Performance comparison between Chaos and quantum-chaos based image encryption techniques

Manju Kumari¹ · Shailender Gupta¹

Received: 29 August 2020 / Revised: 15 January 2021 / Accepted: 24 June 2021 /

Published online: 14 August 2021

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract

Today's digital era has undertaken most of the responsibilities of public and private sectors, not only the industries or big organizations dependent on the internet but individual's household needs also lying on it. To make the data transmission/reception confidential and secure for both internet users and internet service providers, a large number of researches have been done in this field. It has proved that cryptography is the best solution for solving this purpose. Mostly, digital images are continuously transferring on the network rather than texts. Enciphering a digital image is a much bulkier and a complex task. It has been evident from many types of research that chaotic logistic map-based equations provide a great level of randomness. Hence Chaotic logistic maps-based image encryption techniques (also called chaos techniques) were implemented to obtain highly random cipher images. On the other hand, time consumption must be as low as it can be possible to sustain real-time communication. Presently, the advanced encryption schemes based on quantum technology have enhanced efficiency and security because of having a large key-space and less time complexity along with randomness. The quantum-chaos based encryption is done by utilizing uncertainty principles of quantum mechanics on logistic maps. This paper is an effort to compare chaos and quantum chaos-based image encryption schemes. MATLAB 2016a software is used for the execution and the comparison is made based on various security attack analyses. Based on the study and experimental results, the quantum chaos techniques used for bit plane scrambling provides better results in terms of effectiveness, efficiency, and *trustworthy* that can be adopted for highly secured image encryption.

Keywords Cryptography · Security attacks · Chaos techniques · Encryption · Quantum-chaos techniques

✉ Manju Kumari
manjunimesh88@gmail.com

1 Introduction

In the recent past, the augmented usage of the internet has risen the cases of hacking, intrusion, cyberstalking, and many more unauthorized accesses. We can depict this from the report published last year by CISCO cybercrime survey, it is mentioned that the number of attacks has grown by Malware (20%), Data breach (19%), Spyware (14%), Phishing (13%), Ransomware (13%), Malicious spam (13%) [1].

The intruder's consistent involvement on the internet urges the need to enhance the security level [2]. During this pandemic situation of COVID-19, as most of the activities of private and government sector has shifted from their organization's secured intranet to the globally connected internet, hence the solutions from the threat of being hacked are in demand now.

Therefore, researchers are continuously working on the development of novel security techniques [3, 4]. It is evident in previous researches that adopting cryptography is the best solution for cyber-security [5]. Cryptography is the technique of transforming original data into an unreadable form before transmission and recovering the original data from its ciphers at the receiver [6]. To secure data communication numerous techniques have been developed. Initially, the internet was used only for the transmission of text files in the form of emails. The bits representation of text data is very random and limited. But from few decades due to the increase in various multimedia applications, mostly data are transferring in the form of digital images that are bulky and linear. It means most of the information represented in an image are symmetrically correlated with its neighbor pixel.

The traditional cryptography techniques like DES [8], TDES [9], AES [10], BLOWFISH [11], RC4 [12], RC5, etc. are highly efficient, secure, and fast for text files only. If we use these encryption techniques on image files, the schemes consume a large time and generate a less random cipher image. That's why chaos-based encryption techniques have been proposed by the researchers to get better results in image encryption in terms of randomness and time complexity. The chaotic-maps used in chaos-based image encryption schemes possess non-linear characteristics that result in a highly randomized image. The schemes consume less time only for small size data, for big size image the execution time is not sufficient for real-time communication. All the chaos-based techniques cover two major operations, one is for pixel position scrambling called the confusion process and another one is the diffusion process used to modify pixel values. The techniques always use the basic logistic map to generate chaotic keys and also to modify pixel positions or values of the original image.

The equation of the logistic map is represented in sr. no. 1 of Table 2. when $n = 0$, the initial value of x_0 must be assigned in between 0 to 1. μ is a sequence control parameter whose value must be lies in between 0 to 4, to generate highly random sequence x_n . But the map also has some weaknesses like the formation of a blank window when $\mu = 3.828$, stable window, uneven distribution of sequences, and a weak key [15]. That's why we always consider $\mu = 3.999$ in these experiments. Hence to overcome the drawbacks, researches on quantum-based encryption techniques is going on currently. The basic idea about the development of these kinds of techniques is that the information traveled on the internet must be random at its maximum extend. This is done by utilizing uncertainty principles of quantum mechanics on logistic maps which can enhance the randomness property of a ciphered image.

So, when the quantum behavior of the Heisenberg equation of wave motion [16] was applied on chaotic logistic maps, the cryptosystem became highly random because of gaining the qualities of high sensitivity to initial conditions and control parameters, mixing property, high efficiency, and non-periodicity. These properties of the quantum logistic map tend to

enhance the randomness and time complexity with a large key-space. The higher the key sensitivity lesser will be the image perceptual quality and the lesser will be the chance of information to be retrieved on the way of a communication channel. The mathematical representation of the quantum chaotic map is given in sr. no.2 of Table 2.

The equation has all the above-mentioned capabilities but this does not serve the purpose alone, we still needed to analyze them in some well-known performance analyses like Robustness analysis, security analysis, and attacks analysis [17].

To solve the purpose a survey of already published encryption techniques based review paper has been studied. The surveyed research papers are shown in Table 1. A survey of fourteen encryption techniques has been theoretically analyzed by John Justin M et.al [7]. The author did not consider any performance metrics for analysis against attacks on noises. In 2013, B. Padmavathi et.al [13] surveyed the most popular traditional techniques i.e. DES, AES, and RSA encryption techniques. The authors have also performed an analysis of the above mentioned techniques along with the LSB substitution technique. They provide experimentally analysis and comparison in a very effective way. They considered plain and chosen attacks but more attacks need to be considered for better security. Sourabh Chandra et.al has surveyed various symmetric and asymmetric key cryptography techniques [15]. The author has done a comparative analysis of studied encryption techniques without any consideration of noise attacks. Garima Tanwar et.al did a comparative analysis of ten image encryption techniques [14]. They have done comparisons based on theoretical and experimental analysis by calculating various performance metrics. This paper also did not include the main factor of secure encryption technique which is attacks analysis. Kevadia, K. T et.al [27] have done a theoretical survey of fifteen image encryption techniques. This paper includes a comparison without considering attacks and performance metrics. Omar Farook Mohammad et.al [19] have done the experimental analysis of nine encryption techniques. They performed a comparison but did not consider any noise attacks as one of the parameters. Manju Kumari et.al [26], performed a survey and experimental analysis of fifteen image encryption techniques. But in this paper also noise attack analysis has not been included. Pandya, A. et.al [34], has performed a theoretical survey and comparative analysis of three encryption techniques without considering an attack. Younes, M.A.B et.al [35], has performed a survey of the latest fourteen image encryption techniques theoretically without considering any performance metrics and attacks analysis. Patel, S. et al. [36] have surveyed twenty image encryption techniques with compression sensing. This survey was theoretically analyzed without considering any performance metrics and attacks on various noises. Manish Kumar et.al [37] performed a theoretical survey of twenty-four image encryption techniques.

The researchers have compared various image encryption techniques but only a few papers are available which provides a comparison of many traditional and modern encryption techniques. It clearly shows that existing papers have provided limited details of cryptography techniques which can provide experimental details of multiple noises and attacks.

Thus, this paper is an effort for the following contributions:

- Most of the latest encryption algorithms including chaos and quantum chaos-based image encryption techniques are taken into consideration for analysis.
- Analysis of algorithms is performed meticulously by considering various kinds of comprehensive attacks with and without consideration of noises.

Table 1 Available survey papers in literature survey

Author	Title	Year	No. of Techniques Compared	Mode of Comparison on Performance metrics	Security Attacks Analysis
John Justin M et al. [7]	A Survey on Various Encryption Techniques	2012	14 techniques	Theoretically analyzed	Not done
B. Padmavathi et al. [13]	A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique	2013	3 techniques	Experimentally analyzed with the help of algorithm type, Key length, Encryption Ratio, Scalability, Stimulation Speed, Power Consumption, Key used, Hardware and Software implementation	Security Attacks analyzed: plain text, cipher-text attacks
Sourabh Chandra et.al [15]	A comparative survey of symmetric and asymmetric key Cryptography	2014	42 techniques (Symmetric key Cryptography, Asymmetric key Cryptography, newly proposed Symmetric key and Asymmetric key Cryptography techniques)	Theoretically analyzed with the help of: 1. SYMMETRIC KEY CRYPTOGRAPHY: Structure of algorithm, Block size, Key size, Vulnerabilities, Efficiency 2. ASYMMETRIC KEY CRYPTOGRAPHY: Feature, Advantages, Disadvantages, Security solutions 3. NEWLY PROPOSED SYMMETRIC KEY AND ASYMMETRIC KEY CRYPTOGRAPHY: Characteristics, Advantages, Pitfalls, Implementations	Not done
Garima Tanwar et al. [14]	Survey on Image Encryption Techniques	2015	10 techniques	Theoretically and Experimentally analyzed with the help of Imperceptibility, Visual Degradation, Compression friendliness, Speed, Key space, Key Sensitivity analysis, Histogram analysis, Statistical analysis, Correlation coefficient analysis, Encryption Quality	Not done

Table 1 (continued)

Author	Title	Year	No. of Techniques Compared	Mode of Comparison on Performance metrics	Security Attacks Analysis
Kevadia, K.T. et.al [27]	A Literature Survey on Image Encryption.	2016	15 techniques	Theoretically analyzed	Not done
Omar Farook Mohamad et.al [19]	Survey and Analysis of the Image Encryption Methods	2017	9 techniques	Experimental Analysis is done on Visual Assessment, Key space analysis, Statistical analysis and Differential analysis, Entropy, PSNR with Computational Speed	Not done
Manju Kumari et.al [26]	A Survey of Image Encryption Algorithms	2017	15 techniques	Experimentally analyzed with the help of Visual Assessment, Statistical and Differential analysis, Key space and Key sensitivity analysis, Quantitative analysis, Time complexity	Not done
Pandya, A. et.al [34]	Comparative Analysis of Encryption Techniques	2018	3 techniques	Theoretically analyzed with the help of key size, Block size, Cipher type and security	Not done
Younes, M.A.B. [35]	A Survey of the most current image encryption and decryption techniques	2019	14 techniques	Theoretically analyzed	Not done
Patel, S. et.al [36]	A systematic survey on Image Encryption using Compressive Sensing	2020	20 techniques	Theoretically analyzed	Not done
Manish Kumar et.al [37]	Review of Image Encryption Techniques	2020	24 techniques	Theoretically analyzed	Not done

- Performance metrics are calculated for the examination of the studied encryption techniques to get the best technique even in noisy channels. Security analysis, Robustness analysis under the influences of noises and attacks are executed for comparison.
- A comparison has been made, and the best technique is identified from the survey with and without the presence of attack and noises.

In this paper, various chaos-based and quantum chaos-based image encryption techniques have studied theoretically and experimentally besides Robustness analysis, security analysis, and attacks analysis. For robustness analysis, several performance metrics such as Peak Signal

to Noise Ratio (PSNR), Entropy, Correlation (horizontally, vertically, and diagonally) have been analyzed with some predefined values. For security analysis performance metrics like Visual representation of encrypted/decrypted images, Key Space, and time complexity are observed. Lastly, for attacks analysis several parameters are examined like: Unified Average Changing Intensity (UACI), Number of pixel change Rate (NPCR) [18], noise(salt & pepper, gaussian, speckle, Poisson's) attacks.

The rest of the paper is organized as follows: in the section-II, six chaos-based and six quantum chaos-based latest image encryption techniques or schemes has been theoretically explained with the help of block diagrams. Section-III provides simulation set-up parameters along with performance matrices used to evaluate the efficacy of the studied techniques. Section IV gives the results with comparison and it is followed by a conclusion in section-V.

2 Image encryption techniques

As mentioned in the previous section that chaos and quantum chaos image encryption techniques are well enough for providing confidentiality services to internet users for real-time communication services. These methods directly modified the pixel positions and pixel values to maintain a large range of randomness. All of the studied techniques lied under the category of symmetric key cryptography techniques. These techniques have two major processes: Confusion and Diffusion [20]. The confusion process is meant for pixel position modification and the diffusion process modifies the pixel values. Several iterations of confusion and diffusion process have been provided to obtain higher order of randomness and lesser time complexity. The studied encryption techniques are random and confusing because of the presence of complex mathematics and its application to its various processes. Hence, for better understanding, Table 2 is provided which contains a series of maps and their corresponding equations along with a detailed description of the parameter's symbol and their range of values.

In this section, six studied and latest developed chaos and six quantum chaos techniques are tried to be explained as follows:

2.1 Chaos scheme 1: An intertwining chaotic maps based image encryption scheme

A concept of a modified classical logistic map was introduced by Sam et al. [21] in 2012. The author named it as intertwining chaotic maps which are used for the generation of chaotic keys and utilized to perform confusion and diffusion processes of encryption. These maps have highly random properties than a classical logistic map. The complete cryptosystem consists of four encryption processes: permutation to change the pixel value, byte substitution to enable the confusion process, nonlinear diffusion, and sub-diagonal diffusion along with key generation. Three sets of chaotic keys (x, y, and z) have been generated to encrypt the R, G, and B plane with the help of proposed intertwining logistic maps as represented in sr. no. 2 of Table 2.

Each map is iterated $m \times n$ times (size of a plane of the original image) such that a sequence of the compatible size of the plain image can be generated. In the confusion process, firstly initial permutation is carried out to scramble the pixel positions with the help of predefined six random values and then the resulting image is XORed with the first chaotic key(x). After this pixel values have been substituted with the help of S-box (16×16) as used in AES [10] and

Table 2 List of Maps and their Equations used for encryption schemes

Sr. No.	Name of Maps	Equations	Symbol of Control Parameter	Name of Control Parameter	Range
1	Logistic Map	$x_{n+1} = \mu x_n(1-x_n)$	μ	Sequence Control Parameter	[0,4]
2	Intertwining logistic maps	$x_{n+1} = [\mu k_1 y_n(1-x_n) + z_n] \bmod 1$ $y_{n+1} = [\mu k_2 y_n + z_n(1/(1-x_{n+1})^2)] \bmod 1$ $z_{n+1} = [\mu(x_{n+1} + y_{n+1} + k_3) \sin(z_n)] \bmod 1$	μ k_1 k_2 k_3 x_0 y_0 z_0	Sequence Control Parameter Float value as multiplier Float value as multiplier Float value as multiplier Initial value of x Initial value of y Initial value of z	[0,4] >33.5 >37.9 >35.7 0.41324738544344 0.52638928350638 0.98644737157579 1.5,99,111,7,77
3	Chaotic function	$x_{n+1} = [[x_n^2] \bmod S], x_n + x_g] \bmod S$	$p1, p2, p3, p4, p5, p6$ l_0^b S	Six odd random values Transformed binary 1D vector of original monochrome image Length of image	Binary size of $(l_0^b)-1$ $\{1, \dots, \text{Binary size of } (l_0^b)\}$ G
4	Mixed transformed logic maps	$x_{n+1} = [a, (1+x_n)^2, k1, \sin(1/1 + (y_n)^2)] \bmod 1$ $y_{n+1} = [a, x_{n+1}, k2, \sin(x_{n+1} \cdot y_n), (1+(z_n)^2)] \bmod 1$ $z_{n+1} = [a, x_{n+1}, k3, (1+y_{n+1} \cdot z_n)] \bmod 1$	x_0 x_g A k_1 k_2 k_3	pseudo-random seed Initial value of x pseudo-random seed Sequence Control Parameter Predefined keys Predefined keys Predefined keys	G^2 $0 < a \leq 3.999$ >37.7 >39.7 >37.2
5	Peter de jong chaotic map and RC4	$x_{i+1} = [\sin(a_i y_i) - \cos(b_i x_i)]$ $y_{i+1} = [\sin(c_i x_{i+1}) - \cos(d_i x_i)]$ $x_{n+1} = \sin(\pi \cdot x_n)$	a, b, c, d	Control Parameter	0 to 1.8
6	Sine Map	$x_{n+1} = r[(x_n)^2 - y_n]$	$x(0), y(0), z(0)$ x_n^* z_n^* R	pre-defined initial values Conjugate and fixed values of x Conjugate and fixed values of z control parameter	[0,1] 0.002 0.004 [0,4]
7	Quantum logistic map	$y_{n+1} = -y_n e^{-2\beta} + e^{\beta} r[(2-x_n - x_n^*) y_n - x_n z_n^* x_n^* z_n]$ $z_{n+1} = -z_n e^{-2\beta} + e^{\beta} r[(2-x_n^*) z_n - 2x_n y_n - x_n]$	β M $a1$	dissipation parameter Width of discrete lattice Matrix value of Cat map	>=6 256 1
8	2-D Total Automor-phism Map				

Table 2 (continued)

Sr. No.	Name of Maps	Equations	Symbol of Control Parameter	Name of Control Parameter	Range
9	Coupling of the two-dimensional logistic map and Quantum chaotic map	$\begin{pmatrix} r(n+1) \\ s(n+1) \end{pmatrix} = \begin{pmatrix} a11 & a12 \\ a21 & a22 \end{pmatrix} \begin{pmatrix} r(n) \\ s(n) \end{pmatrix} \text{Mod}(M)$	a12, a21 a22	Matrix value of Cat map Matrix value of Cat map	1 1 + a12a21
		Two-dimensional logistic map: $\emptyset(x_n) = \mu_1 x_n(1 - x_n) + {}_1 y_n^2$ $\emptyset(y_n) = \mu_2 y_n(1 - y_n) + {}_2(x_n^2 + x_n^2)$ y_n	μ_1 μ_2 1 2 ε	Control Parameter Control Parameter Control Parameter Control Parameter Coupling constant	2.75 < μ_1 ≤ 3.4 2.75 < μ_2 ≤ 3.45 0.15 < 1 ≤ 0.21 0.13 < 2 ≤ 0.15 [0,1]
10	5-D hyper chaotic map along with quantum cross-exchange of n qubit	Quantum chaotic map: $x_{n+1} = (1 - \varepsilon) \emptyset(x_n) + \varepsilon \emptyset(y_n)$ $y_{n+1} = (1 - \varepsilon) \emptyset(y_n) + \varepsilon \emptyset(x_n)$ 5-D Hyper-chaotic system: $x_1(i+1) = a[x_2(i) - x_1(i)] + x_4(i) + x_5(i)$ $x_2(i+1) = c$ $x_1(i) - x_1(i) \times 3(i) - x_2(i)$ $x_3(i+1) = x_1(i)x_2(i) - bx_3(i)$ $x_4(i+1) = -x_1(i)x_3(i) + px_4(i)$ $x_5(i+1) = qx_1(i)$	a, b, c, p and q $x_1(0), x_2(0), x_3(0), x_4(0)$ and $x_5(0)$	Lyapunov exponents parameter Initial values	10, 8/3, 28, 1.3 and 2.5 0.325, 0.476, 1.256, 0.628, and 1.5

the resulting image is XORed with second Chaotic Key (y). In the diffusion process, pixel values have been modified in two steps: Nonlinear diffusion and Sub-diagonal diffusion. The nonlinear diffusion is obtained by shifting circularly five times forward direction within bits of a pixel and then XORed with First chaotic key (x). The pixel value is modified in the Sub-diagonal diffusion step by XORing the first and second pixels with the third chaotic key (z). The resulting pixel value is XORed with the third-pixel value and the process continues till the last pixel gets modified.

Two rounds of iterations have been carried out for better alteration in the cryptosystem. The cryptosystem is robust against known-plaintext attacks, brute force attacks and also provides good coherence in key space analysis, differential analysis, and statistical analysis. The complete encryption process is shown in Fig. 1. The same process is carried out to decrypt the encrypted image but in reverse order.

2.2 Chaos scheme2: A new image encryption scheme based on chaotic function using linear congruence

An image encryption algorithm is developed by François et al. [22] to utilize the linear congruence based chaotic function in to generate large key spaces. The author mainly targeted the correlation present between the neighboring pixels to enhance the property of randomness in the cipher image. In the very first step, the image is transformed into a binary 1D vector I_0^b and a pseudo random seed ‘ g ’ of the same length of I_0^b is generated with the help of defined chaotic function as specified in sr. no. 3 of Table 2.

The position of the pixels is modified with the help of pseudo-random seed ‘ g ’ and a new scrambled vector I_m^b is generated.

Fig. 1 Block diagram of scheme based on intertwining chaotic maps

$$\begin{aligned}
 Z_1 &= I_0^b(i) \\
 Z_2 &= I_0^b(i+1+x(i)) \\
 Z_3 &= Z_1 \oplus Z_2 \\
 I_m^b(i) &= Z_3
 \end{aligned}$$

This process is repeated for R times and R is obtained from 3 round keys R_1 , R_2 , and R_3 . In the final step, the obtained stream is reshaped as in the dimensions of the original image. This algorithm gives strong resistance against brute-force attacks. The complex algorithm is shown in Fig. 2. The same process is carried out for decryption of the cipher image but in reverse order.

2.3 Chaos scheme 3: A novel image cipher based on mixed transformed logistic map

A mixed transformed logistic map was used to design a cryptosystem for encryption of colored pixels by Sam et al. [23] in 2012. The encryption process consumes nine keys, six of which are denoted as odd secret keys while the rest three (x , y , z) are chaotic keys. The 3 chaotic keys x , y , and z of the same size of the plane image have been generated with the help of mixed transformed logic maps as per the sr. no. 4 of Table 2.

Like every chaotic based encryption scheme, this scheme also completes the confusion and diffusion process. Initially, the pixel positions are permuted with the help of six odd keys and

Fig. 2 Scheme based on chaotic function using linear congruence

XORed with the first chaotic key(X). The diffusion process is completed in two steps: Nonlinear Diffusion and Zig-Zag Diffusion. In the nonlinear Diffusion, 4 times circular shifting is done in forwarding direction within bits of a pixel and the result is XORed with a Second chaotic key(Y). In the zig-zag diffusion, the colored image is separated into three (red, green, and blue) channels and is processed in a zig-zag direction as shown in Fig. 3 to obtain intra-channel mixing.

The resulting zig-zag position pixels are then XORed with the Third Chaotic Key (Z). This image encryption scheme enhanced confidentiality by obtaining mixed transformed logistic maps, initial permutation, nonlinear, and zig-zag diffusion process. These processes reduce the vulnerability against well-known differential attacks. The algorithm has shown a good coherence in various attack analyses including key space analysis, differential analysis, and statistical analysis like key-space, key sensitivity, time complexity, entropy, etc. Figure 4 shows the block diagram of the scheme based on mixed transform logistic maps. For decryption, the same process is carried out but in the reverse direction.

2.4 Chaos Scheme4:An effective image encryption scheme based on Peter De Jong chaotic map and RC4 stream cipher

Hanchinamani and Kulkarni [24] proposed a scheme based on Peter De Jong chaotic map and RC4 Stream Cipher to generate a highly random cryptosystem. The encryption process is completed in three major steps: permutation, pixel rotation, and diffusion. The algorithm utilizes Peter De Jong chaotic map (sr. no. 5 of Table 2) and generates the two sets of keys(x and y) of 128 values with the help of six secret keys as input condition parameters. So, as result, we will get total of 256 key values and the process of round key generation in Table 3.

The process is iterated two times to attain high level of security. The resultant values of x and y are used to arrange in ascending order and denoted by PM and PN respectively. Now the pixel's positions are permuted row wise and column wise according to the values of PM and PN. After this a pseudorandom stream is generated with the help of RC4 stream cipher scheme keeping x and y keys as input for RC4 stream generator. The generated stream is used for scrambling a pixel's bit position by applying circular shifting in forwarding direction horizontally and vertically. Again a pseudo-random stream is generated with the help of an RC4 stream generator and used in the final step which includes a forward and a backward diffusion on the pixel rotated image. The cryptosystem is very effective and it maintained a high level of security by applying only two rounds of encryption/decryption processes. It is highly resistant against brute force, and differential attacks. The complete encryption process is shown in Fig. 5. For decryption, the same process is followed but in reverse order.

Fig. 3 Zig-Zag Diffusion

Fig. 4 Block diagram of scheme based on mixed transformed logistic map

2.5 Chaos scheme5: An innovative image encryption scheme based on chaotic map and Vigenère scheme

In 2016 Bansal et al. [25] introduced a scheme based on chaotic map and Vigenère scheme both for encryption of a color image. This encryption scheme consists of two iterative states: diffusion and confusion. The scheme contains a very complex method of key generation and a different set of chaotic keys are used at every stage of encryption that's why the scheme is very much vulnerable to chosen and plain-text attacks. In a key generation, The two chaotic maps used for key generation, one is Sine Map (sr. no. 6 of Table 2) and another one is a combination of the logistic map (eq. 3) and intertwining chaotic map (eq. 1) with the help of seven random secret keys ($k1 - k7$). Three channels (x-channel, y-channel, and z-channel) are made to encrypt red, green, and blue planes of a color image as explained in Table 4.

Table 3 Key scheming

Rounds	Key values (0:256)	
	Key values (0:127)	Key values (128:255)
1	PM=x(0), x(1), x(2),x(127)	PN=y(0), y(1), y(2),y(127)
2	PM=x(128), x(129),x(255)	PN=y(128), y(129),y(255)
3	PM=x(256), x(257),x(383)	PN=y(256), y(257),y(383)
So on..

Fig. 5 Block diagram of a Scheme based on Peter De Jong chaotic map and RC4 stream cipher

In the diffusion stage, pixel permutation, forward and backward diffusion is done by matching the process with the vignère tables generated according to the sine map and logistic map generated sequences. In the confusion stage, the image is divided into two sequences. One sequence will contain row values and the second sequence contains column values. Then the pixel positions will be interchanged by a position permutation of rows and columns with the help of sine map and logistic map generated sequences, respectively. The same steps will be repeated for green and blue components also. Where the red, green, and blue components of the image are processed by $x_channel$, $y_channel$, and $z_channel$ respectively. In the end, the cipher image will be presented by concatenation of all the three modified planes. The cryptosystem consumes very less time for execution and provides good results of parameters like PSNR and Unified Average Changing Intensity (UACI). Figure 6 shows the complete encryption process. The same process is carried out in a reverse manner to decrypt the image at the receiver side.

Table 4 Details of Key Generation for encryption

Channel	Secret key	Chaotic Map	Resulted sequence	Size	Purpose of sequence Generation
	k_1	Sine Map	Sin_c Sin_d	1:N 1:M	Confusion process Diffusion process and vignère matrix creation
x-channel	k_2, k_5	Intertwining Chaotic Map and Logistic Map	xlog_c xlog_d	1:N 1:M+N	Confusion process Diffusion process and vignère matrix creation
y-channel	k_3, k_6	Intertwining Chaotic Map and Logistic Map	ylog_c ylog_d	1:N 1:M+N	Confusion process Diffusion process and vignère matrix creation
z-channel	k_4, k_7	Intertwining Chaotic Map and Logistic Map	zlog_c zlog_d	1:N 1:M+N	Confusion process Diffusion process and vignère matrix creation

2.6 Chaos scheme6: A novel image encryption scheme based on intertwining chaotic map and RC4stream cipher

In 2018 Kumari et al. [18] proposed a cryptosystem which utilizes intertwining chaotic maps along with the RC4 stream cipher scheme [12] for the generation of three key sequences to encrypt the color image. Likewise, this encryption process also consists of two major steps: diffusion and confusion. The process of encryption is very much similar to the previously discussed scheme. Firstly the plain image is separated into Red, Green, and Blue components, and three channels (x, y, and z) are used for the generation of three sequences of size (1xMN) named xlog_diff, ylog_diff, and zlog_diff respectively with the help of Intertwining Chaotic Map (sr.no. 2 of Table 2). xlog_diff. The sequences were modified with the help of RC4 sequence generator. The resulting sequences are then utilized for the diffusion of the image row-wise and then column-wise in forward and backward directions. Sequences ylog_diff and zlog_diff are used in the confusion process. In the last step, the cipher image is formed by combining all the modified planes into one image. All the red, green, and blue components of the image will be processed with the help of x_channel, y_channel, and z_channel respectively. The complete process is described in pictorial form in Fig. 7. The proposed scheme is very simple, consumes very little time to execute, and also provides good values of parameters like PSNR and Unified Average Changing Intensity (UACI). For decryption, the same process is carried out but in a reverse manner.

2.7 Quantum chaos1: A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces

In 2013, Ahmed A. Abd El-Latif et al. [28] introduced an image encryption technique that enhanced the robustness of the test image by exploiting color spaces. In this, along with the pixel position or value modification color planes were also shuffled. The cryptosystem consists of four steps: Key Generation, Scrambling the Luminance component [29], Diffusion, and confusion as shown in Fig. 8. The adaptive quantum chaotic logistic map (sr. no. 7 of Table 2) is used to generate chaotic keys for diffusion and confusion of the pixel values of a plain image. The n (same as the size of the plain image) no. of iterations has been performed to provide a wide range of complexity in the

Fig. 6 Block diagram of a Scheme based on chaotic maps and Vigenère scheme

key values. Firstly the color image is transformed into YCbCr color model. Since the Y component of the image contains maximum frequencies of information. That's why only the Y component is processed with Linear Wavelet Transform (LWT) and then the pixel positions will be scrambled with the help of 2-D Toral Automorphism Map (sr. no. 8 of Table 2). To recover the image in the same format, Inverse Linear Wavelet Transform (ILWT) is applied and transformed into a RGB color model. The color image is diffused in horizontal and vertical directions according to the key sequence KCQ. In the final step, the diffused image is XORed with the second quantum chaotic key. This step is classified as a confusion stage. The same process is carried out in a reverse manner to retrieve the original image from the encrypted image at the receiver side.

Fig. 7 Block diagram of a Scheme based on intertwining chaotic maps and RC4 Stream cipher

Fig. 8 Block diagram of the encryption process of scheme based on quantum chaotic system, exploiting color spaces

2.8 Quantum chaos2: A new image encryption scheme based on quantum logistic map

Akhshani et al. [30] proposed an image encryption scheme based on a quantum chaos logistic map in 2012. The complete encryption algorithm is shown in Fig. 9. Initially, the plain image $P_{(M \times N)}$ is transformed into a 1D array $I_{(\frac{M \times N}{4} \times 1)}$ in which each entry is filled up by combining 4-pixel values of the original image. A variable k is set to be false.

The quantum logistic map (sr. no. 7 of Table 2) is taken and iterated 1000 times with the help of initial condition and control parameters to remove transient effects. Then the initial condition values are updated with 1001th values of x , y , z obtained from the previous step. Now the same process of iteration is carried out once with keeping the updated initial condition values as the input and a modified sequence is generated by applying function E on I and chaotic sequence (x and y). The function E is defined in eq. 1:

$$C(i) = E[x(i), I(i)] \quad (1.a)$$

$$C(i) = E[y(i), C(i)] \quad (1.b)$$

$$E(a, b) = \text{floor}(ax2^{32}) \bmod 2^{32} \text{ XOR } b \quad (1.c)$$

In every iteration, the value of control parameter (r) will also be modified with the use of simple mathematical operations on $C(i)$ and $z(i)$. In this way the complete image (I) is transformed into a cipher image. K is the iteration control variable, set to be true when all the above defined steps have been completed. For decryption, the same process is carried out in reverse direction.

Fig. 9 Block diagram of the encryption process of Scheme based on quantum logistic map

2.9 Quantum chaos3: A novel color image encryption algorithm based on quantum Chaos sequence

In 2017 H. Liu and C. Jin [31] proposed a color image quantum chaos-based encryption scheme. The scheme utilizes a quantum logistic map and Arnold map for the generation of initial conditions & control parameters and pixel scrambling respectively. The cryptosystem carries three major steps: generation of initial conditions and control parameters, permutation, and diffusion for image encryption as shown in Fig. 10.

1) generation of initial conditions and control parameters The process is completed in 5 steps as defined in Table 5. A control parameter t_i is generated in each step with the help of pre-defined 16 secret keys ($K_1, K_2, K_3, \dots, K_{16}$). The two-dimensional logistic map and a Quantum chaotic map are coupled together to generate pseudo-random numbers in the range of $[0,1]$. This type of coupling is called Nearest-Neighboring Coupled Map Lattice as defined mathematically in sr. no. 9 of Table 2.

2) permutation process The pixel scrambling is done with the help of general Arnold transform as described by Eq.2.

Fig. 10 Block diagram of the encryption process of Scheme based on quantum chaos sequence

Table 5 List of the responsible control parameters for generation of initial conditions and control parameters

Steps	Control Parameter (t_i) Responsible for the generation of initial conditions and control parameters	Initial Conditions and control Parameters
1	t_1, t_2, t_3, t_4	$\mu_1, \mu_2, \mu_3, \mu_4$
2	t_5, t_6, t_7	a_1, a_2, a_3 and b_1, b_2, b_3
3	t_8, t_9, t_{10}	Ku_1, Ku_2, Ku_3
4	t_{11}, t_{12}, t_{13}	Kv_1, Kv_2, Kv_3
5	t_{14}, t_{15}, t_{16}	x_0', y_0', z_0'

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A^n \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} Ku \\ Kv \end{bmatrix} \pmod{256} \quad (2)$$

Where,

n = no. of iterations for matrix A , to get best scrambling n must be set 6.

$$\text{Transform Matrix } A = \begin{bmatrix} 1 & a \\ b & ab + 1 \end{bmatrix};$$

3) diffusion process The folding of the permuted matrix is applied in eight directions separated on each plane. For example, the matrix of R' is divided into two portions as RT and RB and then XOR operation is applied with the corresponding portion of random matrix X . then the remaining part is XORed with the modified portion. The complete rounds of diffusion steps for R plane are defined in Eq. 3:

Round 1

$$RT'(i, j) = RT(i, j) \oplus XT \quad (3.a)$$

$$RB' = RT' \oplus RB \quad (3.b)$$

Round 2

$$Rdr' = Rdr \oplus Xdr \quad (3.c)$$

$$Rdl' = Rdr' \oplus Rdl \quad (3.d)$$

Round 3

$$RR' = RR \oplus Xr \quad (3.e)$$

$$RL' = RR' \oplus RL \quad (3.f)$$

Round 4

$$Ridr' = Ridr \oplus Xidr \quad (3.g)$$

$$Ridl' = Ridr' \oplus Ridl \quad (3.h)$$

Round 5

$$RB' = RB \oplus XB \quad (3.i)$$

$$RT' = RB' \oplus RT \quad (3.j)$$

Round 6

$$Rdl' = Rdl \oplus Xdl \quad (3.k)$$

$$Rdr' = Rdl' \oplus Rdr \quad (3.l)$$

Round 7

$$RL' = RL \oplus XL \quad (3.m)$$

$$RR' = RL' \oplus RR \quad (3.n)$$

Round 8

$$Ridl' = Ridl \oplus Xidl \quad (3.o)$$

$$R_{idr}' = Ridl' \oplus Ridr \quad (3.p)$$

The resulting image R_d is formed by applying XOR operation on an 8 direction folded image R_f with random matrix X as mentioned in Eq.4.

$$R_d = R_f \oplus X \quad (4.a)$$

The same procedure is applied on permuted green and blue planes with random key matrix Y and Z respectively.

$$G_d = G_f \oplus Y \quad (4.b)$$

$$B_d = B_f \oplus Z \quad (4.c)$$

The cipher image is formed by combining the three modified planes. For decryption, the same procedure will be followed as the encryption process but in a reverse direction.

2.10 Quantum chaos4: Bit.Level quantum color image encryption scheme with quantum cross-exchange operation and hyper chaotic system

In 2018, Nanrun Zhou et al. [32] proposed a bit-level quantum color image encryption scheme based on high definition hyper-chaotic system. The system has more complex dynamic behavior. The quantum cross-exchange operations are also performed to exchange bit positions of each pixel of the color image. Due to the existence of these two operations, the proposed cryptosystem becomes highly random and complex. In this, a 5-D hyperchaotic map (sr. no.10 of Table 2) is used for the generation of key sequences along with a quantum cross-exchange of 24 qubits. The channel transmission is also performed in between the color planes.

A color image $|P\rangle$ of size $(2n \times 2n \times 3)$ is considered to perform the experiment. A new quantum multi-channel representation in Eq.5 for the digital image is described below:

$$|P\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} C_{yx}^{RGB} \otimes |yx\rangle \quad (5)$$

Where;

C_{yx}^{RGB} = RGB color image having information of pixel value.

$|yx\rangle$ = information of pixel position.

$\otimes$ = tensor product.

After qubit representation of the color image, the bit position scrambling is done with the concept of quantum cross-exchange as described by Table 6.

The same process bit cross exchange is also performed for G and B plane. The resulted image formed is $|P_K\rangle = |P_R\rangle |P_G\rangle |P_B\rangle$. In the next step, the quantum color image channel transformation is done in two steps, first transform occurs between R and G plane, and the then same is followed for G and B planes.

With the use of 5D hyper chaotic map, 5 sets of chaotic sequences $\{x_1(1:2^n)\}$, $\{x_2(1:2^n)\}$, $\{x_3(1:2^n)\}$, $\{x_4(1:2^n)\}$, $\{x_5(1:2^n)\}$ is obtained and transformed into integer values between

Table 6 quantum bit cross-exchange

Original bit position	7	6	5	4	3	2	1	0
Cross exchanged bit position	0	1	4	5	2	3	6	7

[0,255]. Now, to convert these sequences from 1-D array to 3D matrix (same size of test image), a combination rule is applied with the help of the values of X_5 as described in Table 7.

From this table, three sets of variables H_i^R , H_i^G , H_i^B will be obtained and it is taken as a security key to encryption the scrambled image (see Fig. 11). The decryption process is carried out in reverse direction as of the encryption process.

2.11 Quantum chaos5: Quantum image encryption using intra and inter bit permuted based on logistic map

In 2019, Xingbin Liu et al. [33] proposed a new encryption technique based on Intra and Inter Bit Permutation on the Qubit Lattice represented color image. In this, the bit positions, as well as pixel positions, are permuted. This is the most complex scheme because the computations occur on quantum represented 24 qubit planes of the plain image. Each plane of the image consists of 8-bit planes for each pixel value. The author proposed a novel quantum image representation (NEQR) model, which defines the quantum states as mentioned in Eq.5. The total no. of qubit required in this step are $q + 2n$. The author also utilizes a Quantum Logistic map to enhance the randomness during inter/intra bit permutation and diffusion process as shown in Fig. 12.

- (i) **Intra Bit Permutation:** Firstly, the image will be converted in q qubits binary planes(bpm) then the scrambling of bit's positions is done within a pixel. The scrambling is done with the help of the sequence generated by the quantum logistic map with the help of initial conditions and parameters. From this step, we get 8 sequences of $x_m(1:22n)$, the first N_0 values will be discarded to reduce the transient effect then the sequence is arranged in ascending order, the controlled operation G is applied to exchange the bits of original image bpm with respect to corresponding values of S_m and resulted image $|I\rangle$ is obtained.
- (ii) **Inter Bit Permutation:** In this step, the bit position will be scrambled within its plane only and the xor operation is applied between inter bit planes according to a

Table 7 Combination rule of the 5D hyper-chaotic sequence

X_5	H_i^R, H_i^G, H_i^B
0	X_1, X_2, X_3
1	X_1, X_2, X_4
2	X_1, X_2, X_5
3	X_2, X_3, X_4
4	X_3, X_4, X_5

Fig. 11 Block diagram of the encryption process of Scheme based on quantum cross-exchange operation and hyper chaotic system

- predefined operating sequence set $OS = [0, 2, 4, 6, \dots, q-3, q-1]$. The operator is applied on the intra bit permuted image $|I_1\rangle$ to generate a scrambled image $|I_2\rangle$.
- (iii) **Chaotic Diffusion:** This procedure will modify the pixel values of permuted image. A pseudo-random sequence $P = \{P_0, P_1, P_2, \dots, P_{2^{2n}-1}\}$ is generated from quantum logistic map $N_0 + 2^{2n}$ times, the first N_0 values will be discarded to reduce the transient

Fig. 12 Block diagram of the encryption process of Scheme using intra and inter bit permutation Based on logistic Map

effect and the rest of the 2^{2n} sequences will be used as a key for pixel value diffusion. The sequence PN is combined to form a q qubit matrix of the same size of permuted image is termed as $|K^i_{YX}\rangle$. The final step involves the xor operation between $|K^i_{YX}\rangle$ and $|I_2\rangle$. The decryption process is carried out in reverse direction as of the encryption process.

2.12 Quantum chaos6: A superlative image encryption technique based on bit plane using key-based electronic code book

The proposed encryption scheme [38] works on similar methodologies to the previously described quantum chaos image encryption schemes. It possesses complex confusion processes like bit scrambling on every plane of the colored images with the use of ECB and IP blocks (Similar to S-box of AES) to obtain multilevel matching. These two ECB and IP blocks are dependent on keys and the complete process is also iterated according to one of the key-value (limited to the integer range of 1 to 4) generated from the quantum logistic map (sr. no.7 of Table 2) by which the randomness of the system increases and completely transforms the original image.

The folding procedure (same as the quantum chaos3 scheme) in 8 directions has followed for the diffusion process. This results in a large key space with high redundancy in the process which means even a single bit change in the secret key forms a completely random cipher image such that the unauthorized user cannot detect the data correctly. The processes are applied on three channels of the colored image independently. All the processes utilize different keys, resulting in dissimilar operations for a separate set of keys. Figure 13 shows the basic block diagram of the encryption procedure with the corresponding keys used in each process. The scheme fulfills all the requirements of security and also passes UACI & NPCR tests. The decryption process is executed just in the reverse manner to recover the original image from the cipher image.

The next section provides a simulation set up parameters with various performance metrics.

3 Simulation set-up parameters and performance metrics

3.1 Simulation set-up

All the simulations are carried out on a personal laptop. Table 8, provides the specifications and initial values and parameters.

3.2 Performance metrics

3.2.1 Security analysis

(i) Visual assessment

The analysis of encrypted and decrypted images is done on three images of different sizes. The encrypted image must be random in nature such that no information can be interpreted by simply looking.

Fig. 13 Block diagram of the encryption process of *Scheme based on Bit Plane using key-based Electronic Code Book*

(ii) Key space analysis

Key space analysis is an essential parameter. It defines the key length used in the entire process of encryption. As much as larger the key size lesser will be the feasibility of a brute-force attack.

(iii) Time complexity

Time complexity is the amount of time taken by the execution of the encryption codes.

3.2.2 Robustness analysis

The encrypted images are analyzed to determine the number of similarities among the pixels of encrypted and original image or between the adjacent pixels. Histogram, Correlation analysis and entropy are the three parameters used for this purpose:

(i) Histogram analysis

It is a graph represents the frequency distribution of the pixel values presented in a image. Ideally, it should be uniformly spread on the graph.

(ii) Correlation analysis

Table 8 Simulation Set-up Parameters

Processor	2.3GHz Intel Core i5
Memory	8 GB DDR3 RAM
Operating system	Windows 10
Simulation Platform	MATLAB
Version	2017a
Size of Images	128×128 , 192×192 , 256×256
Type	Color Images (R,G,B)
Initial condition and control parameters used for key generation	
Chaos 1:	
[p1,p2, p3, p4, p5, p6, x, y, z]	[p1=7,p2=31, p3=23, p4=9, p5=15, p6=21, x=33.1, y=37.3, z=35.7]
Chaos 2:	
[Seed g(1:23)]	g=[4713 654, 84,287, 7487, 1984, 12,314, 10, 74,120, 130,014, 95,210, 1914, 70,553, 2835, 19,800, 299,314, 83,721,610,990, 210, 65,521, 396, 1,109,094, 230,014, 63,010, 10,246]
Chaos 3:	
[k1, k2, k3]	[k1=37.8, k2=39.8, k3=37.3]
[oddkey1, oddkey2, oddkey3, oddkey4, oddkey5, oddkey6]	[oddkey1=1, oddkey2=5, oddkey3=99, oddkey4=111, oddkey5=7, oddkey6=77]
Chaos 4:	
[a, b, c, d, X0, Y0]	[a=1.77, b=1.67, c=-0.85, d=2.1, X0=0.6, Y0=0.4]
Chaos 5:	
[u, k1, k2, k3,k4, k5, k6, k7]	[u=3.99, k1=0.01, k2=20, k3=22, k4=19, k5=34, k6=40, k7=36]
Chaos 6:	
[μ , xlog1, ylog1, zlog1, k4, k5, k6,pix]	[μ =3.999, xlog1=20.1, ylog1=22, zlog=19, k4=33.5, k5=37.9, k6=35.7,pix=0.1]
Quantum Chaos1:	
[$Q_1(0)$, $Q_2(0)$, $Q_3(0)$, $Q^*_1(0)$, $Q^*_3(0)$, λ , β , e1 and e2]	[$Q_1(0)=0.463442266$, $Q_2(0)=0.004532285$, $Q_3(0)=0.002136285$, $Q^*_1(0)=0.00186$, $Q^*_3(0)=0.00398$, $\lambda=3.99$, $\beta=4.489$, e1=99,971 and e2=99,809]
Quantum Chaos2:	
[x(0), y(0), z(0), x_n conj, z_n conj, r, β]	[x(1)=0.4523444336, y(1)=0.003453324562, z(1)=0.001324523564, x_n conj=0.002, z_n conj=0.004, r=3.9, $\beta=4.5$]
Quantum Chaos3:	
[a, b, E, r, β , K(1:16)]	[a=3.3; b=3.45; E=0.001; r=3.99; $\beta=6$; K(1:16)=[207, 21, 42, 61, 122, 203, 97, 76, 101, 5, 7, 241, 139, 28, 98, 17]
Quantum Chaos4:	
[a,b,c,p,q,x ₁ (0),x ₂ (0),x ₃ (0),x ₄ (0),x ₅ (0)]	[a=1, b=8/3, c=28, p=1.3, q=2.5, x ₁ (0)=0.325, x ₂ (0)=0.0476, x ₃ (0)=0.1256, x ₄ (0)=0.0628, x ₅ (0)=0.15]
Quantum Chaos5:	
[x ₁ (0), x ₂ (0), x ₃ (0), x ₄ (0), x ₅ (0), x ₆ (0), x ₇ (0), x ₈ (0), N ₀ , α , P(0)]	[x ₁ (0)=0.5, x ₂ (0)=0.52, x ₃ (0)=0.53, x ₄ (0)=0.6, x ₅ (0)=0.37, x ₆ (0)=0.46, x ₇ (0)=0.38, x ₈ (0)=0.61, N ₀ =10,000, $\alpha=3.99999$, P(0)=0.49]
Quantum Chaos6:	
[x, y, z, $\bar{x}$, z, r and β]	[x=0.4523444336, y=0.003453324562, z=0.001324523564, $\bar{x}$ =0.002, $\bar{z}$ =0.004, r=3.9 and $\beta=4.5$]
Initial condition and control parameters used for modified key generation	
Chaos 1:	
[p1,p2, p3, p4, p5, p6, x, y, z]	[p1=7,p2=31, p3=23, p4=9, p5=15, p6=21, x=33.11, y=37.3, z=35.7]
Chaos 2:	
[Seed g(1:23)]	[4714 654, 84,287, 7487, 1984, 12,314, 10, 74,120, 130,014, 95,210, 1914, 70,553, 2835, 19,800, 299,314, 83,721,610,990, 210, 65,521, 396, 1,109,094, 230,014, 63,010, 10,246]
Chaos 3:	
[k1, k2, k3]	[k1=37.81, k2=39.8, k3=37.3]
[oddkey1, oddkey2, oddkey3, oddkey4, oddkey5, oddkey6]	[oddkey1=1, oddkey2=5, oddkey3=99, oddkey4=111, oddkey5=7, oddkey6=77]
Chaos 4:	

Table 8 (continued)

Processor	2.3GHz Intel Core i5
[a, b, c, d, X0, Y0] Chaos 5:	[a=1.771, b=1.67, c=-0.85, d=2.1, X0=0.6, Y0=0.4]
[u, k1, k2, k3,k4, k5, k6, k7] Chaos 6:	[u=3.991, k1=0.01, k2=20, k3=22, k4=19, k5=34, k6=40, k7=36]
[μ, xlog1, ylog1, zlog1, k4, k5, k6,pix]	[μ=3.9991, xlog1=20.1, ylog1=22, zlog=19, k4=33.5, k5=37.9, k6=35.7,pix=0.1]
Quantum Chaos1: [Q ₁ (0), Q ₂ (0), Q ₃ (0), Q [*] ₁ (0), Q [*] ₃ (0), λ, β, e1 and e2]	[Q ₁ (0)=0.4634422661, Q ₂ (0)=0.004532285, Q ₃ (0)=0.002136285, Q [*] ₁ (0)=0.00186, Q [*] ₃ (0)=0.00398, λ=3.99, β=4.489, e1=99,971 and e2=99,809]
Quantum Chaos2: [x(0), y(0), z(0), x _n conj, z _n conj, r, β]	[x(1)=0.4623444336, y(1)=0.003453324562, z(1)=0.001324523564, x _n conj=0.002, z _n conj=0.004, r=3.9, β=4.5]
Quantum Chaos3: [a, b, E, r, β, K(1:16)]	[a=3.31; b=3.45; E=0.001; r=3.99; β=6; K(1:16)=[207, 21, 42, 61, 122, 203, 97, 76, 101, 5, 7, 241, 139, 28, 98, 17]]
Quantum Chaos4: [a,b,c,p,q,x ₁ (0),x ₂ (0),x ₃ (0), x ₄ (0),x ₅ (0)]	[a=1, b=8/3, c=28, p=1.3, q=2.5, x ₁ (0)=0.326, x ₂ (0)=0.0476, x ₃ (0)=0.1256, x ₄ (0)=0.0628, x ₅ (0)=0.15]
Quantum Chaos5: [x ₁ (0), x ₂ (0), x ₃ (0), x ₄ (0), x ₅ (0), x ₆ (0), x ₇ (0), x ₈ (0), N ₀ , α, P(0)]	[x ₁ (0)=0.51, x ₂ (0)=0.52, x ₃ (0)=0.53, x ₄ (0)=0.6, x ₅ (0)=0.37, x ₆ (0)=0.46, x ₇ (0)=0.38, x ₈ (0)=0.61, N ₀ =10,000, α=3.99999, P(0)=0.49]
Quantum Chaos6: [x, y, z, x̄, z̄, r and β]	[x=0.45234443361, y=0.003453324562, z=0.001324523564, x̄=0.002, z̄=0.004, r=3.9 and β=4.5]

The encrypted image should have no similarities between the adjacent pixels. The mathematical values of correlation coefficients lie between -1 to +1. The perfect negative or positive one value represents maximum linear relation, and a zero value represents no linear relation between the adjacent pixel values. This analysis can be done horizontally, vertically, and diagonally. Eq.6 represents the formula of correlation:

$$r_{\alpha\beta} = \frac{\text{cov}(\alpha, \beta)}{\sqrt{D(\alpha)}\sqrt{D(\beta)}} \quad (6.a)$$

$$E(\alpha) = \frac{1}{N} \sum_{i=1}^N \alpha_i \quad (6.b)$$

$$D(\alpha) = \frac{1}{N} \sum_{i=1}^N (\alpha_i - E(\alpha))^2 \quad (6.c)$$

$$\text{cov}(\alpha, \beta) = \frac{1}{N} \sum_{i=1}^N (\alpha_i - E(\alpha))(\beta_i - E(\beta)) \quad (6.d)$$

Where,

α and β denote pixel position of encrypted and plain images.

$D(\alpha)$ is the variance of the image.

$E(\alpha)$ is the mean of the pixel values of the image.

$\text{Cov}(\alpha, \beta)$ is the covariance between encrypted and plain images

(i) Information entropy

Information entropy defines the amount of randomness in the given image. It is measured as bits per message. The formula of entropy is given below:

$$H(S) = \sum_{i=0}^{n-1} P(S_i) \log_2 \left(\frac{1}{P(S_i)} \right) \quad (7)$$

where,

n is the total number of symbols,

S_i is the pixel value.

$P(S_i)$ is the probability of the occurrence of S_i in the entire image.

3.3 Attack analysis

3.3.1 Differential attack analysis

Differential attack analysis is the kind of tests performed to calculate the number of changes in the encrypted image occur after a single bit modification is done in the key value or in the plain image.

3.4 NPCR (number of pixel change rate)

NPCR defines the rate of change in the number of pixels in between the two encrypted images formed by the original key and pixel modified (generally a bit only) key or in plain image.

The formula for NPCR is given in Eq. 7:

$$NPCR = \frac{\sum_{i=1}^H \sum_{j=1}^W \sum_{k=1}^L D(i, j, k)}{W \times H \times L} \times 100\% \quad (7.a)$$

$$D(i, j, k) = \begin{cases} 0 & C1(i, j, k) = C2(i, j, k) \\ 1 & C1(i, j, k) \neq C2(i, j, k) \end{cases} \quad (7.b)$$

where,

$C1$ and $C2$ are the cipher images formed by original and pixel modified key or the plain image.

H , L , and W are the height, length, and width of the image.

D is a bipolar array with a size equivalent to the images $C1$ and $C2$.

3.5 UACI (unified average change in intensity)

UACI defines the average value of differential intensities between the plain and encrypted images.

$$UACI = \frac{1}{W \times H \times L} \left[\sum_{i=1}^H \sum_{j=1}^W \sum_{k=1}^L \frac{|C1(i,j,k) - C2(i,j,k)|}{2^{Q-1}} \right] \times 100\% \quad (8)$$

where,

Q is the number of bits representing respective red, green, and blue channels.

3.5.1 PSNR (peak signal-to-noise ratio)

PSNR is the ratio between the maximum signal power component i.e. maximum pixel value and the mean error value. For calculation, the plain-image is considered to be the signal and the encrypted image is considered as the noise. It is measured as logarithmic quantity or in decibel. The mathematical representation of PSNR is given as:

$$\text{PSNR} = 20 \times \log_{10} \left(\frac{255}{\sqrt{\text{MSE}}} \right) \text{dB} \quad (9.a)$$

$$\text{MSE} = \frac{1}{W \times H \times L} \sum_{i=1}^W \sum_{j=1}^H \sum_{k=1}^L [I(i,j,k) - K(i,j,k)]^2 \quad (9.b)$$

where,

MSE is the mean squared error.

I and K are the pixel values of the original and the encrypted image respectively. (i, j, k) are the pixel position.

3.5.2 Noise attacks

BER: Bit error rate The probability of error defines as number of incorrect bits transmitted per unit time. It can be calculated by dividing the number of wrong bits to the absolute number of bits transmitted. It is a unitless performance measurement quantity. During information(image) transmission over the correspondence channel and their modification of bits may happen because of noises and interference. This is a necessary parameter to compute error. The value of BER increases as the channel quality decreases.

- i. **Salt & Pepper Noise:** This noise is the outer unsettling influence seen on the images. It is also popular as a Impulse Noise. This noise occurs when there is sharp and abrupt aggravations in the image signal. It is visually can be seen as event of white and dark pixels on the image. The impact of Salt and Pepper noise can be seen on image for various estimations of noise density and loss of image information.
- ii. **Gaussian Noise:** It is conspicuous noise brought about by the arbitrary variances in the signal. It is a factual noise which is characterized as Gaussian distribution. The impact of Gaussian noise can be seen on image for various estimations of mean and standard deviation. It is a statistical noise which is defined as normal or Gaussian distribution or probability density function (PDF) p can be defined as:

$$p(z) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-(z-\mu)^2}{2\sigma^2}} \quad (10)$$

where z represents the grey level, μ the mean value and σ the standard deviation.

- i. **Poisson Noise:** This noise occurs because of the statistical nature of electromagnetic waves. The x-ray and gamma beam sources transmit number of photons per unit time which is infused in patient's body from its source. These sources contain arbitrary variance of photons. The resulted picture has spatial and transient arbitrariness. This noise is called as quantum noise or photon noise or shot noise. This noise is calculated from poisson's distribution.
- ii. **Speckle Noise:** This noise is augmentative noise. It is appeared in intelligent imaging frameworks. For example: laser, radar and acoustics. This can exist in an image as Gaussian noise. Its probability density function is calculated from gamma distribution.

4 Results

4.1 Security analysis

4.1.1 Visual analysis

Table 9 shows the visual assessment of the different images of sizes 128*128, 192*192, and 256*256. It illustrates the visual evaluation of the scrambled pictures generated after applying the encryption algorithms on the original image. It is very well seen that quantum chaos based systems give a high scrambling of the pixels in the encoded original image, which means it shows no information to the intermediate user. Finally, all the schemes provide the decrypted images the same as the original images. Table 9 also represents the histograms of original, encrypted, and decrypted images. The histograms of images encrypted by quantum chaos 2, quantum chaos 5 and quantum chaos 6 schemes are uniformly distributed and show no statistical resemblance with the histograms of original images. So, these techniques provide strong resistance against the statistical attacks.

4.1.2 Key space analysis

Key size is one of the important parameter used for cryptanalysis, as it is the only secret key should be kept safe. Key space defines the range of combinations for key generated for diffusion during the encryption. With an increase in key size, complexity will also increase for its identification.

Table 10 gives the key-space calculations for the techniques for the implemented schemes. It is observed that all of the quantum chaos-based techniques have a large key-space which is sufficient to oppose the brute force attacks. Among all of the studied schemes, scheme utilizing a key of a bigger size.

Table 9 Visual Assessment and Histogram Analysis of Image Encryption Schemes.

Size/ Scheme	128*128	192*192	256*256
Chaos Scheme 1
Chaos Scheme 2
Chaos Scheme 3
Chaos Scheme 4
Chaos Scheme 5

4.1.3 Time complexity

Table 11 introduces the time utilities for the execution of the process of encryption for the three test images of the studied techniques. The figure demonstrates that quantum chaos-based Scheme 4 utilizes very little time for execution of the encryption procedure and on the other hand quantum chaos 5 encryption technique will take large time for execution. Hence for the application of real time and fast communication quantum chaos 4 is the best suitable technique.

Chaos Scheme 6	
Quantum Chaos Scheme 1	
Quantum Chaos Scheme 2	
Quantum Chaos Scheme 3	
Quantum Chaos Scheme 4	
Quantum Chaos Scheme 5	
Quantum Chaos Scheme 6	

Table 10 Key Space Analysis

Scheme	Key Space
Chaos Scheme 1	2^{216}
Chaos Scheme 2	$2^{126} \cdot 2^{147}$
Chaos Scheme 3	2^{192}
Chaos Scheme 4	2^{384}
Chaos Scheme 5	2^{448}
Chaos Scheme 6	2^{384} (six keys of 64 bit k_1 to k_6)
Quantum Chaos Scheme 1	2^{224}
Quantum Chaos Scheme 2	2^{256}
Quantum Chaos Scheme 3	2^{128}
Quantum Chaos Scheme 4	10^{72}
Quantum Chaos Scheme 5	$>2^{100}$
Quantum Chaos Scheme 6	2^{432}

4.2 Robustness analysis

4.2.1 Histogram analysis

This is represented in Table 9 collectively in response with visual snapshot of original, encrypted and decrypted image. It represents the frequency distribution of the pixel values presented in a image. It is shown that the frequency of all the studied techniques are uniformly distributed on the graph.

4.3 Correlation analysis

The analysis is performed by the calculated correlation between original and encrypted images. Every one of the pixel sets contains one arbitrarily chosen pixel and another adjoining it. Table 12 shows the original, horizontal, vertical, and diagonal correlation coefficients of the images of size 128×128 , 192×192 , and 256×256 . It is clearly seen that all the quantum chaos-based techniques, gave very low correlation coefficient values for all three images. But out of the implemented schemes quantum chaos 1, 2 and 5 obtained the lowest correlation between original and its neighbor pixel.

Table 11 Time Complexity Values of all Techniques

Size/Scheme	128×128	192×192	256×256
Chaos Scheme 1	14.38301	32.18196	56.63815
Chaos Scheme 2	2.140098	4.965226	8.99707
Chaos Scheme 3	7.189583	15.74994	27.55559
Chaos Scheme 4	6.301881	13.4756	23.93574
Chaos Scheme 5	0.55678	0.789644	1.368821
Chaos Scheme 6	17.92622	9.805815	16.34207
Quantum Chaos Scheme 1	11.98091	6.837741	13.66485
Quantum Chaos Scheme 2	5.858	7.132	8.62
Quantum Chaos Scheme 3	3.798695	2.481566	4.120921
Quantum Chaos Scheme 4	0.250721	0.145437	0.252716
Quantum Chaos Scheme 5	925.8209	320.6599	962.2312
Quantum Chaos Scheme 6	17.92622	9.805815	16.34207

Table 12 Horizontal, Vertical, Diagonal Correlation Plots of Original and Encrypted Image.

This shows to their diminished obstruction against the statistical attacks. The correlation plots of the original and the encrypted pictures are given in Table 12. It is shown that the plots of the encrypted pictures are very non-consistently distributed. The corresponding values of the correlation coefficients which we visually analyzed in Table 12 are given in Table 13.

4.4 Information entropy analysis

The entropy values for highest amount of randomness should be extremely near the perfect estimation of 8. From Fig. 14, except quantum chaos scheme 2 every scheme obtains entropy value nearly equal to 8. Hence all the studied image encryption techniques give highly random encrypted image.

Table 13 Horizontal(H), Vertical(V) and Diagonal(D) correlation values

Size/ Scheme	128 × 128			192 × 192			256 × 256		
	Horizontal Correlation	Vertical Correlation	Diagonal Correlation	Horizontal Correlation	Vertical Correlation	Diagonal Correlation	Horizontal Correlation	Vertical Correlation	Diagonal Correlation
Original	0.940712	0.961066	0.9208359	0.9624182	0.957173	0.9417011	0.978094	0.976509	0.956619
Chaos Scheme 1	-0.016097	-1.52E-02	0.0137199	-1.13E-02	0.0054393	7.48E-03	-0.011327	-5.95E-03	-0.01264
Chaos Scheme 2	-0.003679	5.08E-03	-0.0027	-6.08E-03	0.0038142	4.34E-03	0.006315	5.30E-03	0.0043147
Chaos Scheme 3	-0.006269	2.00E-03	0.0202164	-8.90E-03	0.0145188	1.08E-02	-0.006991	-0.018013	-0.010264
Chaos Scheme 4	0.0043302	-1.51E-02	-0.002805	-9.75E-03	-0.001252	1.05E-02	-0.010351	9.98E-05	0.01158
Chaos Scheme 5	0.0060997	5.65E-03	0.0230068	6.10E-03	-0.001188	-2.35E-03	-0.011054	-3.26E-04	-0.011806
Chaos Scheme 6	0.002769	-0.00684	-0.00982	-0.01237	-0.00613	-0.01285	-0.00232	0.004796	-0.00119
Quantum Chaos Scheme 1	0.002058	0.027612	0.009497	0.022454	0.013432	-0.00488	0.128499	0.136189	0.081143
Quantum Chaos Scheme 2	0.020805	0.05301	0.035518	0.017432	0.023468	0.010631	0.088709	0.161429	0.062789
Quantum Chaos Scheme 3	-0.00227	0.002841	-0.00217	0.013753	0.01272	-0.00113	-0.02943	-0.00946	0.010685
Quantum Chaos Scheme 4	0.003944	-0.02128	-0.00262	0.008257	-0.00552	0.008037	-0.01314	-0.0034	0.006497
Quantum Chaos Scheme 5	0.002073	-0.02454	0.000764	0.027627	0.003291	0.016466	-0.00094	-0.02253	0.014371
Quantum Chaos Scheme 6	0.002769	-0.00684	-0.00982	-0.01237	-0.00613	-0.01285	-0.00232	0.004796	-0.00119

Fig. 14 Entropy of all Techniques for all Image size

4.5 Attack analysis

4.5.1 Differential attack analysis

A experiment have done for encrypt an image on the basis of the steps proposed by the authors to obtain a quantum based encryption scheme. The values of the original key set and modified keys for differential attacks are provided in Table 8. It has seen that, for single bit change either in a pixel of the original image or in the key results in a highly random encrypted image. As per the NPCR and UACI standard values [17], for every three test pictures should be more than 99.4 and 33.2% respectively. It is found that the results after applying these two tests, quantum chaos techniques exceedingly resistive against the differential assaults. Table 14

Table 14 NPCR and UACI values for one bit change in pixel value

Size/ Scheme	128 × 128		192 × 192		256 × 256	
	NPCR	UACI	NPCR	UACI	NPCR	UACI
Chaos Scheme 1	99.658	33.292	99.6121	33.492	99.614	33.546
Chaos Scheme 2	99.578	33.428	99.5813	33.393	99.608	33.421
Chaos Scheme 3	99.591	33.391	99.6247	33.525	99.649	33.413
Chaos Scheme 4	99.682	33.437	99.6718	33.406	99.585	33.555
Chaos Scheme 5	99.585	33.517	99.6257	33.374	99.617	33.551
Chaos Scheme 6	99.591	30.523	99.6184	30.476	99.605	31.89
Quantum Chaos Scheme 1	99.55	33.46	99.64	33.47	99.65	33.47
Quantum Chaos Scheme 2	99.61	33.50	99.65	33.61	99.72	33.62
Quantum Chaos Scheme 3	99.59	33.56	99.61	33.63	99.65	33.65
Quantum Chaos Scheme 4	51.23 (fail)	33.46	52.35 (fail)	33.53	52.39 (fail)	33.57
Quantum Chaos Scheme 5	50.20 (fail)	25.09 (fail)	50.42 (fail)	25.16 (fail)	50.57 (fail)	25.19 (fail)
Quantum Chaos Scheme 6	99.22	33.01	99.12	33.17	99.75	33.41

show the NPCR and UACI test results for 128×128 , 192×192 and 256×256 image for different encryption schemes stating which techniques pass or fail in passing the 0.05 level 0.01 level and 0.001 level of investigation. As seen in the Table 14 that quantum chaos Scheme 4 and 5 doesn't pass the NPCR test while only Scheme 5 doesn't pass the UACI test.

4.6 Quantitative analysis

PSNR PSNR is one of the key parameters to compute the robustness of any encryption technique. The lower value of PSNR results the in high error between the original and cipher image.

Figure 15 shows the PSNR values acquired for the three test pictures for all the techniques illustrated in the literature. Every scheme utilizes practically comparable estimated value of PSNR should be equal to 8 for the 128×128 , 192×192 , and 256×256 test images. The simulation of all the encryption schemes provides the average results of all the techniques. Techniques quantum chaos 3 obtained the highest PSNR and chaos 2 obtained the lowest and best results. Also, chaos Scheme 2 also obtained the nearest PSNR value comparable with chaos Schemes 3, hence we may consider chaos Scheme 2, 3 and quantum chaos 6 are the best techniques in terms to obtain maximum errors in cipher image.

4.7 Noise attacks

BER: Bit error rate Figures 16, 17, and 18 demonstrates the BER values acquired for all techniques available in literature for Salt & Pepper, Gaussian, Speckle and Poisson's Noise Attacks of image size of 128×128 , 192×192 , and 256×256 respectively. Chaos Scheme 5 shows the minimum bit error rate against Speckle noise and quantum chaos 5 shows

Fig. 15 PSNR of the survey techniques for Image size of 128×128 , 192×192 , 256×256

Fig. 16 BER of all Techniques for Salt & Pepper, Gaussian, Speckle and Poisson's Noise Attacks for image size of 128×128

effectively very less amount of Salt & Pepper noise. Chaos scheme1 and chaos Scheme 5 both represents minimum amount of Gaussian noise in comparison with other techniques. In overall comparison, all the studied techniques except Chaos Scheme 5 shows comparable high bit error rate in comparison to other techniques.

Fig. 17 BER of all Techniques for Salt & Pepper, Gaussian, Speckle and Poisson's Noise Attacks for image size of 192×192

Fig. 18 BER of all Techniques for Salt & Pepper, Gaussian, Speckle and Poisson's Noise Attacks for image size of 256×256

5 Conclusion

In search of best secure image encryption technique numerous researchers have proposed higher order of security mechanism. In this paper, twelve Image Encryption techniques proposed in past decade based on chaos and quantum chaos-based encryption are selected. These techniques are theoretically and experimentally analyzed with the help of MATLAB 2016a software. After review of techniques for different sizes of images (128, 192 and 256), results are calculated. On the basis of results a comparison between various quantum chaos encryption schemes are presented. The comparison has been done in terms of Robustness analysis which includes image perceptual quality, PSNR, entropy, time complexity, Security analysis and Attacks analysis on three four type of noises (salt & pepper, gaussian, speckle, Poisson's noise). The image perceptual quality is very low in the case of all the schemes due to uniform histogram distribution. Correlation is nearly equal to zero, thus all the schemes can resist statistical attacks and noise attacks. Also, NPCR and UACI are close to their identical values 99.6% and 33.4% which makes the scheme resistive against differential attacks. The entropy of the schemes is close to the identical value 8. The time complexity is moderate in most of the cases but sufficient for real time communication in case of small size images. Table 15 represents the overall comparison of different techniques existent in the literature. The green colored highlights in the table have identified the best performance parameter of their respective schemes. Hence, this survey paper may help the network service providers to choose the best scheme for a particular application. The latest proposed Quantum chaos tend to be the best technique among all which can resist a limited amount of attacks and but it is having best qualities of confidentiality.

Table 15 Over all comparison

Encryption Scheme	Image Perceptual Quality	Correlation	UACI/ NPCR Test	Key Space	Key Sensitivity	Entropy/ Randomness	Time Complexity	Noise Attacks
Chaos Scheme-1	Very Low	Low	Pass	Large	High	High	High	Resistant
Chaos Scheme 2	Very Low	Low	Pass	Medium	High	High	Very Low	Less Resistant
Chaos Scheme 3	Very Low	Low	Pass	Large	High	High	Low	Less Resistant
Chaos Scheme 4	Very Low	Low	Pass	Large	High	High	Low	Less Resistant
Chaos Scheme 5	Very Low	Low	Pass	Largest	High	High	Low	Highly Resistant
Chaos Scheme 6	Very Low	Low	Pass	Large	High	High	Medium	Less Resistant
Quantum Chaos Scheme 1	Very Low	Low	Pass	Large	High	High	Low	Less Resistant
Quantum Chaos Scheme 2	Very Low	Low	Pass	Large	High	High	Low	Less Resistant
Quantum Chaos Scheme 3	Very Low	Low	Pass	Large	High	High	Low	Less Resistant
Quantum Chaos Scheme 4	Very Low	Low	Pass	Large	High	High	Very Low	Less Resistant
Quantum Chaos Scheme 5	Very Low	Low	Fail	Medium	High	High	High	Resistant for small size image
Quantum Chaos Scheme 6	Very Low	Low	Pass	Very Large	High	High	Low	Less Resistant

References

1. CISO Benchmark Report CiscoCybersecuritySeries (2019)
2. <https://securityboulevard.com/2020/02/20-ransomware-statistics-youre-powerless-to-resist-reading/>
3. Alloghani M, Alani MM, Al-Jumeily D, Baker T, Mustafina J, Hussain A, Aljaaf AJ (2021) A systematic review on the status and progress of homomorphic encryption technologies
4. Al-Maytami B, Fan P, Hussain A, Baker T, Liatsis P (2020) An efficient queries processing model based on multi broadcast searchable keywords encryption (MBSKE). Ad Hoc Netw 98:102028
5. Kumari M, Pawar V, Kumar P (2019) A novel image encryption scheme with Huffman encoding and steganography technique. Int J Netw Secur Its Appl 11(4):49–73. <https://doi.org/10.5121/ijnsa.2019.11404>
6. Rhee MY (2003) Internet security: cryptographic principles, algorithms, and protocols. In: Book, Hoboken. J. Wiley, NJ

7. John Justin M, Manimurugan S (2013) A survey on various encryption techniques. *International Journal of Soft Computing and Engineering (IJSCE)* 2(1). ISSN 2231:2307
8. El-Zoghdy SF, Nada YA, Abdo AA (2011) How good is the DES algorithm in image ciphering. *Int J Advanced Networking and Applications* 02(05):796–803
9. Mitchell CJ (2016) On the security of 2-key triple DES. In: on the security of 2-key triple DES. Royal Holloway, University of London, Information Security Group
10. FIPS 197 (2001) Advanced Encryption Standard (AES)
11. Schneier B (1994) Description of a new variable-length key, 64-bit block cipher (blowfish). In: Anderson R. (eds) *Fast software encryption. FSE 1993. Lecture notes in computer science*, vol 809. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-58108-1_24
12. Fluhrer S, Mantin I, Shamir A (2001) Weaknesses in the key scheduling algorithm of RC4. Springer, *Selected Areas in Cryptography 2001*, volume 2259. ISBN: 978–3–540-43066-7
13. Padmavathi B, Kumari SR (2013) A survey on performance analysis of DES, AES and RSA algorithm along with LSB substitution. *International Journal of Science and Research (IJSR)* 2(4) ISSN 2319:7064
14. Tanwar G, Mishra N (2015) Survey on image encryption techniques. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)* 5(12)
15. Chandra S, Paira S, Alam SS, Sanyal G (2014) A comparative survey of symmetric and asymmetric key cryptography. In: 2014 international conference on electronics, communication and computational engineering (ICECCE) (pp. 83–93). IEEE
16. Lai C-Y, Chung K-M (2019) Quantum encryption and generalized Shannon impossibility. *Des Codes Crypt* 87(9):1961–1972. <https://doi.org/10.1007/s10623-018-00597-3>
17. Wu Y, Agaian S (2011) NPCR and UACI randomness tests for image encryption. *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*:9
18. Kumari M, Gupta S (2018) A novel image encryption scheme based on intertwining chaotic maps and RC4 stream cipher. *3D Res* 9(1). <https://doi.org/10.1007/s13319-018-0162-2>
19. Mohammad OF, Rahim MSM, Zeebaree SRM, Ahmed FY (2017) A survey and analysis of the image encryption methods. *Int J Appl Eng Res* 12(23):13265–13280
20. François M, Grosjes T, Barchiesi D, Erra R (2012) A new image encryption scheme based on a chaotic function. *Signal Process Image Commun* 27(3):249–259. <https://doi.org/10.1016/j.image.2011.11.003>
21. Shatheesh Sam I, Devaraj P, Bhuvaneshwaran RS (2012) An intertwining chaotic maps based image encryption scheme. *Springer Nonlinear Dyn* 69:1995–2007. <https://doi.org/10.1007/s11071-012-0402-6>
22. François M, Grosjes T, Barchiesi D, Erra R (2012) A new image encryption scheme based on a chaotic function. Springer, *Signal Process Image Commun* 27(3):249–259. <https://doi.org/10.1016/j.image.2011.11.003>
23. Sam IS, Devaraj P, Bhuvaneshwaran RS (2012) A novel image cipher based on mixed transformed logistic maps. *Multimed Tools Appl*, Springer 56(2):315–330. <https://doi.org/10.1007/s11042-010-0652-6>
24. Hanchinamani G, Kulkarni L (2015) An efficient image encryption scheme based on a Peter De Jong chaotic map and a RC4 stream cipher. *3D Res* 6(3):30. <https://doi.org/10.1007/s13319-015-0062-7>
25. Bansal et al (2017) An innovative image encryption scheme based on cha.pdf
26. Kumari M, Gupta S, Sardana P (2017) A survey of image encryption algorithms. Springer, *3D Research* 8(4):37
27. Kevadia KT, Nayak AM, Patel KS, Patel BU (2016) A literature survey on image encryption 2:741–746
28. Abd El-Latif AA, Li L, Wang N, Han Q, Niu X (2013) A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. *Signal Process* 93(11):2986–3000. <https://doi.org/10.1016/j.sigpro.2013.03.031>
29. Sirichotedumrong W, Kiya H (2019) Grayscale-based block scrambling image encryption using YCbCr color space for encryption-then-compression systems. *APSIPA Trans Signal Inf Process* 8:e7. <https://doi.org/10.1017/ATSIP.2018.33>
30. Akhshani A, Akhavan A, Lim S-C, Hassan Z (2012) An image encryption scheme based on quantum logistic map. *Commun Nonlinear Sci Numer Simul* 17(12):4653–4661. <https://doi.org/10.1016/j.cnsns.2012.05.033>
31. Liu H, Jin C (2017) A novel color image encryption algorithm based on quantum chaos sequence. *3D Res* 4 8(1). <https://doi.org/10.1007/s13319-016-0114-7>
32. Zhou N, Chen W, Yan X, Wang Y (2018) Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system. *Quantum Inf Process* 17(6):137. <https://doi.org/10.1007/s11128-018-1902-1>
33. Liu X, Xiao D, Xiang Y (2019) Quantum image encryption using intra and inter bit permutation based on logistic map. *IEEE Access* 7:6937–6946. <https://doi.org/10.1109/ACCESS.2018.2889896>

34. Pandya A, Pandey P (2018) Comparative analysis of encryption techniques. *Int Res J Eng Technol* 05(03): 2010–2012
35. Younes MAB (2019) A survey of the most current image encryption and decryption techniques. *Int J Adv Res Comput Sci* 10(1):9
36. Patel S, Vaish A (2020) A systematic survey on image encryption using compressive sensing. *J Sci Res* 64(1):291–296
37. Rachid AML, Chandan A, Surya V, Krishna K, Ram M, Manish K (2020) Review of image encryption techniques. *IOSR Journal of Computer Engineering (IOSR-JCE)* 22(1):31–37
38. Kumari M, Gupta S, Malik A (2020) A superlative image encryption technique based on bit plane using key-based electronic code book. *Springer Multimed Tools Appl* 79:33161–33191. <https://doi.org/10.1007/s11042-020-09627-6>

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Affiliations

Manju Kumari¹ • Shailender Gupta¹

Shailender Gupta
shailender81@gmail.com

¹ Electronics Engineering Department, J.C.Bose University of Science and Technology YMCA, Faridabad, India