Journal of Theoretical and Applied Information Technology
15th April 2023. Vol.101. No 7

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

THREE TIER FRAMEWORK IRIS AUTHENTICATION FOR SECURE IMAGE STORAGE AND COMMUNICATION

P. ALLI[1], J. DINESH PETER[2]

[1]Department of Computer Science and Engineering, Velammal College of Engineering and Technology, Madurai, India.
[2]Department of computer science and Engineering Karunya Institute of Technology and science Coimbatore

[1]E-mail: alli rajus@yahoo.com

ABSTRACT

Due to the increasing popularity of multimedia technology, the need for secure image storage and communication has become more critical, because strangers try to access these data for illegal uses. Most researchers try to provide secure image communication and security frameworks, however, they have some limitations like high cost, minimum level of security, authentication issues, etc. To overcome that issues, our proposed work provides a three-tier architecture with secure iris authentication, secure data storage, and communication. Tier 1 includes user authentication with multifactor, authentication factors are username, password, mobile number OTP and iris authentication. Tier 2 has image encryption technology through a two-fold map concept known as the Twofold Logistic Chaotic Map, here the keys are generated using a pseudo-random number (PSNR) generator for randomness. Tier 3 has the communication phase, if two parties need to communicate between them, quantum key distribution along with PSNR is implemented to ensure secure communication. Finally, the proposed method was subjected to various experiments for performance analysis, including a histogram, an entropy rate, a number of pixels change ratio, and a correlation coefficient, through the analysis of the key space, the method can improve the security and reliability.

Keywords: *Quantum Key Distribution, Image Communication, Logistic Chaotic Map, and Pseudo-Random Number*

1. INTRODUCTION

The rise of the Internet has brought about a new era of convenience and information access for people. Through the Internet, individuals can now connect and store and retrieve vast amounts of data. Images have become more informative compared to text information. They contain more details and are easier to understand. As images become the main source of information, people must be vigilant about the risks associated with information leakage. In 2013, former CIA employee Edward Snowden revealed details of the agency's surveillance program known as the Program for the Evaluation of Strategic Materials, or the PRISM Project [1]. This program allowed the US government to monitor the activities of the public. During the 2018 Winter Olympics in South Korea, the personal information of spectators and athletes was stolen by hackers. This incident caused various negative effects. Due to the increasing number of sensitive information being stored on the Internet, people must take measures to safeguard their data. Traditional encryption methods such as DES and RSA can be used to protect sensitive information. Unfortunately, the applications of these methods are not sufficient to meet the security requirements of image encryption [2]. The field of research mainly focuses on the protection of these images from various threats. Various digital image encryption techniques are used in digital image processing. Some of these include chaos encryption, pixel transformation, random sequence, and image compression coding [3]. The complexity of the chaos technology makes it hard to crack and randomize digital image encryption. Chaos encryption is a new type of digital image encryption that can be more secure and reliable.

Aside from having high data capacity and bulk data capacity, color image encryption also has certain characteristics that make it different from standard text encryption. Although many security

considerations have been discussed in terms of image encryption, many of these schemes are still not high enough. The short cycle length of keystream generators is one of the main factors that make it possible to transmit various attacks. To achieve a pseudo-random sequence, some chaotic stream ciphers have dual chaotic systems. However, when used with random map selection, the result is not secure enough [4]. The concept of confusion and diffused cryptography proposed by Shannon [5] is commonly used in encryption. It involves changing the pixel positions to reduce the complexity of input image data. The goal is to minimize the complexity of the input image by changing the pixel positions. This chaotic system has a weakness; it can only generate iterations that are less than 1000 times faster than the previous versions [6]. A good chaotic generator can help a cryptographic system achieve desirable statistical properties. For instance, a system that has a dense set of periodic windows can benefit from the existence of desirable statistical properties. Although many image encryption schemes can be used in chaotic cryptography, they are not ideal for practical applications [7]. Due to the nature of chaotic cryptography, it is not possible to implement image encryption schemes with good random sources. The author [8] presents an algorithm based on a simple Perceptron procedure. It combines the high-dimensional chaotic system with three sets of pseudorandom categorizations. A nonlinear approach is then used to produce the weight of Perceptron. The strategy is then used to dynamically adjust the chaotic system's parameters to resolve its cycle state issues.

The encryption issue is solved by employing a chaotic system; however, the security does not fulfill without secure authentication. For the secure authentication, we utilized a multifactor: username, password, mobile OTP, and biometric iris. A username is for the identification of a user by a name, password, and mobile OTP are the support factors of authentication. Biometrics is a type of secure authentication that can be used to uniquely identify a person. They can be stored in a secure environment, and they cannot be lost or stolen. This makes them ideal for addressing the security weakness of cryptography. The use of iris, which is considered to be the most reliable and secure biometric, has been widely used to identify people. Captured iris's features are extracted with a fuzzy extractor and the feature vectors are matched for identification. The resulting feature vectors are matched and generated according to a process.

One-time passwords are very secure, but it is not always feasible to share a long-term key between two parties using a communication channel [9]. A quantum key distribution method can provide high-security but it can also lead to issues due to its high cost and lower generation efficiency. If the two parties have a lot of data, then the issue with QKD might become more critical [10]. A pseudo-random algorithm can generate a sequence of random numbers with a fast and stable rate [11]. This type of algorithm guarantees the statistical characteristics of the sequence. PRNG is commonly used in various applications such as statistical sampling, numerical simulation, and gaming. It has a high generation efficiency and is simple to implement [12]. The PRNG algorithm is public, which means its security is completely dependent on the seed's confidentiality. This type of algorithm also ensures that the sequence's random number is always correlated with the seed's random number. To achieve high-efficiency random numbers in communication, a PRNG algorithm is proposed that generates a sequence of pseudo-random numbers at a low key generation rate and a high level of security. The paper shows that this method can be used to solve the issues related to QKD technology and reduce the cost of production. The proposed PRNG algorithm uses a method that allows QKD to share a seed key with the other party in a communication. After the two parties exchange a seed, the resulting algorithm will generate a pseudo-random number. The two parties then share a single pseudo-random number as a one-time pad secret key. This method is significantly different from the traditional QKD protocol, as it uses the security and randomization of QKD to solve the issues related to its generation rate and cost.

The main contributions of this paper are secure authentication, secure image data storage, and secure communication. These three contributions are provided in a three-tier structure.

- Tier 1: Secure authentication with multi factors: Username, password, Mobile number OTP, biometric iris (feature extraction and feature vector matching with fuzzy extractor).
- Tier 2: Secure image data storage: Twofold logistic chaotic map encryption and Pseudo-Random Number (PSNR) for random encryption key generation.
- Tier 3: Secure image data communication: Quantum key distribution with PSNR.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. RELATED WORKS

Ghazanfaripour, H et al [13] - Using the 3D chaotic map, this study proposes a method for encrypting grey-level images. The method achieves many advantages over current techniques. Among these were: it can meet the security requirements of image cryptography and it can resist various attacks. It can also be executed randomly. In this paper, the main goal was to provide a method that applies to various image encryption methods. Although it was mainly focused on gray-level encryption, this approach may be used to encrypt a variety of different color images. This study proposes that the Galois Fields overcome the issues. The restriction of this study was choosing a prime number for a 3D modular chaotic map, it can increase the computation time and lag in security requirements.

Deng et al [14] use a chaotic map to protect images. It has a sensitive key and a huge key space, comparable to a sensitive key. The algorithm is flawed since it does not take into account the encryption attack of choice. Instead, it uses image scramble to achieve encryption. The results of the test show that an algorithm can effectively resist a variety of attacks, and it's sensitive to even little changes in plaintext. The main drawback of this study was that it fails to consider the different types of attack effectivity when choosing a plaintext attack.

Huang et al [15] - constructed a quantum logistic map with a discrete cosine transform (DCT) (QML) structure, which is utilized to convert a frequency domain object. The former provides the security properties of confusion, while the latter makes it fast and secure. The proposed scheme was subjected to various statistical experiments and security assessments. The results of the analysis revealed that the proposed scheme was able to successfully deal with the image of a man in a middle attack, which had been rendered in color and grayscale.. The drawback here is the outweighed computational complexity.

Alli et al [16]- presented a framework that combines the properties of DNA encoding and the mappings of the sequence to create an auto-encoder-induced DNA sequence. It can effectively handle the data losses caused by various attacks, such as those caused by statistical attacks and chosen-plaintext attacks. The proposed framework generates a permuted image with less noise and complexity by activating the auto-encoder. After a secret key is obtained, it is decrypted using SHA-256. The output of the image is then sent via a digital network. Its efficiency is evaluated by taking account of the various metrics. Compared to the current frameworks, the proposed one is faster and more secure. However, it is still vulnerable to exploitation due to its weak encryption performance in terms of randomness.

Man et al [17]- a convolutional neural network algorithm was presented to implement a 2-dimensional encryption algorithm with chaotic sequence. It can resist known-plaintext attacks. A new image fusion method combined the various bits of information in two fused images. It achieves this by taking advantage of the varying characteristics of the binary bits. This study demonstrated the efficacy and security of a two-image fusion-based encryption system. It may be used to encrypt many images and is not restricted to just two. This method only protected two images. In contrast, image fusion can achieve a more secure encryption algorithm by combining the bits containing different information. This method can be used to protect multiple images.

3. PROPOSED THREE-TIER FRAMEWORK FOR DIGITAL IMAGE SECURITY AND COMMUNICATION

The rise of digital communication has made it easy for people to access and share information. Therefore, it is important to protect data from unauthorized access and sharing. There are three measures to be considered when it comes to protecting the data: Authentication, storage, and communication. Our proposed three-tier architecture is based on these considerations, figure 1 displays the three-tier architecture of our proposed framework.

- Tier 1: Secure authentication with multi factors: Username, password, Mobile number OTP, biometric iris (feature extraction and feature vector matching with fuzzy extractor).
- Tier 2: Secure image data storage: Twofold logistic chaotic map encryption and Pseudo-Random Number (PSNR) for random encryption key generation.

- Tier 3: Secure image data communication: Quantum key distribution with PSNR.

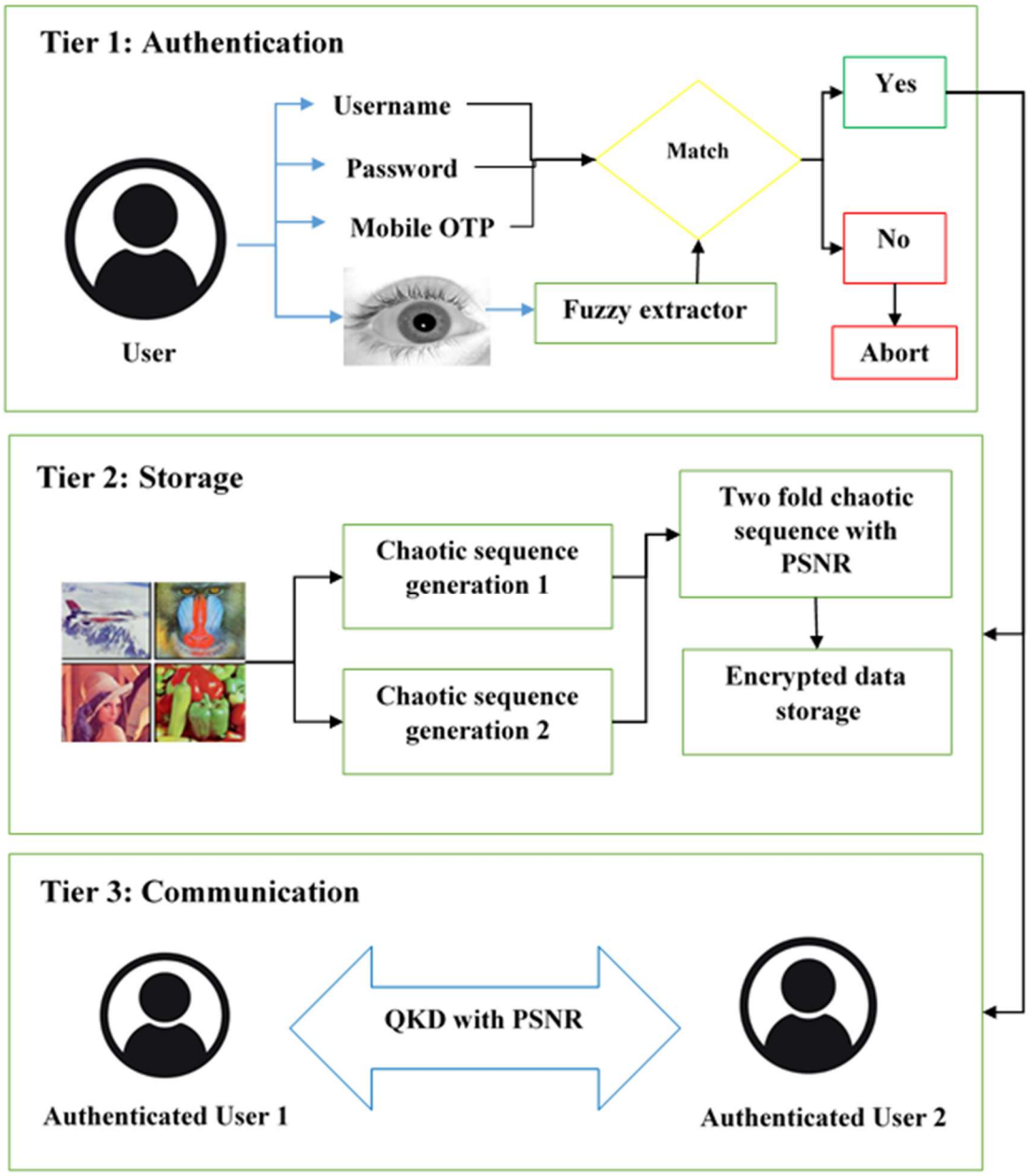


Figure 1: Three-Tier Architecture for Digital Image Security and Communication

3.1 Authentication Phase

In the authentication phase, the user must provide the factors such as Username, password, Mobile number OTP, and biometric iris. The username and password were matched with the stored credentials, the mobile number OTP is randomly generated and it is verified for the corresponding mobile number. Biometric iris features are extracted using a fuzzy extractor and the extracted feature vectors are matched with the iris templates for accurate identification.

3.2 Twofold Logistic Chaotic Map For Secure Image Storage:

Various research on the subject of image communication has been undertaken to increase the security of digital media. Chaotic maps are often used in encryption to achieve tasks like key generation and pixel substitution. The complexity of a system can affect the security of an encrypted key. This paper presents a method that uses the double-logistical chaotic map to generate pseudorandom sequences for digital image encryption. The key is computed using the first and second level chaotic maps. The results of the study indicate that the various parameters of an image, such as its histogram, key size, information entropy, and space size, can be efficiently performed in the decryption process.

3.2.1. Theory of chaotic map

The concept of the chaotic theory is a non-deterministic theory that relates to the random state of systems.

1) The retro of $f(x)$ does not have a definite upper bound;
2) Occupancy S be a countless subsection of I, then the next state of interactions is true:

$$\forall_{x,y} \in S, x \neq y, \lim_{n \to \infty} \sup \left| f^n(x) - f^n(y) \right| > 0 \quad (1)$$

$$\forall_{x,y} \in S, \liminf_{n \to \infty} \sup \left| f^n(x) - f^n(y) \right| = 0 \quad (2)$$

$$\forall_{x,y} \in S, \lim_{n \to \infty} \sup \left| f^n(x) - f^n(y) \right| > 0 \quad (3)$$

(Any intermittent point of f(x) is denoted by Y.)

The *f(x)* is the chaotic system that satisfies the limit points on S, which are distributed and concentrated. It does not correlate with all subsets. Chaotic systems have many characteristics. Some of these include boundedness, ergodically, and internal randomness. The concept of a chaotic system is not connected to all subsets. In chaotic systems, a linearized iterative equation shows the relationship between an insect population and a system. Logistic mapping can be used to evaluate the quantitative breeding models of flies. In the refinement progression, The number of children is greater than the number of parents. This means that if neither parent is present, the number of children can be ignored and the chaotic sequence will appear different depending on the parameter. It will be generated if the condition satisfies the parameter (3, 4). It is similar to the white noise characteristic of sound. Before H. this approach was used to encrypt digital images.

The chaotic system's key sensitivity to the beginning value may be determined using its properties. This indicates that the encryption algorithm will change if the key changes that will have a better encryption effect. The existence of the key can be obtained through a chaotic system. This concept can be used to implement an encryption system that is based on the initial value.

Chaotic systems are used in two forms of encryption. The first is called chaotic synchronization, and the second type is the homogeneous group key. The chaotic system can be used for distinguishing the key sensitive demand and the pseudo-randomness of an encryption process. The different phases in the encryption process may be described as chaotic systems. A mapping algorithm is used for carrying out chaotic mapping operations. It can also be compared with the pseudo-randomness of the encryption system. Chaotic mapping is a process that uses a chaotic representation of a digital object to protect it. This method uses the chaotic sequence to create a pseudorandom number. It avoids using computer software to generate the same result. The image chaotic encryption system is an algorithm that can generate pseudorandom number sequences using an image pixel set and chaotic system. The chaotic system can generate an image pixel set and chaos, which can be used to achieve the opposite process (decryption).

3.2.2 Twofold digital image encryption method

An encryption system is very important to modern cryptography. It involves the transformation of the old keys into new ones, and the target of the encryption is the plaintext space. The decryption key is the one that's used to decrypt the encoded data.. For a framework, the C and P values of the original digital image are used to identify the image pixel that needs to be decrypted after encryption. The spaces obtained by encryption are obtained in an insecure channel. This feature allows the key to be used for various encryption methods. The control of an encryption algorithm is carried out in the key space K. This space contains the basic information that's required to perform the encryption.

The current cryptosystem comprises the key and encryption key operations. The component is the encryption key that is used to transform the encryption space P into the ciphertext space. The space C corresponds to the key that is used to secure the encryption. It can be obtained by sending the plaintext P to an anxious network. The key K is part of an encryption algorithm that can be used to perform various encryption operations. It can also be used to carry out a cryptographic transformation. The chaotic sequence generators are also responsible for the algorithm's development. A chaotic map is composed of two maps. These two maps are used to implement the modules that have to do with digital image encryption.

The pseudorandom sequence formed by the chaotic mapping is not random since the random number generator technique cannot guarantee complete unpredictability. The algorithm used for the random sequence generator is known as the logistic mapping method. The logistic pseudorandom sequence generator is commonly used to generate a pseudorandom order. It is formulated by way of follows.

$$\rho(x) = \begin{Bmatrix} \left(\pi\sqrt{1-x^2}\right)^{-1} & x \in (0,1) \\ 0 & x \notin (0,1) \end{Bmatrix} \quad (4)$$

The following two logistic maps are used for the compeers of pseudorandom orders. The first one is used for the first level and the second one for the second level. The following random number sequence is computed when the value is set. It is used for stream encryption. PRNGs are frequently used to produce a broad range of numbers which are typically used for generating number plots, rounding, linear, and nonlinear congruence. For producing pseudo-random numbers, the linear congruence approach is a simple and reliable method. It may be used to generate random sequences with high-quality random sequences. It uses a linear operation to get the next number.

$$x_{n+1} = (ax_n + c) \bmod m \quad (5)$$

a is a multiplier, c is an increment, m is a modulus in the formula, and xn is a random number. The Q-base and P-base are two kinds of measurement bases, respectively.

$$\left|+\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad , \left|-\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (6)$$

$$\left|0\right\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \quad , \left|1\right\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |1-\rangle) \quad (7)$$

Table 1 shows the four distinct states that were assessed using the two different measurement bases.

Table 1. Measurement Results Of Different States.

	|0>	|1>	+	-
Q-basis	|0>	|1>	50% |0>or 50% |1>	50% |0>or 50% |1>
P-basis	50% |+> or 50% |->	50% |+> or 50% |->	|0>	|1>

3.3 QKD With Pseudo-Random Number Generation Algorithm For Secure Communication

This research suggests a PRNG scheme that enables two parties to share arbitrary numbers without increasing the complexity or cost of QKD technology. The project's goal is to develop a secure QKD-based system with a high level of randomness. The project proposes a QKD-based system that uses a seed key to share a binary bit with two parties. The algorithm used for the PRNG will be the same as the one used for the arbitrary digit producer. The key will then be used to generate a PRNG with the same algorithm. This scheme uses the same pseudo-random number as a key that is used as a secret key. It avoids the high cost and slow generation of QKD. This scheme uses the unconditional security of true randomness to prevent the exploitation of pseudo-random numbers.

Step 1: For the open channel, both sides (sender and receiver) use a linear random number-generating technique.
Step 2: S1 is sent to a receiver after constructing a quantum sequence containing 4n single photons.
Step 3: After receiving S1, the receiver measures S1 at random using the Q-basis or P-basis.
Step 4: Following the preparation of S1's base sequence, the receiver must recreate S2's base sequence. By rejecting the single photon state of the same base, the quantum sequence S2 should be created.
Step 5: The receiver chooses a portion of the single photon and indicates if it is ready.
Step 6: The protocol is stopped if the bit error rate exceeds the threshold.
Step 7: To inspect the photons, both the receiver and the emitter must round them off. After that, the leftover particles form the quantum sequence

S3.

Step 8: The receiver delivers k1 as a seed to a linear congruence algorithm, which returns K2.

This paper shows how to generate a random sequence using two logistic maps. The generated sequence is used for encrypted communication.

The image encryption process begins with two steps: confusing processing and scrambling. The confusing processing takes place when the encryption key is confused.

1) To calculate the Qkd model, set design parameter 1 to the pseudorandom sequence number X.
2) The pseudorandom sequence number will be converted to binary using this approach.
3) Encrypt the grey or color component code of the digital image.
4) The XOR for the first element in G is calculated using the X' gi formula.

$$I'(k) = X'^{(k)} \oplus \{[X'^{(k)} + g_k] \bmod N\} \oplus I'(K+1) \quad (8)$$

The k pixel in the image is represented by k.

5) After the fourth step, the sequence of pixels is reversed and the original components are repositioned to the first and second locations according to formula 8.

4. RESULT AND DISCUSSION

4.1 Simulation Environment

The numerical simulations are carried out using the MATLAB program in a classical computer. We take into account the various plain images such as Baboon, Lena, and Airplane. Due to the complexity of the algorithm and the need for high-end computing hardware, our proposed method was simulated using a classical computer with an Intel(R) Core i7-4760U. The R2015a is equipped with a 64-bit CPU and 8GB of RAM.

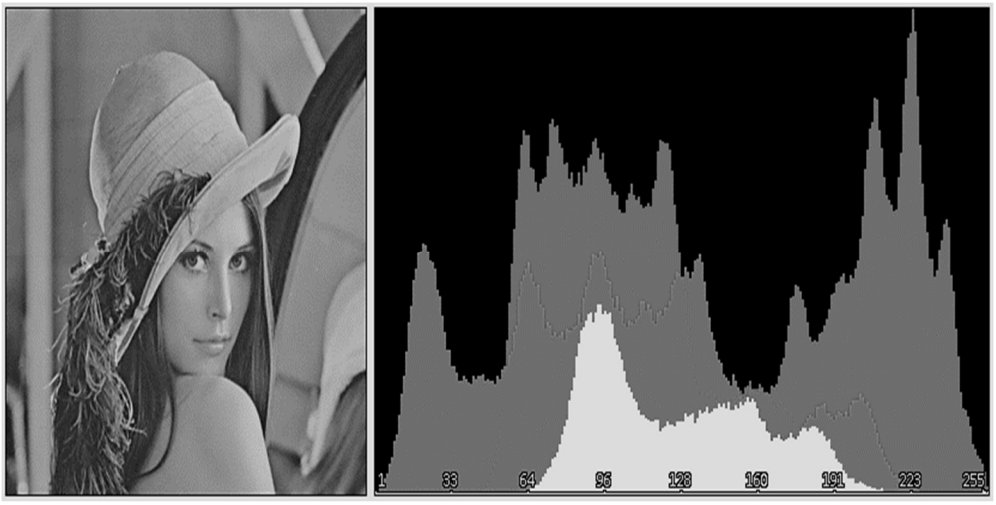


Figure 2: *Original* Lena Image And 3D Histogram

The original image presented in Figure 2 is kept in a 256 * 256 * 3 matrix. It must be grayscale to obtain greater digital encryption. Figure 2 shows Lena's original image, which is a three-dimensional array. It's stored as a matrix 490x490x3. To achieve better encryption, the image should be rendered in grayscale.

4.2 The Histogram Analysis

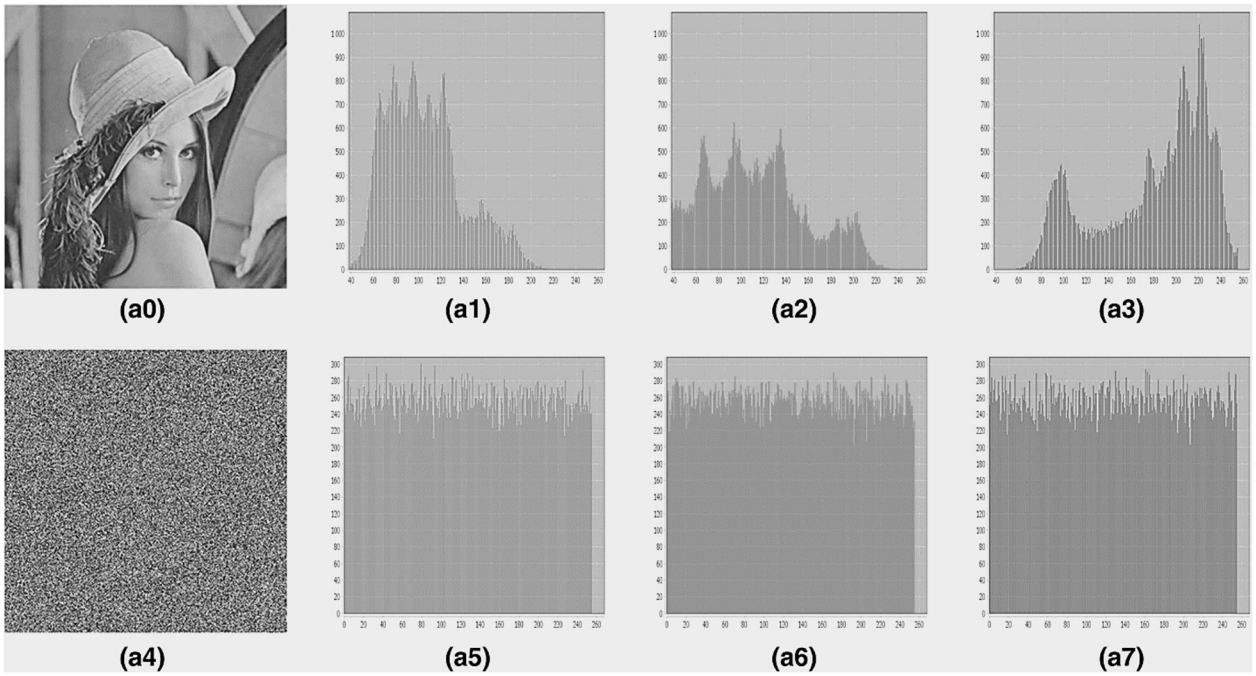
A distributed histogram is a representation of the quality and reliability of an encryption system. It displays the intensity of an image's colors using the x- and y-axis. The values are represented by the y- and the x-axis of the image. Having a flat image histogram helps in the discovery of more diffused colors in an image since it avoids generating random distributions.

For each key, we use the principles of variances to evaluate the uniformity of ciphered images. We also calculate the differences between the encryption keys used for different ciphered images. The values of these factors are then computed to determine the variances of the encoded images. The appearance of encrypted images is determined by the relative values of histograms. The closer the values get, the more

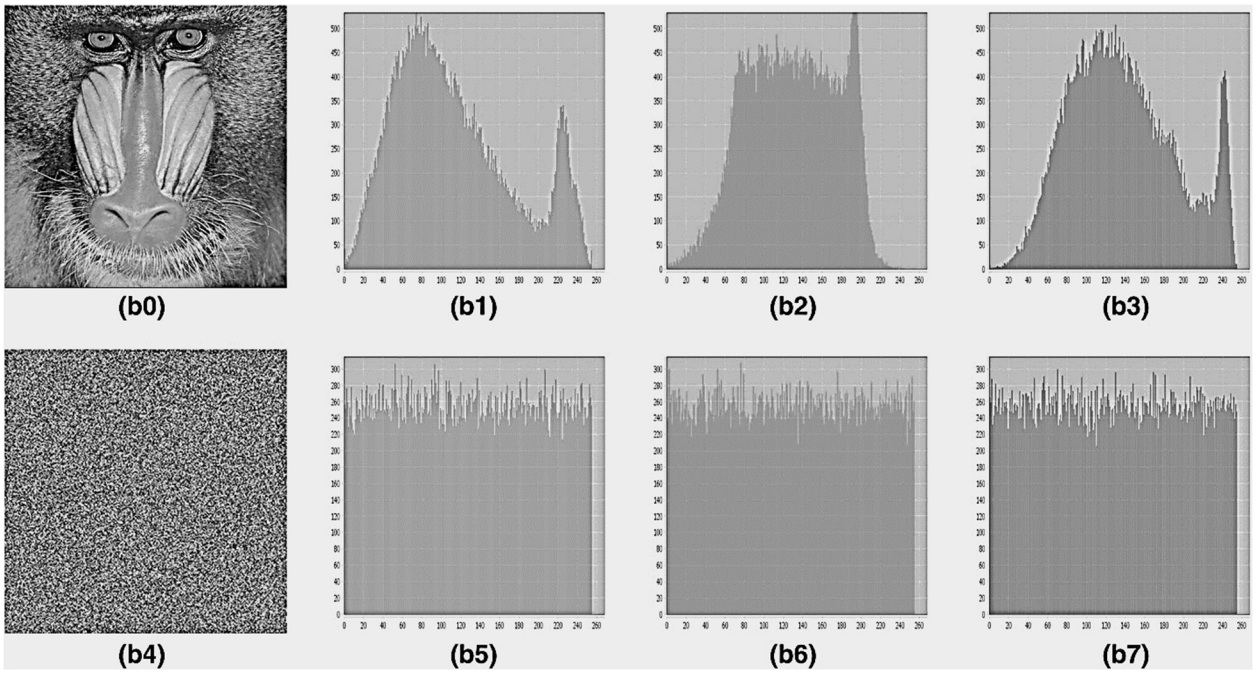
uniform the encrypted images are presented as follows:

$$\text{var}(Z) = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{1}{2}(z_i - z_j)^2, \quad (9)$$

Where Z is the vector of the values z1, z2, and z256, the numbers of pixels are equal to i and j respectively. In experiments, we show how to simulate two ciphered images with different secret keys. In this study, we show how two sets of histograms could be obtained from an image with different secret keys. The encryption algorithm used for this test only changes one parameter of the secret key. The image of Airplane, Lena, and Baboon is tested for encryption and the histogram analysis is presented in Figure 3.



(an)



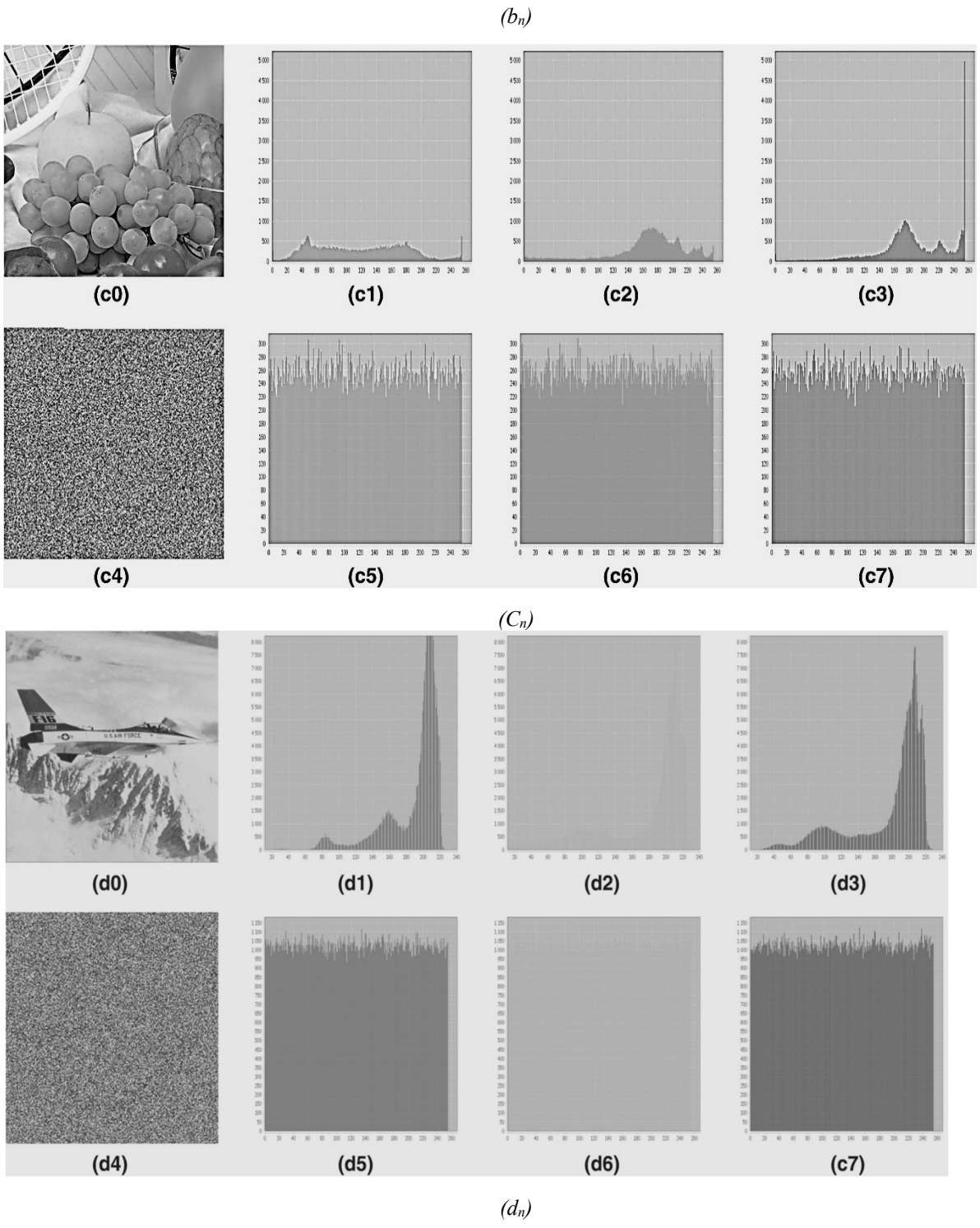


Figure 3: A) Lena, B) Baboon C) Fruits, And D) Airplane Image And Histogram Image Of RGB

4.2.1. Histogram statistics

The standard deviation and variance metrics are used to measure the dispersion of data in graphic histograms. A set of values with the same average size can have the same elements, but their variation can be significant. Squared-point computation is a process that takes the central point and measures its variance. This process is

used to minimize the effects of distributed data and increase the variance of non-standard ones.

$$\alpha = \frac{1}{256}\sum_{i=1}^{256}(x_i - \bar{x})^2 \quad (10)$$

Where,

$$\bar{x} = \frac{M \times N}{256} \quad (11)$$

x_i is the frequency for the intensity value of the histogram is 0 to 255, and the mean is the sum of the histogram's variance.

4.2.2. Histogram uniformity

The ideal uniform histogram should have the same pixel frequencies across all 256 values. The histogram should have 256 standard deviations ranging from 0 to 255. The histogram uniformity percentage is a function that measures the consistency of the intensities across all 256 levels.

$$HUP(\%) = \frac{1}{256}\sum_{i=1}^{256}\rho(i) \quad (12)$$

Where:

$$\rho(i) = \begin{cases} 1 & if\ \rho \geq \bar{x} - \beta\ and\ \rho \leq \bar{x} + \beta \\ 0 & otherwise \end{cases} \quad (13)$$

The acceptable range 'ρ' can be determined by taking into account the variance in the standard deviation 'β' and the mean '$\bar{x}$', while the mean can be derived from the data. For instance, the values of the HUP of the images Lena's and Baboon's encrypted images are 85.01% and 85.54%, respectively,

In experiments, we compare the sensitivity of various secret keys. The results of the tests reveal that changing one parameter can significantly affect the sensitivity of the secret key. Table 2 compares the proportion of histograms variances for all secret keys. The first and next columns' variances are obtained by changing the secret key 1's parameters k1, l, e, g, and c[0]. The number of rows with the lowest and highest variance is computed by dividing the gray value by the number of pixels. The number of rows with the highest and lowest variance is 5000. The calculation of the variance value is performed by taking the sum of the gray value and the plaintext image's variability. The most common way to determine a 10% fluctuation is by changing the K1 key to a secret key.

Table 2: Compares The Percentage Of Variances Difference Of Histograms For All Secret Keys

Ciphered image	K1 (%)	l (%)	e (%)	g (%)	c[0] (%)
Lena	9.8	1.57	1.19	2.22	5.2
Baboon	11.30	3.53	9.96	3.18	1.0
Fruits	8.96	6.59	5.49	2.36	1.42
Airplane	10.56	5.32	3.78	3.63	4.83
Average	10.155	4.2525	5.105	2.8475	3.1125

4.3. Encryption Quality

The various techniques used in validating the encryption of images are discussed in this section. One of the methods that can be used to calculate the signal-to-noise ratio is the mean-square error method. The peak signal-to-noise ratio is the most common component of this equation. $MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[P(i,j) - E(i,j)]^2$ (14)

Where, MXN- image size

P- Plain image

E- Encrypted image

The size and encryption quality of an image is two key factors that are used to consider when choosing one. The MSE analysis is a tool that can be used to test the operation of an encrypted color image and the RGB plain image. The PSNR is a function that shows the ratio between the signal's maximum power and the distortion that affects the quality.

$$PSNR = 20\log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \quad (15)$$

Due to the high MSE of encryption algorithms, the PSNR of encrypted images is expected to be less than 10 dB. Table 3 presents the Comparison of MSE and PSNR (dB) in terms of encrypted images.

Table 3: Comparison Of MSE And PSNR (Db) In Terms Of Encrypted Images

Encrypted Images	MSE			PSNR (dB)		
	R	G	B	R	G	B
Lena	23296	21267	25685	8.3	9.17	7.50
Baboon	9452	8015	9648	8.37	9.09	8.28
Fruits	10677	9105	7200	7.87	8.60	9.68
Airplane	7825	6589	8956	7.56	8.69	8.96

4.4. The Correlation Coefficient

The correlation factor is a statistical measure that shows how similar two variables are to each other. It's commonly used to measure the quality of an encryption scheme. The strength and usefulness of an encryption technique are measured by how it can conceal all of the original data's attributes and produce an uncorrelated encrypted version. In image processing, the correlation between the image's adjacent pixels and the original image is usually very high. On the other hand, if the correlation between the two is very low, then an encryption scheme is very effective. An efficient algorithm should reduce the correlation coefficient as much as possible to zero.

The correlation coefficient is a function that measures the number of pixels in an image. The number of pixels in an image is computed by dividing the distance between the objects by the number of digits. The algorithm used to determine the correlation coefficient is the most advantageous one for achieving the most favorable result in the computed correlation. The Correlation Coefficient rates are computed by taking the coordinate coordinates of three vertical and horizontal coordinate coordinates. They were computed using the MATLAB environment's predefined functions.

$$r_{x,y} = \frac{E((x-E(x))(y-E(y)))}{\sqrt{D(x)D(y)}} \quad (16)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (17)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \quad (18)$$

The number of pixels that were chosen for the image is expressed in the gray area of the two adjacent pixels.

4.5. Differential Attack Analysis

The following equations 19 and 20 are used to analyze the performance of an encryption framework.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (19)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,-j) - C_2(i,j)|}{255}\right] \times 100\% \quad (20)$$

The height and width of the image are respectively indicated by the cipher image before and after it has been changed.

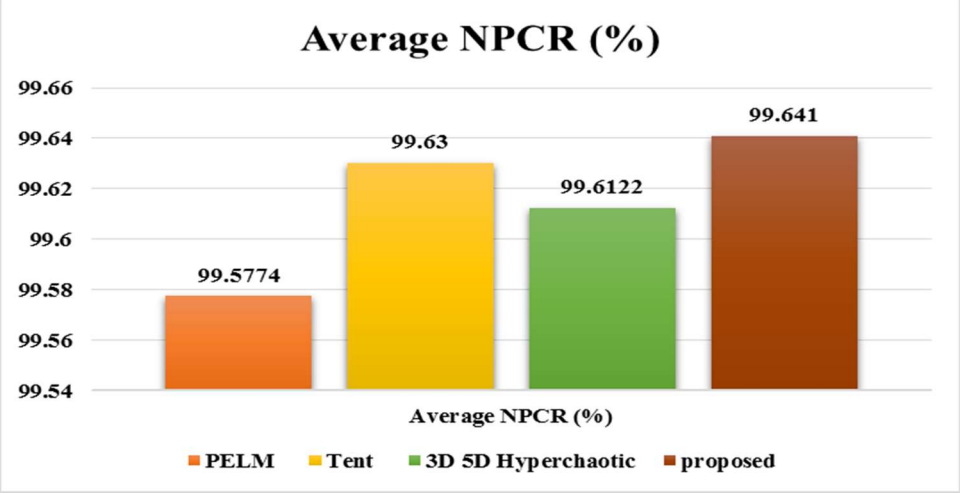


Figure 4: Comparison Of Average NPCR With Existing Methodology

From figure 4, the two-dimensional logistic map with QKD was able to pass the critical values test in the number of pixel change rates (NPCR) analysis. It also exhibited similar results to those obtained from other works [18].

4.6 Robustness evaluation

An excellent encryption system depends on the image's ability to resist the effects of noise and clip attacks.

1 **Clipping attacks:** The quality of an image reconstructed after it has been encrypted will decrease if it is attacked by pixel clipping.

2 **Noise attack:** Existing cryptosystems are prone to noise, especially if a small distortion appears in the cipher text. This issue can render the decrypted image unusable. Figure 5 reveals the images of Lena that have varying amounts of noise, while those with Gaussian noise are shown in Figure 6. This paper proposes a novel algorithm that can effectively suppress noise attacks.

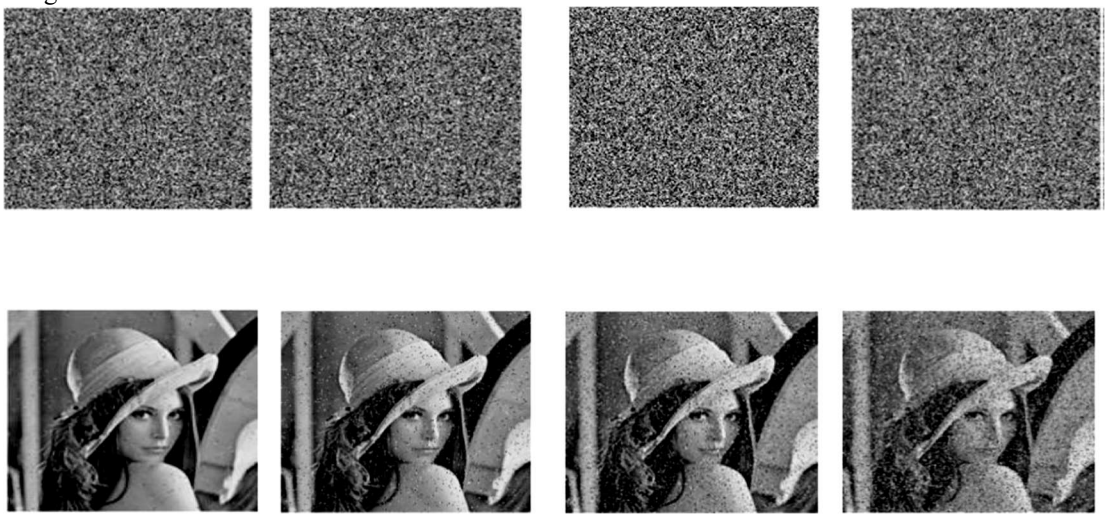


Figure 5: Encrypted Images Of Lena With 1–25 % Of Noise And Their Decrypted Images

Figure 6: The Encrypted Images Of Lena With Gaussian Noise And The Decrypted Images

Table 4: NIST Test Results For Lena Cipher Image

Test name		p values for encrypted image		
	Red	Green	Blue	
Frequency		0.4934	0.9773	0.59773
Block-frequency		0.95857	0.30998	0.7952
Runs (M = 10,000)		0.33534	0.4262	0.3375
Long runs of one		0.1468	0.1468	0.1486
Rank		0.3020	0.3020	0.3020
Spectral DFT		0.57927	0.77447	0.88278
No overlapping templates		0.93396	0.98892	1
Overlapping templates		0.96099	0.96099	0.96999
Universal		0.99550	0.98863	0.98284
Serial	*p values 1*	0.06751	0.4900	0.38419
Serial	*p values 2*	0.22893	0.64973	0.61688
Approximate entropy		0.32616	0.52073	0.29336
Cumulative sums forward		0.45878	0.38780	0.35722
Cumulative sums reverse		0.79386	0.4193	0.39884
Random excursions	*X= -4*	0.88486	0.121568	0.65737
	X= -3	0.5800	0.157192	0.88090
	X= -2	0.61416	0.93205	0.61759
	X= -1	0.64453	0.71386	0.8238
	X= 1	0.31163	0.94425	0.47204
	X= 2	0.129964	0.44806	0.36073
	X= 3	0.1141647	0.63529	0.3365
	X= 4	0.1183702	0.066905	0.98603
Random excursions	*X= -4*	0.81829	0.60299	60.92218
variants	*X= -3*	0.69707	1	0.99865
	X= -2	0.59410	1	0.8920
	X= -1	0.43139	0.93837	0.37949
	X= 1	0.37057	0.34117	0.19200
	X= 2	0.95027	0.52394	0.21146
	X= 3	0.45918	0.50532	0.176001
	X= 4	0.36087	0.28466	0.142555

Table 4 shows the NIST test results, and the suite of statistical tests provided by NIST is used to evaluate the proposed method. The value of the tests is compared with their significance level, which is 0.001. If the test's value exceeds the threshold, the method is considered to be passed. The results show that the proposed approach can achieve a high level of security.

The proposed algorithm is subjected to four image processing attacks to evaluate its robustness. The results show that the design is associated with higher reliability and higher normalized correlation. The results show that the proposed algorithm does not affect image decryption and encryption. In addition, the proposed method's robustness is strengthened by the higher normalized correlation. These are the histograms for encrypted images, which are almost flat and uniform compared to the plain ones. The improved scheme can prevent unauthorized access to an image's data through statistical attacks. Due to the nature of electronic transmission, image transmission can get infected with noise. This is a serious issue that affects the reliability of cryptosystems. A good encryption algorithm should be able to prevent this issue by protecting the data from getting distorted due to a minor change in the encryption algorithm. This could prevent the recovery of the image after an error in one pixel. A good encryption scheme should also consider the robustness of its algorithm against noise. This ensures that the data is not distorted due to propagation errors.

4.7 Image Entropy

Global information entropy is a measure of signal randomization. It should be around 8 bits for a grayscale. Image entropy is a measure of how much information can be presented in a given image. It can be computed by analyzing the color intensity of individual pixels. If the pixel's color intensity is the same across all the images in the same frame, then the resulting image with the minimal entropy value will have the same color. If the computed image entropy value is less than 8, then an image scramble procedure is a good idea. Table 5 shows the entropy values of our proposed method.

Table 5: The Calculated Entropy Values In Our Simulation

Image	The entropy value(original image)	The entropy value
Airplane	7.7047	7.9236
Baboon	7.7033	7.9949
Lena	7.7322	7.9742
fruits	7.7249	7.9743

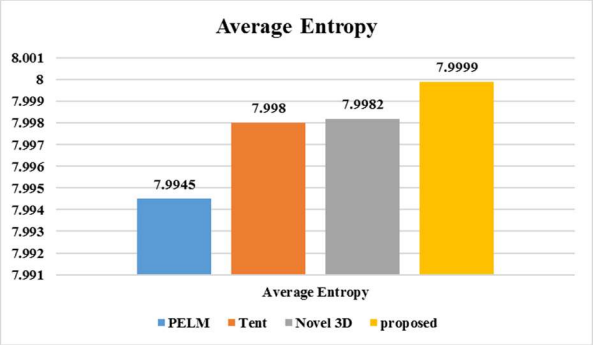


Figure 7: Comparison Of Average Entropy With Different Methodologies

Ideally, digital images with an entropy of 8 should be encrypted. For cryptographic systems, this threshold is maintained to prevent their security from being threatened [19-21]. For the proposed method, the two logistic chaotic maps with QKD and the Lena RGB image are used. For comparison, the results of the same work can be obtained by comparing them to works that use the same image and 8-bit RGB format. In this case, the proposed method shows better results than most of the works. To prevent unauthorized access to the contents of a given ciphertext image, the proposed scheme uses an information entropy attack. This prevents an attacker from extracting information from the image.

4.8 Security Analysis

The algorithm that generates a quantum encryption algorithm is known as a cryptographic algorithm. The security of the quantum encryption algorithm is dependent on the details of its generation process. The length of the key stream and the size of the image are also known to affect the gray value. The length of the key stream is generally determined by the size of the key space. The key must have sensitive bit changes to decipher the image. The number of bit changes

(NBCR) of an image is also known as the key sensitivity.

$$NBCR(B_1, B_2) = \frac{ham(B_1, B_2)}{T_b} \quad (23)$$

If the number of bits from B1 to B2 is less than 50%, then the distance between them is equal to the overall distance between them.

A cryptographic system's total number of secret keys is known as key space. The secret keys are generated using a linear key distribution algorithm. The algorithm generates the secret keys by taking a pseudo-random sequence of digits k2. The seed number k1, which is the pseudo-random sequence k2, is used to input the linear algorithm are shown in Table 6.

Table 6: The Value Of K1 And K2.

Key	The value
K1	01011110001010101010
K2	4654763287593457029738267546594760485937482612`136r26583745640968349568325715364265438765948784673571261436215473265893275984759823658327647215327186487236498365837644712648716983562837657467286735763

4.9 Encryption And Decryption Speed

The main functions of decryption and encryption are similar. They are computed by comparing the length and size of the secret message and the secret key. The time it takes to decrypt or encrypt a message depends on the condition of the secret key and its size. Figure 8 depicts the Encryption/decryption time for different image sizes and secret key lengths

.

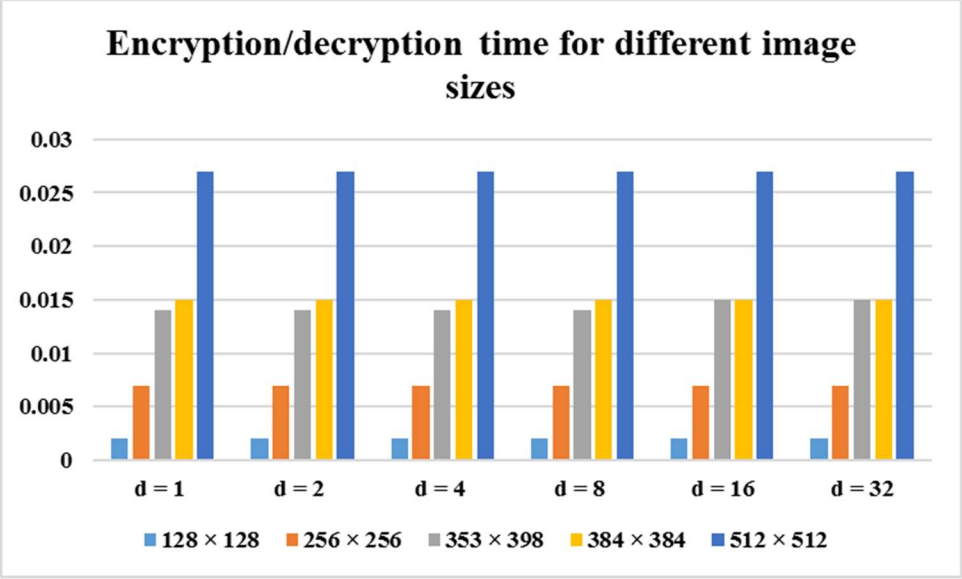


Figure 8: Encryption/Decryption Time For Different Image Sizes And Secret Key Lengths

Table 7 shows the computational cost calculation for cost efficiency; where Te represents the time for one exponential operation, Tb represents the time for one bilinear operation.

Table 7: Computational Cost

Scheme	Encoding Cost **	Decoding Cost **
CP-ABE + Hidden Access policy [22]	3Te	3Tb
CP-ABE + Hidden Access policy [23]	4Te	3Tb
CP-ABE + Partially Hidden Access policy [24]	4Te	3Tb + Te
CP-ABE + Hidden Access policy [25]	3Te	3Tb + Te

CP-ABE + Hidden Access policy [26]	3Te	2Tb + Te
Proposed	3Te	2Tb + 2Te

4.9.1. Effectiveness key sensitivity analysis of the scheme

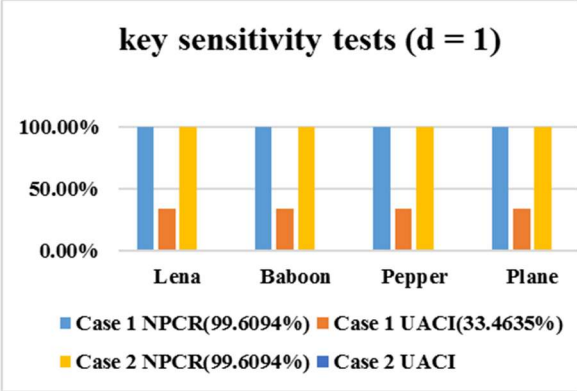
The generation time of k1 is t1, and t1 = 0.00256s. The generation time of k2 is t2 and t2 = 0.00047s.

The key generation efficiency is η1, η1 = 7799.54b / s, and the pseudo-random number generation efficiency obtained by the linear congruence algorithm is η2,

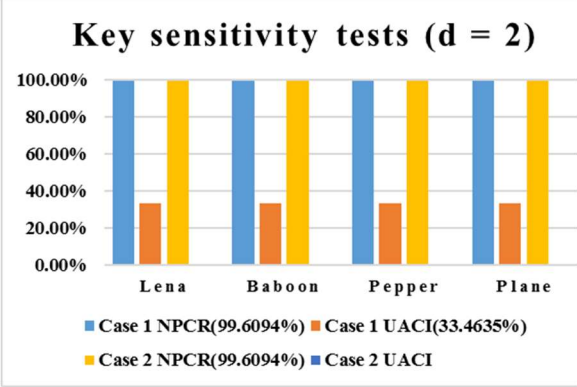
$$\eta 2 = 600bit / (t1+ t2) = 600bit/ (0.00256s+0.00047s) =198216.06b / s \quad (14)$$

In the research, the ratio of generation efficiency to quantum random key efficiency is p,

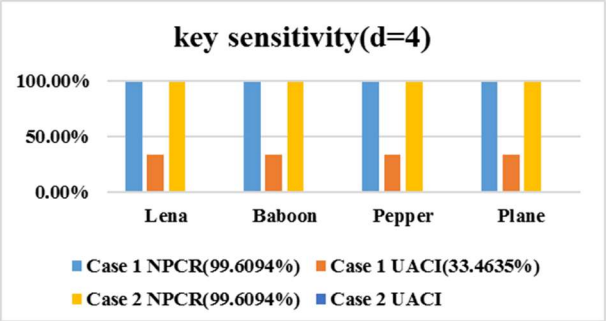
$$p=\eta 2/\eta 1=198216.06/7799.54=25.42 \quad (15)$$



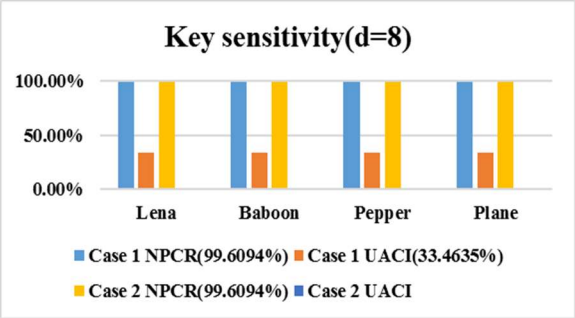
D=1



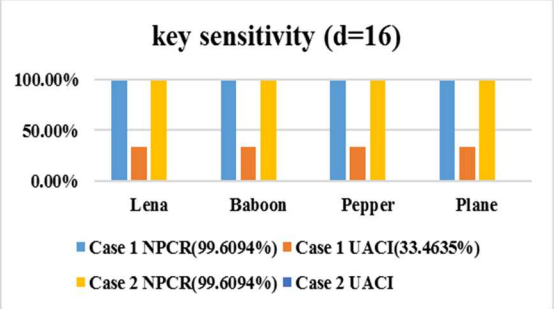
D=2



(D = 4)



(D = 8)



(D = 16)

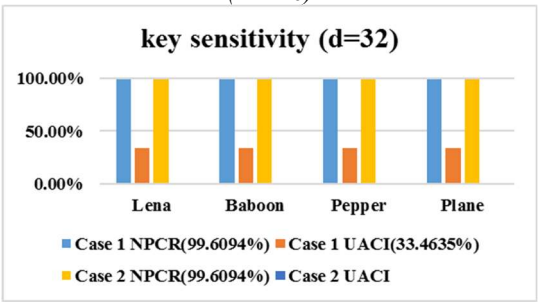
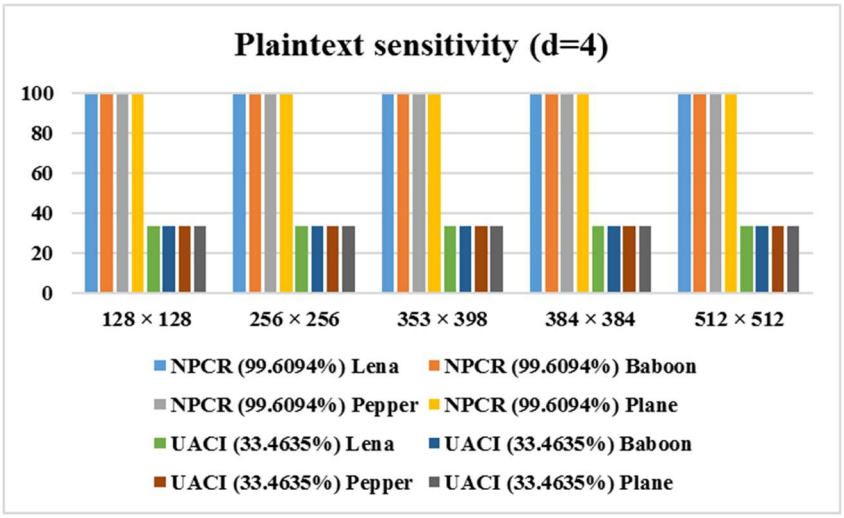


Figure 9: Results Of Key Sensitivity Tests (D = 1, 2, 4,8,16 And 32)

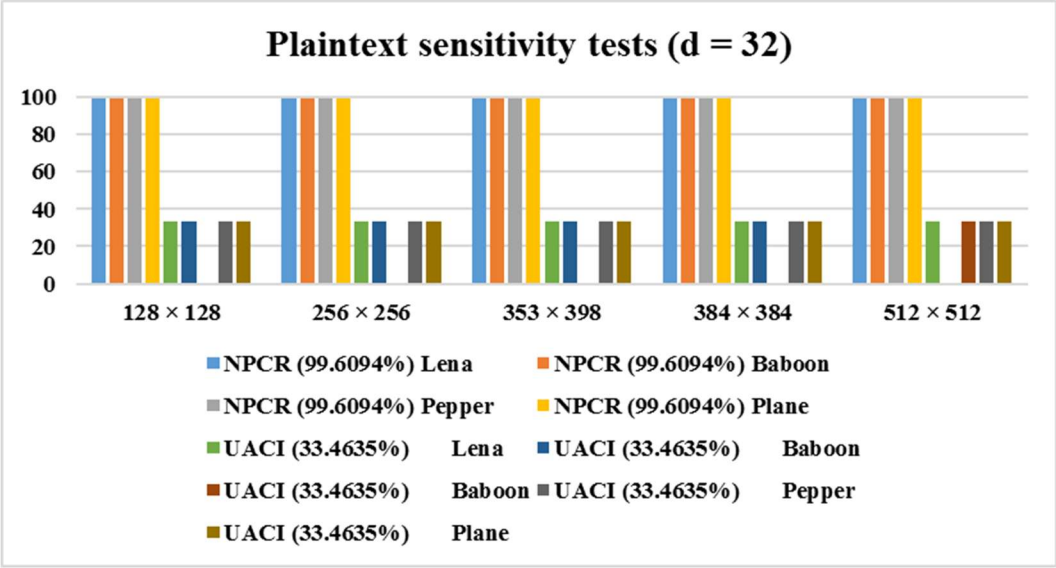
The results of the key sensitivity test are shown in Figure 9. As the number of keys increases, the pseudo-random number's efficiency will improve, which will make it more useful in generation of keys. The ratio of the pseudo-

random to the quantum random key will also increase, which shows that the former is more efficient. Likewise, figure 10 shows the Results of plaintext sensitivity tests. A typical attacker makes a small change in the plain image and then observes the changes in the cipher image. This method can break the encryption process if the change is small. On the other hand, differential analysis is useless when the attacker discovers the relationship between the two. Plain text sensitivity can be computed by comparing the NPCR and the Unified Average Change Intensity (UACI). For instance, if an input is changed slightly, the output changes significantly.

(d = 32)



d=4



d=32

Figure 10: Results Of Plaintext Sensitivity Tests (D = 4 And 32)

4.10. Running Efficiency Analysis

For our proposed encryption algorithm, we consider the efficiency of its transmission. In this paper, we introduce 3 groups with different sizes. For tests, we only selected groups with 256*256.In this paper, we introduce the concept of group images, which are composed of three

images. The test results revealed that the proposed algorithm achieves good transmission efficiency.

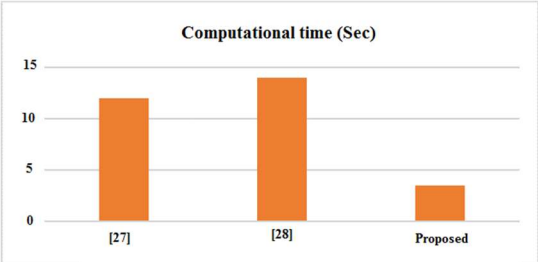


Figure 11: Computation Time With Different Related Works

In addition to the security aspect, the running speed is also an important factor that can be used to measure the image encryption scheme. Figure 11 shows that the time complexity of computation is also significantly reduced compared to that of the existing methodologies.

5. CONCLUSION

Due to the increasing number of applications of communication and networking technology, encryption has become an effective method for protecting the secure transmission of data. This paper shows the three-tier framework for secure image storage, authentication, and communication. An image scrambling procedure has been investigated on two levels. The procedure was performed on various images to evaluate their performance. By calculating the NCAR, entropy, and histogram graphs, where the requirements have been confirmed. Our proposed method surpasses a previous approach in terms of security, key generation efficiency, and cost efficiency. In the future, there will be another phase before the encryption key is applied to a particular site. This will make the confusion on the site even worse. An additional phase will allow developers to create more complex encryption methods.

REFERENCES:

[1] Pan, H., Lei, Y. and Jian, C., 2018. Research on digital image encryption algorithm based on double logistic chaotic map. *EURASIP Journal on Image and Video Processing*, *2018*(1), pp.1-10.

[2] Dupont, B., 2004. Security in the age of networks. *Policing and society*, *14*(1), pp.76-91.

[3] Niu, Y., Zhou, Z. and Zhang, X., 2020. An image encryption approach based on chaotic maps and genetic operations. *Multimedia Tools and Applications*, *79*(35), pp.25613-25633.

[4] Liu, H. and Wang, X., 2010. Color image encryption based on one-time keys and robust chaotic maps. *Computers & Mathematics with Applications*, *59*(10), pp.3320-3327.

[5] C.E. Shannon, Bell System Technical Journal 28 (4) (1949) 656.

[6] Liu, H. and Wang, X., 2011. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. *Optics Communications*, *284*(16-17), pp.3895-3903.

[7] Liu, H. and Wang, X., 2012. Image encryption using DNA complementary rule and chaotic maps. *Applied Soft Computing*, *12*(5), pp.1457-1466.

[8] Wang, X.Y., Yang, L., Liu, R. and Kadir, A., 2010. A chaotic image encryption algorithm based on perceptron model. *Nonlinear Dynamics*, *62*(3), pp.615-621.

[9] Jiang, Y., Liu, B., Guo, C. and Zhao, J., 2021, August. A quantum pseudo-random number generation scheme. In *Journal of Physics: Conference Series* (Vol. 2004, No. 1, p. 012001). IOP Publishing.

[10] Mi, S., Wang, T.J., Jin, G.S. and Wang, C., 2015. High-capacity quantum secure direct communication with orbital angular momentum of photons. *IEEE Photonics Journal*, *7*(5), pp.1-8.

[11] Hadfield, R.H., 2009. Single-photon detectors for optical quantum information applications. *Nature photonics*, *3*(12), pp.696-705.

[12] Tchoffo, M. and Tene, A.G., 2021. Security and communication distance improvement in decoy states based quantum key distribution using pseudo-random bases choice for photon polarization measurement. *Optical and Quantum Electronics*, *53*(8), pp.1-24.

[13] Ghazanfaripour, H. and Broumandnia, A., 2020. Designing a digital image encryption scheme using chaotic maps with prime modular. *Optics & Laser Technology*, *131*, p.106339.

[14] Deng, Z. and Zhong, S., 2019. A digital image encryption algorithm based on chaotic mapping. *Journal of Algorithms & Computational Technology*, *13*, p.1748302619853470.

[15] Ye, G., Jiao, K., Huang, X., Goi, B.M. and Yap, W.S., 2020. An image encryption

scheme based on public key cryptosystem and quantum logistic map. *Scientific Reports*, *10*(1), pp.1-19.

[16] Alli, P. and Dinesh Peter, J., A novel auto-encoder induced chaos based image encryption framework aiding DNA computing sequence. *Journal of Intelligent & Fuzzy Systems*, (Preprint), pp.1-17.

[17] Man, Z., Li, J., Di, X., Sheng, Y. and Liu, Z., 2021. Double image encryption algorithm based on neural network and chaos. *Chaos, Solitons & Fractals*, *152*, p.111318.

[18] Wu, Y.; Noonan, J.P.; Agaian, S. NPCR and UACI randomness tests for image encryption. Cyber J. **2011**, 1, 31–38.

[19] Murillo-Escobar, M.A.; Cruz-Hernández, C.; Cardoza-Avendaño, L.; Méndez-Ramírez, R. A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. Nonlinear Dyn.2017, 87, 407–425.

[20] Palacios-Luengas, L.; Pichardo-Méndez, J.L.; Díaz-Méndez, J.A.; Rodríguez-Santos, F.; Vázquez-Medina, R. PRNG Based on Skew Tent Map. Arabian J. Sci. Eng. 2018, 1–14.

[21] Sahari, M.L.; Boukemara, I. A Pseudo-Random Numbers Generator Based on A Novel 3D Chaotic Map with An Application to Color Image Encryption. Nonlinear Dyn. 2018, 94, 723–744.

[22] Helil, N.; Rahman, K. CP-ABE Access Control Scheme for Sensitive Data Set Constraint with Hidden Access Policy and Constraint Policy. Secur. Commun. Netw. 2017, 2017, 2713595.

[23] Sabitha, S.; Rajasree, M.S. Access control based privacy preserving secure data sharing with hidden access policies in cloud. J. Syst. Archit. 2017, 75, 50–58.

[24] Liu, L.; Lai, J.; Deng, R.H.; Li, Y. Ciphertext-policy attribute-based encryption with partially hidden access structure and it's application to privacy-preserving electronic medical record system in cloud environment. Secur. Commun. Netw. 2016, 9, 4897–4913.

[25] Wu, A.; Zheng, D.; Zhang, Y.; Yang, M. Hidden Policy Attribute-Based Data Sharing with Direct Revocation and Keyword Search in Cloud Computing. Sensors 2018, 18, 2158.

[26] Odelu, V.; Das, A.K.; Khan, M.K.; Choo, K.R.; Jo, M. Expressive CP-ABE Scheme for Mobile Devices in IoT Satisfying Constant-Size Keys and Ciphertexts. IEEE Access 2017, 5, 3273–3283.

[27] Yeoh, W.; Teh, J.; Chern, H. A Parallelizable Chaos-Based True Random Number Generator Based on Mobile Device Cameras for the Android Platform. Multimed. Tools Appl. 2018, 1–21.

[28] Belazi M, E-Latif AAA, Belghith S (2017) Khan efficient cryptosystem approaches: S-boxes and permutation-substitution-based encryption. Wirel Pers Commun 87(1):337–361.