IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Quantum Image Encryption Using A Self-Adaptive Hash Function-Controlled Chaotic Map (SAHF-CCM)

Roayat Ismail Abdelfatah

Electronics and Electrical Communications Engineering Dept., Faculty of Engineering, Tanta University, Tanta, Egypt.

Corresponding author: Roayat Ismail Abdelfatah (royat_esmaeel@f-eng.tanta.edu.eg)

ABSTRACT Recently, quantum image encryption algorithms are attracting more and more attention, due to the upcoming quantum threat problem to the current cryptographic encryption algorithms with the rapid progress toward the quantum computer production. The aim of this paper is to introduce a self-adaptive encryption scheme to protect quantum image efficiently with minimal storage requirements. The methodology is to use two rounds of encryption with two different pseudorandom number sequences which are obtained from a new designed pseudorandom number generator (PRNG). This PRNG consists of two parts. The first part is based on iterating a recently proposed chaotic-based parallel keyed hash function which is used as a controller for a second part. The second part is a multiplication of Tent and Chebyshev chaotic maps (TCM). This combination of hash function and chaotic maps provides high randomness and a dramatical increase in the control parameters and initial values number which achieves extremely large key space and so makes the scheme stronger against brute force attacks. The seed or initial value of PRNG depends on the input image itself which makes the scheme self-adaptive and so it is stronger against chosen plaintext attacks and known-plaintext attacks. In the first round of encryption, the value of each pixel qubits of the input image is changed to a new value by XORing it with the corresponding qubits of the first pseudorandom sequence using CNOT and Toffoli quantum gates then shifting to the next qubit with the Swap quantum gate. In this round, the pixel value is changed. In the second round, diffusion of the changed pixel value is extended to each pixel in the input image using the second pseudorandom sequence and Toffoli quantum gates. The time complexity of the proposed scheme is less than many recently published quantum image encryption schemes. The scheme security analysis is discussed, and the experimental results proved that the scheme is robust, secure and efficient.

INDEX TERMS Quantum encryption, Image, Pseudo random generator, Security analysis, Brute force attack, chosen plaintext attack, tent map, Chebyshev map.

II. INTRODUCTION

A. BACKGROUND

Images are important data carriers as they contain huge digital information with high redundancy and volume. This matter makes it more difficult to transmit or store images in a secure manner than text data. So, security of image has become an important matter and a common concern for researchers. With security, images can be protected against various threats such as illegal duplication and modification and eavesdropping. A lot of image encryption schemes originated from the classical encryption theories. These schemes convert the original images into meaningless form. Recently, with the rapid progress of the Internet, the database required for storing images such as fingerprints collected by Internet of Things (IOT) networks around the world is getting larger and larger which requires more storage space and faster processing speed. Feynman in 1982 first introduced the concept of quantum computer. Since then, quantum computing is continuously developed. In [1], Shor proposed Quantum factorization and quantum search algorithms had been proposed by Shor and Grover respectively in 1990s, [1, 2]. With the quantum computations rapid development, the studies on image processing have been developed from the classical image processing [3] to the quantum image processing (QIP) which has triggered researchers' interest. QIP is a rising field because of the quantum characteristics of coherence, entanglement, superposition and parallelism and so it an excellent tool to achieve real time processing. Also, n bits classical information can be stored with only $\mathrm{Log}_2 n$ quantum bits in QIP [4]. This exponential storage ability makes it more efficient tool to process, store and transmit images and has a significant reduced complexity [5]. However, QIP as rising technology has just begun and encryption of quantum images is still in its infancy in comparison with classical image encryption and research on it is still introductory and in its first steps. Quantum image representation and storage are important issues in QIP. In [6], Venegas-Andraca introduced the concept of Qubit

Lattice. Then Latorre in [7] proposed the Real Ket expression which needs n qubits to represent a $2^n \times 2^n$ image. The authors in [8], introduced Flexible Representation of Quantum Image (FRQI) that is very common model for quantum image expressions due to its simplicity. Some schemes have been proposed to represent the color images [9, 10]. In [9], the authors introduced a Novel Enhanced Quantum Representation (NEQR) model which has many advantages compared to FRQI model where any color is represented with q qubits, and hence 2^q colors can be represented at most. The main problem of quantum computing is that many complex operations are hard to be implemented, so the classical methods to scramble images can't be directly used in QIP. That is why quantum image scrambling schemes have high complexity and still in their first steps. The most common used image scrambling techniques use gray code, Arnold transformation, magic square transformation, ect. But all these scrambling techniques have major deficiency that the scrambling period is too short which causes iterations in image encryption have narrow range. This matter makes the encryption algorithm less secure and impractical. Chaotic systems are suitable for solving these problems due to their special features as initial values sensitivity, high performance, ergodicity, and mixing property. Recently, many schemes for encrypting images have been introduced based on chaotic maps for generating key streams [11, 12], as a Pseudo-Random Number Generator (PRNG). The output sequence of PRNG should have high randomness, high performance, sensitivity and huge key space to be strongly resistant to brute force attacks. PRN are generated by deterministic scheme which starts with initial seed value then pulling it out to obtain a long random sequence by iterations.

Many techniques can be used to implement PRNG such as chaotic maps. However, shorter period and less key space are chaotic maps weakness points. Some techniques are proposed to overcome these problems by combining various maps or multi chaotic maps, cellular automata, genetic algorithm, and hash functions [13, 14].

B. RELATED WORK

Generally, image encryption uses two basic tools which are scrambling and diffusion. Although the quantum image encryption is still in its first steps, researchers begin to study new encryption techniques as in [15-26]. In [15], the authors introduced a quantum medical image encryption scheme which uses gray code and a chaotic map. In [16], Arnold and Sine chaotic map are used in a quantum image encryption. The authors in [18], introduced a scheme for encrypting quantum image using Arnold map and wavelet transforms. A scheme for quantum image encryption scheme using one particle quantum walks on a circle has been proposed in [20]. In [23],3D Lorenz chaotic map and QR decomposition has been used for quantum image encryption. The authors in [24], introduced a quantum image scheme using bit-plane permutation and Sine Logistic map.

In [27], a quantum image encryption scheme using mutation and crossover operation in proposed. The authors in [28], used a key image for quantum image encryption. In [29], XOR operation has been used for encrypting quantum image. Image decomposition has been used for quantum image encrypting in [30]. Discrete Baker map has been used to encrypt quantum image in [31]. The authors introduced in [32], have encrypted quantum image using normal arbitrary superposition state (NASS) and random phase transformation. In [33], the authors used generalized Arnold transform and Logistic map for quantum image encrypting. Intra and inter bit permutation using Logistic map has been used for quantum image encryption in [34]. In [35], a double quantum image encryption based on Arnold transform has been introduced. The authors in [36], have encrypted quantum image with DNA Controlled Not. In [37], the authors used Lorenz hyper-chaotic system for encrypting quantum image. Feistel structure has been used for quantum image encryption [38].

However, most of the current schemes for encrypting quantum images are divided into three types: schemes use scrambling by gray code and bit plane (GC & BP), schemes use scrambling by improved (GC & BP), and schemes use scrambling with (GC & BP), and positioning. So, these schemes use only one tool, which is, scrambling. But the other image encryption tool which is diffusion needs to be more improved. That will be done in this paper.

- *Applications of the proposed scheme:*

Generally, image encryption has many applications in Internet communication, multimedia systems, healthcare, and military systems, where storage and transmission of images requires protection from different types of threats such as eavesdropping, unauthorized duplication and modification. Recently, with the fast growing of the Internet, the databases required for storing images become larger and larger which requires more space for storing and less processing time. As the proposed scheme incorporates quantum computing with image processing and due to the quantum properties, such as parallel computations, exponential storage capability, and tamper-proof security it could be used for powerful storing, processing, and retrieving of images and it is very suitable for real-time communications.

C. CONTRIBUTION AND PAPER ORGANIZATION

In this paper, a scheme for encrypting a quantum image using a new design for PRNG is introduced. The PRNG consists of two parts: the first part is used as a controller to the second one. The controller is an adaptive as its seed or initial value is extracted from the input original image and depends on iterating a chaotic-based parallel keyed hash function which has been introduced recently in [39]. It has five control parameters besides a secret seed or initial value. The second part of the PRNG is a multiplication of Tent and Chebyshev chaotic maps (TCM) and so it has four

control parameters and one secret initial value. Image encryption consists of only two rounds of simple CNOT, Toffoli, and Swap quantum gates operations. Each round uses a pseudorandom sequence generated by the combined PRNG but with different control parameters and initial values.

The key contributions of this paper are summarized as following

1. Using a novel design for PRNG which combines hash function and chaotic maps including four different chaotic maps: Chebyshev, Logistic, Sine and Tent maps providing higher randomness and dramatically enlarges the space of control parameters and secret values. The combined PRNG has nine control parameters and two secret seeds which gives a huge key space against brute force attacks.
2. The proposed PRNG is self-adaptive as its seed or initial value depends on the hash function SHA256 of the input image and varies with it. So, it can strongly resist both known-plaintext and chosen-plaintext attacks.
3. Most of the existing quantum image encryption schemes as in [15-18], [22], [24-26], [31, 32], and [34-37] use two independent rounds, scrambling and diffusion. In the scrambling round, the qubits are reordered with different types scrambling as gray code, bit-plane, Arnold map, Baker map, Hilbert transform, while in the diffusion round the qubit values are changed using XOR with a secret key. Generally, scrambling confuses the relation between the encrypted and unencrypted images, while diffusion spreads one qubit value change in the unencrypted image to the whole encrypted image. *Unlike* these existing schemes, the proposed scheme, uses two rounds for quantum image encryption, *but* each round combines both scrambling and XOR diffusion using a different secret key obtained from the proposed PRNG with different control parameters and initial values. This matter will double the total number of the control parameters from 9 to 18 and the number of initial secret values from 2 to 4 which provides extremely huge key space and so achieves much higher security.
4. The first round of encryption is designed such that each qubit of the input pixel affects *all* the 8 qubits of the output pixel. This is done by using Toffoli gates with the first pseudorandom sequence and Swap gates. This effect is extended to all the qubits of the encrypted image in the second round of encryption with Toffoli gates and the second pseudorandom sequence. This design is different from most of the previously mentioned known scrambling methods in which each input qubit affects only one or two output qubits of the encrypted image. So, the proposed scheme achieves complex relation between the key and the encrypted image and a complex relation between the unencrypted image and the quantum encrypted image. This ensures that small differences in the input image or in the keys lead to substantial changes in encrypted quantum image such that a potential attacker is unable to analyze the encrypted image.

Security analysis of scheme shows that the scheme has higher security and at the same time less complexity compared with other recent quantum image encryption schemes.

Although, the proposed scheme mixes some of already available techniques is the design of the proposed PRNG, but this is done in a new different way. These techniques are the keyed hash function (Khash) introduced recently in [39], Tent and Chebyshev chaotic maps. Firstly, Khash has been introduced in [39] as a novel structure for chaotic-based parallel hash function, but in the proposed scheme, it is modified to be used as PRNG by iteration. Secondly, this PRNG is in turn used as a controller for a second chaotic-based PRNG combing Tent and Chebyshev chaotic maps but in a new multiplicative form. The target of this mix is to merge larger number of different chaotic maps with huge number of control parameters in one new design PRNG and hence enhance the security of the scheme.

Besides, the quantum image encryption itself has a different design from most of the recently existing schemes as it has been explained previously.

The rest of the paper is organized as following: in Section II, the preliminaries are presented; in Section III, the proposed scheme is introduced. Section IV incudes performance analysis, simulation results, and comparisons. Conclusions are given in Section V

III. PRELIMINARIES

A. QUANTUM QUBITS AND GATES

A qubit is used to store, manipulate and measure information in quantum computing. Quantum mechanics is used to describe the qubit. A unit vector in two-dimension Hilbert space is used to describe the quantum state of a single qubit which denoted by the notation $|\ \ \rangle$. A qubit $|\varphi\rangle$ can be written in a general form as:

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\begin{bmatrix}1\\0\end{bmatrix} + \beta\begin{bmatrix}0\\1\end{bmatrix} = [\alpha \quad \beta]^T \quad (1)$$

where $\alpha, \beta \in C$, C is the complex set and $|0\rangle$and $|1\rangle$ are the two-dimensional quantum computational basis states. α, β are the amplitude of the basis states$|\alpha|^2 + |\beta|^2 = 1$.

$\otimes$ is the tensor product. Let X be a $i \times i$ matrix and Y be a $j \times j$ matrix, then the tensor product $X \otimes Y$ is a $ij \times ij$ block matrix defined as:

$$X \otimes Y = \begin{bmatrix} X_{0,0}Y & \cdots & X_{0,i-1}Y \\ . & \cdots & . \\ . & \cdots & . \\ X_{i-1,0}Y & \cdots & X_{i-1,i-1}Y \end{bmatrix} \quad (2)$$

Quantum gates are the basic components of the quantum circuit. Any complex quantum gate can be represented by a series of one-qubit and two-qubit gates [40]. A quantum gate for n-qubit can be described by a $2^n \times 2^n$ unitary matrix.

The proposed scheme for encrypting quantum image uses the quantum gates: Controlled-NOT gate (CNOT), Swap gate, and Toffoli (Controlled CNOT) gate. The matrix and

symbol representations of these gates are shown in Figure 1:

CNOT gate: It acts on 2 qubits, and carries out the NOT operation on the second qubit only when the first qubit is $|1\rangle$,and otherwise leaves it unchanged. The CNOT (or controlled Pauli-*X*) gate can be described as the gate that maps the basis states $|a,b\rangle \rightarrow |a, a \oplus b\rangle$,where ($\oplus$) is XOR logic operation.

SWAP gate: It swaps two qubits.

Toffoli gate: It is related to the classical AND ($\wedge$) and XOR ($\oplus$) operations as it performs the mapping $|a,b,c\rangle \rightarrow |a,b,\ c \oplus (a \wedge b)\rangle$.

B. QUANTUM IMAGE REPRESENTATION

NEQR [9] is a better alternative to FRQI [8] as it uses the basic states of qubit sequence to substitute the probability of amplitude which help in the accurate recovery of original image. An image of size $2^n \times 2^n$ can be represented with $2n+q$ qubits, where $2n$ qubits represent the position of the pixels while q bits represent the gray values. A $2^n \times 2^n$ grayscale image I with a 256-pixel values from 0 to 255 can represented as follows:

$$|I\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|C_i\rangle \otimes |i\rangle \quad (3)$$

where $|C_i\rangle = |C_{i7}\, C_{i6}\, \ldots\ldots C_{i1}\, C_{i0}\rangle$,$C_{ik} \in \{0,1\}$, $k = \{0, \ldots\ldots, 7\}$.. represents the gray information of corresponding pixel in the position $|i\rangle$.

C. CHAOTIC MAPS

Confusion and diffusion are the two basic tools for encrypting images in most of the modern schemes. Confusion is to make more complex relation between the ciphertext and the key as possible. Diffusion is to completely dissipate the statistic of plaintext in the ciphertext statistics. In cryptography, chaotic maps have been used as a tool of achieving confusion and diffusion due to its high sensitivity to its control parameters and seeds. This matter makes the system more random. So, by making these parameters secret, chaotic maps can be used for encryption.

Chaotic maps are classified into two types: one-dimensional which has little parameters and high dimensional chaotic maps which has larger parameter space but are more complex.

Examples of one-dimensional maps are Sine map, Logistic, Chebyshev, and Tent map which are defined as follows:

Sine map:

$$z_{n+1} = r \times (\sin(\pi \times z_n)) \quad (4)$$

Logistic map:

$$z_{n+1} = \mu \times z_n(1 - z_n) \quad (5)$$

Chebyshev map:

$$z_{n+1} = \cos\left(\gamma \times cos^{-1}(z_n)\right) \quad (6)$$

Tent map:

$$z_{n+1} = \omega \times \left(1 - 2 \times abs(z_n - 0.5)\right) \quad (7)$$

Where z_0 is initial value, $z_n \in [0, 1]$ and r, μ, γ and ω are control parameters.

D. CHAOTIC-BASED KEYED HASH FUNCTION

Hash function is a very important tool of achieving message integrity in cryptography. Hash function is classified into unkeyed hash function as MD5, SHA-1, SHA-2, and SHA-3 and keyed hash function which takes the message and secret keys as input. In [39], the authors proposed a parallel keyed hash algorithm using multiple chaotic maps which are Logistic, Tent, and Sine maps.

In this algorithm the coupling lattice structure is modified and the diamond lattice is used as a new structure. Its output length is 128 or 256. This algorithm achieved many advantages compared with recently published schemes such as higher efficiency, simplicity, and speed. The authors in [39] give quantitative indicators for these advantages by making a speed comparison with other schemes as [41-43]. The speed in [41] is 0.697 Gbps. In [42], the speed is 0.761 Gbps, while in [43], it is 0.314 Gbps. The Keyed hash (Khash) used in the proposed PRNG has the highest speed among these schemes which is 0.883 Gbps.

The structure of this algorithm is shown in Figure 2. Where, M_1, M_2, M_3……., M_L are the input message blocks. Where M_i refers to i^{th} input message block. A is a logistic map used to generate Tent map initial values for the next stage, F_1 is Tent map, F_2 is Sine map, and F_3 is Logistic map. The secret keys are initial value x_0, control parameters r_1, r_{s2}, r_{s3}, q, and proportion coefficient p. More details about this algorithm are provided in [39].

IV. PROPOSED SCHEME METHODOLOGY AND PARAMETERS

A. PROPOSED PRNG

A new design of PRNG is introduced in this paper which combines two parts:

The first part:

It is a controller to the other part. The controller is based on iterating the keyed hash function Khash, proposed in [39]. The output length is 256 bits. The basic operation of the algorithm is as following:

For i =1 to m:

$$h_i = KHash(h_{i-1} \oplus seed) \quad (8)$$

where $seed$ is the initial value of length 256 bit.

Thus, the pseudorandom sequence output of the controller is $h_1 || \ h_2 || \ \ldots\ldots\ldots || \ h_m$.

The secret keys for this part are:

The seed h_0 , the secret key SK_1, Logistic map initial value x_0, and control parameters r_1, r_{s2}, r_{s3}, q, and proportion coefficient p.

The second part:

It is the multiplication of both Tent and Chebyshev chaotic maps (TCM) as follows:

$$Z_n = \mu \times (1 - 2 \times abs(Z_{n-1} - 0.5)) \times \cos\left(k \times cos^{-1}(Z_{n-1})\right) \quad (9)$$

The secret keys for TCM are: Z_0 , μ and k.

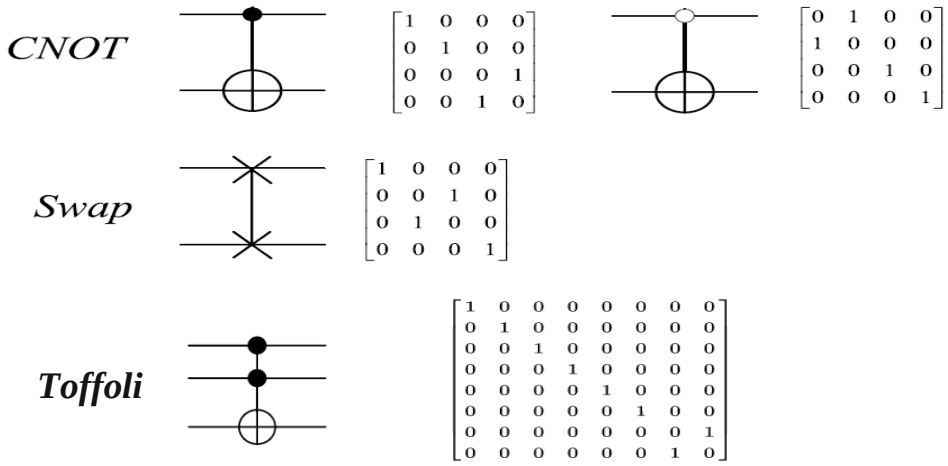


FIGURE 1. Symbols and metrices of some basic quantum gates

The proposed PRNG:

It is a combination of the controller and TCM as shown in Figure 3

Its operation is as follows:

When the binary output of the controller is 0 the TCM is iterated as in Eqn. (9) with control parameters , μ_1 and k_1, while when the binary output of the controller is 1, the TCM is iterated as in Eqn. (9) but with different control parameters μ_2, and k_2.

So, the secret key for the proposed PRNG:

The initial values: Z_0 h_0, x_0 and SK_1, the control parameters $r_1, r_{s2}, r_{s3}, q, p, \mu_1, k_1, \mu_2,$ and k_2.

The basis for the selection of these parameters

The control parameters range for the first part of the proposed PRNG are as follows:

r_1, r_{s2} and $r_{s3} \in [3.57, 4]$.

$q \in [1, 2]$.

$p \in [0, 1]$.

The control parameters range for the second part of the proposed PRNG are as follows:

Both μ_1 and $\mu_2 \in [0, 2]$.

Both k_1 and $k_2 \geq 2$.

SP800–22 tests by NIST can be used to measure the randomness of the proposed PRNG output as it is one of the most common standards. It consists of 17 tests on binary data [44] shown in Table 1, where one or more P values are computed.

If P is greater than 0.01, the test is passed, otherwise, the test is failed. 10^6 bit binary sequence output of the proposed PRNG is tested by SP800–22 with10^3 iterations and the results are shown Table 1. The proposed PRNG output passes all the 17 tests as P-values are greater than 0.01.

B. PROPOSED QUANTUM IMAGE ENCRYPTION

The block diagram of the proposed scheme is indicated in Figure 4. The image encryption consists of two rounds. Each round needs a PR sequence of size $2^n \times 2^n$ (same size of input image).

1) GENERATION OF THE TWO PR SEQUENCES

1. Use SHA-256 to compute the hash of the input image then use it as a seed to the controller of the proposed PRNG (Keyed hash) as follows:

$$\text{Seed}_1 = h_0 = SHA_{256}(\text{input image}) \quad (10)$$

2. Set the appropriate values for the Control Parameters#1 $[x_0, r_1, q, r_{s2}, r_{s3}, p]$ as follows:
   - The first logistic map: x_0 = 0.98765 and r_1 = 3.9393. The Tent map: q = 1.5151.
   - The second and third Logistic maps: r_{s2} = 3.83, and r_{s3} = 3.73 respectively.
   - A proportion coefficient: p = 0.6543.
   - The controller output will be obtained by iterating Eqn. (8) to obtain a binary sequence of size $2^n \times 2^n$ from $h_1 || h_2 || \ldots\ldots\ldots || h_m$.
   - With the Control Parameters #2, iterate Eqn. (9) to obtain PR_1 sequence of size $2^n \times 2^n$ as follows:
     - When the controller output is "1" then iterate the TCM with values: $\mu_1 = 0.56$, $k_1 = 5.782595812953629$, and $Z_0 = 0.25$.
     - When the controller output is "0" then iterate the TCM with different values: $\mu_2 = 0.55$, $k_2 = 5.792595812953629$, and $Z_0 = 0.25$.
     - So, the Control Parameter#2 = $\{Z_0, \mu_1, k_1, \mu_2, k_2\}$.
     - The output of the TCM is the required first pseudo random sequence of the first round (PR_1).
3. To obtain the pseudo random sequence for the second round (PR_2) use the proposed PRNG but with different seed computed as follows:

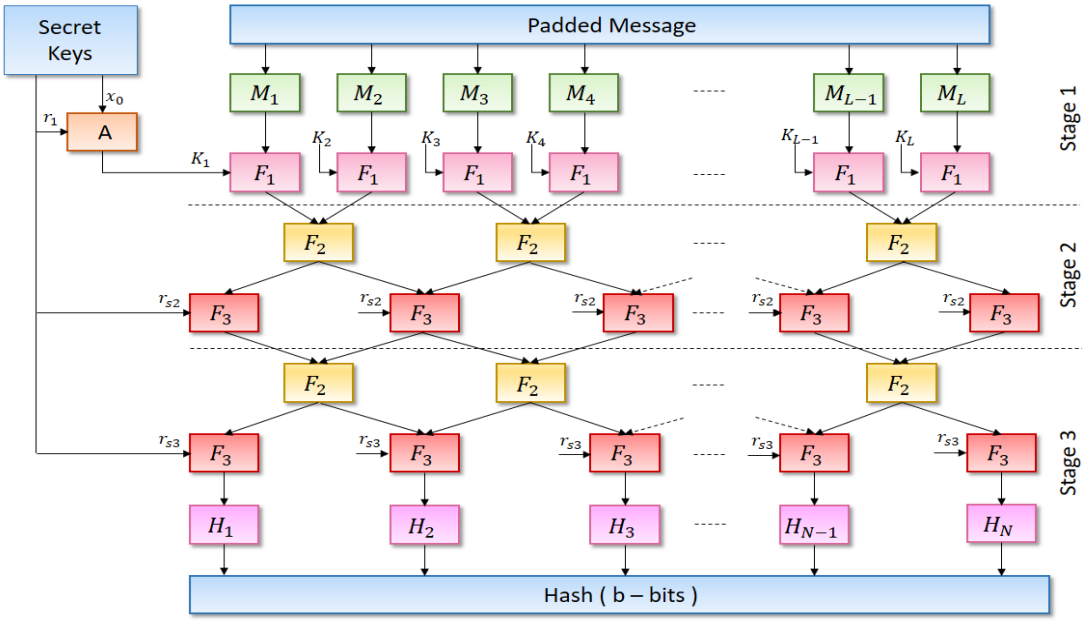


FIGURE 2. The structure of the keyed parallel hash function

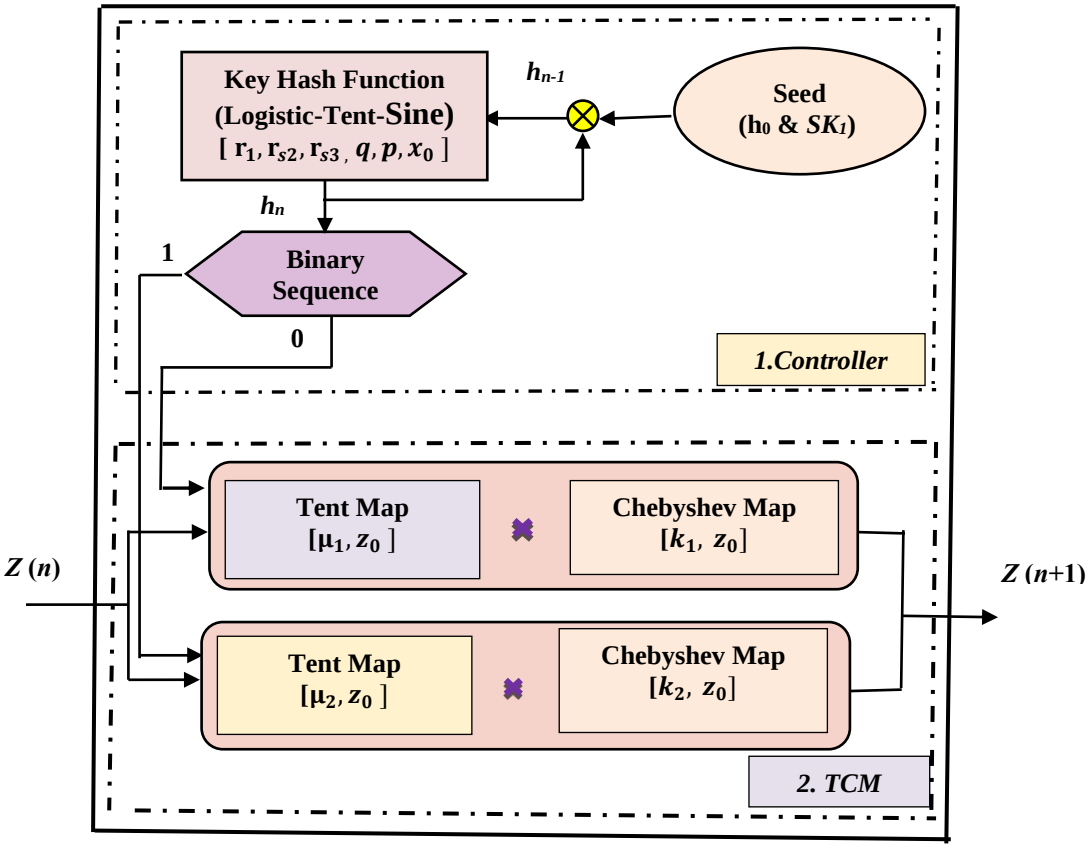


FIGURE 3. The Proposed Combined PRNG

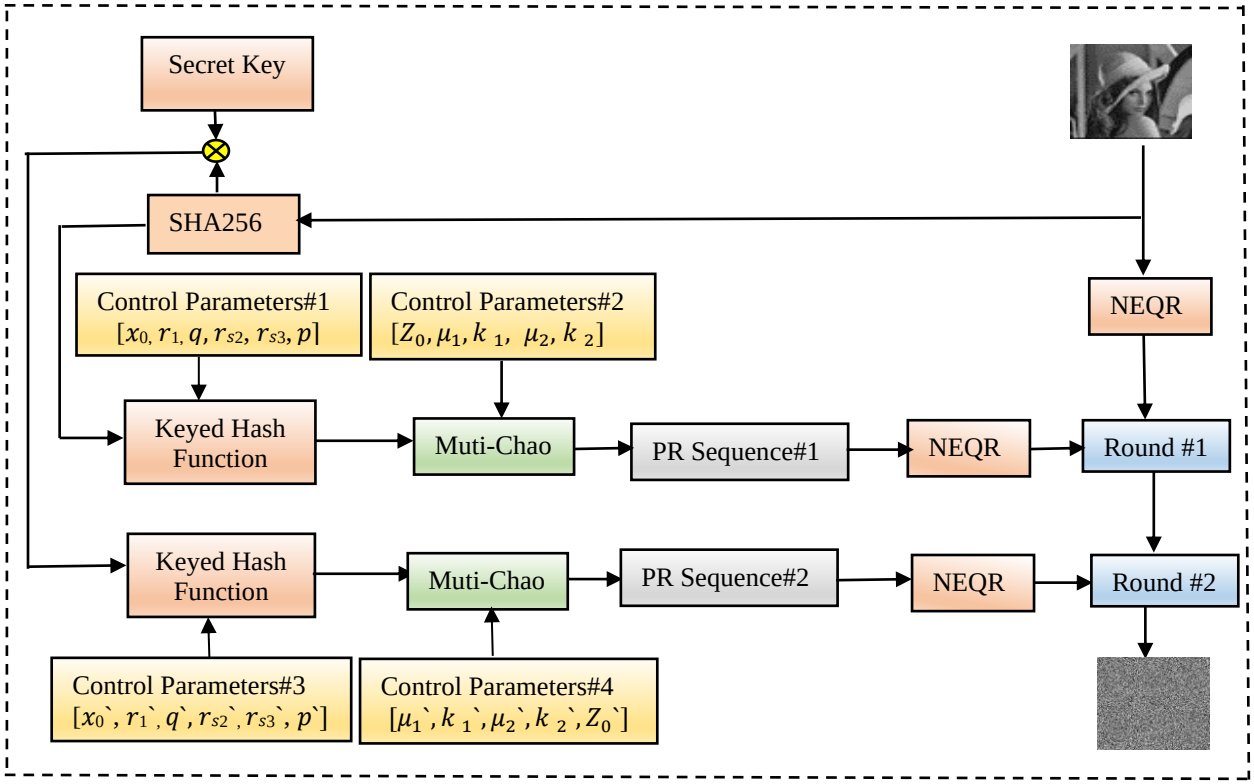


FIGURE 4: The Block diagram of the proposed scheme

TABLE I
RESULTS OF SP800-22 FOR PROPOSED PRNG

Test name	P-value	Results
Monobit frequency	0.32817	Pass
Block frequency	0.12663	Pass
Runs	0.90055	Pass
Longest-run-of-ones in a block	0.97111	Pass
Binary matrix rank	0.99291	Pass
Discrete Fourier transform (spectral)	0.68134	Pass
Non-overlapping template matching	0.93882	Pass
Overlapping template matching	0.20494	Pass
Maurer's universal statistical	0.81224	Pass
Linear complexity	0.82925	Pass
Serial test	{0.09665, 0.08326 }	Pass
Approximate entropy	0.60390	Pass
Cumulative sums	0.29440	Pass
Random excursions	{0.29154, 0.46718 , 0.38049 , 0.31633 , 0.84738 , 0.49063 , 0.81958 , 0.45791 }	Pass
Random excursion variant	{0.67186, 0.64381 , 0.75916, 0.81035 , 0.77945 , 0.46724 , 0.20216 , 0.08486, 0.08869 , 0.91198 , 0.77885, 0.88991, 0.78274 , 0.50247, 0.40848 , 0.26972, 0.24422 , 0.39988 }	Pass
Cumulative sums test reverse	0.37194	Pass
LempelZiv compression	1.	Pass

$$\text{Seed}_2 = h_0 \oplus SK_1 \quad (11)$$

where SK_1 is a secret key of length 256 bit. It uses also different control parameters: Control Parameters#3: $[x_0`, r_1`, q`, r_{s2}`, r_{s3}`, p`]$, and TCM control parameters#4 :$\{\mu_1`, k_1`, \mu_2`, k_2`, Z_0`\}$.

2) IMAGE ENCRYPTION

The original image of size $2^n \times 2^n$ is first represented with NEQR model as in Eqn. (3).

where $|C_i\rangle = |C_{i7}^{old} C_{i6}^{old} \ldots\ldots C_{i1}^{old} C_{i0}^{old}\rangle, C_{ik} \in \{0,1\}, k = \{0, \ldots\ldots, 7\}$ represents the gray information for each pixel its position is *i*.

Also, both the two pseudo random sequences PR_1 and PR_2 are represented with NEQR model as follows:

The first pseudo random sequence:

$$|PR_1\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1} |K_i\rangle \otimes |i\rangle \quad (12)$$

where $|K_i\rangle = |K_{i7} K_{i6} \ldots\ldots K_{i1} K_{i0}\rangle, K_{ik} \in \{0,1\}, k = \{0, \ldots\ldots, 7\}$.

The second pseudo random sequence:

$$|PR_2\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1} |R_i\rangle \otimes |i\rangle \quad (13)$$

where $|R_i\rangle = |R_{i7} R_{i6} \ldots\ldots R_{i1} R_{0i}\rangle, R_{ik} \in \{0,1\}, k = \{0, \ldots\ldots, 7\}$.

First round of encryption:

In this round, XOR operation with the corresponding qubit of the first pseudorandom sequence PR_1 is used to change the value the qubit of each pixel at position i, where $0 \leq i \leq 2^{2n} - 1$ of the input image. The quantum gates used are

CNOT and Toffoli gates then the new value is shifted to the next qubit with the Swap quantum gate. In this round, the pixel value is changed such that each qubit affects all the new value of all the subsequent qubits but in the same pixel at position *i*. In this round, the gray information of each pixel in the image at position *i* is changed from $|C_i^{old}\rangle = |C_{i7}^{old} C_{i6}^{old} \ldots\ldots C_{i1}^{old} C_{i0}^{old}\rangle$ to $|C_i^{new}\rangle = |C_{i7}^{new} C_{i6}^{new} \ldots\ldots C_{i1}^{new} C_{i0}^{new}\rangle$ by using the first pseudo random sequence PR_1 of gray information $|K_i\rangle = |K_{i7} K_{i6} \ldots\ldots K_{i1} K_{i0}\rangle$. For each pixel at position *i*, the gray information change operation from C_{old} *to* C_{new} can be defined by as follows:

$$C_{i0}^{new} = K_0 \oplus C_{i0}^{old} \quad (14)$$
$$C_{i1}^{new} = (K_1 \wedge C_{i0}^{new}) \oplus C_{i1}^{old} \quad (15)$$
$$C_{i2}^{new} = (K_2 \wedge C_{i1}^{new}) \oplus C_{i2}^{old} \quad (16)$$
$$C_{i3}^{new} = (K_3 \wedge C_{i2}^{new}) \oplus C_{i3}^{old} \quad (17)$$
$$C_{i4}^{new} = (K_4 \wedge C_{i3}^{new}) \oplus C_{i4}^{old} \quad (18)$$
$$C_{i5}^{new} = (K_5 \wedge C_{i4}^{new}) \oplus C_{i5}^{old} \quad (19)$$
$$C_{i6}^{new} = (K_6 \wedge C_{i5}^{new}) \oplus C_{i6}^{old} \quad (20)$$
$$C_{i7}^{new} = (K_7 \wedge C_{i6}^{new}) \oplus C_{i7}^{old} \quad (21)$$

These operations are followed by the qubits shifting or permutation of qubits of each pixel at position *i*, where, $0 \leq i \leq 2^{2n}$-1, which changes the order of the qubits in each pixel. This operation is done by swap gates indicated in Figure 5, where the gray value of the pixel at position *i* is changed from $|C_{i7}^{new} C_{i6}^{new} C_{i5}^{new} C_{i4}^{new} C_{i3}^{new} C_{i2}^{new} C_{i1}^{new} C_{i0}^{new}\rangle$ to $|C_{i6}^{new} C_{i5}^{new} C_{i4}^{new} C_{i3}^{new} C_{i2}^{new} C_{i1}^{new} C_{i0}^{new} C_{i7}^{new}\rangle$

To make the effect of this one pixel change of the input image be extended to all the next pixels of the image, there will be a second round of encryption as follows:

Second round of encryption:

The input to this round is the output of the first round $|C_i^{new}\rangle = |C_{i7}^{new} C_{i6}^{new} \ldots\ldots C_{i1}^{new} C_{i0}^{new}\rangle$,

where *i* is the pixel position, $0 \leq i \leq 2^{2n}$-1. In this round, each pixel at position *i* will be diffused to all the subsequent pixels of the image.

The new value of current pixel at position *i*+1, ($0 \leq i \leq 2^{2n}$-2):

$|C``_{i+1}^{new}\rangle = |C``_{(i+1)7}^{new} C``_{(i+1)6}^{new} \ldots\ldots C``_{(i+1)1}^{new} C``_{(i+1)0}^{new}\rangle$ is the addition of the new value of the previous pixel at position *i*, $|C``_{i}^{new}\rangle = |C``_{(i)7}^{new} C``_{(i)6}^{new} \ldots\ldots C``_{(i)1}^{new} C``_{(i)0}^{new}\rangle$ with the current value of the second pseudorandom sequence $PR_2 = |R_{i+1}\rangle = |R_{(i+1)7} R_{(i+1)6} \ldots\ldots R_{(i+1)1} R_{(i+1)0}\rangle$ then XORed with the current value of pixel output from the first round $|C_{i+1}^{new}\rangle = |C_{(i+1)7}^{new} C_{(i+1)6}^{new} \ldots\ldots C_{(i+1)1}^{new} C_{(i+1)0}^{new}\rangle$.

$$|C``_{i+1}^{new}\rangle = |C_{i+1}^{new}\rangle \oplus (|C``_{i}^{new}\rangle \wedge |R_{i+1}\rangle) \quad (22)$$
$$\text{and } |C``_{0}^{new}\rangle = |C_{0}^{new}\rangle \oplus |R_0\rangle \quad (23)$$

This operation is done with Toffoli gates, one for each qubit of the image pixels.

For decryption, the encryption process shown in Figure 4 is reversed.

Note: We can apply the proposed scheme to color images as follows:

- Decompose the original RGB image of size $2^n \times 2^n$ into three layers (R = Red, G = Green, and B = Blue).
- Apply the encryption scheme separately to each layer.
- Each layer R, G, and B is represented with NEQR model as in Eqn. (3).
- Apply the proposed PRNG three times but with different control parameters and initial values to obtain six different pseudorandom sequences PRs: two PRs for each layer.
- Use SHA-256 to compute the hash of each layer R, G, and B then use it as a seed h_0 to the controller of the proposed PRNG. Also, three different secret keys SK_1 are used: one for each layer.
- Finally, after applying the encryption scheme to each layer, recompose the three encrypted layers into one RGB image.

The number of secret keys for RGB images is three times that of the gray scale ones.

V. PERFORMANCE ANALYSIS AND SIMULATION

Due to difficulty of building quantum computer till now and its unavailability for practical implementation of quantum image encryption, all recent quantum image encryption schemes in [15-38] and [45] depends on experimental results obtained by using software simulation to prove security and performance of encryption.

Similarly, MATLAB platform on classical computer will be used to verify the security and performance of the proposed scheme because MATLAB provides facility to represent and manipulate large arrays of vectors and matrices, and hence effective stimulation for quantum states and operator. The laptop used is 11th Gen Intel(R) Core (TM) i7-1165G7@2.80GHz,2803 Mhz, 4 Cores, 8L. RAM 16 GB. Windows 11 Pro (64-bit), MATLAB 2017a.

Basically, Heisenberg uncertainty principle and quantum no-cloning theory is the main reason for the security of proposed quantum image encrypting scheme. That is due to the destruction of a quantum superposition state and its collapse to a determinate quantum state irreversibly with measurement. So, the intended receiver will detect changes when any attack takes place. This will provide strong defense against eavesdropping and leakage during transmission.

Further, the image is secured by the two rounds of encryption with the two different pseudo random outputs and huge number of secret keys.

To prove the security and efficiency of the proposed scheme, some simulation experiments will be carried out. Without losing generality, public test images taken from the USC-SIPI Image Database are adopted. Test images are 8-bit grayscale images with a size of 256 × 256, such as Lena, Cameraman, Baboon, Pepper, and Barbara. Also, the scheme is applied to a 512 ×512 Baboon image as an example of larger size images.

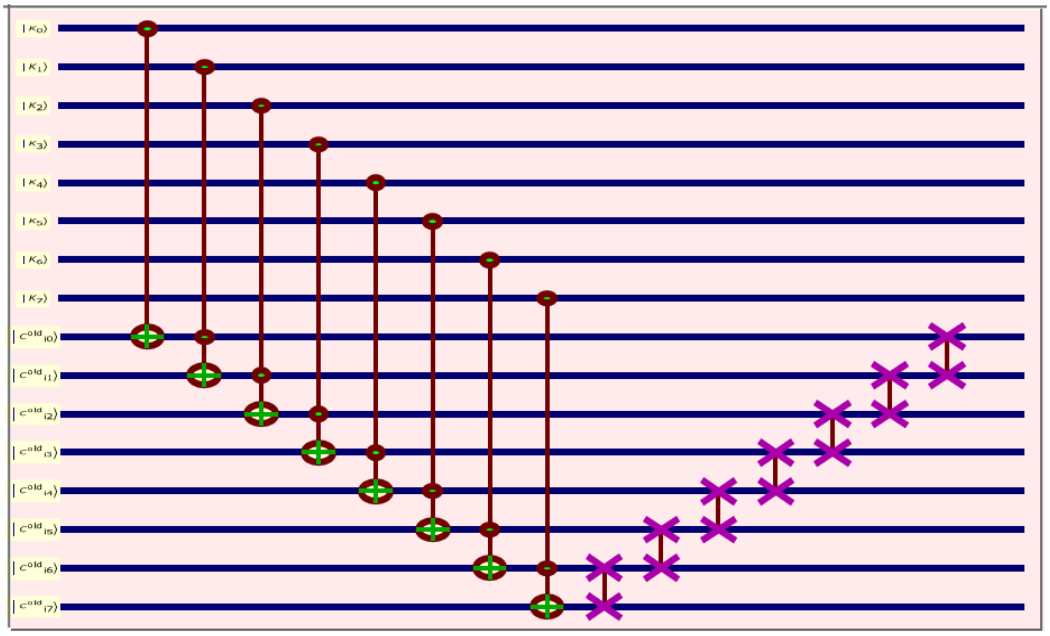


FIGURE 5: **Encryption first round**

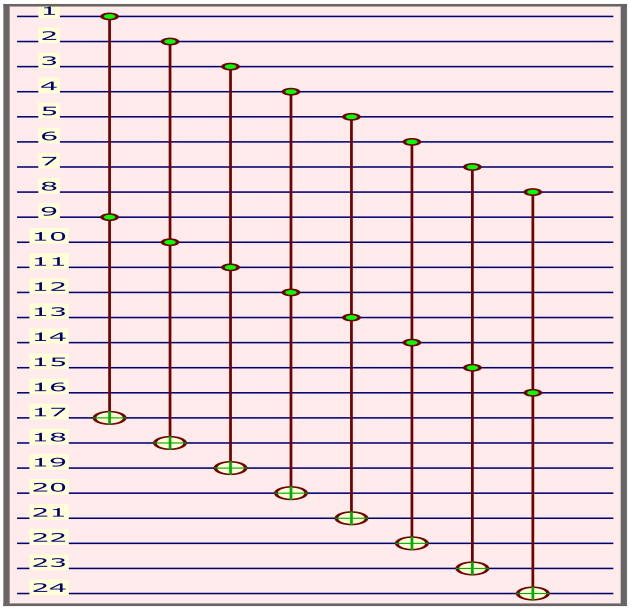


FIGURE 6: **Encryption second round**

A. VISUAL EFFECTS

The proposed scheme is applied to the five images of size 256 × 256 and results are indicated in Figure 7. Also, it is applied to Baboon 512 × 512 image to prove its security and robust performance when applied to larger size image. In Figure 6, the qubits from 1 to 8 represent the current pixel value, the qubits from 9 to 16 represent the previous pixel value, while the qubits from 17 to 24 represent the current qubits of the second pseudorandom sequence PR_2. The proposed scheme transfers the input images (as in Figure. 7 (a)-(e)) into approximately random meaningless encrypted images (as in Figure 7 (k)-(o)) and no information can be seen from it. So, it visually secures the original image. While the decrypted images and the original images are identical (Figure 7 (u)-(y)). Figure 8 shows Baboon 512×512 plain image, its corresponding cipher image, and the histogram of both.

B. STATISTICAL ANALYSIS

The ability of the proposed scheme to resist statistical analysis attacks can be measured by different metrices such as, histogram, correlation coefficients, information entropy, UACI and NPCR. It is a good judge for the scheme advantages and disadvantages.

1) HISTOGRAM

Histogram is a graph which measures the pixels intensities distribution of the image. In Figure 7, the histogram of the original images: Lena, Baboon, Cameraman, Pepper and Barbara is from (f)-(j), histogram of the corresponding encrypted images is from (p) to (t). It is shown that the encrypted images histogram has nearly flat uniform distribution. There is another measure of evenly distributed pixels of encrypted image called "histogram variance" given as follows:

$$Var(y) = \frac{1}{n^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\frac{1}{2}(y_i - y_j)^2 \qquad (24)$$

Table 2 indicates the *Var* of both the original and the encrypted images and comparison with other recent schemes as [16], [24], [36] which indicates that our scheme has smaller value of *Var*. It is clear that the original images have high *Var* while the encrypted images have very low values. After encryption, the variance is reduced.

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3212899

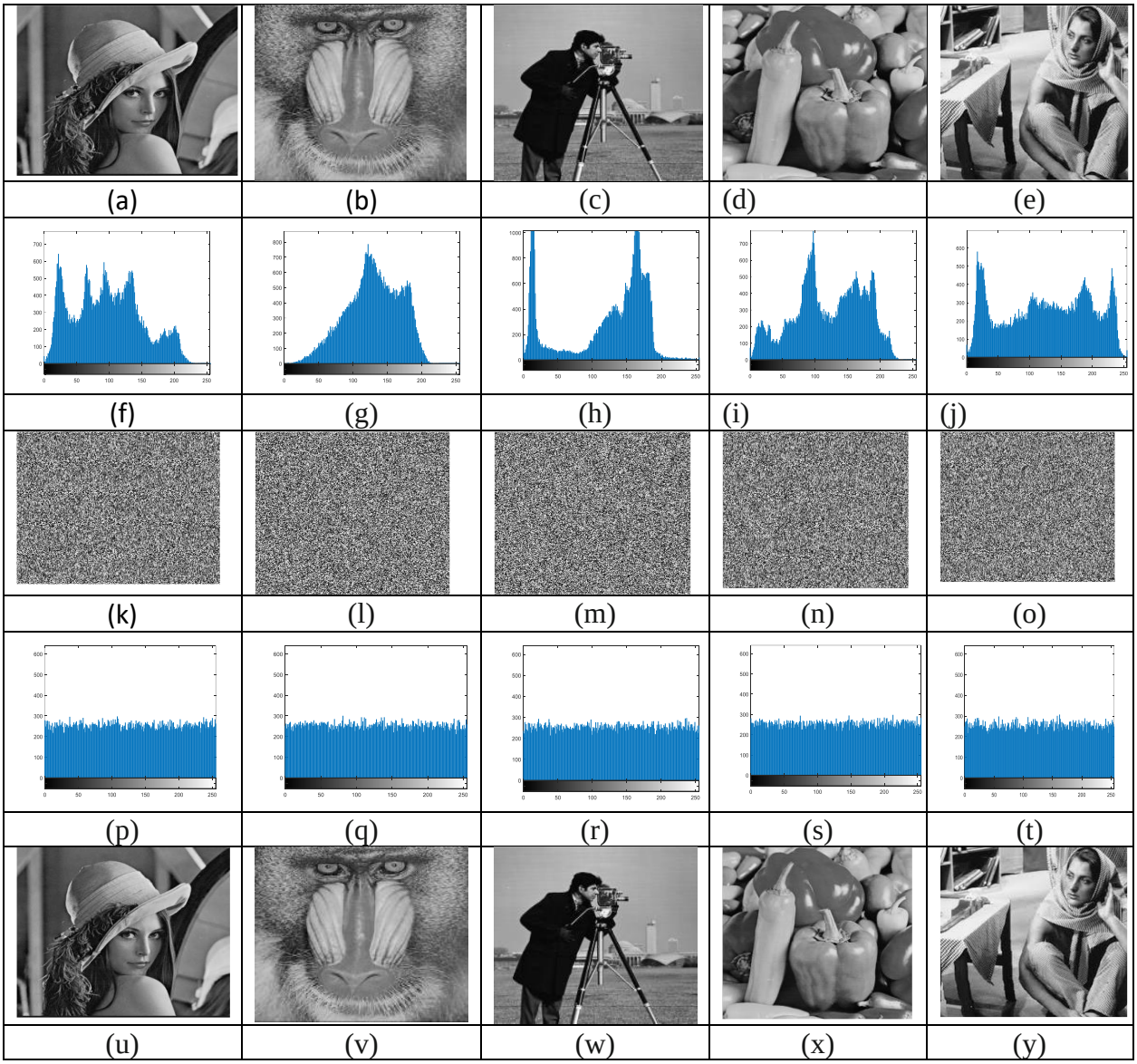


FIGURE 7: Experimental results for images of 256×256 size: (a) Lena; (b) Baboon; (c) Cameraman; (d) Pepper; (e) Barbara; (f)-(j) Corresponding images histogram (a)-(e); (k)-(o) Corresponding encrypted images of (a)-(e);(p)-(t) Corresponding encrypted images histogram (k)-(o); (u)-(y) Corresponding decrypted images of images (a)-(e).

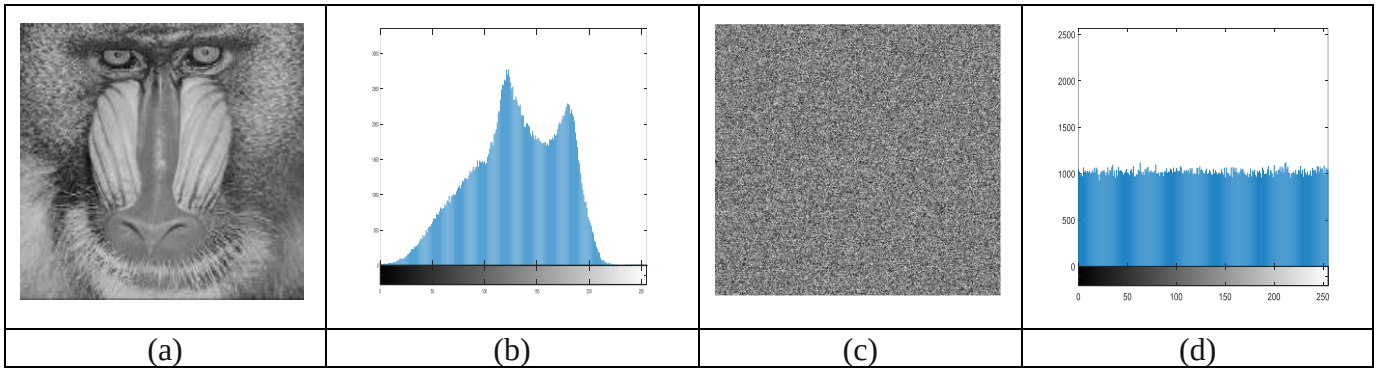


FIGURE 8: Experimental results for Baboon 512 × 512: (a) Baboon plain image (b) Baboon plain image histogram (c) Baboon Cipher image (d) Baboon cipher image histogram.

When the variance decreases, the uniformity of pixels distribution increases and the strength of encryption scheme against statistical attack increases.

2) CORRELATION COEFFICIENT

In general, unencrypted image adjacent pixels correlation is strong. But, after encryption this correlation has to be reduced. The following equation defines the correlation coefficient (CC) :

$$CC = \frac{\sum_{j=1}^{2^n}(x_j-\bar{x})(y_j-\bar{y})}{\sqrt{\sum_{j=1}^{2^n}(x_j-\bar{x})^2 \sum_{j=1}^{N}(y_j-\bar{y})^2}} \quad (25)$$

Where x_j and y_j represents two neighboring pixels gray values, respectively. $\bar{x}$ and $\bar{y}$ represent corresponding mean values. For the proposed scheme, 10^4 pairs of pixels of the original and encrypted images are chosen in random in horizontal, vertical, and diagonal dimensions. When the correlation value between adjacent pixels gets closer to 0, this increases the difference between them, and hence makes it harder for an opponent attack the scheme from this side. The CC values are of the tested images are shown in Table. 3. It is clear that CC values of original images are closer to1, where the CC of the encrypted images are closer to 0. For more clarifying of the difference, Baboon image is taking as an example and the correlation distribution is the three dimensions are shown in Figure 9.

3) INFORMATION ENTROPY

Generally, the entropy measures system confusion. According to Shannon's definition for entropy in information theory, a 8-bit image with probability distribution P, the information entropy is E is given as follows:

$$E = -\sum_{j=0}^{2^8-1} P(j) log_2 P(j) \quad (26)$$

where $P(j)$ is the probability of an image gray value j. When all the gray values with equal probability, this means that pixels of the image have enough confusion, and the ideal value of E is 8. Table 4 shows the entropy values of both the unencrypted and original tested images. These values prove that our scheme has high confusion as the values exceed 7.99 and extremely near 8.

The same table also shows a comparison with other recent quantum image schemes. This comparison proves that our scheme is more resistant against entropy attack.

4) UACI AND NPCR ANALYSIS

A measure of an encryption scheme pixel change sensitivity is the unified average changing intensity (UACI) and number of pixels change rate (NPCR) which is used as a good tool to evaluate the resistance against differential attack. It is given as following:

$$UACI = \frac{1}{2^{2n}}\sum_{i,j}\frac{|C_1(i,j)-C_2(i,j)|}{255} \times 100\% \quad (27)$$

$$NPCR = \frac{1}{2^{2n}}\sum_{i,j}|D(i,j)| \times 100\% \quad (28)$$

where C_1 and C_2 represent encrypted images of the original image and the original image with one pixel change, respectively. If two pixels $C_1(i,j)$ and $C_2(i,j)$ have equal value the $D(i,j)$ equals 0, while there is a difference between the two pixels $C_1(i,j)$ and $C_2(i,j)$ then $D(i,j)$ equals 1. Theoretically, NPCR = 99.6094% and UACI = 33.4635%. Table 5 lists the results compared with some recent schemes.

Tables 3, 4, and 5 listed the experimental results of images of size 256×256, while all the results of Baboon 512×512 image are listed in Table 6 as an example of larger size images. The results shown in Table 6 prove that the proposed scheme achieves high security for lager size images also.

5) SPECTRAL ANALYSIS

Fourier spectrum measures the statistical property of the encrypted image [20]. It is studying image properties with using Fourier transform. If $I(x,y)$ is an image, the discrete Fourier transform $FT(u,v)$ of the image $I(x,y)$ is defined as following:

$$FT(u,v) = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} I(x,y)e^{-2\pi i(\frac{ux}{N}+\frac{vy}{N})} \quad (29)$$

The amplitude spectrum of $FT(u,v) = FT_{real}(u,v) + iFT_{im}(u,v)$ is given by

$$||FT(u,v)|| = \sqrt{(FT_{real}(u,v))^2 + (FT_{im}(u,v))^2} \quad (30)$$

Spectrum analysis mainly measures the encryption scheme robustness against statistical attacks. Figure 10 indicates the spectrum of the tested original and encrypted images. It is clear that the original image has a non-uniform amplitude spectrum, while the encrypted image has nearly uniform amplitude spectrum. This proves that the attacker cannot extract any beneficial data from the spectrum amplitude, so the proposed scheme is well resistant against spectrum attack.

C. KEY SPACE ANALYSIS

The larger key space the stronger resistance against brute force attack. With the current computing abilities, the key space should exceed 2^{100}. The proposed scheme has 24 secret key parameters which are:

- h_0 the hash function of the input image of length 256 bit.
- The secret key SK_1 of length 256 bits.
- The control parameters#1 $[x_0, r_1, q, r_{s2}, r_{s3}, p]$.
- The control parameters#2: $[\mu_1, k_1, \mu_2, k_2, Z_0]$
- The control parameters#3: $[x_0`, r_1`, q`, r_{s2}`, r_{s3}, p`]$.
- The control parameters#4: $[\mu_1`, k_1`, \mu_2`, k_2`, Z_0`]$.

For computation precision around 2^{52} [46], the key space equals

$$(2^{256})^2 \times (2^{52}\times 2^{52}\times 2^{52}\times 2^{52}\times 2^{52}\times 2^{52})^2 \times (2^{52}\times 2^{52}\times 2^{52}\times 2^{52}\times 2^{52}\times 2^{52})^2 = 2^{1656}$$

In comparison with other schemes, the proposed scheme has extremely wide key space as shown in Table 7. So, it is stronger against brute force attack.

TABLE 2
ORIGINAL AND ENCRYPTED IMAGES VARIANCE VALUES HISTOGRAM

Image	Original	Encrypted	Ref. [24]	Ref. [36]	Ref. [45]
Cameraman	11097.3304	**233.0666**	270.5625	-	291.53
Peppers	34877.9687	**238.3372**	243.6953	239.4871	286.64
Baboon	65912.5468	**238.0235**	-	254.8438	-
Barbara	35966.6718	**280.3921**	259.3906	-	-
Lena	30542.9333	**254.8549**	-	-	-

TABLE 3
CC VALUES OF ORIGINAL AND ENCRYPTED IMAGES INDICATED IN FIGURE 7

Correlation Coefficient	Horizontal	Vertical	Diagonal
Lena	0.9552	0.9150	0.9421
Encrypted Lena	**-0.000465**	**-0.0037**	**-0.0036**
Pepper	0.9671	0.9298	0.9594
Encrypted Pepper	**0.0025**	**-0.0035**	**-0.0075**
Baboon	0.7944	0.7426	0.8442
Encrypted Baboon	**0.0085**	**0.0023**	**0.0030**
Barbara	0.9606	0.9170	0.9415
Encrypted Barbara	**0.0010**	**0.0026**	**-0.003**
Cameraman	0.9592	0.9075	0.9331
Encrypted Cameraman	**0.0041**	**0.0023**	**0.0030**

TABLE 4
ORIGINAL AND ENCRYPTED IMAGES ENTROPY

Image	Original	Encrypted	Ref. [20]	Ref. [24]	Ref. [36]	Ref. [38]	Ref. [45]
Cameraman	7.0097	**7.9974**	7.9967	7.9970	7.9970	-	7.9974
Peppers	7.6000	**7.9974**	-	7.9973	7.9972	7.9976	-
Baboon	7.1273	**7.9974**	7.9973	-	7.9972	7.9971	7.9972
Lena	7.5836	**7.9972**	7.9967	-	-	7.9973	-

TABLE 5
UACI and NPCR COMPARISONS

Image	UACI (%)					NPCR (%)				
	Ours	Ref. [20]	Ref. [24]	Ref. [36]	Ref. [45]	Ours	Ref. [20]	Ref. [24]	Ref. [36]	Ref. [45]
Cameraman	33.5951	34.76	33.5685	33.69	-	99.6170	99.58	99.5804	99.61	99.7901
Peppers	33.5449	-	33.5291	33.57	-	99.6094	-	99.5300	99.59	-
Baboon	33.5126	27.31	-	33.17	-	99.6246	99.58	-	99.60	99.6582
Lena	33.5791	34.08	-	33.39	-	99.6353	99.58	-	99.63	-

TABLE 6
LARGER SIZE IMAGE EXPERIMENTAL RESULTS

Image	Variance	Correlation Coefficient	Entropy	NPCR	UACI
Baboon 512×512	1058.64	0.00027	7.9993	99.59%	33.49%

TABLE 7
KEY SPACE COMPARISON

	Ours	Ref. [18]	Ref. [20]	Ref. [22]	Ref. [29]	Ref. [32]	Ref. [36]	Ref. [38]	Ref. [45]
Key Space Size	2^{1656}	($\approx 9.017\times10^{14}$)	(2^{701}–2^{500})	($\approx 2^{255}$)	10^{56}	$\approx 2^{256}$	$4^{256*256}$	2^{112}	-

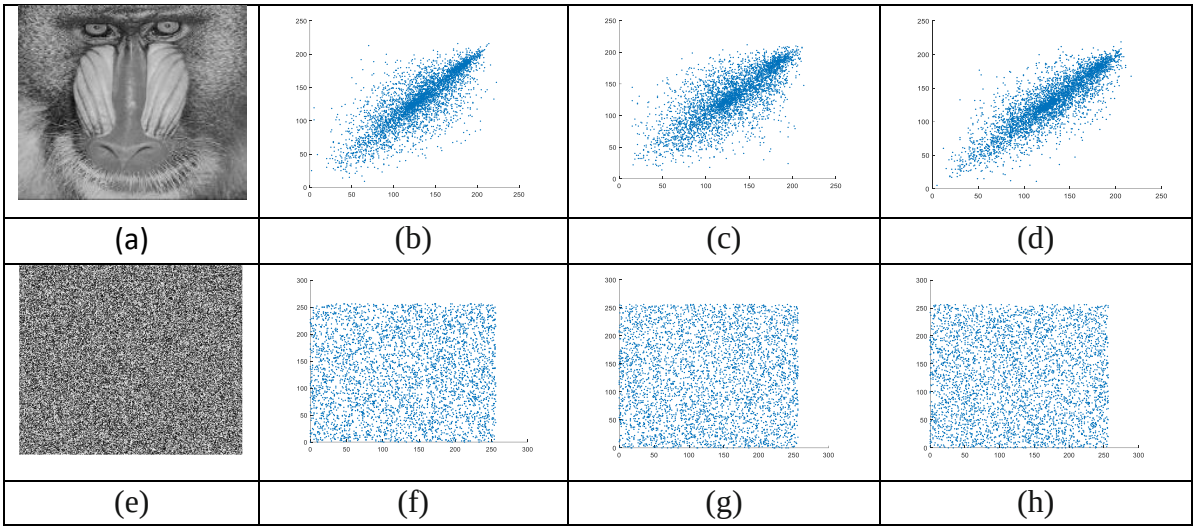


FIGURE 9: Correlation Coefficient (CC): (a) Baboon; (b) Baboon horizontal CC; (c) Baboon vertical CC; (d) Baboon diagonal CC; (e) Encrypted Baboon; (f) Encrypted image horizontal CC; (g) Encrypted image vertical CC; (h) Encrypted image diagonal CC.

D. KEY SENSITIVITY ANALYSIS

A reliable quantum image encryption scheme should have high sensitivity to any small change in the key's values. So, a little change in the values of the keys causes a highly changed cipher image. To evaluate this property for the proposed scheme, Baboon plain image is encrypted as in Figure 11 with certain keys (control parameters) values, then tiny changes are applied to the keys values as shown in Table 8 and the obtained cipher images are shown in Figure 11 (c) -(k). The correlation coefficient (CC) and NPCR are displayed in Table 8. Its is obvious from these values that both the cipher image obtained by encryption by the original keys and the cipher images obtained with tiny change in the key's values are not statistically similar. It is a proof that the proposed scheme has high sensitivity to the secret control parameters.

E. ATTACK RESISTANCE ANALYSIS DUE TO SELF-ADAPTATIVE PROPERTY

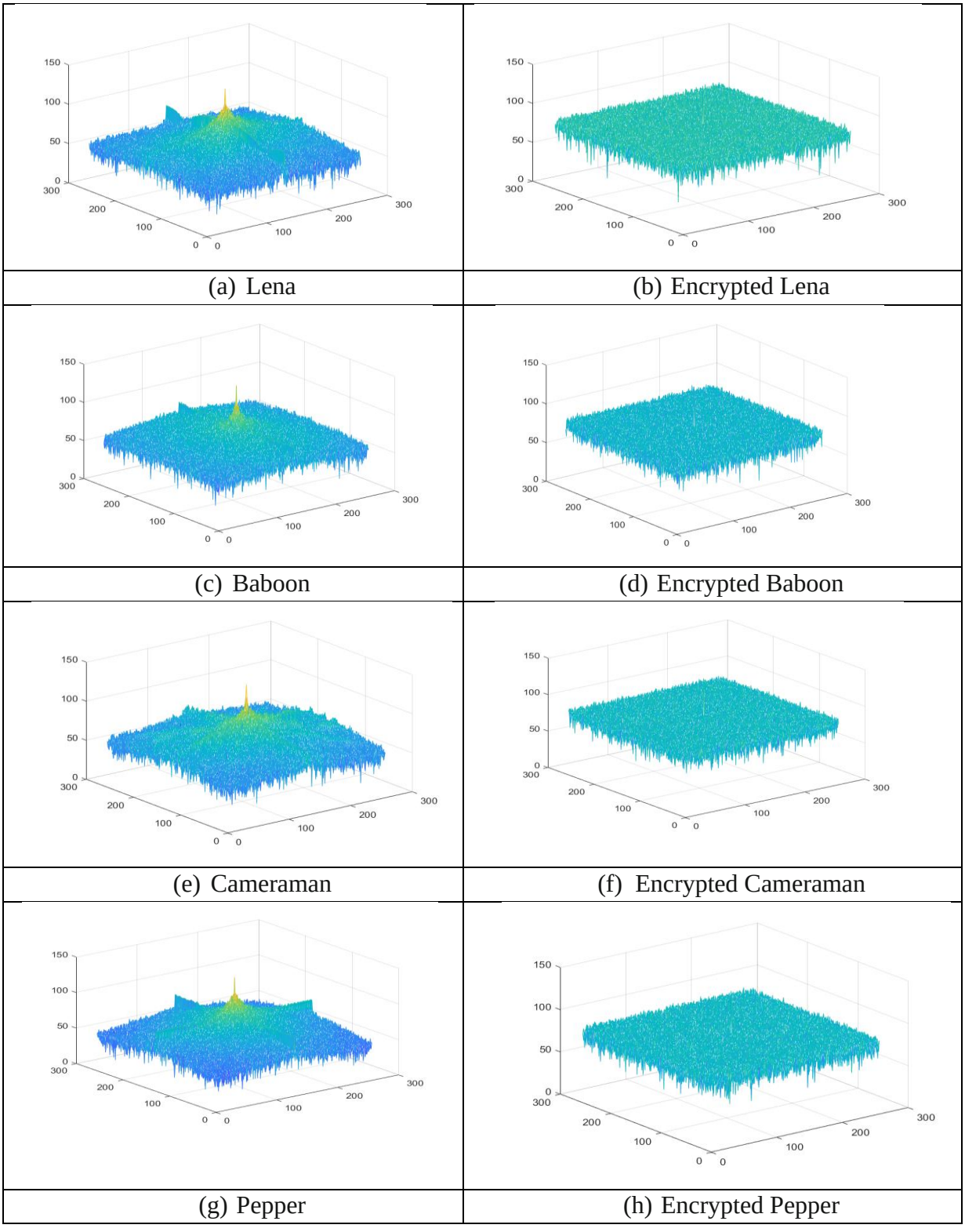
In general, there are four types of common attacks on encryption scheme. These types are ciphertext-only attack, known plaintext attack, chosen plaintext attack, and chosen ciphertext attack. Chosen-plaintext attack is the most powerful one among these attacks because the attacker may choose a plaintext and obtain its corresponding ciphertext. If the encryption scheme is strong against this type of attack, it can resist all other types of attack.

The proposed PRNG uses the hash function of the plain image (h_o) as a secret key for encryption, so the key depends on the plain image and varies with it which makes the proposed scheme self-adaptive. As a result, the attacker will be unable to penetrate the encryption scheme if he chooses some plain images to encrypt and decrypt. So, the scheme will resist chosen-plaintext attack and hence other types of attack.

This is proven by the experimental values of NPCR and UACI shown in Table 5 which measure the sensitivity of the cipher image to one pixel value change in the plain image. One reason for high sensitivity is the self-adaptive criteria of the proposed PRNG, besides the design of the encryption rounds. It is clear that the proposed scheme has greater values for NPCR comparing with other schemes which reflects its plain image higher sensitivity.

F. COMPUTATIONAL COMPLEXITY ANALYSIS

The elementary gates such as Control-Not gate which is a two-qubit quantum exclusive OR gate and NOT gate which is a one -qubit quantum gate are the basic units in computing the quantum circuit complexity of any unitary operation $U(2^n)$ on n qubits [47]. As mentioned in [47], a $C^n(U)$ quantum gate is represented as $2(n-1)$ Toffoli gates $(C^2(X))$ and one two -qubit controlled U gate $(C^1(U))$, where n is the control qubits number, X is NOT gate and U is any 2×2 unitary matrix. Toffoli gate is represented with five two-qubit quantum gates. So, a $C^n(U)$quantum gate has a circuit complexity equals $2(n-1)\times 5+1=10n-9$. In [48], the authors proved that the time complexities of image preparation and recovery for NEQR are $O(qn2^{2n})$ and $O(2^{2n})$, respectively. But in general, these two-time complexities are neglected, and the time complexity of encryption and decryption process only are considered.



(a) Lena (b) Encrypted Lena

(c) Baboon (d) Encrypted Baboon

(e) Cameraman (f) Encrypted Cameraman

(g) Pepper (h) Encrypted Pepper

FIGURE 10: Spectrums of original and encrypted images

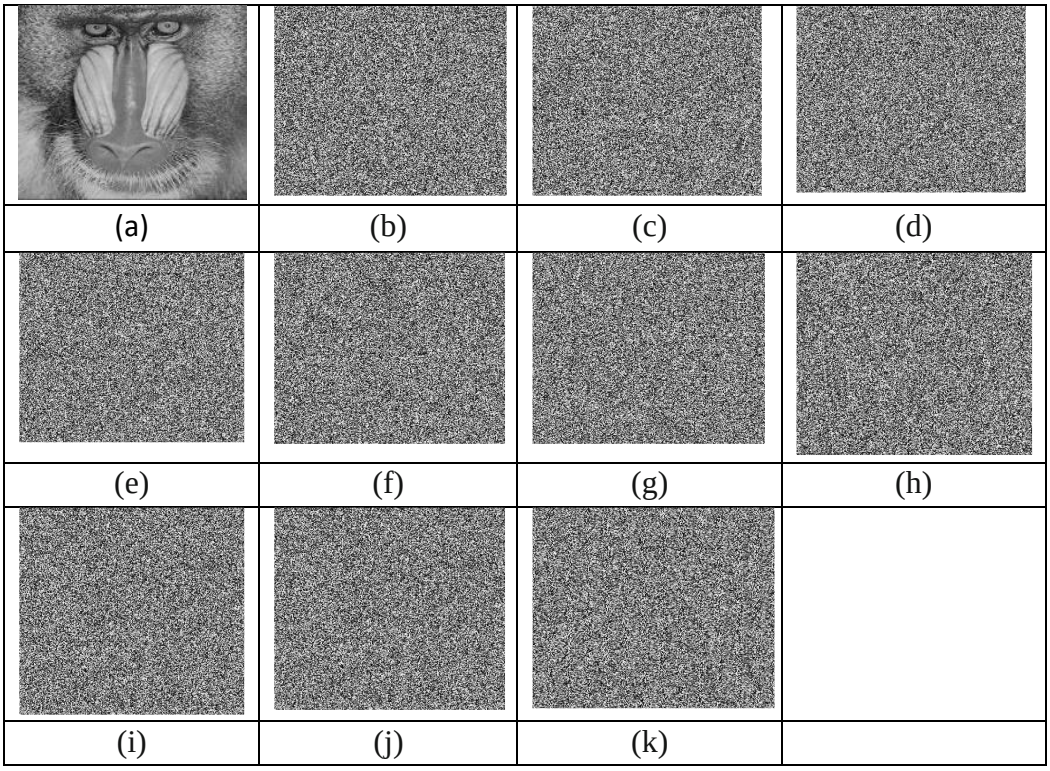


FIGURE 11: Key sensitivity test: (a) Baboon 256×256 plain image; (b) Cipher image with original keys; (c)-(k) Cipher images with tiny changed keys

So, the circuit complexity of our scheme can be computed as following: the Toffoli gate is represented by 5 CNOT gates, while the swap gate is composed of 3 CNOT gates. The first round of encryption shown in Figure 5 includes one CNOT gate, 7 Toffoli gate, and 7 swap gates. So, there are a total of $1 + 7 \times (5) + 7 \times (3) = 57$. So, the encryption first round complexity is *O(n).* The second round of encryption consists of 8 Toffoli gate which equivalent to 40-CNOT gates. The encryption second round complexity is *O(n).* So, the overall computational complexity of the proposed scheme is *O(n).* Generally, the time complexity of a quantum computer is greatly reduced compared to the classical computer which needs $O(2^{2n})$ operation to encrypt an image. This is due to the quantum parallel computations of the superposition states which represent a quantum computer input and output. So, our scheme has a much better computational complexity compared to the classical computer and some recent quantum image encryption schemes listed in Table 9.

G. COMPARATIVE ANALYSIS

A comparative analysis of the proposed scheme with other related works will be given. The security metrics used for comparison are variance, correlation coefficient, entropy, UACI, NPCR, key space, and computational complexity. The comparison listed in Table 10 shows that the proposed scheme has approximately the lowest variance, the lowest correlation coefficient, the highest entropy, UACI, and NPCR values, the largest key space and the lowest computational complexity which proves its robustness and efficiency.

H. PERFORMANCE AND SECURITY WITH QUANTUM COMPUTER

As mentioned previously, the security and performance of the proposed scheme are verified with numerical simulation by MATLAB platform on a classical computer due to the quantum computer lack, but if quantum computer is used, how the security and performance results will differ?

1) PERFORMANCE

Quantum computer has the advantage of parallel computing and so the complexity of the proposed scheme will be greatly reduced. It is estimated that the quantum computer is thousands of times faster than classical computer. So, the running time will be greatly reduced by using quantum computer compared to classical computer.

2) SECURITY

with the existence of quantum computer, the proposed scheme will remain secure due to the following: firstly, it depends on creating quantum states for encryption, which provides an inherent level of security against attacks, as any trial to measure the encrypted state will collapse it into a random state which is non-readable.

TABLE 8
KEY SENSITIVITY ANALYSIS

Control Parameter	Correct Value	Tiny Changed Value	Cipher image	CC	NPCR
r_1	3.9393	r_1 + 0.0000001	Figure10 (c)	-0.007	99.61%
r_{s2}	3.83	r_{s2} + 0.0000001	Figure 10 (d)	-0.001	99.62%
r_{s3}	3.73	r_{s3} + 0.0000001	Figure 10 (e)	0.002	99.59%
q	1.5151	q + 0.00000001	Figure 10 (f)	0.001	99.57%
p	0.6543	p + 0.0000001	Figure 10 (g)	-0.003	99.63%
μ_1	0.56	μ_1 + 0.01	Figure 10 (h)	-0.002	99.63%
μ_2	0.55	μ_2+ 0.01	Figure 10 (i)	-0.001	99.61%
k_1	5.782595812953629	k_1 + 0.00000001	Figure 10 (j)	0.001	99.61%
k_2	5.792595812953629	k_2 + 0.00000001	Figure 10 (k)	0.009	99.56%

TABLE 9
COMPUTATIONAL COMPLEXITY COMPARISON

	Ours	Ref. [18]	Ref. [20]	Ref. [22]	Ref. [29]	Ref. [32]	Ref. [36]	Ref. [38]	Ref. [45]
Time Complexity	$O(n)$	$O(n^2)$	–	$O(n2^{n+1})$	$O(n)$	$O(n2^n)$	$O(2^{2n})$	-	$O(n^2)$

TABLE 10
COMPARISON WITH RELATED WORKS

Scheme	Variance	Correlation Coefficient	Entropy	UACI	NPCR	Key Space	Computational Complexity
Ref. [18]	-	0.0023	-	-	-	-	$O(n^2)$
Ref. [20]	-	−0.0013	7.9967	27.31	99.58	2^{701}–2^{500}	-
Ref. [22]	-	0.0351	-	-	-	$\approx 2^{255}$	$O(n2^{n+1})$
Ref. [24]	243.69	− 0.0219	7.9970	33.52	99.53	-	-
Ref. [29]	-	− 0.0013	-	-	-	10^{56}	$O(n)$
Ref. [32]	-	−0.0800	-	-	-	$\approx 2^{256}$	$O(n2^n)$
Ref. [36]	239.48	0.0019	7.9970	33.17	99.60	$4^{256*256}$	$O(2^{2n})$
Ref. [38]	-	0.001	7.9971	-	-	2^{112}	-
Ref. [45]	286.64	-0.0201	7.9972	-	99.65	-	$O(n^2)$
Ours	238.33	-0.000465	7.9974	33.51	99.62	2^{1656}	$O(n)$

Secondly, the proposed scheme is a symmetric key encryption which will remain secure against quantum computer as it has enough long key. The proposed scheme doesn't depend on computational hard problem such as RSA or ECC public key schemes which are threaten by quantum computer existence. These hard problems as integer factorization problem could be broken in a very little time with quantum computer. But for the symmetric key encryption, there is no known quantum algorithm, to attack it. Only Grover' quantum algorithm can speed-up a brute force attack on it. So, the proposed scheme will remain secure even with the existence of quantum computer as long as it has long enough key. AES-256 will remain secure against quantum computing with a key space size of 2^{256}. The proposed scheme key space size is 2^{1656} which is much larger than that of AES.

V. CONCLUSION

In this paper an adaptive quantum image encryption scheme is introduced. It consists of only two rounds with two different pseudorandom number sequences of length equals the input image size. These two different pseudorandom number sequences are obtained from a new designed pseudorandom number generator (PRNG) consists of two parts. One of them is based on iteration of a recently proposed chaotic-based parallel keyed hash function which is used as a controller for a second part. The second part is a multiplication of Chebyshev and Tent chaotic maps. This combination of hash function and chaotic maps provides high randomness and dramatically enlarges control parameters and initial values space, which provides a huge key space and hence makes the scheme stronger against brute force attacks. This PRNG combines four different chaotic map which are Chebyshev, Logistic, Sine and Tent maps. The seed of the keyed hash function depends on the input image itself which makes the scheme adaptive and stronger against chosen plaintext attacks. In the first round, the input image and the two pseudorandom sequences are converted into qubits using the novel enhanced quantum representation (NEQR). Then the qubits of each pixel of the input image is modified to a different value by XOR operation with the corresponding qubit of the first pseudorandom sequence by using Controlled CNOT

quantum gate then shifting to the next qubit with the Swap quantum gate. In this round, the pixel value is changed. In the second round, diffusion of changed pixel value to each pixel in the image with the second pseudorandom sequence and by using Controlled CNOT quantum gates is performed. The time complexity of the scheme is less than many recently published quantum image encryption schemes. Performance and robustness analysis of scheme has been discussed. The results show that the scheme is highly secure and efficient.

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation Discrete logarithms and factoring," in Proc. 35th Ann. Symp. on Foundations of Computer Science (IEEE Comput. Soc. Press,) pp. 124–134, 1994.

[2] L. K. Grover, in Proc. of the 28th Ann. ACM Symp. on Theory of Computing (ACM Press), pp. 212–219, 1996.

[3] B. Jin, L. Cruz, N. Goncalves, "Deep facial diagnosis: Deep transfer learning from face recognition to facial diagnosis," IEEE Access 8, pp. 123649–123661, 2020.

[4] R. G. Zhou, D.Q. Liu, "Quantum image edge extraction based on improved Sobel operator," Int. J. Theoret. Phys. 58, 2019.

[5] F. Yan, A.M. Iliyasu, S. E. Venegas-Andraca, "Quantum Image Processing," Springer, Berlin (2020).

[6] Y. Zhang, K. Lu, Y. Gao and M. Wang, "Quantum Inf. Process," 12, 2833 (2013).

[7] Y. Zhang, K. Lu, Y. Gao and K. Xu, Quantum Inf. Process. 12, 3103 (2013).

[8] P.Q. Le, F. Dong, K. Hirota, "A flexible representation of quantum images for polynomial preparation, image compression, and processing operations," Quantum Inf. Process. 10(1), pp. 63–84 , 2011.

[9] Y. Zhang, K. Lu, Y. Gao, M. Wang, "NEQR: a novel enhanced quantum representation of digital images," Quantum Inf. Process. 12(8), pp. 2833–2860, 2013.

[10] L. Wang et al., Opt. Commun. 438, 147 (2019).

[11] R. Ismail Abdelfatah, "A new fast double-chaotic based Image encryption scheme," *Multimedia Tools and Applications*, vol. 79, October 2019. *Springer* Science +Business Media, LLC, part of Springer Nature, pp. 1241-1259, 2019.

[12] R. Ismail Abdelfatah, "Secure Image Transmission Using Chaotic-Enhanced Elliptic Curve Cryptography," *IEEE Access*, vol. 8, December, pp. 3875-3890, 2019.

[13] A. Gholipour and S. Mirzakuchaki, "A Pseudorandom Number Generator with KECCAK Hash Function," International Journal of Computer and Electrical Engineering, Vol. 3, No. 6, December 2011.

[14] A. Boldyreva, V. Kumar, "A New Pseudorandom Generator from Collision-Resistant Hash Functions, "Proceedings of the Cryptographers' Track of the RSA Conference (CT-RSA' 12), Springer 2012.

[15] A. A. Abd El-Latif, B. Abd-El-Atty M. Talha, "Robust encryption of quantum medical images," *IEEE Access*, vol. 6, pp. 1073_1081, 2018.

[16] X. Liu, D. Xiao, W. Huang, C. Liu, "Quantum block image encryption based on Arnold transform and sine chaotication model," IEEE *Access*, vol. 7, pp. 57188_57199, 2019.

[17] M. Khan,A. Rasheed, "Permutation-based special linear transforms with application in quantum image encryption algorithm," *Quantum Inf. Process.*, vol. 18, no. 10, p. 298, Oct. 2019.

[18] W.-W. Hu, R.-G. Zhou, J. Luo, S.-X. Jiang, and G.-F. Luo, "Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms," *Quantum Inf. Process.*, vol. 19, no. 3, p. 82, Mar. 2020.

[19] N. Jiang, X. Dong, H. Hu, Z. Ji, and W. Zhang, "Quantum image encryption based on henon mapping," *Int. J. Theor. Phys.*, vol. 58, no. 3, pp. 979_991, Mar. 2019.

[20] B. Abd-El-Atty, A. A. Abd El-Latif, and S. E. Venegas-Andraca, "An encryption protocol for NEQR images based on one-particle quantum walks on a circle," *Quantum Inf. Process.*, vol. 18, no. 9, p. 272, Sep. 2019.

[21] H. Liu, B. Zhao, and L. Huang, "Quantum image encryption scheme using Arnold transform and S-box scrambling," *Entropy*, vol. 21, no. 4, p. 343, Mar. 2019.

[22] H.-S. Li, C. Li, X. Chen, and H. Xia, "Quantum image encryption based on phase-shift transform and quantum Haar wavelet packet transform," *Modern Phys. Lett. A*, vol. 34, no. 26, Aug. 2019, Art. no. 1950214.

[23] P. Rakheja, R. Vig, P. Singh, "Double image encryption using 3D lorenz chaotic system, 2D non-separable linear canonical transform and QR decomposition," *Opt. Quantum Electron.*, vol. 52, no. 2, p. 103, Feb. 2020.

[24] X. Liu, D. Xiao, and C. Liu, "Quantum image encryption algorithm based on bit-plane permutation and sine logistic map," *Quantum Inf. Process.*, vol. 19, no. 8, p. 239, Aug. 2020.

[25] Y. Luo, S. Tang, J. Liu, L. Cao, and S. Qiu, "Image encryption scheme by combining the hyper-chaotic system with quantum coding," *Opt. Lasers Eng.*, vol. 124, Jan. 2020, Art. no. 105836.

[26] F. Musanna, S. Kumar, "Image encryption using quantum 3-D Baker map and generalized gray code coupled with fractional Chen's chaotic system," *Quantum Inf. Process.*, vol. 19, no. 8, p. 19, Aug. 2020.

[27] H. Lui, B. Zhao, and L. Huang, "A novel quantum image encryption algorithm based on crossover operation and mutation operation," Multimedia Tools and Applications, **78**, pp. 20465–20483 (2019), Springer. https://doi.org/10.1007/s11042-019-7186-3.

[28] J. Wang, Y. Cong Geng, L. Han, and J. Q. Lui, "Quantum Image Encryption Based on Quantum Key Image," International Journal of Theoretic Physics, 58, pp. 308–322 (2019) Springer. https://doi.org/10.1007/s10773-018-3932-y.

[29] L. H. Gong, X. T. He, S. Cheng, T. X. Hua, and N. R. Zhou, "Quantum Image Encryption Algorithm Based on Quantum Image XOR Operation," Int. J Theor Phys. Springer, 55, pp. 3234–3250, 2016. DOI 10.1007/s10773-016-2954-6.

[30] J. Zhang, Z. Huang, X. Li, M. Wu. X. Wang, Y. Dong, "Quantum Image Encryption Based on Quantum Image Decomposition," international Journal of Theoretical Physics, Springer, 60, pp. 2930–2942 (2021) https://doi.org/10.1007/s10773-021-04862-5.

[31] C. Hou and X. Liu, "Quantum image scrambling algorithm based on discrete Baker map," Modern Physics Letters A, 2050145 (18 pages) © World Scientific Publishing Company DOI: 10.1142/S021773232050145X.

[32] H. S. Li, C. Li, X. Chen, H. Xia, "Quantum Image Encryption Algorithm Based on NASS," International Journal of Theoretical Physics, (2018) 57, pp. 3745–3760, Springerhttps://doi.org/10.1007/s10773-018-3887-z.

[33] W. W. Hu, R. G. Zhou, S. Jiang, X. Liu, J. Luo, "Quantum image encryption algorithm based on generalized Arnold

transform and Logistic map," CCF Transactions on High Performance Computing, **2**, pp. 228–253 (2020). https://doi.org/10.1007/s42514-020-00043-8.

[34] X. Liu, D. Xiao,Y. Xiang, "Quantum Image Encryption Using Intra and Inter Bit Permutation Based on Logistic Map," IEEE Access, volume 7, (2019) 6937-6946.

[35] X. Liu, D. Xiao, and C. Liu, "Double Quantum Image Encryption Based on Arnold Transform and Qubit Random Rotation," Entropy, MDPI, 2018, 20, 867; doi:10.3390/e20110867.

[36] S. Zhou, A Quantum Image Encryption Method Based on DNACNot, IEEE Access, Volume 8, pp. 178336-178344 2020.

[37] R. G. Zhou, Y. B. Li, "Quantum image encryption based on Lorenz hyper-chaotic system," International Journal of Quantum Information, Vol. 18, No. 5 (2020) 2050022 (21 pages), World Scientific Publishing Company. DOI: 10.1142/S0219749920500227.

[38] L. Guo, H. Du, D. Huang, "A quantum image encryption algorithm based on the Feistel structure," Quantum Information Processing (2022) 21:20 https://doi.org/10.1007/s11128-021-03364-x.

[39] R. I. Abdelfatah, E. Abdelkhalek, M. E. Nasr, "Keyed Parallel Hash Algorithm Based on Multiple Chaotic Maps (KPHA-MCM)," IEEE Access, volume 9, 2021, pp. 130399-130409.

[40] M.A. Nielsen, I.L. Chuang, "Quantum Computation and Quantum Information," Cambridge University Press, Cambridge (2000).

[41] H. Liu, A. Kadir, and J. Liu, ``Keyed hash function using hyper chaotic system with time-varying parameters perturbation," *IEEE Access*, vol. 7, pp. 37211_37219, 2019.

[42] M. A. Chenaghlu, S. Jamali, and N. N. Khasmakhi, ``A novel keyed parallel hashing scheme based on a new chaotic system," *Chaos, Solitons Fractals*, vol. 87, pp. 216_225, Jun. 2016.

[43] J. S. Teh, A. Samsudin, and A. Akhavan, ``Parallel chaotic hash function based on the shuffle-exchange network," *Nonlinear Dyn.*, vol. 81, no. 3, pp. 1067_1079, Aug. 2015.

[44] F. Pareschi, R. Rovatti, G. Setti, "On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution," IEEE Trans Inform Forensics Sec 7(2), pp. 491–505, 2012.

[45] H.S. Li, X. Chen, S.X. Son., et al, "A block-based quantum image scrambling for GNEQR," IEEE Access. 7, pp. 138233–138243, 2019.

[46] D. Lambic, "Cryptanalyzing a novel pseudorandom number generator based on pseudo randomly enhanced logistic map," Nonlinear Dyn., vol. 89, no. 3, pp. 2255–2257, Aug. 2017.

[47] M.A. Nielsen, I.L. Chuang, "Quantum Computation and Quantum Information," Cambridge University Press, Cambridge (2000).

[48] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197_213, Jan. 2017.