[1]Shilpa M. Satre
[2]Dr. Bharti Joshi

Quantum Image Cryptography of Continuous Chaotic Maps by Using Pixel Shuffeling

Abstract: - Images are important data carriers because, compared to text data, they are harder to transfer or store securely and include higher volumes and redundancies of digital data. Images can be shielded against a variety of risks with security, including eavesdropping and illegal copying and alteration. Because of the potential quantum risk to the existing cryptographic encryption methods and the quick advancement towards the development of quantum computers, quantum image encryption algorithms have recently drawn increasing amounts of attention. The majority of quantum image encryption techniques such as diffusion and scrambling, involve two separate rounds. In this model, the three different chaotic maps are used separately for scrambling the images to determine the performance of the quantum image cryptography with different combination of the model. At first, the hash256 algorithm is used for generating the quantum key and the forward diffusion takes place for diffusing the first pixel to final pixel of the input image information. Then, the three different chaotic maps such as pixel permutation, Chen attractor and Lorenz attractor are used for scrambling the input image. Finally, the bit-level permutation and backward diffusion process are considered for the scrambled image. For evaluating the performance of the quantum image cryptography based on the three different chaotic maps, the NPCR, UACI, Entropy, SSIM, correlation characteristics and histogram analysis are determined. The attained NPCR, UACI, Entropy and SSIM of the CASIA2 dataset for Lorenz attractor are improved than the pixel permutation and Chen attractor. Thus, from the attained values, the Quantum Image Cryptography Based on Continuous Chaotic Map such as Lorenz attractor performs better for the statistical and differential analysis than the other chaotic maps.

Keywords: Hash256, Chen attractor, Lorenz attractor, Quantum cryptography, chaotic map.

I. INTRODUCTION

Cryptosystems are associated with chaotic systems that have recently attracted a lot of attention, especially because of their possible application regarding data security. Desirable characteristics of chaotic systems include mixing property, ergodicity, and sensitivity to initial circumstances and factors [1]. Furthermore, personal computers and microprocessors may easily build chaotic systems. Chaotic cryptosystems are often faster and less expensive than many standard cyphers, which makes them more suitable for encrypting multimedia data [2]. Chaotic cryptosystems have gained recognition as a viable substitute for conventional cryptographic algorithms due to the majority of the previously described characteristics. Numerous encryption approaches based on chaos have been developed, motivated by the minor similarities between cryptosystems and chaotic systems. To obtain possible widespread functions, cryptosystems still need to address weaknesses in the majority of the designed schemes.

A chaos-based algorithm typically has two main phases: the diffusion and the permutation phase. The plain image's pixel locations are changed using a chaotic map during the permutation phase [3]. The permutation phase is completed and a sufficient amount of large key space is provided by the basic Arnold transform with keys. A slight alteration in a single pixel of the plain image results in an entirely new cipher image due to the diffusion stage utilisation of chaotic sequences to change the values of the shuffled image's pixels [4]. The specified cryptosystem's uncertainty and complexity were enhanced by chaotic sequences that is generated by the quantum chaotic map, which also accomplished the diffusion stage [5]. To enhance security, the diffusion-permutation algorithm should have a wide key space and a long periodicity of permutation. Numerous researchers are investigating advanced chaos-based algorithms with huge key spaces and effective diffusion and permutation strategies in order to achieve this goal [6]. Given the global cryptanalysis of digital image encryption techniques, there are two primary reasons for the existing algorithm is insecure.

*[1]*Shilpa M. Satre, Research Scholar, Dept. of Computer Engineering, D. Y. Patil deemed to be University, Ramrao Adik Institute of Technology, Nerul, Mumbai, Maharashtra 400706 India; Dept. of Information Technology, University of Mumbai, Bharati Vidyapeeth College of Engineering, Navi Mumbai, Maharashtra 400614 India, shilpamshelar.3184@gmail.com*
[2]Dr. Bharti Joshi, Professor, Dept. of Computer Engineering, D. Y. Patil deemed to be University, Ramrao Adik Institute of Technology, Nerul, Navi Mumbai, Maharashtra 400706 India, bharti.joshi@rait.ac.in

Firstly, the encryption scheme's chaotic system is not sufficiently secure. There are reports that certain dynamics of chaotic encryption systems are insufficiently complex, increasing the likelihood that they will be estimated or detected [7]. Secondly, there are security flaws in the encryption algorithm structure that make it vulnerable to assaults by cryptanalysis algorithms. For instance, the process of generating a chaotic key sequence is not dependent on plaintext, which makes plaintext attacks easy to launch against them [8]. The main factor is that identical keys exist in the cryptosystem yet the encryption procedure operates in plain images independently. Furthermore, the image cryptosystem computational complexity and its hardware technological development are not given as much concern [9]. Additional research should be done on the aforementioned components, since they are crucial to improving image encryption algorithm from theoretical to practice. Therefore, the innovative proposed model is built taking into account the aforementioned shortcomings of the current methodologies. The proposed framework takes the place of continuous chaotic maps like the Lorenz and Chen attractors as well as the actual pixel permutation found in chaotic theory. Major contributions of the proposed model are

- Quantum Image Cryptography Based On Continuous Chaotic Maps is designed and implemented in this model
- Hash 256 algorithm is used for generating the 256 bit secret key for encrypting the image to secure digital media
- Forward diffusion is employed in input image to diffuse the data from the initial pixel to final pixel.
- For pixel permutation, the Chen attractor and Lorenz attractor are used separately for pixel-level permutation.
- For permuting the bits in the cipher image, the bit-level permutation is employed to swap columns of the pixels.
- Backward diffusion is employed to bit-level permutation image for diffuse data from the final pixel to the initial pixel.

The following portions of the paper are organized as follows, section 2 reviews various articles related to the Quantum Image Cryptography Based on Chaotic Maps. Section 3 and 4 illustrates the proposed methodology and experimental outcomes obtained from the model. Section 5 concludes the entire designed model.

II. LITERATURE REVIEW

Many research works related to the Image Cryptography are studied and some of the articles are reviewed with the pros and cons of the designed model.

An image segmentation encryption algorithm based on hybrid chaotic system was introduced by Man, Z et al [10]. An efficient technique for maintaining the privacy of digital images was image encryption. An encryption algorithm for segmenting images based on a hybrid chaotic system was presented in this article. A key pool was generated using a 4-D hyperchaotic system by first iterating a Quantum Cellular Neural Network (QCNN) to produce a chaotic sequence, which was subsequently jumbled. Second, QCNN that use various beginning values and chaotic pointers produced by 3-D chaotic systems were used to access the key pool and retrieve the keys for image segmentation, diffusion, and scrambling. Then, using the chaotic segmentation approach, two blocks constitute the plain image and made scrambled by exchanging pixels within and between blocks. Furthermore, when joining the image blocks, the cipher-image was acquired through dynamic diffusing, and two blocks are statically diffused. This approach was more efficient when a key pool was used, and the cipher-image pixel correlation was decreased when chaotic segmentation was used and has a high degree of security, which was faster and has a high sensitivity, according to the simulation findings and performance analysis.

Comparison of the performance of image encryption algorithms based on quantum-chaos and chaos was developed by Kumari, M., & Gupta, S [11]. Digital image encoding was a far more involved and demanding process. Numerous studies have demonstrated that a significant degree of randomness was provided by chaotic logistic map-based mathematical equations. Therefore, in order to produce highly unpredictable cypher images, chaotic logistic maps-based image encryption techniques commonly referred to as chaos techniques were used. On the other hand, to maintain real-time communication, time consumption needs to be as minimal as feasible. Presently, modern quantum-based advanced encryption techniques are more efficient and secure due to their vast key space, reduced temporal complexity, and unpredictability. Quantum mechanics' uncertainty concepts are used to logistic maps to provide encryption based on quantum chaos. The comparison of chaotic and quantum chaos-based image encryption techniques was the primary objective of this article. The comparison was based on several security threat evaluations, and the execution was done using MATLAB 2016a software. Highly secure image encryption can be achieved by using quantum chaotic bit plane scrambling techniques, which provide better outcomes with regards to effectiveness, performance, and reliability, according to studies and experimental results.

DNA coding and quantum chaotic map-based image encryption technique was designed by Zhang, J., & Huo, D [12]. Currently, there are many different DNA-encoded image encryption algorithms that have been developed. In these algorithms, to generate image pixel diffusion, Four DNA base pairs are used to encode the image pixel values. Still, most methods for selecting the DNA encoding principles remain constant. This study found that the developers provide an innovative encryption technique that combines the Lorenz chaotic map, DNA coding, and the quantum chaotic map. It employs 4 DNA base pairs to select 8 different DNA addition and XOR rules dynamically, in addition to eight distinct DNA encoding rules. Security as well as dependability have greatly improved as a result of this tactic. This approach exhibits a high security level and also have to withstand many types of attacks, including statistical and brute-force attacks, as demonstrated by experimental simulations and the findings of correlations, number of pixels change rate (NPCR) and histograms assessments.

Image encryption technique constructed using a novel parallel DNA and chaotic map coding was developed by Zhu, S et al [13]. This study developed a 1-dimensional fractional chaotic map that is then utilized in the development of a parallel DNA coding image encryption system. Combining a fraction operation and a sine map yields the new chaotic system's mathematical model. This chaotic system was more suited for information encryption applications since it have superior chaotic properties and a wider range of chaotic parameters than the older one-dimensional chaotic systems. Furthermore, a parallel DNA coding-based image encryption technique was developed, addressing the drawback of popular DNA coding-based image encryption algorithms. Algorithms for encryption and decryption operate much more quickly. To ensure that the algorithm was resistant to a chosen-plaintext attack, the cryptosystem's initial key was designed to be associated with the plaintext image's SHA-3 hash value. The results of security analyses and simulation experiments provided that the identified image encryption method have strong robustness against attacks involving noise and data loss, as well as good encryption performance and minimal time overhead. These factors indicated image encryption method have excellent possibility for usage in applications involving secure communication.

An encryption technique for color images that utilizes DNA computing and hyper-chaos was introduced by Malik, M. A et al [14]. This work presents the invention of a unique method with high plaintext sensitivity that combines DNA computing with a hyper chaotic dynamic system. To cut expenses, distinct key streams have been produced from the same chaotic data acquired from the chaotic dynamical system's iterations by a selection process utilising a tent map. Following their separation from the input colour image, the three channels get blurred and distorted. To begin with, these channels are decimal-level diffused and are subsequently permuted. These channels are also used for DNA encoding. Additionally, DNA level diffusion is carried out to boost the image's degree of unpredictability even more. The final step in creating the cipher image is to translate the DNA encoded image into decimal. The demonstrated scheme's robustness is strongly demonstrated by both the security analysis and the experimental findings.

Most of the existing techniques used for image encryption performs better but some of the drawbacks are still required to be solved. QCNN [10] challenges are High computational requirements, Needs large amount of labelled data, large memory footprint, Interpretability challenges, Limited effectiveness for sequential data and Tend to be much slower [11]. Low key space and lower sensitivity to starting conditions [12]. There are flaws in the chaotic map's resistance to differential attacks because its initial state is independent of the plain image. Certain encryption methods failed to recover the plain image when the encrypted image was assaulted using noise and data cut [13]. Due to the non-flat histogram of the encrypted image, certain methods are vulnerable to statistical assaults [14].

III. PROPOSED METHODOLOGY

Multimedia data comprised of images and video is being used more and more, due to the Internet's quick expansion and advancements in digital multimedia technology. Since lots of digital images hold sensitive data, including personal and confidential details, image encryption technique research has gained a lot of attention recently. Conventional image encryption techniques like DES and AES typically encrypt the image data. But in modern times with strong computational power, resistance to differential attacks and key security are major difficulties. Chaotic systems provide good cryptographic properties like randomness, ergodicity, sensitivity and aperiodicity to system parameters and beginning values. Hence, in this model, Chaos theory and quantum mechanics combined with image encryption method is developed.

Figure 1 illustrates the Overall process flow of the proposed quantum image cryptography on the basis of continuous chaotic maps. In this designed model, the plain image is encrypted with the hash 256 key bit. Then, Using cipher text feedback, the image is conducted for forward diffusion that the input image data diffuses from the initial to the final pixel. After forward diffusion, the Chen attractor, Lorenz attractor and pixel permutation are used separately for image permutation for enhancing the security of the images by swapping the pixels of an image. Then, the bit permutation is processed for three permutation techniques to perform bit-level permutation, where the pixel column is swapped. Finally, the bit-level permutated images are considered for backward diffusion to diffuse from the final to the initial pixel. This encrypted cipher image can be considered as a secured image from any attacks. For decrypting the cipher image, the entire process of encryption is reversed and the hash 256 key is employed to decrypt the image to attain the original plain image.

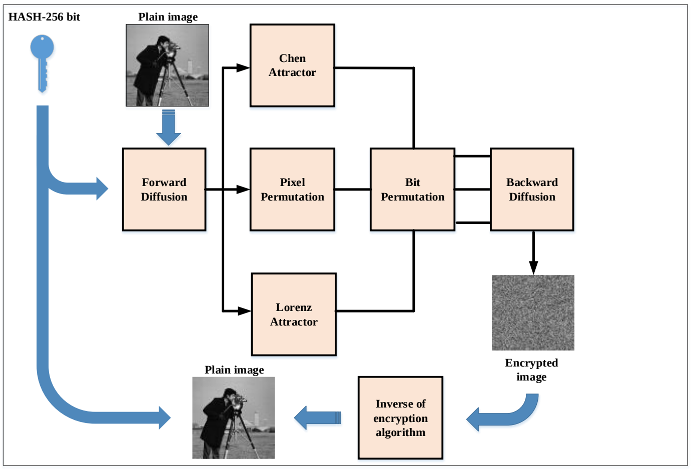


Fig. 1 Encryption and decryption process of the proposed model.

A. Quantum Image Cryptography Based on Continuous Chaotic Maps

A chaotic picture cryptosystem built upon the "diffusion-permutation-diffusion" framework. By generating a chaos-based cypher text feedback diffusion method, a plaintext correlation approach serves for enhancing security. For the proposed quantum image cryptosystem, Figure 1 presents the block drawings for the encryption and decryption processes, respectively. More intricate dynamics and quantum features can be found in the quantum logistic map. By linking the harmonic oscillator path to the dissipative quantum system, one can generate a quantum logistic map and quantum correction.

$$\begin{cases} a_{n+1} = v(a_n - |a_n|^2) - vb_n \\ b_{n+1} = -b_n e^{-2\beta} + e^{-\beta} v[(2 - a_n - a_n^*)b_n - a_n c_n^* - a_n^* c_n] \\ c_{n+1} = -c_n e^{-2\beta} + e^{-\beta} v[2(1 - a_n^*)c_n - 2a_n b_n - a_n] \end{cases} \tag{1}$$

Where, $a =< x >, b =< \delta x \dagger \delta x >, c =< \delta x \delta x >, \beta$ is represented as the dissipation parameter and v is the control parameter. The conjugate complex values of a_n and c_n are represented as a_n^* and c_n^*, respectively. In general, a_n^*, c_n^* , b_n are also complex numbers and both a_n and c_n are plurals. Chaotic state is defined in Equation (1) if $a_n \in [0, 1]$, $b_n \in [0, 0.1]$, $c_n \in [0, 0.2]$, $\beta \in [6, +\infty]$, and $v \in [0, 4]$.

1) Secret key

The cryptosystem secret key consists of a 256-bit hash and 3 values for initiating the quantum chaos of the plain image [15]. The unique key space are {hash256, $a(0)$, $b(0)$, $c(0)$}, whereas $a(0)$, $b(0)$, $c(0)$ are represented as the three initial values of equation (1) and hash256 represents the 256-bit hash value. The following describes the specific actions taken by the encryption machine:

Step 1: Sequences of quantum chaotic encryption

The initial values of the quantum chaos are dynamically disturbed by the plaintext hash value in order to defend against differential attacks. As a result, the matching key sequences for various plaintexts are not set. Dynamic disturbance is used in the following manner:

$$\begin{cases} a'(0) = a(0) + \sum_{i=1}^{5} h_i \times 10^{-5} + \frac{h_6 \oplus h_7 + \cdots \oplus h_{10}}{10^8} \\ b'(0) = b(0) + \sum_{i=1}^{15} h_i \times 10^{-5} + \frac{h_{16} \oplus h_{17} + \cdots \oplus h_{20}}{10^8} \\ c'(0) = c(0) + \sum_{i=21}^{25} h_i \times 10^{-5} + \frac{h_{26} \oplus h_{27} + \cdots \oplus h_{32}}{10^8} \end{cases} \tag{2}$$

Where the quantum chaos's updated initial values following the disturbance are represented by the values as,$a'(0), y'(0), z'(0)$. It occurs without mentioning that the modified initial values will vary depending on the plain image. The chaotic sequence is then pre-processed after that. It is commonly decided to remove the prior l=300 iterative sequences in order to prevent the detrimental transitory effect of chaotic mapping. The quantum logistic chaotic map produces the following diffusion sequence:

$$\begin{cases} kd_1 = mod(fix(a_i \times 10^8), 256) \\ kd_1 = mod(fix(z_i \times 10^{10}), 256) \end{cases} \tag{3}$$

Where the length of sequence is extensive as the image of $H \times W$size, and i = 1, 2. . . $H \times W$ is utilized to encryption of forward and backward diffusion, respectively. In a similar manner, the permutation sequence is produced by

$$\begin{cases} [value_1, kp_1] = sort\big(y(l{:}\,H)\big) \\ [value_2, kp_2] = sort\big(y(H + l{:}\,H + W)\big) \\ [value_3, kp_3] = sort\big(y(H + W + l{:}\,H + 9W)\big) \end{cases} \tag{4}$$

Where, the terms kp_1,kp_2 and kp_3 refers to the pixel rows, columns, and bit columns index sequences that the sort operation produces. Following the elimination of l=300, y represents the quantum chaotic map's sequence. The overall length is denoted as $H + 9W$, while the index sequences lengths are H, W and $8W$. The numerical sequences $value_1$, $value_2$, and $value_3$ are sorted.

Step 2: Forward diffusion

The forward diffusion process involves using cipher text feedback is performed to the input image to diffuse the data from the initial to the last pixel [16]. The encryption process of first pixel is defined as follows

$$C_1(i) = mod\big(mod\big(p(1)\big) + kd_1(1), 256\big) \oplus kd_1(1) + C_0, 256 \tag{5}$$

Where, C_0 is represented as the forward diffusion initial key have a value ranges from 0 and 255, C1 is represented as the forward diffusion output image, p is denoted as the given plain image, and quantum chaos produced first key sequence is denoted as kd_1. The encryption procedure for $C_1(i)$ pixels is stated as follows:

$$C_1(i) = mod\big(mod\big(p(i)\big) + kd_1(i), 256\big) \oplus kd_1(i) + C_1(i-1), 256 \tag{6}$$

Where For each repetition of i = 2, 3. . . HW, the diffused cipher text encrypted pixel values represented as C_1 are retrieved.

Step 3:

a. Pixel permutation

The following describes the permutation of the pixel position of picture C1 following forward diffusion encryption:

$$C_2(x, y) = swap(C_1\big(mg_1(x)\big), C_1(x, y) \tag{7}$$

The image following pixel-level permutation is C_2, and the operation for exchanging element values is represented by the variables *i = 1, 2, . . . , H, j = 1, 2, . . . , W,* swap (·).

b. Chen Attractor

A novel chaotic attractor from the following system has just been discovered in the quest for anticontrol of chaos, also known as chaotification, which is the process of turning a nonchaotic system chaotic [17].

$$\begin{cases} \dot{a} = x(b - a) \\ \dot{b} = (z - x)a - ab + zb \\ \dot{c} = ab - yc \end{cases} \tag{8}$$

Where, a, b, c are the state variables of the system and x, y, z are the parameters of the system [18]. The Chen system exhibits chaotic behaviours when the parameters are in the chaotic zone. If not, it is stable and returns to a stable equilibrium regardless of the beginning situation.

c. Lorenz Attractor

Due to the deterministic nature of the Lorenz system, it is theoretically possible to predict the future values of the variables as they vary over time provided by the exact beginning values [19]. Lorenz demonstrated that if you begin this model by choosing some values for x, y, and z, and then do it again with just slightly different values, then you will quickly arrive at fundamentally different results

$$\begin{cases} \frac{da}{dt} = \sigma(a-b) \\ \frac{db}{dt} = va - ac - b \\ \frac{dc}{dt} = ab - yc \end{cases} \tag{9}$$

Where, a, b, c, t are variables which take real values and parameters σ, v, y are positive real constants. σ and y are called Prandtl and Rayleigh Number. Early chaos researchers used this attractor as their symbol, and Lorenz 1972 article introduced the metaphor based on the attractor's resemblance to butterfly wings.

Step 4: Bit permutation

Following pixel permutation, bit-level permutation is applied to the image C2, it can be expressed in the following manner:

$$C_3(i,j) = swap\left(C_2\left(:, kp_3(k)\right), C_2(:, k)\right) \tag{10}$$

Where, after bit-level permutation the image is represented as C_3, k = *1, 2. . . 8W*. Keep in mind that the bit-level picture is extended in the 2nd cycle of permutation based on the row-invariant principle; therefore, the permutation applies to the extended column permutation.

Step 5: Backward diffusion

Backward diffusion uses ciphertext feedback for diffusing received image data from the final to the first pixel, in contrast to forward diffusion. With the complementary qualities of forward and backward, it further improves the characteristics of confusion and dissemination.

When *i=HW*,

$$C(i) = mod(mod(C_3(i) + kd_2(i), 256) \oplus kd_2(i) + C_{end}, 256) \tag{11}$$

Then, if *i=HW*-1… 2, 1,

$$C(i) = mod(mod(C_3(i) + kd_2(i), 256) \oplus kd_2(i) + C(i+1), 256) \tag{12}$$

Where, $C_{end}$is denoted as the initial key value of backward diffusion, C is represented as the final ciphertext image and Quantum chaos produces the encryption sequence is kd_2.

Decryption machine

Two points need to be noted in order to decrypt the image, the first is that each module's operating sequence needs to be switched. Sequential execution is recommended for the bit permutation, pixel permutation, forward diffusion, and backward diffusion. Additionally, the diffusion process reverses the sequence of pixel iterations. An IoT secure communication situation in general can make use of this image cryptosystem. Digital image storage, display, and transmitting capabilities are provided by embedded terminals on both the sending and receiving ends. The digital image is encrypted at the transmitting end to improve information confidentiality and prevent hackers and criminals from stealing data sent over the network. With the right key, the original plaintext data can be successfully restored once the ciphertext picture has been obtained by the authorised user on the receiving end. Thus, a variety of IoT secure communication scenarios can make use of this proposed image cryptosystem.

IV. RESULTS AND DISCUSSION

Implementation of the Quantum Image Cryptography based On Continuous Chaotic Maps such as Chen attractor and Lorenz attractor are done and evaluated for performance. The MATLAB R2018a platform is used for evaluating the performance of the model with the system configuration of Intel i5 10th processor with 2.50GHz and 32GB RAM. For designing the model in Matlab, the cameraman and peppers image are used as the input image and the first step is quantum chaotic encryption is done with the hash 256 key. Then, the forward diffusion takes place for diffusing the pixels in the image. After the forward diffusion, the pixel permutation, Chen attractor and Lorenz attractor are used separately for permuting the image. The images from the three chaotic maps are bit permutated and backward diffused. To find the performance of the model, the third stage of the process such as pixel permutation is used as the basic quantum chaotic map and by replacing the continuous chaotic map such as Chen attractor and Lorenz attractor for the other two models.

A. *Experimental results for Quantum chaotic image cryptosystem*

This research presents comparisons between these three methods using parameters for image encryption. The proportion of different pixel count between the encrypted and the plane image are evaluated with the differential and statistical analysis [20]. Differential analysis is a method of decision-making that analyses the net outcomes of two options after examining the advantages of each. For differential analysis, the Unified Average Changing Intensity (UACI) and Net Pixel Transformation Rate (NPCR) are evaluated. Statistical analysis for images are evaluated for the patterns and trends from the image. For evaluating the statistical analysis, the Entropy, Histogram Analysis, Correlation Coefficient and Structural Similarity Index Measure (SSIM) are evaluated.

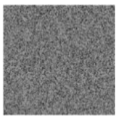
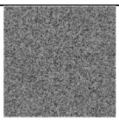
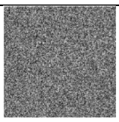
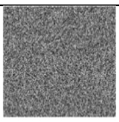
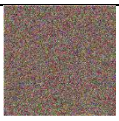
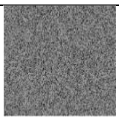
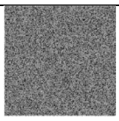
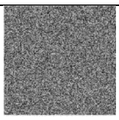
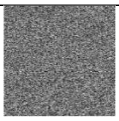
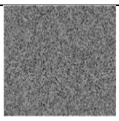
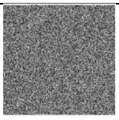
Quantum chaotic image cryptosystem with pixel permutation					
Input image	**Forward Diffusion**	**Pixel Permutation**	**Bit Permutation**	**Backward Diffusion**	**Inverse Encryption**
					
					
Quantum chaotic image cryptosystem with chen Attractor					
Input image	**Forward Diffusion**	**Chen attractor**	**Bit Permutation**	**Backward Diffusion**	**Inverse Encryption**
					
Quantum chaotic image cryptosystem with Lorenz Attractor					
Input image	**Forward Diffusion**	**Lorenz attractor**	**Bit Permutation**	**Backward Diffusion**	**Inverse Encryption**
					

Fig. 2 Quantum chaotic image cryptosystem with pixel permutation, Chen attractor and Lorenz attractor.

Figure 2 illustrates the image cryptosystem based on quantum chaotic with three permutation techniques such as standard pixel permutation, Chen attractor and Lorenz attractor. The above illustrated table determines input image, forward diffusion, pixel permutation, Chen attractor, Lorenz attractor, Bit permutation and Forward diffusion. The Inverse encryption is process of reversing all the algorithms that are implemented on the encryption process.

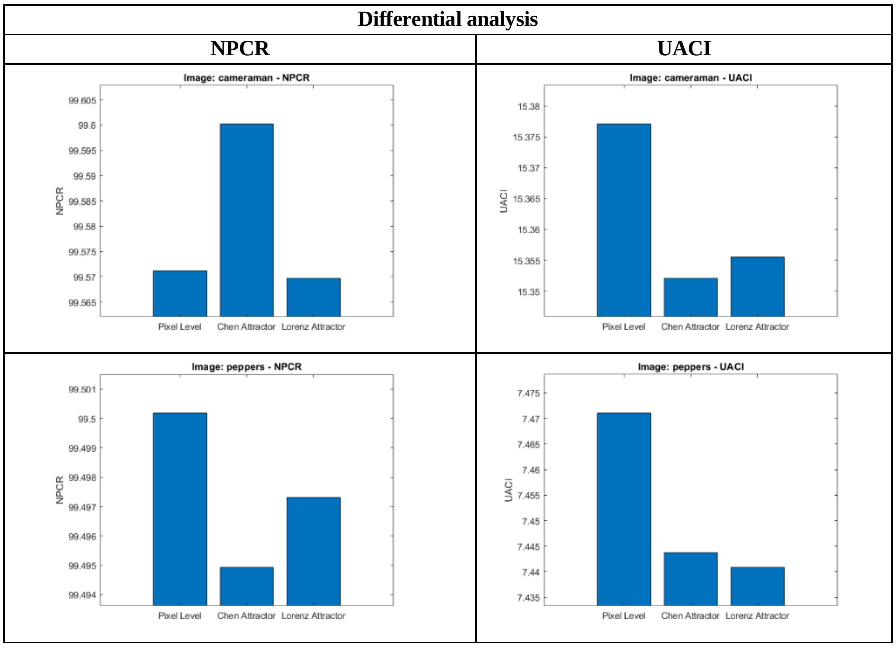


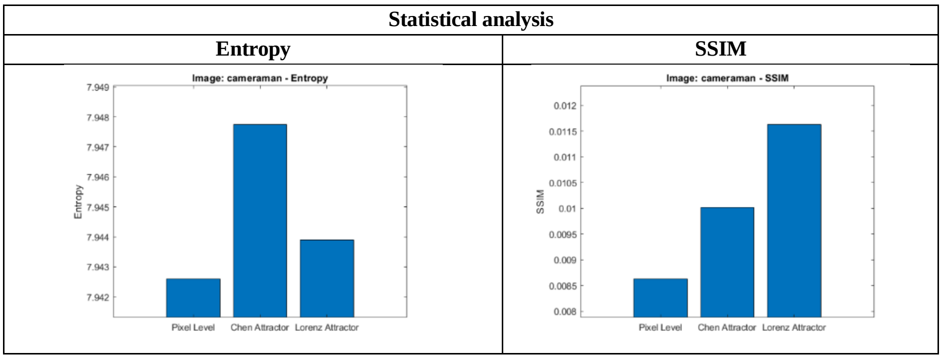
Fig. 3 Comparison of NPCR and UACI for pixel permutation, Chen Attractor and Lorenz attractor.

Figure 3 illustrates the differential analysis for three chaotic maps such as pixel permutation, Chen Attractor and Lorenz attractor. The proportion of various pixel counts between the encrypted and planar images is indicated by NPCR, while the average intensity variance between the two images is stated by UACI.

Table 1. Comparison values of NPCR and UACI of cameraman and peppers.

Images	Name of Measures	Pixel Permutation	Chen Attractor	Lorenz Attractor
Cameraman	NPCR	99.57122803	99.60021973	99.56970215
	UACI	15.37708357	15.35210105	15.35551782
Peppers	NPCR	99.50018989	99.49493408	99.49730767
	UACI	7.471078777	7.443733298	7.440880337

Table 1 illustrates the comparison values of NPCR and UACI for cameraman and peppers. The chaotic map used for cryptography such as pixel permutation, Chen attractor and Lorenz attractor. From this evaluation, the cameraman is grey image and the peppers is a colour image. The Chen attractor NPCR and UACI values are better for the cameraman (Grey level image), whereas the NPCR value of the pixel permutation and UACI value of Lorenz attractor are better for pepper (RGB image).



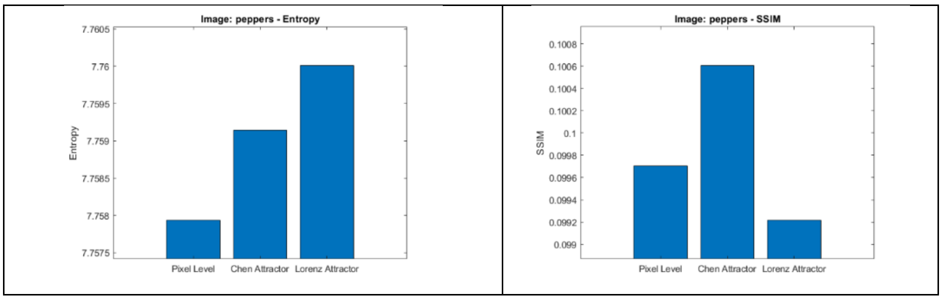


Fig. 4 Comparison of Entropy and SSIM for pixel permutation, Chen Attractor and Lorenz attractor.

Figure 4 illustrates the comparison of entropy and SSIM for cameraman and peppers image with the three models such as pixel permutation, Chen Attractor and Lorenz attractor. One statistical tool for characterizing the texture of an input image is entropy. A technique for forecasting the overall quality of cinematic pictures and digital television, along with other types of digital videos and images, is the structural similarity index measure (SSIM). SSIM is a tool for evaluating two images' similarity.

Table 2. Entropy and SSIM comparison of cameraman and peppers.

Images	**Name of Measures**	**Pixel Permutation**	**Chen Attractor**	**Lorenz Attractor**
Cameraman	Entropy	7.942598166	7.947750673	7.943907202
	SSIM	0.008628907	0.010019535	0.011629538
Peppers	Entropy	7.757935316	7.759145906	7.760011573
	SSIM	0.099702309	0.100606753	0.099216679

Table 2 illustrates the comparison values for Entropy and SSIM of cameraman and peppers with three models such as pixel permutation, Chen Attractor and Lorenz attractor. From this evaluation, the entropy of the Chen attractor is better for cameraman and Lorenz attractor for peppers. Likewise, the SSIM of the Lorenz attractor is better for cameraman and Chen attractor for Peppers.

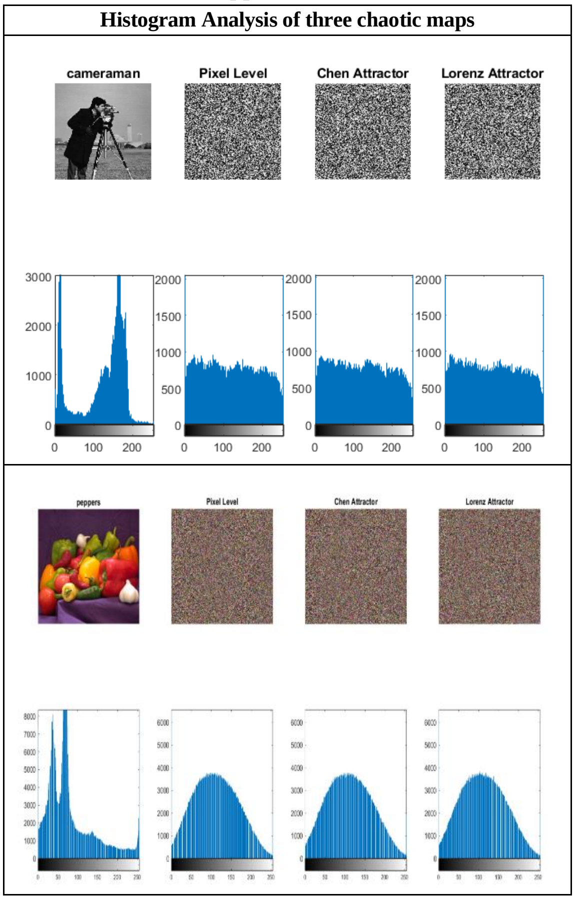


Fig. 5 Histogram Analysis of three chaotic maps.

Figure 5 illustrates the histogram analysis of the three chaotic maps such as pixel permutation, Chen Attractor and Lorenz attractor. The graphical representation of a digital image's tonal distribution is achieved through the use of an image histogram. Each tonal value's pixel count is plotted. A viewer can evaluate the complete tonal distribution in a glance by glancing at the histogram for a given image. Based on this evaluation, the original image histogram of cameraman and peppers is varied based on the intensity of the original image pixels. After the conversion of chaotic maps and pixel diffusion, the histogram of the images are linearized with the equal pixel level intensity. This attainment of the encryption image results that the encrypted images are tamper proof and secure for transmission. For cameraman and pepper image, the histogram of Lorenz attractor is plotted better in linear manner than the Chen attractor and pixel permutation.

Correlation properties between Cameraman and Pepper image

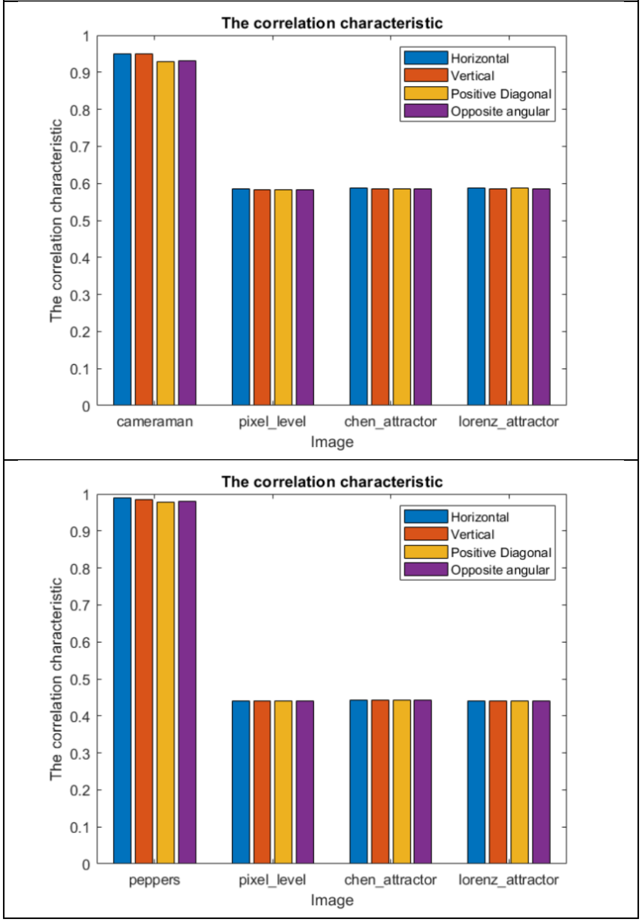


Fig. 6 Correlation properties between the Cameraman and Pepper image based on Horizontal, Vertical, Diagonal and Angular Directions.

Figure 6 illustrates the Correlation properties between the Cameraman and Pepper images according to the angular, horizontal, vertical, and diagonal directions for the three models such as Chen Attractor, Lorenz attractor and pixel permutation. Measurement and description of the relation between two or more variables are done statistically using correlation. Correlations have three important characteristics such as the form (shape), direction, and the degree (strength) of the relationship between two or more variables. Correlation-based relationship direction clarifies the nature of the two variables and can be either positive or negative. When two variables are positively correlated, they usually transfer in the same direction. When one variable rises, the other usually does too. When one drops, the other usually decreases as well. Likewise, in a negative relationship the variables typically follow opposite trends: when one rises, the other usually falls, and vice versa. Then, a relationship's form or shape describes how straight or curved the relationship is. Lastly, the degree (strength) of the association between two variables is determined by a correlation coefficient.

Table 3. Correlation Characteristics for Horizontal, Vertical, Diagonal and Angular Directions of original image and different cipher images.

Correlation → **Name of Ciphers** ↓	**Vertical Direction**	**Horizontal Direction**	**Positive Diagonal Direction**	**Opposite Angular Direction**
Cameraman (Plain Image)	0.9488	0.9503	0.9282	0.931
Pixel Permutation (Cameraman)	0.5846	0.583	0.5828	0.5831
Chen Attractor (Cameraman)	0.5867	0.5849	0.5842	0.5849
Lorenz Attractor (Cameraman)	0.5877	0.5854	0.5867	0.5844
Peppers (Plain Image)	0.9904	0.9849	0.9788	0.9801
Pixel Permutation (Peppers)	0.441	0.4412	0.4411	0.4414
Chen Attractor (Peppers)	0.4422	0.442	0.4426	0.442
Lorenz Attractor (Peppers)	0.4407	0.4412	0.4414	0.441

Table 3 illustrates the Correlation properties of Cameraman image for Vertical, Horizontal, Diagonal and Angular Directions with Pixel Permutation, Chen Attractor and Lorenz Attractor. One can use correlations as a tool in making predictions and are able to assume that two variables will remain correlated in the future if they have been shown to remain the same in the past. From the evaluation of correlation coefficient for different direction of the cameraman and pepper image, the correlation coefficient of the Chen attractor for the cameraman and pepper image is equal for all the directions.

B. Experimental analysis CASIA2 dataset

For analysing the designed quantum chaotic cryptosystem more effective, the CASIA2 [21] dataset is used for evaluation that consist of 7493 images of environmental creatures. The evaluation the proposed model consist of NPCR, UACI, Entropy, Histogram Analysis, Correlation Coefficient and SSIM are evaluated. These evaluated values of 7493 images are considered average for evaluating the performance of the quantum chaotic cryptosystems.

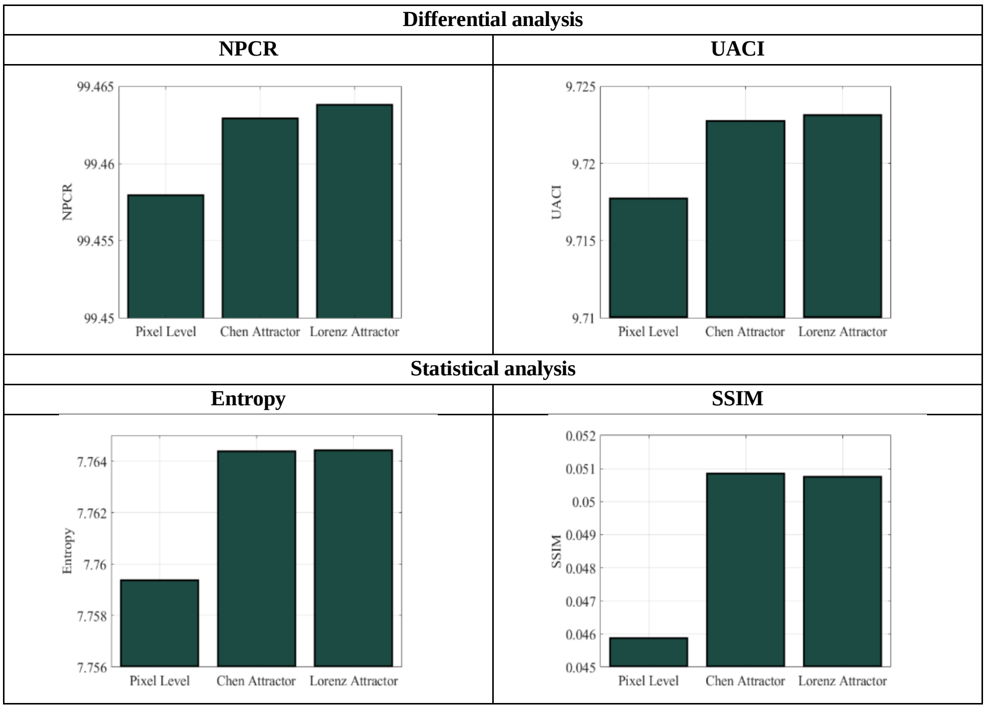


Fig. 7 Comparison of NPCR, UACI, Entropy and SSIM for CASIA2 dataset.

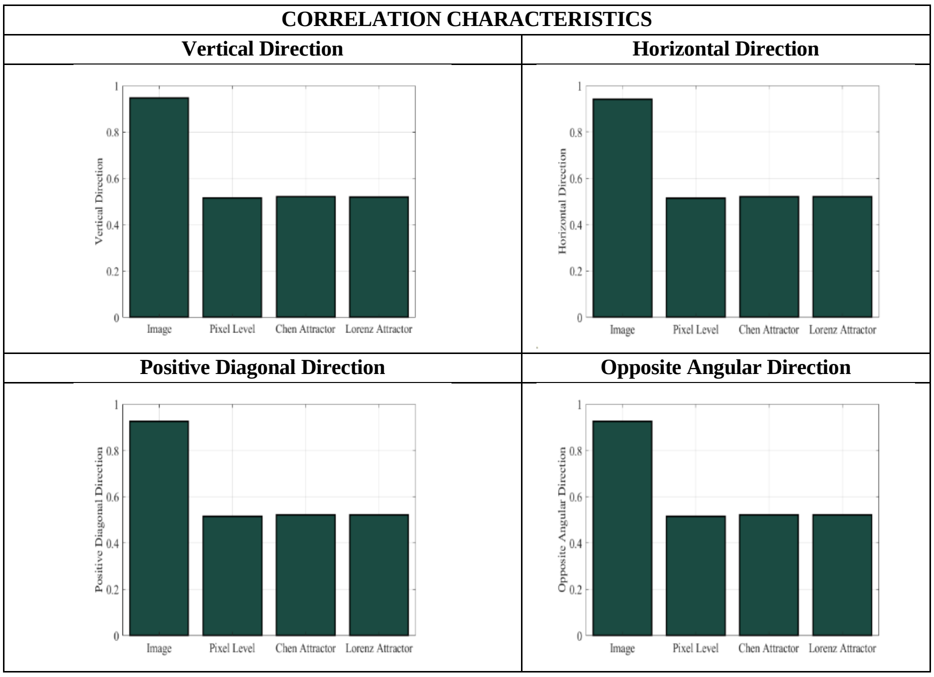
Figure 7 illustrates the comparison of NPCR, UACI, Entropy and SSIM for CASIA2 dataset are evaluated with the pixel permutation, Chen attractor and Lorenz attractor. The below table 4 illustrates the attained parameters of the 7493 Image Encryption.

Table 4. Comparison of 3 Approaches with Average of CASIA2 dataset Image Encryption Evaluation Measures.

Images	Name of Measures	Pixel Permutation	Chen Attractor	Lorenz Attractor
AVERAGE OF CASIA2 dataset	Entropy	7.759385174	7.764383836	7.764416446
	SSIM	0.045871678	0.050854076	0.050746304
	NPCR	99.45792798	99.46290476	99.46377914
	UACI	9.717727414	9.722741309	9.723135942

From this evaluation, the NPCR, UACI and Entropy of the Lorenz attractor for CASIA2 dataset are greater and the Chen attractor of SSIM are greater than the other encryption chaotic maps. Thus, from the evaluation of statistical and differential analysis of the 7493 images, the Lorenz attractor performs better encryption chaotic maps than the existing pixel permutation and Chen attractor.

Comparison of Correlation Characteristics for Vertical, Horizontal, Diagonal and Angular Directions with Pixel Permutation, Chen Attractor and Lorenz Attractor of CASIA2 dataset are illustrated at figure 8. The below table illustrates the attained values of the Correlation Characteristics for Average of CASIA2 dataset.


CORRELATION CHARACTERISTICS

Vertical Direction

Horizontal Direction

Positive Diagonal Direction

Opposite Angular Direction

Fig. 8 Comparison of Correlation Characteristics for Vertical, Horizontal, Diagonal and Angular Directions of CASIA2 dataset.

Table 5. Comparison of Correlation Characteristics for Average of CASIA2 dataset.

Correlation → **Name of Ciphers ↓**	**Vertical Direction**	**Horizontal Direction**	**Positive Diagonal Direction**	**Opposite Angular Direction**
AVERAGE OF CASIA2 dataset.	0.946609345	0.940827929	0.923906791	0.92480241
Pixel Permutation	0.515372	0.515486679	0.515358496	0.515430668
Chen Attractor	0.52040967	0.520429918	0.520417268	0.520423198
Lorenz Attractor	0.520315265	0.520299431	0.520330955	0.520343194

Table 5, From this evaluation, the Correlation Characteristics for Horizontal, Vertical, Diagonal and Angular Directions with Pixel Permutation, Chen Attractor and Lorenz Attractor of 7493 images are attained. The Chen attractor used of this chaotic maps has similar correlation characteristics for all the directions than the pixel permutation and Lorenz attractor. Based on the evaluation of the encryption chaotic maps such as Pixel Permutation, Chen Attractor and Lorenz Attractor with cameraman, peppers and CASIA2 dataset, the Lorenz attractor performs better for some of the evaluation metrics. Thus, the Lorenz attractor used in this model for scrambling the images performs better for quantum chaotic cryptography.

V. CONCLUSION

Implementation of the proposed model with different chaotic maps are achieved and determined for evaluating the performance of the quantum image cryptography based on continous chaotic maps. In this designed model, the cameraman, peppers and CASIA2 dataset are used for evaluating the three different continuous chaotic map combination. At first, the images of cameraman, peppers and CASIA2 dataset are encrypted using the Hash256 algorithm to create a secret key for the input image and then then the images are forward diffused by transferring the pixel information from first to last. These forward diffused images are scrambled using the pixel permutation and chaotic maps such as Chen attractor and Lorenz attractor. The determined scrambled images are bit level permutated and backward diffused for swapping and tranfserring the pixels of the scrambled images of the cameraman, peppers and CASIA2 dataset to make the process of quantum image cryptography more efficient and secure. For evaluating the performance of the three different combination of quantum image cryptography, the performance metrics such as NPCR, UACI, entropy and SSIM are evaluated for all the three scramblers such as pixel permutation, Chen attractor and Lorenz attractor. The attained NPCR, UACI, Entropy and SSIM values for the pixel permutation, Chen attractor and Lorenz attractor are 99.45792798, 99.46290476 and 99.46377914, 9.717727414, 9.722741309 and 9.723135942, 7.759385174, 7.764383836 and 7.764416446, 0.045871678, 0.050854076 and 0.050746304. From these evaluated values of the pixel permutation, Chen attractor and Lorenz attractor, the Lorenz attractor attains better performance metrics than the pixel permutation and Chen attractor. Thus, the quantum image cryptography based on Lorenz attractor performs better for the continuous chaotic map. In future, the designed Quantum image cryptography algorithm can be used to evaluate the encryption of image using the discrete chaotic map and this algorithm can determine a better image encryption than the continuous chaotic map.

ACKNOWLEDGMENT

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] M. Naseri, M. Abdolmaleky, A. Laref, F. Parandin, T. Celik, A. Farouk, and H. Jalalian, “A new cryptography algorithm for quantum images,” Optik, vol. 171, pp. 947-959, 2018.

[2] J. Wang, Y.C. Geng, L. Han, and J.Q. Liu, “Quantum image encryption algorithm based on quantum key image,” International Journal of Theoretical Physics, vol. 58, pp. 308-322, 2019.

[3] W.W. Hu, R.G. Zhou, S. Jiang, X. Liu, and J. Luo, “Quantum image encryption algorithm based on generalized Arnold transform and Logistic map,” CCF Transactions on High Performance Computing, vol. 2, pp. 228-253, 2020.

[4] N.R. Zhou, L.X. Huang, L.H. Gong, and Q.W. Zeng, “Novel quantum image compression and encryption algorithm based on DQWT and 3D hyper-chaotic Henon map,” Quantum Information Processing, vol. 19, pp. 1-21, 2020.

[5] M. Khan, and A. Rasheed, “A fast quantum image encryption algorithm based on affine transform and fractional-order Lorenz-like chaotic dynamical system,” Quantum Information Processing, vol. 21, no. 4, pp. 134, 2022.

[6] C. Li, and X. Yang, “An image encryption algorithm based on discrete fractional wavelet transform and quantum chaos,” Optik, vol. 260, pp. 169042, 2022.

[7] B. Abd-El-Atty, and A.A. Abd EL-Latif, “Applicable image cryptosystem using bit-level permutation, particle swarm optimisation, and quantum walks,” Neural Computing and Applications, 1-17, 2023.

[8] X. Song, G. Chen, and A.A. Abd El-Latif, “Quantum color image encryption scheme based on geometric transformation and intensity channel diffusion,” Mathematics, vol. 10, no. 17, pp. 3038, 2022.

[9] Z. Jiang, and X. Liu, “Image Encryption Algorithm Based on Discrete Quantum Baker Map and Chen Hyperchaotic System,” International Journal of Theoretical Physics, vol. 62, no. 2, pp. 22, 2023.

[10] Z. Man, J. Li, X. Di, and O. Bai, “An image segmentation encryption algorithm based on hybrid chaotic system,” IEEE access, vol. 7, pp. 103047-103058, 2019.

[11] M. Kumari, and S. Gupta, “Performance comparison between Chaos and quantum-chaos based image encryption techniques,” Multimedia Tools and Applications, vol. 80, pp. 33213-33255, 2021.

[12] J. Zhang, and D. Huo, “Image encryption algorithm based on quantum chaotic map and DNA coding,” Multimedia Tools and Applications, vol. 78, pp. 15605-15621, 2019.

[13] S. Zhu, X. Deng, W. Zhang, and C. Zhu, “Image encryption scheme based on newly designed chaotic map and parallel DNA coding,” Mathematics, vol. 11, no. 1, pp. 231, 2023.

[14] M.A. Malik, Z. Bashir, N. Iqbal, and M.A. Imtiaz, “Color image encryption algorithm based on hyper-chaos and DNA computing,” IEEE Access, vol. 8, pp. 88093-88107, 2020.

[15] R.I. Abdelfatah, “Quantum Image Encryption Using a Self-Adaptive Hash Function-Controlled Chaotic Map (SAHF-CCM),” IEEE Access, vol. 10, pp. 107152-107169, 2022.

[16] D. Wei, M. Jiang, and Y. Deng, “A secure image encryption algorithm based on hyper-chaotic and bit-level permutation,” Expert Systems with Applications, vol. 213, pp. 119074, 2023.

[17] F. Musanna, and S. Kumar, “Image encryption using quantum 3-D Baker map and generalized gray code coupled with fractional Chen’s chaotic system,” Quantum Information Processing, vol. 19, pp. 1-31.

[18] D.A.Q. Shakir, A. Salim, S.Q. Abd Al-Rahman, and A.M. Sagheer, “Image Encryption Using Lorenz Chaotic System,” Journal of Techniques, vol. 5, no. 1, pp. 122-128, 2023.

[19] A. Malik, S. Gupta, and S. Dhall, “Analysis of traditional and modern image encryption algorithms under realistic ambience,” Multimedia Tools and Applications, vol. 79(37-38), pp. 27941-27993, 2020.

[20] R. Santhiya Devi, R. John Bosco Balaguru, R. Amirtharajan, and P. Praveenkumar, “A novel quantum encryption and authentication framework integrated with IoT,” Security, privacy and trust in the IoT environment, pp. 123-150, 2019.

[21] ABDULRAHMANMUKHLEF(2023),Kaggle:[https://www.kaggle.com/datasets/abdulrahmanmukhlef/casia2]. Accessed on 5-11-2023.