fig 1. Chaotic attractor of the 4D Lorenz system: (a) in (x, y, z) space and (b) in (y, z, w) space.

3. Proposed image encryption algorithm

Consider a gray scale image P of size $m \times n$. Let $P(i,j)$ represents the pixel value at position (i,j). The proposed image encryption algorithm consists of the following major stages: Generation of chaotic key matrix, pixel confusion and diffusion, attaching digital signature of original image to the encrypted image. The step by step encryption algorithm is mentioned below.

Step-1: The 32 character (256 bits) secret key and the plain image *P* are taken as inputs in the proposed algorithm. A user defined function given in equation (2) returns a digital signature matrix (DSM) D_1 of size $m \times 1$ from the input plane image P. The number of elements in D_1 is same as the number of rows in the plain image. The function is given by,

$$D_1(k,1) = \frac{1}{n-1}\sum_{i=1}^{n-1} P(k,i+1) - P(k,i), \quad (2)$$

where $D_1(k,1)$ represents the mean of the consecutive differences of the pixel values in the *k*-th row. The variable *k* in equation (2) varies from 1 to *m*.

Step-2: The digital signature matrix D_1 is reshaped into another matrix D_2 of size 16×16 by taking the first 256 elements of D_1. Now restrict the elements of D_2 within the range of 0 to 256 by performing the operation $D_2 \leftarrow round(mod(D_2 * 10^5, 256))$. Next, from D_2 we produced another two matrices D_3 and D_4 of size 16×1 and 1×16 respectively by using the following equations mentioned below

$$D_3(q,1) = round\left(mod\left(\left(\frac{10^5}{15}\sum_{i=1}^{15} D_2(q,i+1) - D_2(q,i)\right),255\right)\right) \quad (3)$$

$$D_4(1,q) = round\left(mod\left(\left(\frac{10^5}{15}\sum_{i=1}^{15} D_2(i+1,q) - D_2(i,q)\right),255\right)\right) \quad (4)$$

.

Here *q* varies from 1 to 16. After that construct a one dimensional array M_i (*i* varies from 1 to 32) using the alternate elements of D_3 and D_4.

Step-3: Now convert the 32 character secret key into a double precision one dimensional array of 32 elements and divide each element of this array by 127 and extract four digits to the right of the decimal point to construct a new array K_i (*i* varies from 1 to 32). Convert K_i in the range 0 to 256 by the operation $K_i = round(\mathrm{mod}(K_i, 256))$.

Step-4: Generate the four initial conditions of the 4D chaotic Lorenz system using the following algebraic combination of M_i and K_i as follows:

$$x_0 = \frac{1}{256}\sum_{i=1}^{8}\left(K_i + \left(\frac{K_i M_i}{256}\right) + M_i\right) \quad (5)$$

$$y_0 = \frac{1}{256}\sum_{i=9}^{16}\left(K_i + \left(\frac{K_i M_i}{256}\right) + M_i\right) \quad (6)$$

$$z_0 = \frac{1}{256}\sum_{i=17}^{24}\left(K_i + \left(\frac{K_i M_i}{256}\right) + M_i\right) \quad (7)$$

$$w_0 = \frac{1}{256}\sum_{i=25}^{32}\left(K_i + \left(\frac{K_i M_i}{256}\right) + M_i\right) \quad (8)$$

Now solve the equation (1) using the above initial conditions defined in the equations (5) to (8) and produce a 2D array $S_{i,j}$ of size $m \times n$. Next extract four digits to the right of the decimal point of each element of this array and construct a new array $A_{i,j}$ of dimension $(mn/32) \times 32$. Convert $A_{i,j}$ in the range 0 to 256 by the operation $A_{i,j} = round(\mathrm{mod}\,(A_{i,j}, 256))$.

Step-5: Perform bitwise XOR operation between the i^{th} row of *A* and the secret key *K* to get $CK_{i,j} = A_{i,j}\ XOR\ K_j$. (*i* is constant for *i*-th row and *j* varies from 1 to 32). Next execute the circular shift operation of the elements of K by *P* times, where $P = mod(CK_{i,32}, 32)$. After that perform bitwise XOR operation between the $(i+1)^{th}$ row of *A* and the shifted key *K* to get $CK_{i+1,j} = A_{i+1,j}\ XOR\ K_j$.

Step-6: Perform step-5 for $i = mn/32$ times to get the $CK_{i,j}$ array of dimension $(mn/32) \times 32$. Next reshape the array $CK_{i,j}$ to another array $C_{i,j}$ of dimension $m \times n$. Now, reshape the array $A_{i,j}$ into dimension $m \times n$.

Step-7: Execute the pixel shuffling operation of the plain image *P* by changing the pixel positions according to $P_{C_{i,j},C_{j,i}} \leftrightarrow P_{A_{i,j},A_{j,i}}$ (*i* varies from 1 to *m* and *j* varies from 1 to *n*). The pixel confusion of the shuffled plain image is done by performing bitwise XOR operation between $C_{i,j}$ and $P_{i,j}$ to get encrypted image $E_{i,j} = C_{i,j}\ XOR\ P_{i,j}$. Next attach the digital signature matrix D_1 to the $E_{i,j}$ according to the Fig. 2 to get the required encrypted image E_p of dimension $m \times (n+1)$.

Pixel (1,1)	Pixel (1,2)	Pixel (1,3)	---	Pixel (1,n-1)	Pixel (1,n)	D_1 (1,1)
Pixel (2,1)	Pixel (2,2)	Pixel (2,3)	---	Pixel (2,n-1)	Pixel (2,n)	D_1 (2,1)
Pixel (3,1)	Pixel (3,2)	Pixel (3,3)	---	Pixel (3,n-1)	Pixel (3,n)	D_1 (3,1)
---	---	---	---	---	---	
Pixel (m-1,1)	Pixel (m-1,2)	Pixel (m-1,3)	---	Pixel (m-1,n-1)	Pixel (m-1,n)	D_1 (m-1,1)
Pixel (m,1)	Pixel (m,2)	Pixel (m,3)	---	Pixel (m,n-1)	Pixel (m,n)	D_1 (m,1)

Fig 2. An encrypted image and digital signature matrix D_1 (last column).

The decryption algorithm has been written in reverse way of the encryption algorithm.

4. Security analysis

A chaotic cryptosystem can be termed as secure and efficient if it is resistive to any kind of known attacks. Security analysis tests the robustness of an image encryption system. The security analysis like key space analysis, key sensitivity analysis, peak signal to noise ratio, mean absolute error, statistical analysis and differential analysis are carried out in the present work to prove the efficiency of the proposed cryptosystem. The grey scale images are used to carry out the test results and to prove the validity of the proposed algorithm. Five different images are taken and the key **c Q** t@##%^&,./<>frtQWMO./*:;ZAk is used for encryption. The decryption using same key c Q t@#$$%^&,./<>frtQWMO./*:;ZAk produces exact image but the decryption using slightly wrong key c Q t@#$$%^&,./<>frtQWMO./*:;ZAl is not possible, which proved the effectiveness of the algorithm. The encryption and decryption results for different test images are shown in Fig. 3.

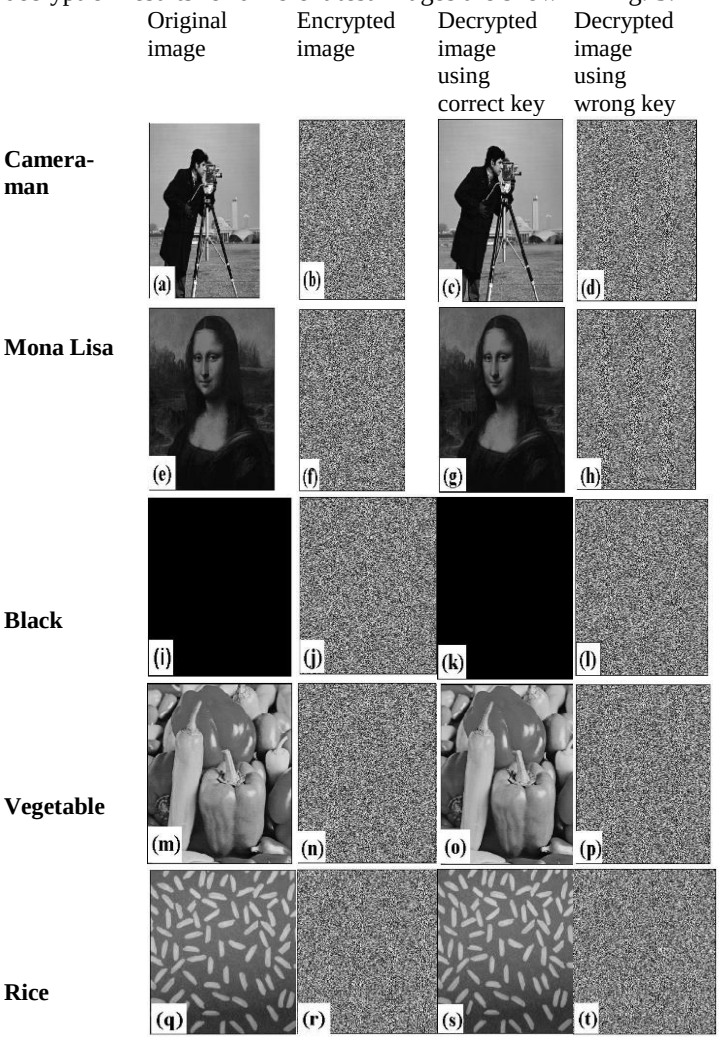


Fig 3. First column: different plain images. Second column: encrypted images using key c Q t@#$$%^&,./<>frtQWMO./*:;ZAk. Third column: decrypted images using same key c Q t@#$$%^&,./<>frtQWMO./*:;ZAk. Fourth column: decrypted images using wrong key c Q t@#$$%^&,./<>frtQWMO./*:;ZAl.

4.1. Key space analysis

In the present paper we have a 32 character key. Hence in terms of number of bits the key is 256 bits long. Thus the key space is 2^{256}, which means that many different keys can be used for the image encryption process which is sufficiently

large enough to withstand brute-force attacks.

4.2 Key sensitivity analysis

The proposed encryption and decryption algorithm is highly sensitive to the input secret key. A single bit change in the secret key used for encryption causes the encrypted images to differ to a very large extent. Also if the encrypted image is decrypted using a wrong key which has only a bit change with respect to the key used for encryption, the decrypted image will not be the same as original image. The results are shown in Fig. 3. Hence it can be said that the proposed algorithm is sensitive to secret key and is resistive to known plain text attacks.

4.3 Mean squared error

The mean squared error (MSE) is termed as the average squared difference between original input image and the ciphered image. A high value of MSE is desirable to prove the dissimilarity between the original image and the encrypted image. The MSE can be defined as

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left(P(i,j) - E(i,j)\right)^2. \quad (9)$$

The notations $P(i,j)$ and $E(i,j)$ denote the pixel values of the i^{th}row and j^{th} column of the original and the encrypted images respectively. The results using different images are shown in Table-1.

Table 1. Parameters of encryption quality.

Images	MSE	PSNR	Information entropy	
			Plain image	Encrypted image
Cameraman	9409.4	8.3952	7.0097	7.9972
Mona Lisa	13044.9	6.9763	6.3503	7.9975
Black	21403.7	4.8259	0	7.9918
Vegetable	8279.5	8.9507	7.5327	7.9973
Rice	7484.1	9.3894	7.0115	7.9973

4.4 Peak signal to noise ratio

The peak signal to noise ratio (PSNR) is widely used to measure the degree of distortion of an image. In this regard the comparison between the original plain image and the encrypted image is done. A PSNR value of 100 dB will mean that the original image and encrypted image are the same. Hence for a good encryption algorithm the value of PSNR should be as low as possible. The PSNR is calculated using the following formula [22] given by

$$PSNR = 10 log_{10} \left(\frac{I_{MAX}^2}{MSE}\right), \quad (10)$$

where I_{MAX} is the maximum value of the pixel of the given image. The results for different images are shown in Table-1.

4.5 Information entropy analysis

The entropy is quantitative measure to measure how random an image encryption algorithm behaves. A secure image encryption algorithm should be such that the encrypted image shall not provide any information of the original image. The entropy is calculated using the equation mentioned below

$$Entropy = \sum \left(p(i) * log \left(\frac{1}{p(i)}\right)\right), \quad (11)$$

where $p(i)$ denotes the probability of occurrence of a pixel with grey scale value i. The desirable value of entropy of an encrypted image is 8 if the pixel of the image is represented by 8-bits. The information entropy analysis has been carried out on different images and the obtained results are shown in Table-1.

4.6 Correlation analysis

The pixel correlation is performed between two adjacent pixels along horizontal, vertical and diagonal directional of the plain image and the encrypted image respectively to test the similarity among the pixels in a particular direction of the image [23]. To execute it 2000 pairs of adjacent pixels in horizontal, vertical and diagonal directional from both the plain image and the encrypted image were selected randomly. The calculated values of the correlation coefficient using the following formulas [24] stated below are given in Table-2 and the corresponding scatter plots are shown in Fig. 4.

$$r_{xy} = cov(x,y)/\left(\sqrt{D_x}\right)\left(\sqrt{D_y}\right), \quad (12)$$

$$E_x = \frac{1}{N}\sum_{i=1}^{N} x_i, \quad (13)$$

$$D_x = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2, \quad (14)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right). \quad (15)$$

Here *x*, *y* stands for the grey scale values of two adjacent pixels in the image to be considered and *N* is the term used to denote the total number of duplets (*x*, *y*) obtained from the image under consideration. Basically, the measured value of correlation coefficient of the plain image depends on the nature of the image, in general this value should be nearly equal to one. The measured value of correlation coefficient of the encrypted image should be very low or zero for good cryptosystem.

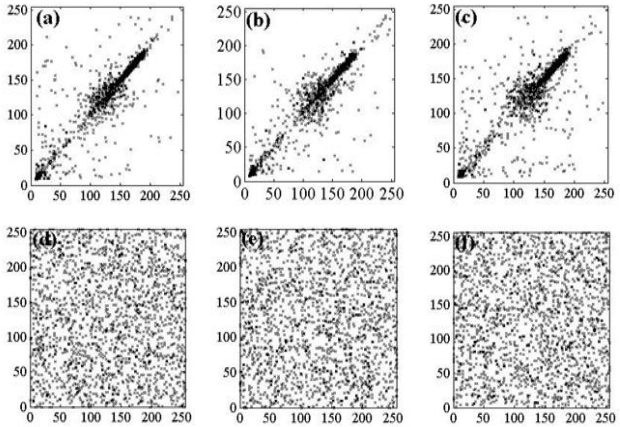


Fig 4. Correlation between two adjacent pixels of cameraman: Distribution of horizontally adjacent pixels (a) in plain image and (d) in encrypted image. Distribution of vertically adjacent pixels (b) in plain image and (e) in encrypted image. Distribution of diagonally adjacent pixels (c) in plain image and (f) in encrypted image.

On the other hand the correlation value between plain image and its encrypted version are also calculated using the formula (Norouzi et al. 2013) given below:

$$CC = \frac{\left(\sum_{i=1}^{m}\sum_{j=1}^{n}(A_{ij}-A)(B_{ij}-B)\right)}{\sqrt{\left(\sum_{i=1}^{m}\sum_{j=1}^{n}(A_{ij}-A)^2\right)}\sqrt{\left(\sum_{i=1}^{m}\sum_{j=1}^{n}(B_{ij}-B)^2\right)}} \quad (16)$$

Here *A* represents the plain image matrix and *B* represents the encrypted image matrix. The quantities $\dot{A}$, $\dot{B}$ represent the mean value of the matrices *A* and *B* respectively. Here *m*, *n* represents the number of rows and columns respectively of the image under consideration (original/encrypted). Ideally the correlation coefficient between the plain image and encrypted image should be zero to show both the images are perfectly dissimilar. The test results carried out using different images are shown in Table-2.

Table 2. Correlation coefficients.

Images	Horizontal		vertical		diagonal		Correlation between plane and encrypted image(CC)
	plane image	encrypted image	plane image	encrypted image	plane image	encrypted image	
Cameraman	0.0056	0.0023	0.9592	-0.0029	0.9087	-0.0045	0.0018
Mona Lisa	0.9903	0.00046	0.9883	-0.0024	0.9803	-0.0035	-0.0046
Black	0	0.0086	0	-0.0025	0	-0.0026	0
Vegetable	0.9478	0.0086	0.9482	-0.0025	0.9036	-0.0026	0.0086
Rice	0.9264	-0.0010	0.9432	-0.0015	0.8978	0.0015	0.0071

4.7 Histogram analysis

In statistical perspective histogram is an important tool in judging the quality of encrypted image. Basically through histogram analysis we can observe the number of times a particular grey level occurs in an image matrix. For a plain image the histogram plot would be irregular showing spikes. The spikes represent occurrence of a particular grey level more frequently. For a good quality encryption it desired that the histogram plot of the encrypted image should be uniform which ensures it's resistance to statistical attack. The histogram plot of various plain images and their encrypted versions are shown in Fig. 5.

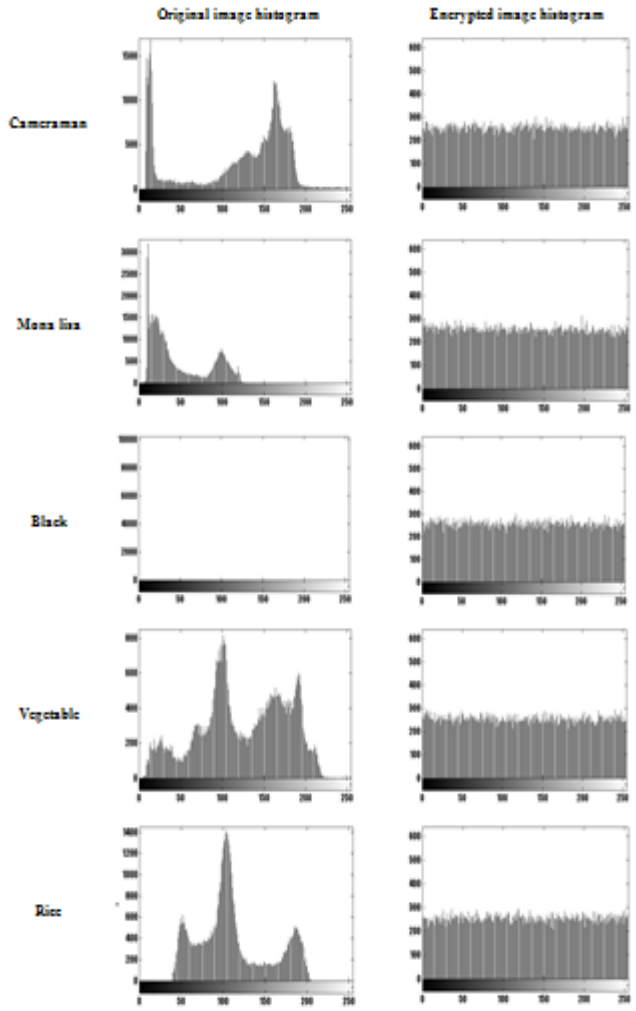


Fig 5. Histogram of original images and thei corresponding encrypted images.

4.8 Differential attack analysis

It may happen that cryptanalysts may have the encrypted image and the proposed algorithm. They make a small change in the plain image and encrypt the image using the said algorithm. Now they compare the two encrypted images and find relation between them. This is called differential attack. In order to tackle this type of attack the encryption algorithm should be designed such that a small change in the plain image should produce a vast change in the encrypted image. Two common measures are used to study the effect of one pixel change in the encrypted image by measuring the number of pixels change rate (NPCR) and unified average changing intensity (UACI). Let there be two cipher images C_1 and C_2. Their corresponding plain images differ only by one pixel. $C_1(i,j)$ and $C_2(i,j)$ are the pixel values at location (i,j). Now, we construct D a bipolar array with same dimensions as C_1 and C_2 and $D(i,j)$ may be 0 or 1 depending on the following condition:

$$D(i,j) = \begin{cases} 1, & if\ C_1(i,j) \neq C_2(i,j). \\ 0, & Otherwise \end{cases} \quad (17)$$

Therefore, NPCR and UACI may be written as follows

$$NPCR = \frac{\sum_{i,j} D(i,j)}{m \times n} \times 100\%, \quad (18)$$

$$UACI = \frac{1}{m \times n}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\%. \quad (19)$$

The NPCR and UACI values should be high as possible for a good encryption system. NPCR and UACI tests are carried out on various images and the obtained results are listed in the Table-3.

Table 3. NPCR and UACI values for one pixel difference in a plain image.

Images	Pixel positions	Changed value of pixel	NPCR	UACI
Cameraman	(1,1)	156 → 155	99.49	33.44
	(127, 218)	156 → 157	99.60	33.41
	(255,100)	98 → 99	99.59	33.46
Mona Lisa	(1,1)	94 → 95	99.62	33.49
	(127, 218)	32 → 33	99.61	33.58
	(255,100)	10 → 11	99.64	33.49
Black	(1,1)	0 → 1	99.64	33.56
	(127, 218)	0 → 1	99.61	33.47
	(255,100)	0 → 1	99.61	33.40
Vegetable	(1,1)	0 → 1	99.63	33.60
	(127, 218)	113 → 114	99.58	33.25
	(255,100)	200 → 199	99.60	33.54
Rice	(1,1)	122 → 121	99.56	33.47
	(127, 218)	99 → 100	99.58	33.44
	(255,100)	57 → 56	99.62	33.73

4.9 Randomness test

The encrypted image passes the random and pseudo-random sequence test standard SP 800-22 [25]. This test standard consists of sixteen different tests and the result of each test gives a p-value.

A good random and pseudo-random sequence should pass all the tests. If the p-value $\geq \alpha$ (In SP 800-22 test $\alpha = 0.01$) the sequence passed the test. The SP 800-22 test results for the cipher image is shown in Table-4. Since the test image is 256×256, thus the total numbers of bits used in this test is 524288.

Table 4. SP 800-22 random and pseudo-random sequence test results.

Test Name		Cipher image	
		p-value	Remarks
Frequency		0.2573	Success
Block frequency (M=128)		0.2846	Success
Runs		0.3953	Success
Longest runs of one (M=128, N=49, K=5)		0.0816	Success
Rank		0.2475	Success
Spectral DFT		0.6231	Success
Non overlapping templates(m=9, B=101000111)		0.6781	Success
Overlapping templates(M=1032, N=508)		0.2725	Success
Universal (L=6, Q=640, K=86741)		0.9719	Success
Linear Complexity (M=500)		0.4253	Success
Serial (m=10)	p-value 1	0.8356	Success
	p-value 2	0.7721	Success
Approximate entropy (m=10)		0.5665	Success
Cumulative sums	Forward	0.2732	Success
	reverse	0.2164	Success
Random excursions (x=1)		0.7732	Success
Random excursions variant (x=1)		0.2351	Success

5. Conclusion

In this paper a novel approach of 4D chaotic Lorenz system is proposed to design a cryptosystem. The proposed algorithm presents high security according to cryptanalysis results. A large key space of 2^{256} is sufficient to resist any type of brute force attack. The initial conditions are made extremely sensitive to the secret key as well as the input plain image. Hence a slight bit change in the key or the plain image will produce a significant change in the encrypted image. High values of NPCR = 99.64 and UACI =33.73 are sufficient to prove sensitivity of the proposed algorithm. The entire encryption and decryption algorithm was developed and tested in MATLAB. Overall it can be said that the proposed algorithm is a good competitor to other cryptographic algorithms.

Acknowledgments

This research work is supported by the DST-FIST, Govt. of India through Order no. SR/FST/PSI-007/2011.

References:

[1]. Bellare, M., Bennet, Y., (2003). Forward security in private key cryptography. RSA Conference, San Francisco, CA, USA, April 13–17, 2003.

[2]. Faragallah, O.S., (2011). An Efficient Block Encryption Cipher Based on Chaotic Maps for Secure Multimedia Applications. Information Security Journal: A Global Perspective, 20(3):135–147.

[3]. Rothblum, R. (2011). Homomorphic encryption from private key to public key. Theory of Cryptography. TCC Conference, Providence, RI, USA, 219-234, March 28-30, 2011.

[4]. Rao, R.C.G.A.V., Lakshmi, P.V., Shankar, R.N. (2013). A new modular multiplication method in public key cryptosystem. International J. Network Security, 15, 23-27.

[5]. Shannon, C.E. (1949). Communication theory of secrecy systems. Bell Systems Technical Journal, 28, 656-715.

[6]. Pareek, N.K., Patidar, V., Sud, K.K. (2006). Image encryption using chaotic logistic map. Image and Vision Computing, 24, 926–934.

[7]. Zhang, L., Liao, X., Wang, X. (2005). An image encryption approach based on chaotic maps. Chaos Solitons Fractals, 24, 759–765.

[8]. Honglei, Y., Shou .W.G., Ting, W., Diantao, L, Jun, Y., Weitao. M., Yu, F., Shaolei, Yi., Yuankao, (2009). An image encryption algorithm based on two dimensional baker map. Int. Conf. of Intelligent Computation Technology and Automation, Changsha, Hunan, China, October 10-11, 2009, 536-540.

[9]. Sathishkumar, G.A., Bagan, K.B., and Sriraam, N. (2011). Image encryption based on diffusion and multiple chaotic maps. Int. J. Network Security and Applications, 3, 181-194.

[10]. Wang, X.Y., Yu, Q. (2009). A block encryption algorithm based on dynamic sequences of multiple of multiple chaotic systems. Commun. Nonlinear Sci. Numer. Simulat. 14, 574-81.

[11]. Ahmad, M., Alam, M. S. (2009). A new algorithm of encryption and decryption of images using chaotic mapping. International J. Computer Science and Engineering, 2, 46-50.

[12]. Tabash, F. K., Rafiq, M.Q., Izharrudin, M. (2013). Image encryption algorithm based on chaotic map. International J. Computer Applications. 64, 1-10.

[13]. Devaraj, P. (2011). Dynamic substitution and diffusion based image encryption using modified logistic map. International Conference on Advanced Computing, Networking and Security. Surathkal, India, 593-601, December 16-18, 2011.

[14]. Akhshani, A., Behnia, S., Akhavan, A., Hassan, H.A., Hassan, Z. (2010). A novel scheme for image encryption based on 2D piecewise chaotic maps. J. Opt. Commun. 283, 3259-3266.

[15]. Akhavan, A., Samsudin, A., Akhshani, A. (2013). A novel parallel hash function based on 3D chaotic map. J. Advs. Signal Process. 2013, 126-1-12.

[16]. Nkapkop, J.D.D., Effa, J.Y., Fouda, J.S.A.E., Alidou, M., Laurent, B., Monica, B. (2014). A fast image encryption algorithm based on chaotic maps and the linear diophantine equation. Computer. Sci. Appl, 1, 232-243.

[17]. Kabi, K.K., Bidyut, J.S., Chauhan, A., Pradhan, C. (2015). Implementation of new framework for image encryption using Arnold 3D cat map. Information Systems Design and Intelligent Applications. 339, 379-384.

[18]. Thapliyal, P., Sharma, M. (2015). Image encryption and authentication scheme using 3D chaotic map. International Journal of computer Applications, 117, 15-18.

[19]. Mathews, R.A.J. (1989). On derivation of a chaotic encryption algorithm. Cryptologia 13, 29-42.

[20]. Lorenz, E.N. (1963). J. Atmos. Sci. 20, 131.

[21]. Si, G.Q., Cao, H., Zhang, Y.B. (2011). A new four-dimensional hyper chaotic lorenz system and its adaptive control. Chin. Phys. B. 20, 10509-9.

[22]. Sinha, A., Singh, K. (2003). A technique for image encryption using digital signature. J. Optics Communication, 218, 229-234.

[23]. Norouzi, B., Seyedzadeh, S. M., Mirzakuchaki, S., Mosavi, M.R. (2013). A novel image encryption based on hash function with only two-round diffusion process. Multimedia Systems, 20, 45-64.

[24]. Mandal, M.K., Kar, M., Singh, S.K., Barnwal, V.K. (2014). Symmetric key image encryption using chaotic Rossler system. Security Comm. Networks 7, 2145-2152.

[25]. Rukhin, A., et al. (2010). A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST 800-22.