Multimedia Tools and Applications (2019) 78:27611–27637
https://doi.org/10.1007/s11042-019-07881-x

A novel image encryption scheme based on Arnold scrambling and Lucas series

Syeda Iram Batool[1,2] · Hafiz Muhammad Waseem[3]

Received: 12 December 2018 / Revised: 21 May 2019 / Accepted: 10 June 2019 /
Published online: 25 June 2019

Abstract
Secure data transmission over the public channels have high impact and increasingly important due to theft and manipulation in contents. The requirement of public/ private organizations to develop an efficient scheme to provide security to their contents. We developed a digital contents encryption scheme based Arnold scrambling and Lucas series, which is very simple to implement but almost impossible to breach in this article. We perform encryption at standard images by using Lucas series at different iterations of scrambled images of Arnold transform. Numerical simulation analyses performed to analyze the efficiency and effectiveness of the projected structure.

Keywords Arnold scrambling · Lucas encryption · Data security · Diffie-Hellman algorithm

1 Introduction

The existing digital world become a global village due to fast expansion of internet. The access of digital contents from any part of digitally advanced world is quite easy. But there are several circumstances in daily existence, when it is significant to hide the actual contents of secret information transmitted over an insecure line of communication. Many traditional cryptosystems are utilized to perform these tasks in order to secure the confidential information [47]. Digital contents such as documents, images, audio and videos files are transmitted over insecure communication medium. This easiness sure added comfort in our daily live but on the other side it creates a massive threat to our secret information. The faith of nationals highly depends upon their secret information that has to be covered from eavesdropper. The

✉ Syeda Iram Batool
syedairambatool@gmail.com

[1] Cyber and Information Security Lab (CISL), Institute of Space Technology, Islamabad, Pakistan

[2] Department of Avionics Engineering, Institute of Space Technology, Islamabad, Pakistan

[3] Department of Electrical Engineering, Institute of Space Technology, Islamabad, Pakistan

confidentially of information can be achieved through encryption process. The modern block ciphers utilized the idea of substitution-permutation network (SP-Network) which is one of the fundamental aspect while designing strong encryption algorithm. The SP-network fundamentally utilized notions of confusion and diffusion. In quantitative sense, confusion can be achieved through substitution cipher whereas diffusion can be achieved through permutation [9, 14, 15, 33, 38, 41, 47, 55, 56].

The terms diffusion and confusion were acquainted by Claude Shannon with catch the two fundamental structure hinders for any cryptographic framework. Shannon's concern was to prevent cryptanalysis dependent on statistical security examination. Each block cipher algorithm includes a change of a block of plaintext into a block of ciphertext, where the change relies upon the key. The designing of diffusion looks to make the measurable connection between the plaintext and ciphertext as unpredictable as conceivable so as to foil endeavour's to conclude the key. Confusion tries to make the connection between the measurements of the ciphertext and the estimation of the encryption key as mind boggling as could be allowed, again to impede endeavours to find the key.

In this manner, diffusion and confusion in catching the quintessence of the ideal properties of a block ciphers that they have turned into the foundation of present day modern block ciphers. Structuring an encryption strategy utilizes both of the standards of confusion and diffusion. Diffusion implies that the procedure definitely changes information from the contribution to the yield, for instance, by interpreting the information through a non-straight table made from the key. We have bunches of approaches to turn around straight block ciphers, so the more non-direct it is the more investigation instruments it breaks. Diffusion implies that changing a single character of the info will change numerous characters of the yield [3–6, 26, 29, 42, 43, 57, 60, 61].

In order to achieve the good quality confusion, substitution boxes were utilized in literature [26, 29]. The construction of S-boxes with optimal characteristic is one of the most interesting problems in cryptography. Different types of mathematical structures for instance Galois field, Galois ring, chaos theory and optimization techniques were utilized to construct a confusion component of modern block ciphers [23–25, 28, 58, 59]. Moreover, diffusion can also be achieved through different chaotic systems.

Decent diffusion process distributes those patterns widely through the output, and if there are several patterns making it through they scramble each other. This makes patterns vastly harder to spot, and massively upsurges the quantity of data to analyse to break the cipher. In recent research in the field of chaos and especially on systems with complex (chaotic) behaviour have showed potential applications in various fields including healthcare, medicine and defence. The special characteristics, such as sensitivity to initial conditions, randomness, probability and ergodicity make chaos mapping as a potential candidate to analyse security issues. Chaotic maps and cryptographic algorithms have some similar properties: both are sensitive to tiny changes in initial conditions and parameters; both have random like behaviours; and cryptographic algorithms shuffles and diffuse data by rounds of encryption, while chaotic maps spread a small region of data over the entire phase space via iterations. The only difference in this regard is that encryption operations are defined on finite sets of integers while chaos is defined on real numbers. Integrating chaotic systems into a block cipher utilizes chaotic properties rapidly to scramble and diffuse data. Two general principles that guide the design of block ciphers are diffusion and confusion. These two principles are closely related to the mixing and ergodicity properties of chaotic maps [34, 51–54]. The chaotic systems can be classified into two broader branches namely discrete dynamical systems and continuous chaotic systems. The discrete dynamical systems use discrete iterative maps whereas continuous chaotic systems use differential equations. In literature researchers utilized one

dimensional, two dimensional and three dimensional chaotic iterative maps and their different combinations in order to add confusion and diffusion capabilities in modern block ciphers. The development of new chaotic systems for modern block ciphers is one of the unavoidable area of research [17–29, 32, 35, 36, 38–49]

In this regard, a Russian mathematician Vladimir Igorevich Arnold proposed a new two dimensional map based on continuous automorphism on the torus (CAT) in 1960's. A complete chaotic system can be constructed by utilizing Arnold cat transformation. By randomization in digital image can be achieved by utilizing the repeated applications of Arnold cat map which randomized the order of pixels. The repeated iteration of CAT map enough number of times, produced the actual image which shows the periodic nature and occurrence of fixed points [8]. The periodicity of CAT transformation attracted researchers interest. Keating et al., discussed the periodicity and approximate solution of Arnold transformation with the help of number theory and probabilistic approach at infinity [17]. Dyson and Falk solved the period problem of Arnold map and determined the upper bound of periodicity [13]. Then after several image encryption schemes were developed based on Arnold map. W. Chen et al., proposed am encryption scheme based on inference technique and Arnold transformation [12]. Zhengjun Lie et al., combined Arnold transform with discrete cosine transforms to propose a technique for color image encryption [36]. Ali Soleymani et al., devised an encryption scheme by combining Arnold transform and Henon chaotic map [44]. A. Q Alhamad proposed optical encryption technique based on double phase encoder and Arnold transform for color image confidentiality [16]. Recently, Majid Khan utilized Fourier series in order to encryption an image [22]. Different types of series were developed and utilized in diverse image encryption techniques. Among them Lucas and Fibonacci series most famous for image encryption. Minati M. et al., projected an encryption scheme based on Lucas and Fibonacci series with quite handsome security features [37].

An efficient image encryption scheme with Arnold transform and Lucas series is proposed here, which resist the statistical analyses, known and chosen plain text attacks. In this article, we have scrambled different images of data base [50] by changing the iteration process and perform encryption on scrambled images using Lucas series. The number of iterations selected by key known to sender and receiver using Diffie Hellman algorithm. Section 2 of this article is about some preliminaries which demonstrate the Diffie Hellman algorithm, Arnold transform and Lucas series. The designed algorithm and its implementation is presented in section 3. Performance and security analyses discussed in detail in section 4 and concluding remarks given in section 5.

2 Preliminaries

This section fundamentally demonstrated some basic concepts of Diffie-Hellman algorithm, Arnold transform and Lucas series which will be used in different sections of this article. We have analyzed the scrambled images with different iterations decided by Diffie-Hellman algorithm in section 2.2.

2.1 Exchange of keys

This algorithm provides securely exchanging secrets over a public channel, i.e., establish common secret over an insecure line of communication. The common key refers the number of

iterations in scrambling process and choose the starting position of Lucas series for encryption. The idea behind exchanging of secret is described by colors as follow in Fig. 1 [49].

Let both parties, Alice and Bob agree upon some prime numbers n and g, they produce common key with their own secrets as follows:

ALICE	Bob
Secret = a	Secret = b
$A = g^a \bmod n$	$B = g^b \bmod n$
Common key = $K_1 = B^a \bmod n$	Common key = $K_2 = A^b \bmod n$
$K_1 = K = K_2$	

Now, suppose both parties agree upon the prime numbers $n = 11$ and $g = 5$, they may vary their secrets each time for communication.

a. When $a = 4$ *and* $b = 5$, then their secret key $K = 1$.
b. When $a = 2$ *and* $b = 3$, then their secret key $K = 5$.
c. When $a = 4$ *and* $b = 6$, then their secret key $K = 9$.

2.2 Arnold transform

Cat-face scrambling process transform the content similar to white noise in directive to distribute the energy of an image uniformly. Scrambling increases, the bandwidth of channel which provides the enough space for data implanting, if image is considered as information source [18]. Among the scrambling techniques, cat face transforms extensively used, which is produced by Arnold in the research of ergodic theory. This process aligns the pixels' position

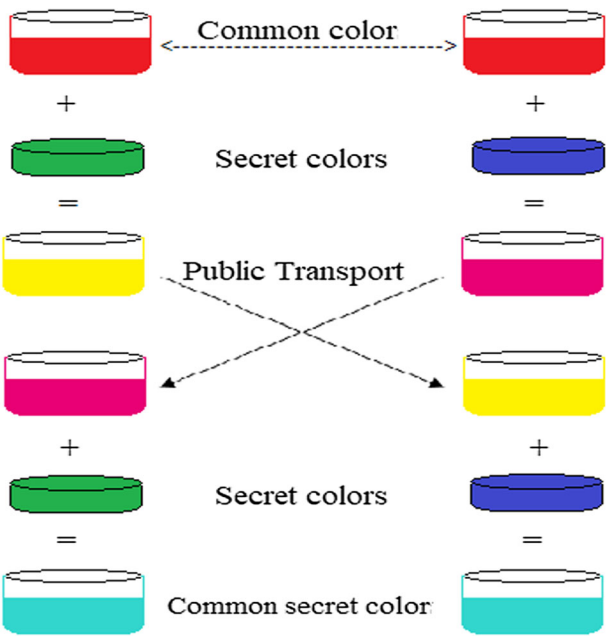


Fig. 1 Illustration of Diffie-Hellman algorithm with colors

of digital image by clipping and splicing [7]. The two dimensional cat face transform for (x, y) is expressed as;

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\mathrm{mod}\, N), \tag{1}$$

where x, and y demonstrate the pixels' position of an image, x' and y' denotes the new pixels' position after transform and N represent the size of an image. We perform scrambling analyses for *'T'* iterations, provided by Diffie-Hellman process for $T = 1, 5$ and 9, such that $T[x', y']$ follow in Fig. 2. The scrambled images of Fig. 2, operated by Lucas series given in section 3.1 to enhance the security of contents. To enhance the level of security, we can increase the number of iterations of cat face transform to process scrambling of image pixels more efficiently and uniformly. We perform encryption after 9 iteration of scrambling to analyze the results given in below sections.

2.3 Lucas sequence

In nineteenth-century, a French Mathematician E. Lucas produce the sequence in the research of recurrent sequences. This is similar to Rabbits theory problem of Fibonacci sequence [31] presented in Fig. 3 except the initial conditions. The Fibonacci sequence is defined as:

$$F_n = \begin{cases} 0, & if\ n = 0 \\ 1, & if\ n = 1 \\ F_{n-1} + F_{n-2}, & if\ n > 1 \end{cases}. \tag{2}$$

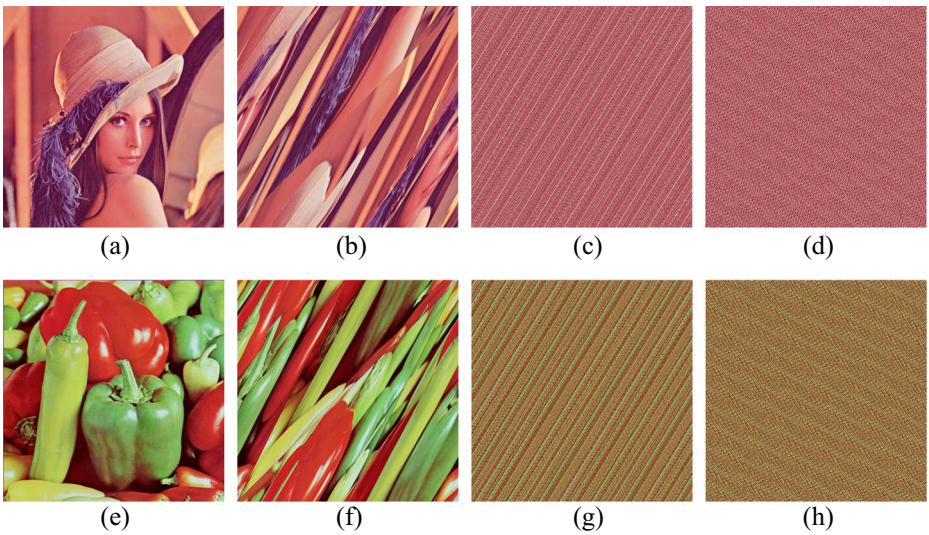
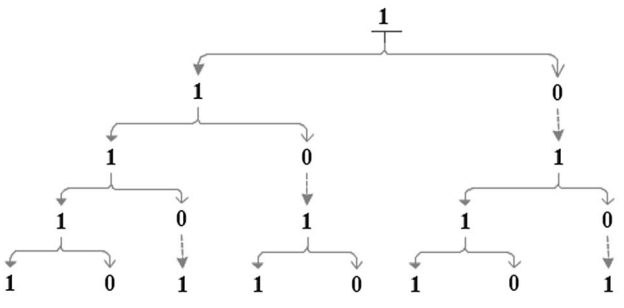


Fig. 2 Scrambling of Lena and Pepper images for different iterations *T*. **a** Lena image, **b** Scrambled Lena image for $T = 1$, **c** Scrambled Lena image for $T = 5$, **d** Scrambled Lena image for $T = 9$. **e** Pepper image, **f** Scrambled Pepper image for $T = 1$, **g** Scrambled Pepper image for $T = 5$, **h** Scrambled Pepper image for $T = 9$



No. of Ones	No. of Zeros
1	0
1	1
2	1
3	2
5	3

Fig. 3 Generation of Fibonacci sequence

while Lucas sequence is defined as:

$$L_n = \begin{cases} 1, & if\ n = 0 \\ 3, & if\ n = 1 \\ L_{n-1} + L_{n-2}, & if\ n > 1 \end{cases}. \tag{3}$$

The initial numbers of the Lucas sequence are 1 and 3, the succeeding numbers are addition of the previous two. The sequence becomes 1, 3, 4, 7, 11, 18, 29, 47, …. Lucas numbers can be generated from Fibonacci sequence as declared below:

$$L_n = F_{n+1} + F_{n-1}. \tag{4}$$

3 Proposed algorithm

We scrambled the contents of Lena and Pepper images of size 512 × 512 in section 2.2 and also explain the Lucas series for encryption in section 2.3 (Fig. 4).

The most relevant factor of this algorithm is key. As we deal in public key, both sender and receiver use Diffie-Hellman algorithm to establish key secretly over the public channel. This key decides the number of iterations for Arnold transform and indicate the starting position of Lucas series. The steps to encrypt the digital images as follows:

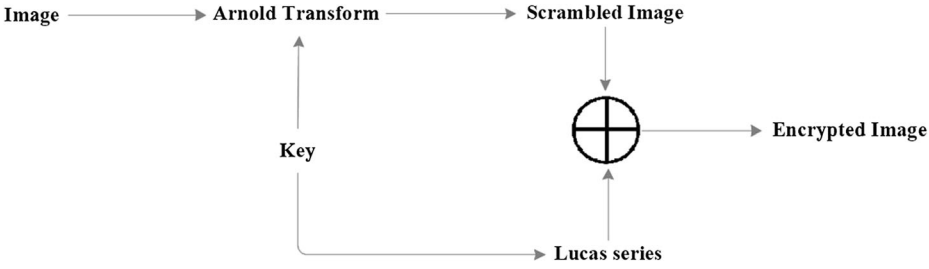


Fig. 4 Proposed encryption design

1. Key distribution between two parties using Diffie-Hellman algorithm.
2. Apply Arnold transformation with respect to key to scramble the image.
3. Select the starting point of Lucas series with key and set it with respect to image size and dimension.
4. Perform XOR operation between scrambled image and the selected Lucas series to get encrypted result.

3.1 Experimentation of anticipated structure

We assume here the iteration key $K = 9$, discussed in section 2.1 and process the images of Fig. 2 for $T = 9$ with the modulus 256 of Lucas sequence starting from 76 up to 512 × 512 position number. Layer wise operation is performed on images to evaluate the algorithm results.

4 Performance analyses for anticipated structure

Different standard performance analyses accomplished in this section on standard digital contents to sustain the performance and sanctuary of anticipated scheme. These assessments

Table 1 NIST test results for enciphered Lena image

Test		p – values of enciphered image layer wise				Comments
		Gray	Red	Green	Blue	
Frequency		0.36110	0.16410	0.46703	0.25495	Pass
Block frequency		0.24862	0.64862	0.53145	0.17988	Pass
Rank		0.39181	0.29191	0.29191	0.29191	Pass
Runs (M = 10,000)		0.51765	0.21762	0.90595	0.54043	Pass
Long runs of ones		0.64524	0.67514	0.71270	0.71270	Pass
Overlapping templates		0.74489	0.85988	0.85988	0.85988	Pass
No overlapping templates		0.99289	0.92285	0.54825	0.99989	Pass
Spectral DFT		0.78464	0.88464	0.38399	0.02952	Pass
Approximate entropy		0.36074	0.16074	0.33744	0.69469	Pass
Universal		0.99892	0.99445	0.99292	0.99659	Pass
Serial	*p values 1*	045133	0.17143	0.03998	0.65972	Pass
Serial	*p values 2*	0.77835	0.87464	0.00606	0.98104	Pass
Cumulative sums forward		0.45823	0.36470	0.34767	0.35256	Pass
Cumulative sums reverse		0.66215	0.35221	0.89099	0.77967	Pass
Random excursions	$X = -3$	0.99314	0.77296	0.00446	0.066231	Pass
	$X = -2$	0.98624	0.61069	0.054643	0.2397	Pass
	$X = -1$	0.97465	0.78256	0.4719	0.69271	Pass
	$X = 1$	0.97465	0.97787	0.53038	0.91026	Pass
	$X = 2$	0.14465	0.72112	0.52621	0.032984	Pass
	$X = 3$	0.0000082	0.59346	0.33854	0.091826	Pass
Random excursions variants	$X = -3$	0.65472	0.27249	0.20969	0.22314	Pass
	$X = -2$	0.5637	0.86763	0.66161	0.23818	Pass
	$X = -1$	0.61708	0.66501	0.44839	0.55126	Pass
	$X = 1$	0.61708	0.77283	0.82009	0.93216	Pass
	$X = 2$	1	0.67692	0.13671	0.9217	Pass
	$X = 3$	0.82306	0.69854	0.077906	0.59405	Pass

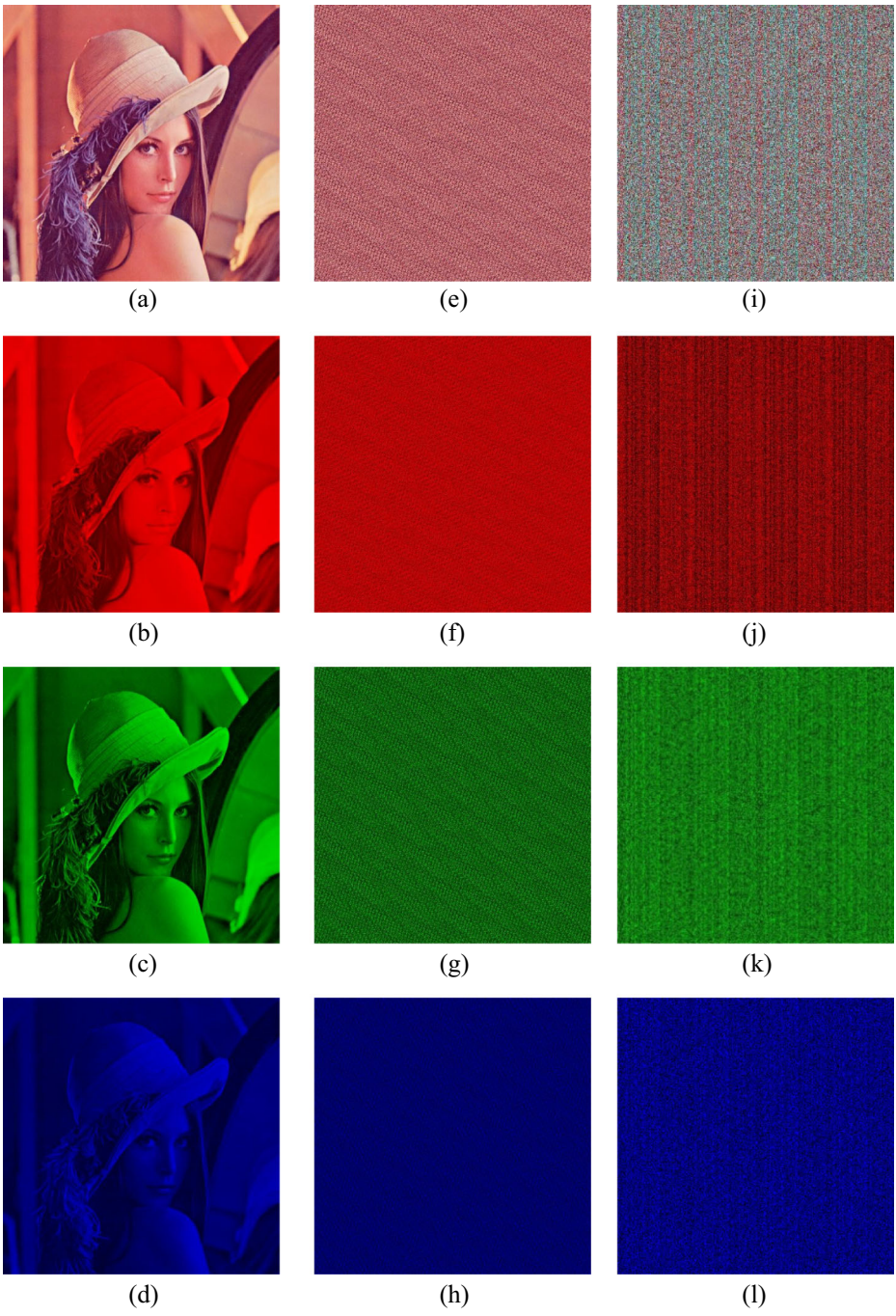


Fig. 5 Plain, scrambled and encrypted contents of Lena image. (a-d) Plain Lena image and its corresponding red, green and blue contents, (e-h) Scrambled Lena image and its corresponding red, green and blue contents, (i-l) Encrypted Lena image and its corresponding red, green and blue contents

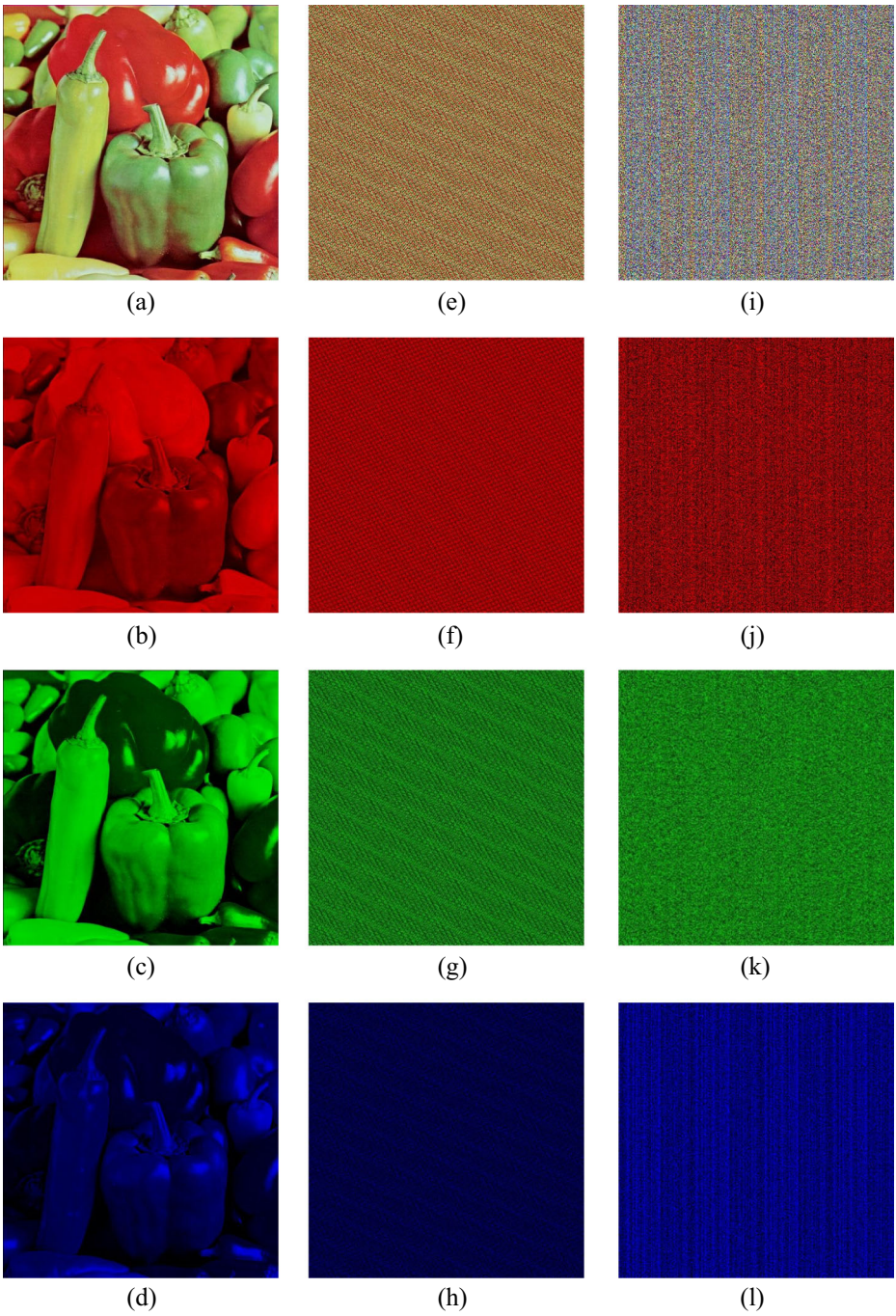


Fig. 6 Plain, scrambled and encrypted contents of Pepper image. (a-d) Plain Pepper image and its corresponding red, green and blue contents, (e-h) Scrambled Pepper image and its corresponding red, green and blue contents, (i-l) Encrypted Pepper image and its corresponding red, green and blue contents

contain the sensibility examination, factual and irregularity investigation and loophole tests for encrypted data. Different analyses discussed in subsection of 4 in detail to examine the sensitivity of proposed algorithm.

4.1 Randomness analyses

With a specific end goal to justify the prerequisites of long period, uniform scattering, high complexity and efficiency for proposed cryptosystem, we perform NIST analysis of version SP 800–2 to testify the uncertainty of digital contents. The encoded Lena image is employed to accomplish NIST tests and the aftereffects results presented in Table 1. By analyzing the outcomes, the anticipated encryption scheme effectively passes all the NIST tests. The production of random ciphers in projected scheme are irregular in the light of accomplished outcomes.

4.2 Histogram uniformity analyses

Histograms uniformity of enciphered images estimates the security of encryption framework. [22]. We have computed the histograms of 256 dark level original, scrambled and encrypted images of size 512×512, that have different contents. The histograms of plain and scrambled images contain sharp rises took after sharp decline, while

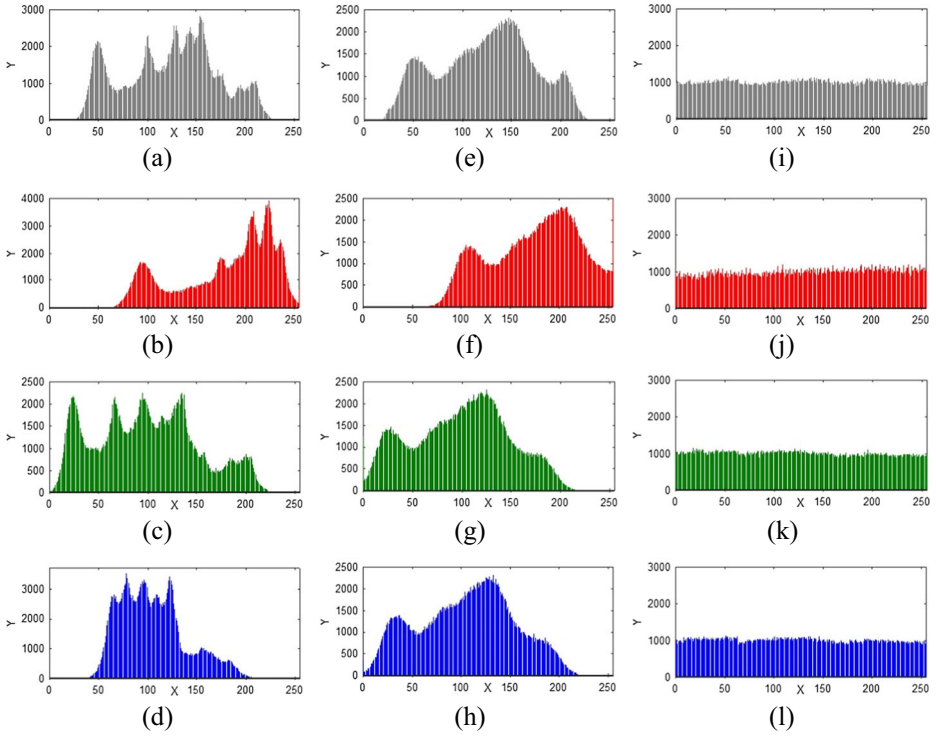


Fig. 7 Plain, scrambled and encoded layer wise histograms of Lena image. (a-d) Plain Lena image and its corresponding red, green and blue layer histograms, (e-h) Scrambled Lena image and its corresponding red, green and blue layer histograms, (i-l) Encrypted Lena image and its corresponding red, green and blue layer histograms

enciphered images contain uniformity and much differ from original and scrambled ones shown in Figs. 5 and 6, which makes statistical attacks hard [25]. Consequently, it doesn't provide any information consumed in assessable investigation attack on encrypted images (see Figs. 7 and 8).

4.3 Entropy analyses

The leading feature of randomness specified by Entropy. Specified an independent source of random trials from set of probable distinct events $\{x_1, x_2, x_3, ..., x_n\}$ with similar possibilities, the average output of source evidence called entropy (Figs. 9, 10, 11 and 12).

$$H = -\sum_{n=0}^{2^N-1} p(x_n)\log_2 p(x_n), \tag{5}$$

where x_n is the source image and 2^N referred to the aggregate of data. Shannon entropy for perfectly farraginous of 8-bit digital contents is 8. Table 2 demonstrate the entropies of different standard plain images and their scrambled, encrypted contents.

The entropy esteems of encrypted images are very close to ideal Shannon esteem, which implies the leakage of data in proposed encryption algorithm is inappropriate and the mechanism is secure upon entropy attacks [59]. The information entropies of suggested scheme for

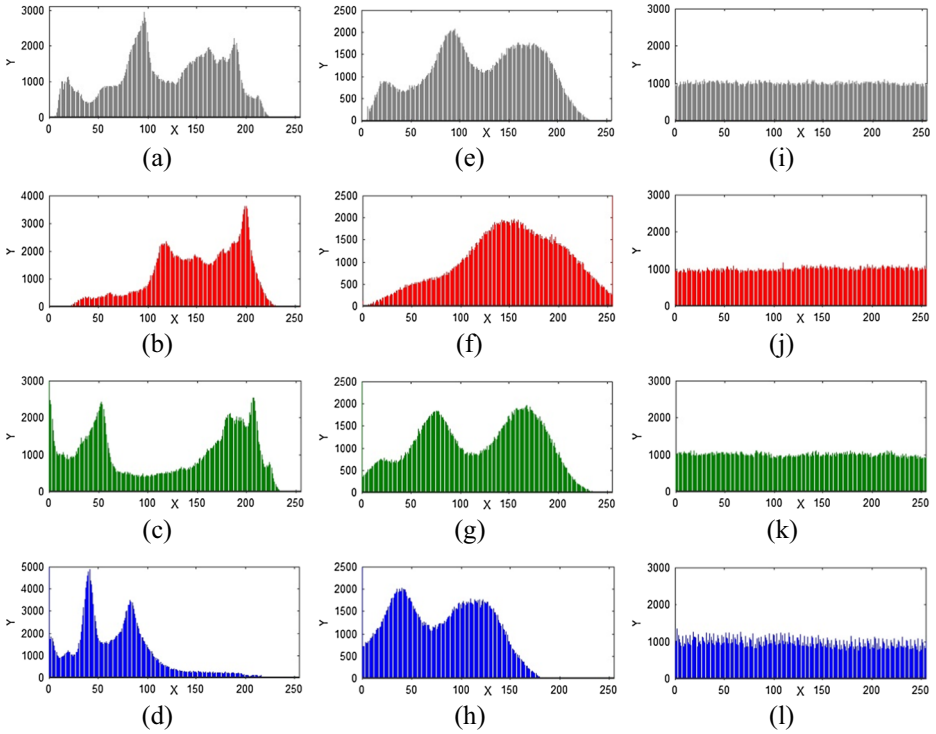


Fig. 8 Plain, scrambled and encoded layer wise histograms of Pepper image. (a-d) Plain Pepper image and its corresponding red, green and blue layer histograms, (e-h) Scrambled Pepper image and its corresponding red, green and blue layer histograms, (i-l) Encrypted Pepper image and its corresponding red, green and blue layer histograms

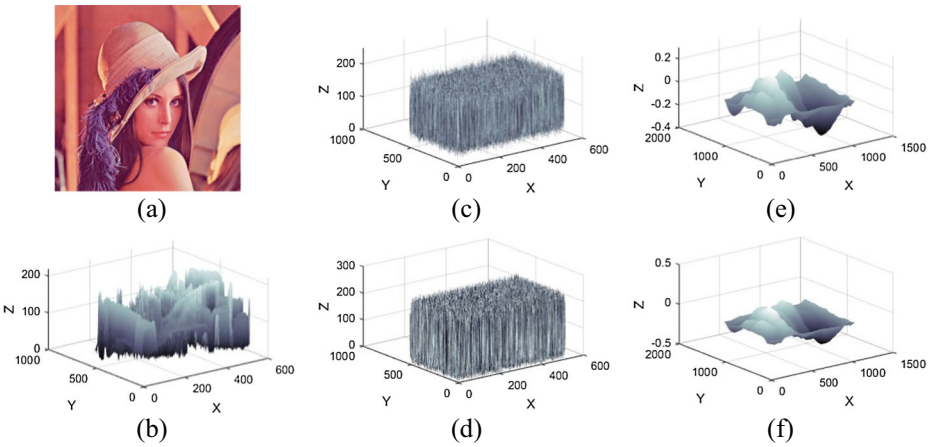


Fig. 9 Normalized cross-correlation surface plots for Lena image. (a-b) Lena image and its surface plot, (c-d) Surface plots for scrambled and encoded images, (e- f) Surface plots for cross correlation between b-c and b-d

encrypted images have superior results, when compared with existing approaches. Table 3 demonstrate the comparison of proposed technique with existing approaches foe Lena image, while Table 13 validate for the comparison of different standard images.

4.4 Pixels' correlation analyses

The adjacent pixels of an image are exceedingly associated in horizontal, vertical and diagonal directions. The encrypted data must unrestraint this affiliation to improve the barrier opposing to quantifiable analysis. To testify the association among neighboring pixels in plain, scrambled and the encrypted images, initially 10,000 sets of two adjacent pixels from digital content is selected [23].

$$r_{x,y} = \frac{\sigma_{x,y}}{\sqrt{\sigma_x^2 \sigma_y^2}}, \tag{6}$$

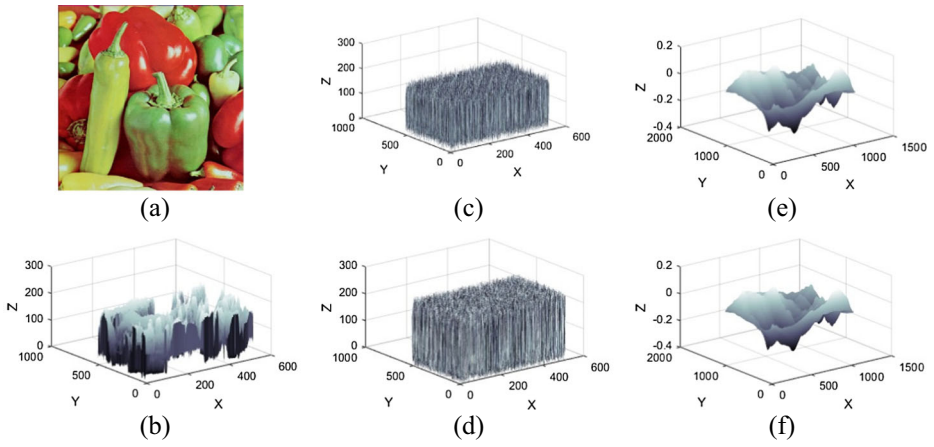


Fig. 10 Normalized cross-correlation surface plots for Pepper image. (a-b) Pepper image and its surface plot, (c-d) Surface plots for scrambled and encoded images, (e- f) Surface plots for cross-correlation between b-c and b-d

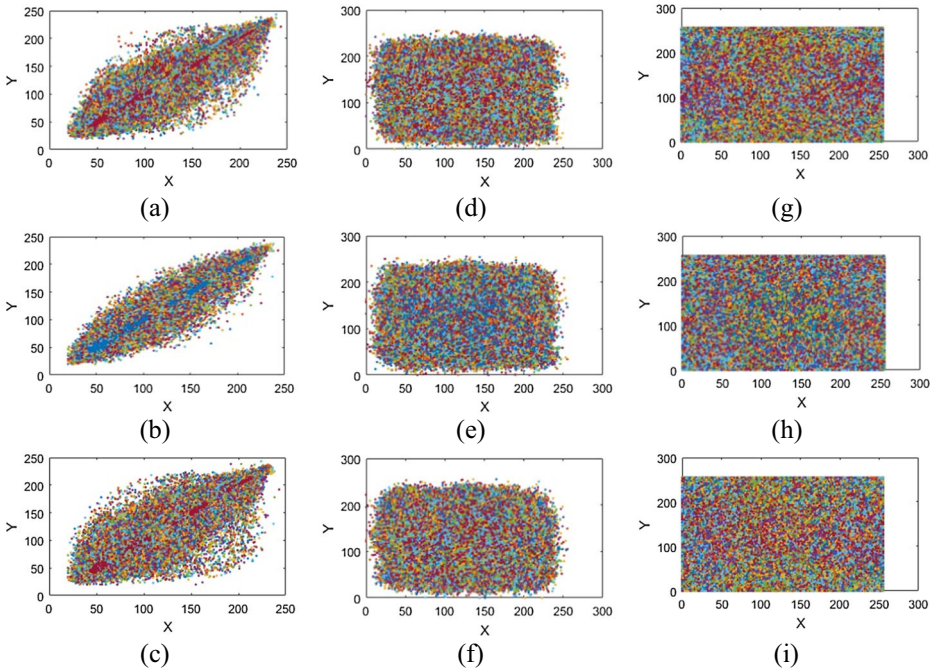


Fig. 11 Correlation among pixels' pairs for Lena image. (a-c) Horizontal, vertical and diagonal directions correlation for plain image, (d-f) Scrambled image correlation in horizontal, vertical and diagonal directions, (g-i) Encrypted image correlation in horizontal, vertical and diagonal directions

where x and y are two adjoining pixels approximation at gray scale, $\sigma_{x,y}$ is the covariance and σ_x^2, σ_y^2 are variances of random variables x and y.

The coefficients of correlation for plain, scrambled and encrypted images having dissimilar contents conveyed in Tables 4 and 5. The association among various couples of original, scrambled and encrypted images evaluated by calculating the two dimensional correlation coefficients among the original - scrambled and original – encrypted images [24, 58]. The succeeding calculation is employed to compute the correlation coefficients.

$$r = \frac{\sum_{i,j=1}^{M,N} \left(P_{ij} - \overline{P}\right)\left(C_{ij} - \overline{C}\right)}{\sqrt{\left(\sum_{i,j=1}^{M,N} \left(P_{ij} - \overline{P}\right)^2\right)\left(\sum_{i,j=1}^{M,N} \left(C_{ij} - \overline{C}\right)^2\right)}} \tag{7}$$

where P and C signifies the plain and cipher images, $\overline{P}$ and $\overline{C}$ represents the mean values of P and C, M and N demonstrates the height and width of original / cipher images. The estimated coefficients of correlation for the plain, scrambled and encrypted images in the direction of horizontal, vertical and diagonal expressed in Tables 4 and 5.

The quantifiable investigation for corresponding coefficients in dynamic symmetry conferred in Table 5 for plain, scrambled and encoded images at RGB scale.

The plain and enciphered contents are extensively dissimilar from one another and the enciphered coefficients are exceptionally near zero. The evaluation of correlation coefficients for anticipated structure with existing approaches using standard images specified in Tables 6 and 7.

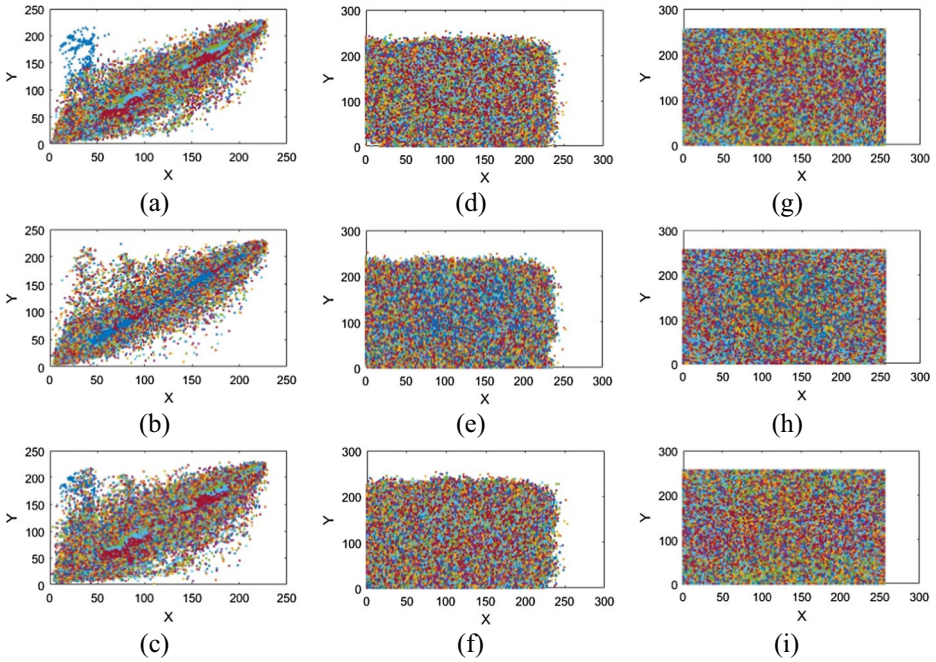


Fig. 12 Correlation among pixels' pairs for Pepper image. (a-c) Horizontal, vertical and diagonal directions correlation for plain image, (d-f) Scrambled image correlation in horizontal, vertical and diagonal directions, (g-i) Encrypted image correlation in horizontal, vertical and diagonal directions

The outcomes of our proposed structure have inferior values coefficients, which meet the necessities for competent technique in real time application for enciphering.

4.5 Pixels' resemblance analyses

The pixel's resemblance fundamentally reveals the similarity among different digital contents. There are variety of similarity measures in order to approximate the structural detail for digital contents. We have analyzed the structural similarity index metric (SSIM), normalized cross correlation (NCC) and structural content (SC) between plain ($P_{i,j}$) and cipher images ($C_{i,j}$) in order to evaluate the structure similarity among different images from their reference. SSIM used to compare the luminance, structure and contrast of plain and enciphered contents. Let us consider here two images $P_{i,j}$ and $C_{i,j}$ with mean values μ_p, μ_c and the standard deviation σ_{pc}. If there will be any resemblance between plain and ciphered contents, the quantitative analysis close to 1 and the value approaches 0 for dissimilarity in contents (Table 8).

$$SSIM = \frac{\left(2\mu_p\mu_c + C_1\right)\left(2\sigma_{pc} + C_2\right)}{\left(\mu_p^2 + \mu_c^2 + C_1\right)\left(\sigma_p^2 + \sigma_c^2 + C_2\right)}. \tag{8}$$

NCC measures the structural similarity between two images and if the quantitative analysis quite close to unity, the structure similarity between images is resilient. We perform this

Table 2 Layer wise information entropies analyses for plain, scrambled and enciphered digital contents of size 512 × 512.

Image	Plain				Scrambled				Encrypted			
	Gray	R	G	B	Gray	R	G	B	Gray	R	G	B
Lena	7.4455	7.2703	7.5881	7.0026	7.5291	7.2276	7.5881	7.0026	7.9984	7.9911	7.9980	7.9981
Pepper	7.5835	7.3587	7.6157	7.1495	7.6586	7.7153	7.6970	6.9603	7.9991	7.9983	7.9986	7.9771
Baboon	7.7666	7.7444	7.4493	7.7513	7.8476	7.8311	7.5593	7.8132	7.9988	7.9984	7.9981	7.9980
Airplane	6.6879	6.7489	6.8106	6.2682	7.4401	7.2110	7.1012	7.0049	7.9989	7.9980	7.9984	7.9978
House	7.5112	7.4493	7.2632	7.4891	7.6954	7.6164	7.4484	7.5612	7.9988	7.9984	7.9980	7.9982
Jelly beans	6.6098	5.3111	5.7424	6.5942	7.2257	7.1103	7.1231	7.1859	7.9961	7.9897	7.9925	7.9928
Sail boat	7.7675	7.3166	7.6443	7.3030	7.8918	7.5742	7.7824	7.5150	7.9987	7.9981	7.9983	7.9980
Splash	7.3232	7.0807	6.9771	6.2126	7.5216	7.2816	7.1211	7.0051	7.9953	7.9982	7.9971	7.9983
Tree	7.5634	7.2798	7.4610	6.9923	7.6214	7.3398	7.6836	7.2105	7.9980	7.9965	7.9964	7.9962

Table 3 Comparison of proposed technique with existing approaches foe Lena image of size 512 × 512

Image	Proposed	Sun's [59]	Xiang's [59]	Wong's [59]	Baptista's [59]
Lena	7.9984	7.9965	7.9950	7.9690	7.9260

experiment at the original-scrambled and the original-encrypted images to analyze the similarity between them. The expression for determining the NCC as follows:

$$NCC = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} \frac{P_{i,j} \times C_{i,j}}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} P^2{}_{i,j}}. \tag{9}$$

The structural detail of an image and quality in terms of noise level and sharpness assessed here by calculating the SC. For structure similarity between digital contents, SC value quite closed to unity, whereas away from unity specify the dissimilarity in digital contents. Higher estimation of SC indicates the low quality of picture and it tends to be determined as:

$$SC = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} \frac{P^2{}_{i,j}}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} C^2{}_{i,j}}. \tag{10}$$

4.6 Pixels' disparity analyses

The digital contents eminence based on pixels' disparity analyzed here by evaluating the mean absolute error (MAE), mean square error (MSE) and peak signal to noise ratio (PSNR).

The most widely recognized method used to quantify the precision for continuous variables is MAE. The average absolute disparity between plain-scrambled and plain-encrypted images specified by MAE and its esteem must be higher to enhance the security level. It can be calculated as follows:

$$MAE = \frac{1}{M \times N} \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} |P_{i,j} - C_{i,j}|. \tag{11}$$

Table 4 Correlation coefficients at gray scale for plain, scrambled and encoded images

Image	Plain			Scrambled			Encrypted		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9737	0.9869	0.9610	−0.0024	0.0457	−0.0465	−0.0041	−0.0110	0.0011
Pepper	0.9814	0.9833	0.9665	−0.0429	0.0623	−0.0947	−0.0068	0.0018	0.0011
Baboon	0.8534	0.7598	0.7300	−0.0033	−0.0245	0.0044	0.0013	−0.0027	−0.0017
Airplane	0.9662	0.9639	0.9368	0.0040	0.0088	−0.0786	−0.0049	−0.0022	0.0011
House	0.9501	0.9571	0.9012	0.0021	0.0465	−0.0274	−0.0038	0.0027	−0.0054
Jelly beans	0.9779	0.9818	0.9625	−0.0329	0.0048	−0.0763	0.0013	−0.0019	−0.0022
Sail boat	0.9817	0.9710	0.9121	0.0034	−0.0357	0.0025	0.0014	−0.0034	−0.0044
Splash	0.9798	0.9899	0.9696	0.0438	−0.0643	−0.0148	−0.0032	0.0011	0.0021
Tree	0.0600	0.9614	0.9368	−0.0127	0.0045	0.0035	0.0018	−0.0019	−0.0022

Table 5 Plain, scrambled and encoded layer wise correlation coefficients of standard images

Image		Plain			Scrambled			Encrypted		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	R	0.9759	0.9878	0.9637	−0.0142	0.0393	−0.0459	−0.0095	−0.0009	−0.0074
	G	0.9814	0.9833	0.9665	−0.0429	0.0623	−0.0947	−0.0055	0.0025	0.0011
	B	0.8534	0.7598	0.7300	−0.0033	−0.0245	0.0044	0.0015	−0.0021	−0.0018
Pepper	R	0.9662	0.9639	0.9368	0.0040	0.0088	−0.0786	−0.0046	−0.0019	0.0012
	G	0.9479	0.957	0.9132	0.0021	0.0465	−0.0274	−0.0028	0.0087	−0.0034
	B	0.9787	0.982	0.9646	−0.0329	0.0048	−0.0763	0.0017	−0.0023	−0.0023
Baboon	R	0.9625	0.9313	0.9166	0.0034	−0.0357	0.0025	0.0010	−0.0033	−0.0014
	G	0.9121	0.8530	0.8232	0.0438	−0.0643	−0.0148	−0.0042	0.0012	0.0016
	B	0.9696	0.9558	0.9380	−0.0127	0.0045	0.0035	0.0028	−0.0013	−0.0035
Airplane	R	0.9759	0.9729	0.9516	0.0524	0.0465	0.0559	−0.0021	0.0023	−0.0082
	G	0.9757	0.9753	0.9546	0.0258	0.0211	0.0349	0.0046	0.0053	−0.0014
	B	0.9699	0.9603	0.9396	0.2888	0.3576	0.0944	0.0084	−0.0023	0.0055
House	R	0.9713	0.9756	0.9506	0.0207	0.1325	0.0344	0.0011	0.0017	0.0028
	G	0.9581	0.9659	0.9282	0.2731	0.1163	0.0984	0.0029	0.0032	0.0013
	B	0.9817	0.9827	0.9674	0.0422	0.2943	−0.0643	0.0019	−0.0015	−0.0055
Jelly beans	R	0.9772	0.9791	0.9592	0.1671	0.2028	0.1301	−0.0016	−0.0028	−0.0041
	G	0.9815	0.9852	0.9694	0.1191	0.1518	0.0949	−0.0019	0.0058	0.0049
	B	0.9916	0.9906	0.9843	0.3663	0.4663	0.1941	0.0064	−0.0036	−0.0091
Sail boat	R	0.9791	0.9759	0.9610	0.0559	0.0454	0.0531	0.0093	−0.0017	0.0075
	G	0.9850	0.9831	0.9711	0.0244	0.0196	0.0297	0.0044	−0.0012	−0.0061
	B	0.9874	0.9880	0.9782	0.2855	0.3499	0.0858	−0.0027	0.0053	0.0037
Splash	R	0.9943	0.9978	0.9926	0.0589	0.0527	0.0560	0.0024	0.0028	0.0017
	G	0.9894	0.9937	0.9837	0.0551	0.0726	0.0535	−0.0083	−0.0061	0.0014
	B	0.9891	0.9904	0.9809	0.2859	0.3583	0.0899	0.0021	0.0036	0.0022
Tree	R	0.9770	0.9596	0.9460	0.0545	0.0420	0.0617	−0.0049	−0.0093	0.0027
	G	0.9800	0.9639	0.9522	0.0258	0.0170	0.0316	−0.0072	0.0041	−0.0018
	B	0.9830	0.9678	0.9583	0.2921	0.3654	0.0903	−0.0082	0.0032	0.0053

Table 6 Correlation coefficients comparison of proposed with recent modern approaches at gray scale

Image	Proposed encryption			Ref. [28, 45]			Ref. [48]		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	−0.0041	−0.0110	0.0011	0.0009	0.0021	−0.0007	−0.0045	−0.0070	0.0013
Pepper	−0.0068	0.0018	0.0011	0.0007	−0.0012	0.0001	−0.0055	0.0025	0.0011
Baboon	0.0013	−0.0027	−0.0017	0.0039	−0.0045	0.0039	0.0015	−0.0021	−0.0018
Airplane	−0.0049	−0.0022	0.0011	−0.0016	0.0008	0.0033	−0.0046	−0.0019	0.0012
House	−0.0038	0.0027	−0.0054	−0.0028	−0.0041	0.0045	−0.0028	0.0087	−0.0034
Jelly beans	0.0013	−0.0019	−0.0022	−0.0033	0.0018	−0.0045	0.0017	−0.0023	−0.0023
Sail boat	0.0014	−0.0034	−0.0044	−0.0040	−0.0051	0.0001	0.0010	−0.0033	−0.0014
Splash	−0.0032	0.0011	0.0021	0.0017	−0.0041	0.0015	−0.0042	0.0012	0.0016
Tree	0.0018	−0.0019	−0.0022	0.0019	−0.0021	0.0036	0.0028	−0.0013	−0.0035

Essentially, scrambled and encrypted digital contents have dissimilarity concerning the plain image. The image encryption quality can be assessed by MSE and PSNR, while MSE signifies the cumulative square error measure and PSNR indicates the peak error between original and ciphered images. To improve the encryption quality, MSE esteem must be higher and PSNR values must be low or vice versa. To calculate PSNR, first we have to calculate the MSE using following expression:

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(P_{ij}-C_{ij}\right)^2}{M \times N}, \tag{12}$$

where P_{ij} and C_{ij} refers the pixels position at i^{th} row and j^{th} column of plain and ciphered images distinctly. Superior the MSE esteem represents the enhancement of encryption strategy [30]. PSNR ratio determines the quality measurement between the original and ciphered image described by the succeeding expression.

$$\mathrm{PSNR} = 20\log_{10}\left[\frac{I_{MAX}}{\sqrt{MSE}}\right], \tag{13}$$

where I_{MAX} is the utmost pixel's estimation of image. On comparing with immense difference between the plain and ciphered images, PSNR should be low esteem. The feasibility of proposed approach assessed for MSE and PSNR for standard digital images accumulated in Table 9.

4.7 Texture and visual strength analyses

To analyze the texture and visual quality of proposed strategy, distinctive gray level co-occurrence matrix (GLCM) examinations which are homogeneity, contrast and energy performed [20]. The homogeneity of a picture is characterized as:

$$Homogeneity = \sum_{i,j}\frac{\rho(i,j)}{1+|i-j|}, \tag{14}$$

where i and j indicates the row and column position of pixel in image. This examination

Table 7 Correlation coefficients comparison of proposed with recent modern approaches at RGB scale

Image		Proposed strategy			Ref. [10]			Ref. [34]		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	R	−0.0095	−0.0009	−0.0074	−0.0283	−0.0317	−0.0344	−0.0348	0.0282	0.0212
	G	−0.0055	0.0025	0.0011	−0.0026	−0.0173	−0.0015	0.0207	0.0035	−0.0464
	B	0.0015	−0.0021	−0.0018	−0. 0217	−0.0036	0.0191	−0.0357	−0.0137	−0.0422
Pepper	R	−0.0046	−0.0019	0.0012	−0.0202	−0.0113	−0.0041	–	–	–
	G	−0.0028	0.0087	−0.0034	−0.0060	−0.0116	−0.0117	–	–	–
	B	0.0017	−0.0023	−0.0023	−0.0001	−0.0212	−0.0037	–	–	–
Baboon	R	0.0010	−0.0033	−0.0014	−0.0072	−0.0201	−0.0016	0.0305	−0.0088	−0.0128
	G	−0.0042	0.0012	0.0016	−0.0260	−0.0220	−0.0175	0.0296	−0.0206	−0.0279
	B	0.0028	−0.0013	−0.0035	−0.0099	−0.0034	−0.0066	0.0101	0.0215	0.0146

Table 8 Pixels resemblance between plain-scrambled and plain-encrypted standard images

Standard image	Plain-scrambled Pixels resemblance			Plain-encrypted Pixels resemblance		
	SSIM	SC	NCC	SSIM	SC	NCC
Lena	0.023086	0.1821	0.1295	0.011087	0.0049	0.1070
Pepper	0.016996	0.1958	0.1640	0.010084	0.0084	0.1201
Baboon	0.014385	0.1647	0.1319	0.001605	0.0206	0.1109
Airplane	0.012219	0.2874	0.1181	0.003088	0.0089	0.1005
House	0.035466	0.1799	0.1236	0.012137	0.1013	0.1202
Jelly beans	0.021198	0.1809	0.1540	0.015412	0.0079	0.1104
Sail boat	0.023646	0.1943	0.1447	0.010456	0.0088	0.1188
Splash	0.041214	0.1619	0.1516	0.015483	0.1030	0.1203
Tree	0.025632	0.1872	0.1489	0.009906	0.0097	0.1032

executes the familiarity of dissemination in GLCM to GLCM diagonally and its range is characterized somewhere in between of 0 and 1.

Contrast analysis allow the observer to spot the object within the texture of image and it's outlined as:

$$Contrast = \sum_{i,j} |i-j|^2 \rho(i,j). \tag{15}$$

The range of contrast is characterized somewhere in between 0 and (size (image))^2. Greater the value of contrast represents the large number of variations in the pixels of an image, while consistent image has 0 contrast.

The energy analysis of an image returns the aggregate of squared components in GLCM and characterized as:

$$Energy = \sum_{i,j} \rho(i,j)^2 \tag{16}$$

The energy is characterized somewhere in the range of 0 and 1, while the consistent picture has 1 energy. GLCM analyses for scrambled and enciphered images are given in Table 10.

Table 9 Pixels disparity analyses between plain-scrambled and plain-encrypted standard images and their comparison with existing methodologies

Image	Plain-scrambled Pixels disparity			Plain-encrypted Pixels disparity			Ref. [40]	Ref. [39]	
	MAE	MSE	PSNR	MAE	MSE	PSNR	MAE	MSE	PSNR
Lena	76.66	4666.515	11.4409	79.84	7715.767	9.2570	78.24	–	–
Pepper	71.25	5839.190	10.4672	81.45	8392.826	8.8917	75.64	8261	8.9603
Baboon	77.11	5201.746	11.9934	83.56	8219.664	8.4865	71.38	7385	9.4474
Airplane	66.38	5984.739	10.2165	79.95	8553.773	8.8954	–	–	–
House	66.72	4215.083	12.0112	69.22	7924.865	9.0195	–	7699	9.2667
Jelly beans	65.38	4438.932	11.1294	64.89	7566.127	9.3354	–	–	–
Sail boat	68.28	5656.784	10.8739	78.32	8142.869	8.5162	–	7701	9.2653
Splash	65.23	3998.143	12.8904	62.11	7106.738	9.9852	–	–	–
Tree	71.34	4578.774	11.2685	77.98	8436.104	8.4345	–	–	–

Table 10 GLCM analyses for plain-scrambled and plain-encrypted images and their comparison with existing approaches

Image	GLCM analyses of scrambled image			GLCM analyses of encrypted image			Ref. [27]	Ref. [1]	Ref. [27]
	Homogeneity	Contrast	Energy	Homogeneity	Contrast	Energy	Homogeneity	Contrast	Energy
Lena	0.9792	5.0350	0.0328	0.9791	10.5463	0.0157	–	10.5432	–
Pepper	0.9792	6.4912	0.0265	0.9791	10.5103	0.0156	0.464131	–	0.0282
Baboon	0.9793	6.0102	0.0211	0.9790	10.5001	0.0155	–	10.4511	–
Airplane	0.9794	7.0753	0.0287	0.9793	10.6231	0.0156	–	10.4784	–
House	0.9792	5.8623	0.0401	0.9791	10.4421	0.0158	–	–	–
Jelly beans	0.9794	6.4412	0.0375	0.9792	10.5101	0.0157	–	–	–
Sail boat	0.9796	5.5414	0.0356	0.9794	10.5136	0.0157	–	10.4423	–
Splash	0.9795	6.0127	0.0425	0.9795	10.5006	0.0159	–	–	–
Tree	0.9793	6.0104	0.0297	0.9791	10.5001	0.0156	–	–	–

Table 11 Differential attack analyses between original and scrambled standard images

Image	NPCR				UACI			
	Gray	R	G	B	Gray	R	G	B
Lena	99.42	99.99	99.47	99.81	31.71	38.79	32.63	26.61
Pepper	99.53	99.81	99.62	99.40	28.21	38.48	27.81	25.68
Baboon	99.61	99.19	99.17	99.29	30.41	31.73	29.42	33.17
Airplane	99.64	99.79	99.27	99.14	30.31	32.44	26.45	28.88
House	99.44	99.59	99.47	99.71	32.74	28.16	29.68	34.11
Jelly beans	99.58	99.42	99.26	99.55	32.23	34.66	31.61	29.68
Sail boat	99.32	99.17	99.65	99.59	31.88	31.79	30.34	30.61
Splash	99.61	99.42	99.29	99.38	28.21	33.88	27.76	29.68
Tree	99.34	99.42	99.44	99.63	29.74	24.18	31.78	32.21

4.8 Differential attacks analyses

To testify the robustness against differential attacks for anticipated scheme, an adjustment of one pixel in plain image modifies the encrypted image for comparing, with a probability of half pixel altering. For a change in i^{th} chunk of permuted digital image affects the i^{th} chunk of ciphered image directly. We ensure that our structure has appropriate influence capacity to plain images to affirm the impact of modifying a solitary pixel in a plain image and the entire enciphered image. For a specific objective to measure the impact of minor alteration in plain image on its enciphered one, the number of pixels changing rate (NPCR) bound together to originate the unified average change intensity (UACI) [30]. The NPCR and UACI tests for two encoded images $C_1(i,j)$ and $C_2(i,j)$ in which one image just varied by one pixel can be evaluated by using the succeeding expressions.

$$\mathrm{NPCR} = \sum_{i,j} \frac{D(i,j)}{W \times H} \times 100\%, \tag{17}$$

Table 12 NPCR analyses between plain and encrypted standard images and their comparison with existing techniques

Image	NPCR				Ref. [45]			Ref. [10]		
	Gray	R	G	B	R	G	B	R	G	B
Lena	99.89	99.76	99.71	99.88	–	–	–	99.63	99.62	99.62
Pepper	99.88	99.82	99.81	99.81	99.60	99.63	99.58	99.62	99.61	99.62
Baboon	99.87	99.88	99.86	99.78	99.63	99.59	99.62	99.61	99.62	99.62
Airplane	99.92	99.82	99.84	99.87	99.61	99.61	99.60	–	–	–
House	99.85	99.67	99.88	99.86	99.63	99.59	99.60	–	–	–
Jelly beans	99.87	99.62	99.81	99.79	99.60	99.58	99.61	–	–	–
Sail boat	99.90	99.81	99.88	99.83	99.61	99.61	99.59	–	–	–
Splash	99.79	99.71	99.77	99.82	99.61	99.59	99.59	–	–	–
Tree	99.88	99.81	99.76	99.83	99.58	99.54	99.56	–	–	–

Table 13 UACI analyses between plain and encrypted standard images and their comparison with existing techniques

Image	UACI				Ref. [45]			Ref. [10]		
	Gray	R	G	B	R	G	B	R	G	B
Lena	33.66	33.91	33.44	33.68	–	–	–	33.67	33.79	33.62
Pepper	33.62	34.12	33.44	34.42	33.42	33.49	33.41	33.66	33.65	33.73
Baboon	33.52	34.11	34.16	33.81	33.48	33.54	33.53	33.64	33.59	33.67
Airplane	33.75	34.13	34.64	34.22	33.47	33.40	33.37	–	–	–
House	33.34	32.87	33.41	32.91	33.52	33.53	33.48	–	–	–
Jelly beans	33.19	33.14	32.85	32.98	33.52	33.61	33.46	–	–	–
Sail boat	33.52	32.96	33.91	33.15	33.49	33.56	33.43	–	–	–
Splash	33.47	34.42	32.14	33.24	33.49	33.54	33.46	–	–	–
Tree	33.29	33.43	32.55	33.21	33.48	33.36	33.32	–	–	–

where $D(i,j) = \begin{cases} 0, & C_1(i,j)=C_2(i,j) \\ 1, & C_1(i,j)\neq C_2(i,j) \end{cases}$

$$UACI = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} \frac{\left| C_1(i,j) - C_2(i,j) \right/ 255 |}{W \times H \times 100\%.} \tag{18}$$

To evaluate the sensitivity of plain image, encrypt the plain image and randomly choose and altered one pixel in plain image. Better the encryption analysis by higher the UACI esteem depicted in Tables 11, 12 and 13, which provides the experimental outcomes for scrambled and encrypted results and comparison with latest techniques.

The evaluation of the entropy and differential analyses for our projected technique with contemporary approaches using standard images presented in Table 14. The outcomes of our proposed structure have superior results for entropy and differential analyses, which are suitable in real time applications for image enciphering.

Table 12 validates the NPCR esteems for anticipated scheme which is closed to the perfect estimation of 1 and UACI esteems also have better results than existing approaches depicted in Table 13. These outcomes show that projected scheme has great degree sensitive to minor change in plain image, irrespective of whether the two ciphered images have 1-bit alteration

Table 14 Comparison of information entropies and differential analyses for proposed scheme with existing techniques

Image	Entropies		Differential analysis		Ref. [46]	Ref. [11]		Ref. [28]		
	Plain	Encrypted	NPCR	UACI	Encrypted	NPCR	UACI	Encrypted	NPCR	UACI
Lena	7.4455	7.9984	99.89	33.66	7.9931	99.22	33.12	7.9979	99.66	33.50
Pepper	7.5835	7.9991	99.88	33.62	7.9962	99.15	33.14	7.9974	99.66	33.50
Baboon	7.7666	7.9988	99.87	33.52	7.9958	99.12	33.11	7.9974	99.65	33.55
Airplane	6.6879	7.9989	99.92	33.75	–	99.18	33.11	7.9972	99.64	–
House	7.5112	7.9988	99.85	33.34	7.9954	98.87	32.16	7.9973	–	–
Jelly beans	6.6098	7.9961	99.87	33.19	–	–	–	–	–	–
Sail boat	7.7675	7.9987	99.90	33.52	–	–	–	–	–	–
Splash	7.3232	7.9953	99.79	33.47	–	–	–	–	–	–
Tree	7.5634	7.9980	99.88	33.29	–	–	–	–	–	–

Table 15 execution time of proposed scheme in seconds and comparison with existing techniques

Image	Anticipated scheme	Ref. [1]	Ref. [2]
Lena	1.61	2.76	3.68
Pepper	1.59	–	–
Baboon	1.58	2.25	3.23
Airplane	1.63	2.55	3.53
House	1.54	–	–
Jelly beans	1.55	–	–
Sail boat	1.48	2.66	3.55
Splash	1.44	–	–
Tree	1.57	–	–

[30]. The anticipated structure has superior ability to hostile the differential attacks in investigation with alternative approaches (see Table 14).

4.9 Time complexity analyses

Most of the time algorithms consider and analyzed by time and space complexity. The amount of time in seconds taken by proposed algorithm to run as a function of length of input referred as time complexity, while memory taken by algorithm referred to space complexity. There are lot of things regarding time and space complexity like hardware, operating system etc. Here we are interested in execution time of proposed scheme only, so we didn't consider any factor while analyzing the algorithm. Time sensitivity analysis of proposed strategy for standard images and comparison with existing approaches accumulated in Table 15.

The anticipated plan in this article utilizes minimum assets and least computational complexity and cost, which validate the effectiveness of proposed plan than already existing methodologies.

5 Conclusion

The proposed algorithm refers public key cryptography. The key is an important factor which is decided by Diffie-Hellman algorithm. Key decides the number of iterations performed on images to for scrambling and also decide the starting position of either Lucas or Fibonacci sequence. These ranges produce unique results to secure the data. The algorithm has low computational complexity and resist brute-force attacks. We can enhance the security level by just increase number of iterations in scrambling process before encryption. The proposed structure is suitable for real time applications because of small processing time and superior performance and capacity to hostile attacks than other encryption schemes. The future direction we would like to proposed here to use quantum iterative maps instead of Lucas series on scrambled data to enhance security level much high.

Acknowledgements Both authors Hafiz Muhammad Waseem and Dr. Syeda Iram Batool are greatly thankful to Vice Chancellor Dr. Syed Wilayat Husain, Dean Iqbal Rasool Memon and Director Cyber & information security Dr. Muhammad Amin, Institute of Space Technology, Islamabad Pakistan, for providing decent atmosphere for research and development.

Compliance with ethical standards

Conflict of interest We have no conflict of interest to declare concerning the publication of this article.

References

1. Ahmad J, Hwang SO (2016) A secure image encryption scheme based on chaotic maps and affine transformation. Multimed Tools Appl 75(21):13951–13976
2. Ahmed F, Anees A, Abbas VU, Siyal MY (2014) A noisy channel tolerant image encryption scheme. Wirel Pers Commun 77(4):2771–2791
3. Aljawarneh S, Aldwairi M, Yassein MB (2018) Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. J Comput Sci 25:152–160
4. Aljawarneh S, Radhakrishna V, Kumar PV, Janaki V (2016) A similarity measure for temporal pattern discovery in time series data generated by IoT. In: 2016 International conference on engineering & MIS (ICEMIS) (pp. 1–4). IEEE
5. Aljawarneh SA, Vangipuram R (2018) GARUDA: Gaussian dissimilarity measure for feature representation and anomaly detection in Internet of things. J Supercomput:1–38
6. Aljawarneh SA, Vangipuram R, Puligadda VK, Vinjamuri J (2017) G-SPAMINE: An approach to discover temporal association patterns and trends in internet of things. Futur Gener Comput Syst 74:430–443
7. Arnold VI (1968) The stability problem and ergodic properties for classical dynamical systems. In: Vladimir I. Arnold-Collected Works (pp. 107–113). Springer, Berlin, Heidelberg
8. Arnold VI, Avez A (1968) "Ergodic Problems of Classical Mechanics," Benjamin, 1968. J Franks "Anosov diffeomorphisms" in global Analysis, proc Sympos, Pure math, American Mathematical Society 14:61–93
9. Belazi A, El-Latif AAA, Diaconu AV, Rhouma R, Belghith S (2017) Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Opt Lasers Eng 88:37–50
10. Belazi A, Khan M, El-Latif AAA, Belghith S (2017) Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption. Nonlinear Dynamics 87(1):337–361
11. Boriga RE, Dăscălescu AC, Diaconu AV (2014) A new fast image encryption scheme based on 2D chaotic maps. IAENG Int J Comput Sci 41(4):249–258
12. Chen W, Quan C, Tay CJ (2009) Optical color image encryption based on Arnold transform and interference method. Opt Commun 282:3680–3685
13. Dyson FJ, Falk H (1992) Period of a discrete cat mapping. Am Math Mon 99:603–614
14. El-Latif AAA, Abd-El-Atty B, Talha M (2018) Robust encryption of quantum medical images. IEEE Access 6:1073–1081
15. El-Latif AAA, Li L, Niu X (2014) A new image encryption scheme based on cyclic elliptic curve and chaotic system. Multimed Tools Appl 70(3):1559–1584
16. Elshamy AM, El-Samie FEA, Faragallah OS, Elshamy EM, El-sayed HS, El-zoghdy SF, Rashed ANZ, Mohamed AE-NA, Alhamad AQ (2016) Optical image cryptosystem using double random phase encoding and Arnold's Cat map. Opt Quant Electron, Springer 48:212
17. Fang L, YuKai W (2010) Restoring of the watermarking image in Arnold scrambling. In: Signal Processing Systems (ICSPS), 2010 2nd International Conference on (Vol. 1, pp. V1–771). IEEE
18. Guo Q, Liu Z, Liu S (2010) Color image encryption by using Arnold and discrete fractional random transforms in IHS space. Opt Lasers Eng 48(12):1174–1181
19. Huang HF (2010) An Image Scrambling Encryption Algorithm Combined Arnold and Chaotic Transform. In Int. Conf. China Communication (pp. 208–210)
20. Hussain I, Anees A, Aslam M, Ahmed R, Siddiqui N (2018) A noise resistant symmetric key cryptosystem based on S_8 S-boxes and chaotic maps. The European Physical Journal Plus 133:1–23
21. Keating JP (1991) Asymptotic properties of the periodic orbits of the cat. Nonlinearity 4:277–307
22. Khan M (2015) An image encryption by using Fourier series. J Vib Control 21:3450–3455
23. Khan M (2015) A novel image encryption scheme based on multiple chaotic S-boxes. Nonlinear Dynamics 82(1–2):527–533
24. Khan M, Asghar Z (2018) A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S 8 permutation. Neural Comput & Applic 29(4):993–999
25. Khan M, Munir N (2019) A novel image encryption technique based on generalized advanced encryption standard based on field of any characteristic. Wirel Pers Commun. https://doi.org/10.1007/s11277-019-06594-6
26. Khan M, Shah T (2014) A construction of novel chaos base nonlinear component of block cipher. Nonlinear Dynamics 76(1):377–382
27. Khan M, Shah T (2014) A novel image encryption technique based on Hénon chaotic map and S 8 symmetric group. Neural Comput & Applic 25(7–8):1717–1722
28. Khan M, Shah T (2015) An efficient chaotic image encryption scheme. Neural Comput & Applic 26:1137–1148
29. Khan M, Shah T, Batool SI (2016) A new implementation of chaotic S-boxes in CAPTCHA. SIViP 10(2): 293–300

30. Khan M, Waseem HM (2018) A novel image encryption scheme based on quantum dynamical spinning and rotations. PLoS One 13(11):e0206460
31. Khan M, Waseem HM (2019) A novel digital contents privacy scheme based on Kramer's arbitrary spin. Int J Theor Phys. https://doi.org/10.1007/s10773-019-04162-z
32. Khawaja MA, Khan M (2019) A new construction of confusion component of block ciphers. Multimed Tools Appl. https://doi.org/10.1007/s11042-019-07866-w
33. Khawaja MA, Khan M (2019) Application based construction and optimization of substitution boxes over 2D mixed chaotic maps. Int J Theor Phys. https://doi.org/10.1007/s10773-019-04188-3
34. Li L, Abd-El-Atty B, El-Latif AAA, Ghoneim A (2017) Quantum color image encryption based on multiple discrete chaotic systems. In 2017 Federated Conference on Computer Science and Information Systems (FedCSIS) (pp. 555–559). IEEE
35. Liu Z, Chen H, Liu T, Li P, Xu L, Dai J, Liu S (2011) Image encryption by using gyrator transform and Arnold transform. Journal of Electronic Imaging 20(1):013020
36. Liu Z, Xu L, Liu T, Chen H, Li P, Lin C, Liu S (2011) Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. Opt Commun 284:123–128
37. Minati M, Priyadarsini M, Adhikary MC, Sunit K (September 2012) Image encryption using fibonacci-lucas transformation. International Journal on Cryptography and Information Security (IJCIS) 2(3)
38. Munir, N. and Khan, M., 2018, September. A Generalization of Algebraic Expression for Nonlinear Component of Symmetric Key Algorithms of Any Characteristic p. In 2018 International Conference on Applied and Engineering Mathematics (ICAEM) (pp. 48–52). IEEE.
39. Norouzi B, Mirzakuchaki S, Seyedzadeh SM, Mosavi MR (2014) A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. Multimed Tools Appl 71(3):1469–1497
40. Norouzi B, Seyedzadeh SM, Mirzakuchaki S, Mosavi MR (2015) A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos. Multimed Tools Appl 74(3):781–811
41. Premaratne P, Premaratne M (2012) Key-based scrambling for secure image communication. In International Conference on Intelligent Computing (pp. 259–263). Springer, Berlin, Heidelberg
42. Radhakrishna V, Aljawarneh SA, Kumar PV, Choo KKR (2018) A novel fuzzy gaussian-based dissimilarity measure for discovering similarity temporal association patterns. Soft Comput 22(6):1903–1919
43. Radhakrishna V, Kumar GR, Aljawarneh S (2017) Optimising business intelligence results through strategic application of software process model. International Journal of Intelligent Enterprise 4(1–2):128–142
44. Soleymani A, Nordin J, Sundararajan E (2004) A chaotic cryptosystem for images based on Henon and Arnold cat map. Hindawi Scientic World, pp. 1–21
45. Stoyanov B, Kordov K (2015) Image encryption using Chebyshev map and rotation equation. Entropy 17(4):2117–2139
46. Wang XY, Zhang YQ, Bao XM (2015) A colour image encryption scheme using permutation-substitution based on chaos. Entropy 17(6):3877–3897
47. Waseem HM, Khan M (2018) Information Confidentiality Using Quantum Spinning, Rotation and Finite State Machine. Int J Theor Phys 57(11):3584–3594
48. Waseem HM, Khan M (2019) A new approach to digital content privacy using quantum spin and finite-state machine. Appl Phys B Lasers Opt 125(2):27
49. Waseem HM, Khan M, Shah T (2018) Image privacy scheme using quantum spinning and rotation. Journal of Electronic Imaging 27(6):063022
50. Weber AG (1997) The USC-SIPI image database version 5. USC-SIPI Report 315:1–24
51. Wei Z, Moroz I, Sprott JC, Wang Z, Zhang W (2017) Detecting hidden chaotic regions and complex dynamics in the self-exciting homopolar disc dynamo. International Journal of Bifurcation and Chaos 27(02):1730008
52. Wei Z, Pham VT, Kapitaniak T, Wang Z (2016) Bifurcation analysis and circuit realization for multiple-delayed Wang–Chen system with hidden chaotic attractors. Nonlinear Dynamics 85(3):1635–1650
53. Wei Z, Yu P, Zhang W, Yao M (2015) Study of hidden attractors, multiple limit cycles from Hopf bifurcation and boundedness of motion in the generalized hyperchaotic Rabinovich system. Nonlinear Dynamics 82(1–2):131–141
54. Wei Z, Zhu B, Yang J, Perc M, Slavinec M (2019) Bifurcation analysis of two disc dynamos with viscous friction and multiple time delays. Appl Math Comput 347:265–281
55. Yan X, Wang S, El-Latif AAA, Niu X (2015) New approaches for efficient information hiding-based secret image sharing schemes. SIViP 9(3):499–510
56. Yassein MB, Aljawarneh S, Al-huthaifi RK (2017) Enhancements of LEACH protocol: Security and open issues. In 2017 International Conference on Engineering and Technology (ICET) (pp. 1–8). IEEE.
57. Yassein MB, Aljawarneh S, Qawasmeh E, Mardini W, Khamayseh Y (2017) Comprehensive study of symmetric key and asymmetric key encryption algorithms. In: 2017 international conference on engineering and technology (ICET) (pp. 1–7). IEEE

58. Younas I, Khan M (2018) A New Efficient Digital Image Encryption Based on Inverse Left Almost Semi Group and Lorenz Chaotic System. Entropy 20(12):913
59. Zhang G, Liu Q (2011) A novel image encryption method based on total shuffling scheme. Opt Commun 284:2775–2780
60. Zhou Y, Agaian S, Joyner VM, Panetta K (2008) Two Fibonacci p-code based image scrambling algorithms. In: Image Processing: Algorithms and Systems VI (Vol. 6812, p. 681215). International Society for Optics and Photonics
61. Zhou NR, Hua TX, Gong LH, Pei DJ, Liao QH (2015) Quantum image encryption based on generalized Arnold transform and double random-phase encoding. Quantum Inf Process 14(4):1193–1213

Syeda Iram Batool is a prominent researcher in information hiding and cryptography. She has done her PhD from Quaid-i-Azam University Islamabad, Pakistan in Dec. 2017. Recently, she is working as assistant professor in Department of Avionics at institute of space technology, Islamabad, Pakistan. Her active areas of research are digital watermarking, steganography, cryptography and cryptovirology.

Hafiz Muhammad Waseem is MS student at Electrical Engineering Department at Institute of Space Technology, Islamabad, Pakistan. He is working in cryptography.