This article has been accepted for publication in IEEE Transactions on Consumer Electronics. 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/TCE.2024.3415411

Chaotic Quantum Encryption to Secure Image Data in Post Quantum Consumer Technology

Muhammad Shahbaz Khan, *Graduate Student Member, IEEE,*, Jawad Ahmad, *Senior Member, IEEE*, Ahmed Al-Dubai, *Senior Member, IEEE*, Nikolaos Pitropakis, Baraq Ghaleb, Amjad Ullah, Muhammad Attique Khan, *Member, IEEE*, William J. Buchanan, *Member, IEEE*,

***Abstract*—The rapid advancement in consumer technology has led to an exponential increase in the connected devices, resulting in an enormous and continuous flow of data, particularly the image data. This data needs to be processed, managed, and secured efficiently, especially in the quantum-enabled consumer technology era. This paper, in this regards, presents a quantum image encryption scheme featuring a novel two-phase chaotic confusion-diffusion architecture. The proposed architecture consists of four distinct confusion-diffusion modules that perform a simultaneous qubit and pixel-level encryption on both the position and intensity of quantum encoded pixels. Moreover, quantum circuits for ′qubit-level chaotic transformation′ and ′chaos-based selective perfect shuffle operation′ have been implemented, which collectively enhance the encryption strength of the proposed scheme. Extensive evaluation has been performed based on various statistical security parameters, such as entropy and correlation. When subjected to differential attacks, the proposed scheme proved its resilience exhibiting ideal results of average 99.6% NPCR (Number of Pixels Change Rate) and 33.5% UACI (Unified Average Changing Intensity). Besides, the proposed scheme also demonstrated resilience against occlusion attacks. Tests involving 50% data occlusion from encrypted images validated the proposed scheme's capability to successfully decrypt the tampered images, recovering maximum information.**

***Index Terms*—Quantum image encryption, chaos, quantum cryptography, chaotic quantum encryption, qubit transformation, consumer technology.**

I. Introduction

QUANTUM computing, which harnesses the principles of quantum mechanics like coherence, entanglement, and superposition of qubits, can revolutionise various industries including consumer technology (CT) [1], [2]. The growing complexity of CT and the increase in number of connected devices is generating huge amount of data that must be processed and managed efficiently. Among this data, there has been an increase in the transmission of image data across various networks for consumer applications, including smart homes, healthcare, banking, and smart education [3], [4]. Traditional computers can't keep up with this massive data overload in these interconnected environments. Quantum computers, however, hold immense potential to handle this large volume of data and can transform the ever-evolving field of consumer technology [5]. However, the transmission/storage of this enormous amount of post-quantum CT data raises significant concerns about its security and privacy, and necessitates a re-evaluation of data security protocols, especially for image data. Image data will make up a significant portion of the information that will be transmitted extensively in post-quantum consumer technology (CT) applications, including smart cities, healthcare, and digital rights management. The unauthorised access of digital image data can result into financial fraud, intellectual property rights issues, and identity theft [6]. Image encryption plays a crucial role in securing these images from unauthorised access and cyber attacks [7], [8]. Various encryption techniques can be found in literature that have been proposed to secure digital data including images and videos [9]–[12]. But these techniques might not be suitable in the post quantum CT era. For the security of post-quantum computing systems, quantum cryptography is required [13]. Quantum cryptography, especially quantum image encryption (QIE), ensures the privacy and integrity of images in this new era of quantum-enhanced consumer technology. Focusing on the security of the image data in post quantum CT scenarios, this paper aims at designing of a new and robust quantum image encryption method, which proves to be secure and efficient for the quantum computing platforms.

Quantum image encryption techniques can be primarily categorized into either spatial or frequency domain approaches. A generalised framework of quantum image encryption is depicted in Fig. 1. To apply quantum image encryption algorithms on classic image data, the classic images need to be represented in quantum domain using quantum image repre-

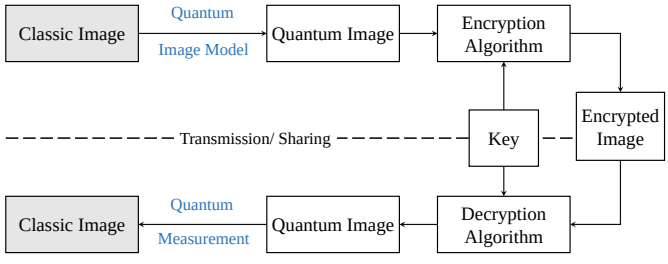


Fig. 1: A generalized schematic of quantum image encryption.

Manuscript received xxxx xx, 2024; revised xxxx xx, 2024; accepted xxxx xx, 2024.

Muhammad Shahbaz Khan, Jawad Ahmad, Ahmed Al-Dubai, Nikolaos Pitropakis, Baraq Ghaleb, Amjad Ullah, and William J. Buchanan are with the School of Computing, Engineering and the Built Environment, Edinburgh Napier University, Edinburgh EH10 5DT, UK (e-mail: muhammadshahbaz.khan@napier.ac.uk; j.ahmad@napier.ac.uk; a.al-dubai@napier.ac.uk; n.pitropakis@napier.ac.uk; b.ghaleb@napier.ac.uk; a.ullah@napier.ac.uk; b.buchanan@napier.ac.uk

Muhammad Attique Khan is with the Department of Computer Science, HITEC University, Taxila 47080, Pakistan (e-mail: attique.khan@ieee.org

(Corresponding Author: Jawad Ahmad)

Authorized licensed use limited to: Edinburgh Napier University. Downloaded on June 26,2024 at 01:31:46 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. 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/TCE.2024.3415411

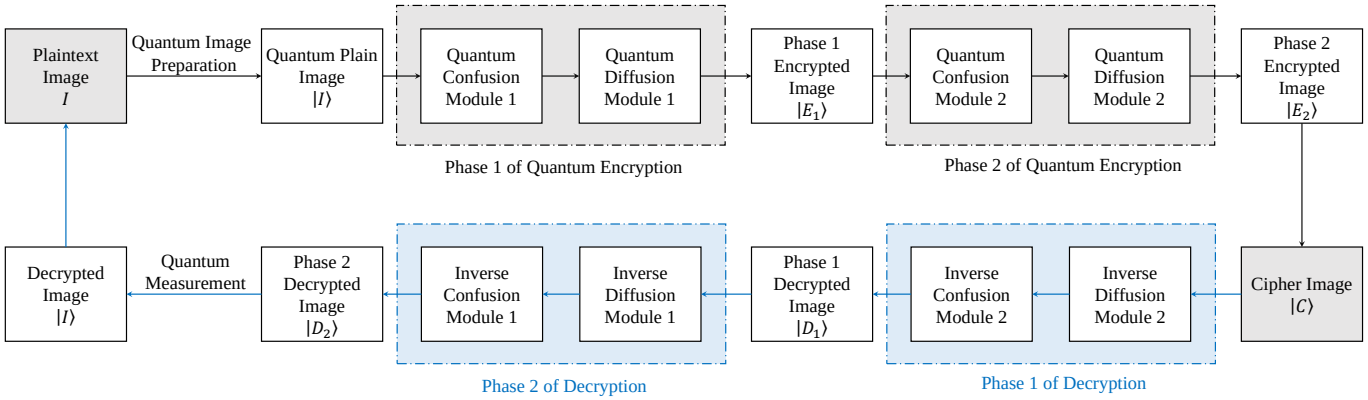


Fig. 2: A high-level flowchart of the proposed two-phase confusion-diffusion quantum encryption algorithm

sentation (QIR) models [14], [15]. These QIRs are designed to encode classic images in the quantum domain based on certain criteria; for instance, some models use the color model or visual contrasts to encode image content, some others utilize coordinate systems to extract image information, and yet others encode both color and position data of pixels. In the context of color model and visual contrast category, a technique for encoding and retrieving geometrical shapes in binary images is introduced in [16]. They use maximally entangled quantum states for this purpose. In addition, one of the most utilised QIR in this category is the Flexible Representation for Quantum Images (FRQI), designed to integrate grayscale color and position data of an image into a standardized quantum state [17]. This model encodes a $2^n \times 2^n$ grayscale image using 2^{n+1} qubits by mapping the pixel's coordinate data onto $2n$ qubits within computational basis states and encoding color data into a singular qubit through angle encoding. Furthermore, to simulate human visual perception accurately, QIRs for full-color images have also been designed that cater all three RGB (Red, Green, Blue) channels of a color image. These representations use dual quantum state sets to represent a specific number of colors (M) and pixels (N) within an image [18], or they might also utilise varying angular levels for RGB data combined with location information (along the Y- and X-axes) for image representation [19], [20]. The most common RGB QIR is the Multi-Channel Quantum Images (MCQI) model [21].

Similarly, for the QIR category that utilises coordinate system representations, an early example includes the qubit lattice that maps each pixel to an individual qubit, organizing images into two-dimensional qubit arrays without preliminary processing [22]. The previously described FRQI model also utilizes the Cartesian system, and comprehensive studies have been conducted on it for quantum operations such as flipping, coordinate swapping, orthogonal rotations, etc. [23], [24]. Finally, sveral QIRs have also been designed for the third category that uses two basic parameters of image information, i.e., color and position. For instance, some models establish a one-to-one correspondence between the color frequency of a monochromatic wave and a qubit's angular parameter to encode color data, as seen in qubit lattice models [22], FRQI [17], and Quantum States for M Colors and N Coordinates (QSMC and QSNC) [18].

One of the most utilised quantum representation, that utilises the color intensity and position information is the the novel enhanced quantum representation (NEQR) model [25]. In this QIR, the image with its color (intensity) information is stored in only two qubit sequences, and this information is actually encoded in the basis states. This is an improved version of the FRQI model, and stores a n-qubit basis states to represent the intensity of the pixel in a range of $[0, 2^n - 1]$. Furthermore, the Generalized NEQR (GNEQR) model has also been proposed in [26] employs 2^{n+10} qubits to represent a $2^n \times 2^n$ RGB color image, showcasing advancements in quantum image representation for enhanced storage capabilities.

The two fundamental characteristics of a secure encryption algorithm are confusion and diffusion [27]. Similarly, quantum encryption algorithms also comprise of these two components: scrambling (diffusion) and replacement (confusion). The Quantum scrambling and replacement techniques focus on two important parameters of a pixel, i.e., position and intensity/color information [28].Scrambling (diffusion) techniques shuffle the positions of pixels, while replacement (confusion) techniques change the pixel values to modify the image's statistical characteristics [29]. Notable quantum scrambling methods include the Hilbert [30], Arnold [31], and Fibonacci transforms [31]. The Arnold and Fibonacci transforms utilize simple and modular addition to rearrange the pixels, whereas the Hilbert method relies on a recursively generated scanning matrix for this purpose. Speaking of replacement techniques, a technique introduced in [32] combines bit-plane shuffling with the Arnold Transform within the NEQR model to transform the pixel values effectively, and to enhance the securityof the encryption scheme. Similarly, quantum image decomposition has been introduced in [33] by breaking down grayscale images into smaller feature sets using a binary tree structure. This is used in conjunction with encryption through random phase and quantum rotation techniques. Focusing on RGB images, Yan et al. [34] developed a technique that simultaneously applies color and geometric transformations to improve the scrambling process, enhancing the overall image security.

A strong encryption algorithm should incorporate both confusion and diffusion processes, simultaneously at the pixel

Authorized licensed use limited to: Edinburgh Napier University. Downloaded on June 26,2024 at 01:31:46 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. 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/TCE.2024.3415411

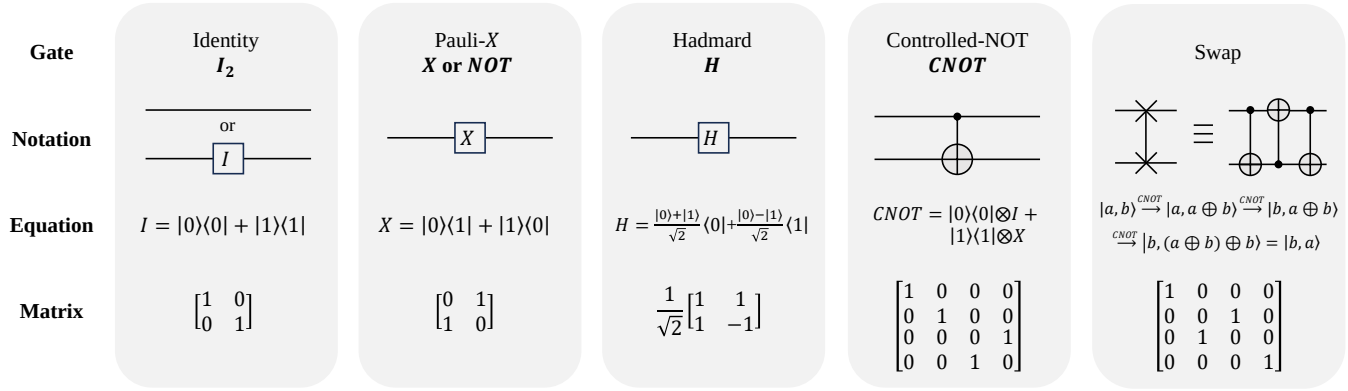


Fig. 3: Basic quantum gates with their notations, equaitons, and matrices.

and qubit-level to increase the non-linearity and randomness in the encrypted image. Most of the existing QIE schemes primarily focus either on the quantum confusion modules or the diffusion modules, with very few incorporating both to make a robust confusion-diffusion architecture. Moreover, the quantum circuits utilised in existing schemes are not controlled by chaotic maps that introduce an extra layer of complexity and non-linearity in the quantum operations. This paper, in this regards, proposes a quantum image encryption algorithm featuring a novel two-phase chaotic confusion-diffusion architecture. This architecture consists of four strong confusion-diffusion modules. A high-level flowchart to depict the proposed two-phase quantum image encryption scheme is given in Fig. 2. Each phase implements a standalone confusion-diffusion architecture. The final encrypted image undergoes two distinct confusion-diffusion architectures and the output of the first phase is encrypted again in the second phase resulting in the final encrypted image. The four confusion-diffusion modules utilise quantum circuits for qubit-level chaotic transformation, chaotic permutation, and a fast geometric transformation block, which collectively enhance the encryption strength of the proposed algorithm.

The main contributions of this paper are:

1) A quantum image encryption algorithm, featuring a novel two-phase confusion-diffusion architecture is developed. The architecture consists of four distinct confusion-diffusion modules that encrypt both the coordinates(positions) and pixel intensities of the quantum image. Each phase ensures encryption at both the qubit and the pixel level.
2) A quantum circuit for qubit-level transformation is presented. This circuit randomly permutes and transforms the qubits of each pixel based on a chaotic key and quantum CNOT gates.
3) A quantum circuit for chaotic selective perfect-shuffle operation is presented. This operation is chaotic key controlled and ensures a random qubit-plane shift operation on each pixel using the quantum SWAP gates.
4) A quantum circuit for multi-geometric transformation block is presented. This circuit performs three different block-wise fast geometric transformations on the 'position qubits' of each pixel resulting in a pixel-level scrambling.

The rest of the paper is organised as follows. Section II presents the preliminary knowledge and basic theory of quantum computing and quantum image encryption. Section III entails the procedure of encoding a classic image into quantum representation. Section IV provides details on the chaotic key generation process. Section V presents the design and implementation for the proposed encryption scheme. Section VI presents the results of the proposed scheme and its performance against various attacks followed by a clear and concise conclusion in Section VII.

II. Preliminaries

A. Quantum Bits and Registers

Similar to the concept of a classic bit, a qubit or quantum bit is the most fundamental block/unit of data in quantum computers [35]. The main difference is that a qubit can exist in a superposition state. This state is described as a unit vector in two-dimensional Hilbert space. This vector or a qubit is described as:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{1}$$

$$|\psi\rangle = \alpha|\uparrow\rangle + \beta|\rightarrow\rangle \tag{2}$$

where $|\uparrow\rangle$ and $|\rightarrow\rangle$ are the basis states orthogonal to each other, and α and β are the probability amplitudes. The probabilities for $|\phi\rangle$ to be in the $|\uparrow\rangle$ and $|\rightarrow\rangle$ states are $|\alpha|^2$ and $|\beta|^2$, respectively, satisfying the normalization condition $|\alpha|^2 + |\beta|^2 = 1$. This statement means that the qubit's state vector has been normalized to a length of 1. By defining $|\uparrow\rangle$ as $|0\rangle$ and $|\rightarrow\rangle$ as $|1\rangle$, $|\psi\rangle$ can be expressed as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{3}$$

where $|0\rangle$ and $|1\rangle$ become the computational basis states that establish an orthonormal basis in this vector space.

Authorized licensed use limited to: Edinburgh Napier University. Downloaded on June 26,2024 at 01:31:46 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. 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/TCE.2024.3415411

In quantum computing, the qubit states $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}^T$ and $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}^T$ serve as the computational basis, spanning a two-dimensional Hilbert space H_2.

A quantum register consists of several qubits and serves as the quantum counterpart to a classical computer's register. In quantum computing, operations are carried out by manipulating the qubits within such a register. The states of individual qubits in the quantum register determines the overall state of the quantum register. To determine this, a tensor product $\otimes$ of the states of these individual bits is taken. The tensor product $|u\rangle \otimes |v\rangle$, involving two quantum states $|u\rangle$ and $|v\rangle$, is often abbreviated as $|uv\rangle$ or $|u\rangle|v\rangle$. Similarly, $A^{\otimes n}$ represents the n-times product (tensor) of the matrix A with itself .

For example, in a quantum register holding two qubits, there are four basic computational states: $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$. These two qubits can be in a superposition of these four states and can be expressed as:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \tag{4}$$

The tensor product, represented by the symbol $\otimes$, is a mathematical operation that merges smaller vector spaces to form a larger vector space, specifically within the context of a Hilbert space. When applied to two matrices, where M is an $n \times n$ matrix and N is an $m \times m$ matrix, the result of the tensor product $M \otimes N$ is a new matrix of size $nm \times nm$. This resultant matrix is structured as a block matrix, where each block is constructed by multiplying the elements of matrix M with the entire matrix N and is given as:

$$M \otimes N = \begin{bmatrix} M_{0,0}N & \cdots & M_{0,n-1}N \\ \vdots & \ddots & \vdots \\ M_{n-1,0}N & \cdots & M_{n-1,n-1}N \end{bmatrix} \tag{5}$$

In a 2^n-dimensional Hilbert space for an n-qubit system, a computational basis state $|i\rangle$, with i ranging from 0 to $2^n - 1$, is constructed via the tensor products of n computational basis states:

$$|i\rangle = |i_{n-1}\rangle \otimes |i_{n-2}\rangle \otimes \cdots \otimes |i_1\rangle \otimes |i_0\rangle = |i_{n-1}i_{n-2}\cdots i_1 i_0\rangle \tag{6}$$

where $i = \sum_{j=0}^{n-1} i_j \times 2^j$, with each i_j being either 0 or 1.

An n-qubit quantum system can be described as a superposition of its 2^n quantum computational basis states:

$$|\psi\rangle = \sum_{k=0}^{2^n-1} a_k |k\rangle \tag{7}$$

where k is the binary string $k_{n-1}k_{n-2}\cdots k_1 k_0$, and a_k are complex coefficients satisfying the normalization condition:

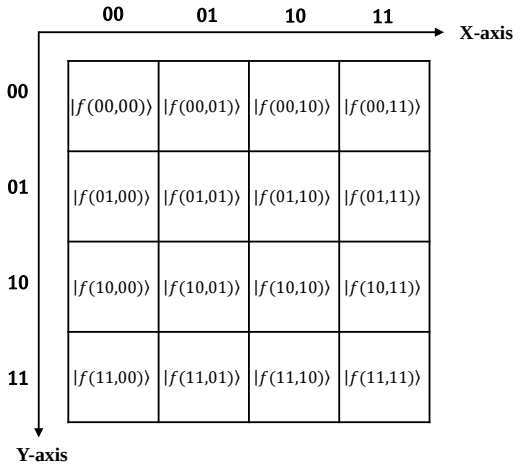
$$\sum_{k=0}^{2^n-1} |a_k|^2 = 1 \tag{8}$$

B. Quantum Circuits and Gates

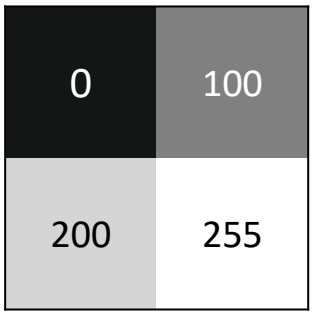
Quantum circuits provide the essential framework that facilitates quantum computing by enabling the manipulation and processing of quantum information. It actually enables the execution of quantum operations or computations. A quantum operation, whereas, is a combination of logic gates, more particularly, the quantum logic gates, commonly referred to as just 'quantum gates'. A quantum circuit is read from left to right, representing the passage of time or movement of a photon from one place to another [35]. Quantum gates are written in the form of unitary matrices. For a quantum gate, the count of qubits at both the input and output must match. Therefore, a gate that operates on n qubits is depicted by a unitary matrix of size $2^n \times 2^n$.

III. Novel Enhanced Quantum Image Representation (NEQR) and GNEQR

The NEQR [25] stores the pixel intensity and position information of a pixel in two entangled qubit sequences. It stores the the complete image in the superposition of the two qubit sequences. The NEQR model is preferred because it supports quantum image processing more efficiently than FRQI and most importantly it offers flexible and easy computational



(a)



$$|I\rangle = \frac{1}{2}\begin{pmatrix}|0\rangle \otimes |00\rangle + |100\rangle \otimes |01\rangle + |200\rangle \otimes |10\rangle + \\ |255\rangle \otimes |11\rangle\end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix}|00000000\rangle \otimes |00\rangle + |01100100\rangle \otimes |01\rangle + \\ |11001000\rangle \otimes |10\rangle + |11111111\rangle \otimes |11\rangle\end{pmatrix}$$

(b)

Fig. 4: NEQR image representation. (a) A 4x4 quantum image. (b) NEQR expression for a 2x2 sample image.

Authorized licensed use limited to: Edinburgh Napier University. Downloaded on June 26,2024 at 01:31:46 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. 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/TCE.2024.3415411

state preparation and measurement process as compared to FRQI. In NEQR, for an image with the grayscale pixel inensity range 2^q, the binary sequence $C_0^{YX}C_1^{YX}\dots C_{q-2}^{YX}C_{q-1}^{YX}$ encodes the gray-scale value $f(Y,X)$ of the corresponding pixel (Y,X) as: $f(Y,X) = C_0^{YX}C_1^{YX}\dots C_{q-2}^{YX}C_{q-1}^{YX}$, where $C_k^{YX} \in [0,1], \quad f(Y,X) \in [0, 2^q-1]$.

The NEQR representation of a $2^n \times 2^n$ image is as follows:

$$\begin{aligned} |I\rangle &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|f(Y,X)\rangle|YX\rangle \\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{i=0}^{q-1}|C_i^{YX}\rangle|YX\rangle \end{aligned} \tag{9}$$

A 4x4 NEQR quanutm image representation is shown in Fig. 4a, whereas a 2x2 sample image with its NEQR expression is given in Fig. 4b, and the quantum circuit for the NEQR preparation of the sample image given in Fig. 4b is given in Fig. 5.

The generalised model of NEQR is an extension of the NEQR. GNEQR is more efficient and can handle large range of pixel intensities by using fewer bits. The benefit of using GNEQR is that it can represent images more efficiently, especially with varying level of detail and colour depth. Most

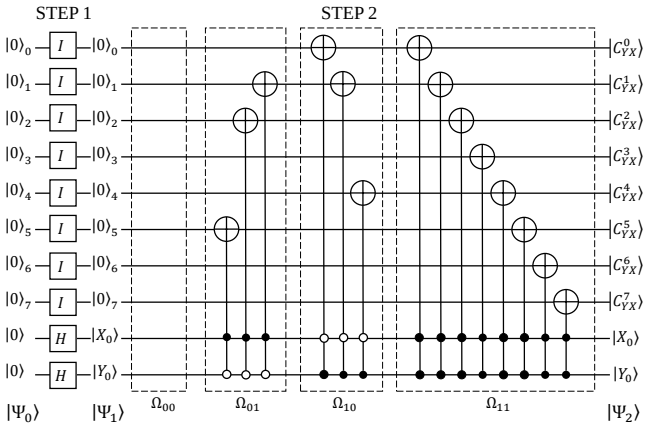


Fig. 5: Quantum circuit for the NEQR preparation of images.

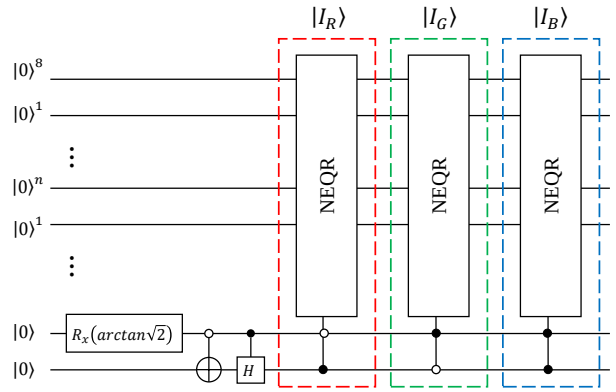


Fig. 6: Quantum circuit for the GNEQR preparation of images.

importantly, it reduces the resources required for the quantum image processing tasks. GNEQR is defined as [36]:

$$\begin{aligned} |G\rangle &= \frac{1}{\sqrt{3}}\left(|I_R\rangle|01\rangle + |I_G\rangle|10\rangle + |I_B\rangle|11\rangle\right) \\ &= \frac{1}{\sqrt{3}} \times \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left(|R_{YX}\rangle|YX\rangle|01\rangle + |G_{YX}\rangle|YX\rangle|10\rangle \right. \\ &\quad \left. + |B_{YX}\rangle|YX\rangle|11\rangle\right) \end{aligned} \tag{10}$$

This model is based on the decomposition of a colored image into three channels: Red, Green, and Blue, which in their decomposed form are expressed as:

$$\begin{aligned} |I_R\rangle &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|R_{YX}\rangle|YX\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{K=0}^{q-1}\left|R_{YX}^K\right\rangle|Y\rangle|X\rangle, \\ |I_G\rangle &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|G_{YX}\rangle|YX\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{K=0}^{q-1}\left|G_{YX}^K\right\rangle|Y\rangle|X\rangle, \\ |I_B\rangle &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|B_{YX}\rangle|YX\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{K=0}^{q-1}\left|B_{YX}^K\right\rangle|Y\rangle|X\rangle, \end{aligned} \tag{11}$$

where $|R_{yx}\rangle$, $|G_{yx}\rangle$, and $|B_{yx}\rangle$ are defined as:

$$\begin{aligned} |R_{yx}\rangle &= |r_{q-1,yx}r_{q-2,yx}\dots r_{0,yx}\rangle, \\ |G_{yx}\rangle &= |g_{q-1,yx}g_{q-2,yx}\dots g_{0,yx}\rangle, \\ |B_{yx}\rangle &= |b_{q-1,yx}b_{q-2,yx}\dots b_{0,yx}\rangle. \end{aligned} \tag{12}$$

The quantum circuit of GNEQR is given in Fig. 6. Here, the quantum balck-box (the quantum-oracle NEQR) prepares the quantum image and the unitary operation $R_x(\arctan(\sqrt{2}))$ is defined as:

$$\begin{aligned} R_x(\arctan(\sqrt{2})) &= \begin{bmatrix} \cos(\arctan(\sqrt{2})) & \sin(\arctan(\sqrt{2})) \\ \sin(\arctan(\sqrt{2})) & -\cos(\arctan(\sqrt{2})) \end{bmatrix} \\ &= \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{\sqrt{2}}{\sqrt{3}} \\ \frac{\sqrt{2}}{\sqrt{3}} & -\frac{1}{\sqrt{3}} \end{bmatrix} \end{aligned} \tag{13}$$

IV. The Proposed Quantum Image Encryption Scheme

The proposed quantum image encryption algorithm consists of two phases. Each phase consists of standalone confusion-diffusion modules. Each phase ensures the encryption of both parameters: the position and the intensity of each pixel. The combination of confusion-diffusion modules, consisting of various quantum transformations and operations, ensures that in each phase, the input image undergoes encryption at both the qubit-level and pixel-level. The detailed flowchart of the proposed scheme is given in Fig. 9, whereas the quantum circuit for the complete encryption stage is given in Fig. 10. The details of individual modules and operations utilised in the proposed approach are described below.

A. Chaotic Key Generation Module

1) The De Jong Fractal Map: The De Jong Fractal Map, recognized for its intriguing and chaotic properties, is attributed to Peter de Jong. It is characterized by a specific set of parametric equations given below [37].

Authorized licensed use limited to: Edinburgh Napier University. Downloaded on June 26,2024 at 01:31:46 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. 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/TCE.2024.3415411

$$x_{\gamma+1} = \sin(a \cdot y_\gamma) - \cos(b \cdot x_\gamma) \tag{14}$$
$$y_{\gamma+1} = \sin(c \cdot x_\gamma) - \cos(d \cdot y_\gamma) \tag{15}$$

In these equations, $x_{\gamma+1}$ and $y_{\gamma+1}$ represent the new positions in the system, derived from the preceding positions x_γ and y_γ, respectively. Adjusting the values of the parameters a, b, c, and d within these equations can lead to more complex chaotic fractal patterns. These patterns for different parameters are illustrated in the Fig. 7.

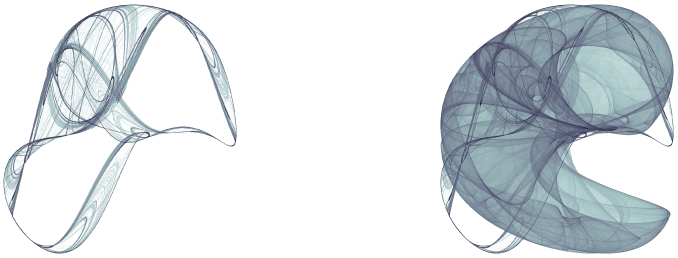
2) Van Der Pol Oscillator: The discretized version of the Van der Pol oscillator, a non-linear dynamical system, is expressed through the following equations [38]:

$$\frac{x_{\gamma+1} - x_\gamma}{h} = v_\gamma \tag{16}$$
$$\frac{v_{\gamma+1} - v_\gamma}{h} = \mu(1 - x_\gamma^2)v_\gamma - x_\gamma \tag{17}$$

Here, x_γ and v_γ serve as discrete approximations for $x(t)$ and its time derivative $\frac{dx}{dt}$ at discrete time intervals $t = \gamma h$, respectively. The timestep h and the nonlinearity parameter μ play crucial roles in dictating the system's behavior, which includes chaotic dynamics as depicted in Fig. 7.

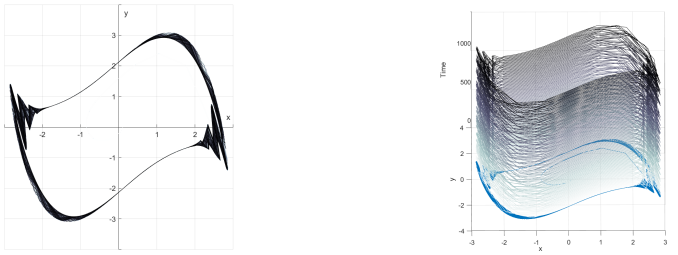
B. Step-1: Chaotic Qubit-Level Transformation

This transformation serves as the first confusion module of Phase 1, named as $\mathbb{P}_1^{M1}$ in Fig. 9. In this step, a chaotic qubit-level transformation operation is performed on each pixel (Y, X). This operation transforms the grayscale value of the pixel by performing a random qubit-level permutation of each pixel. The permutation sequence is key controlled, obtained by the chaotic De-Jong map. An 8-bit key is generated for each pixel, which defines the order of qubit permutation. These qubits get X-ored with eachother using quantum CNOT gates, and hence result in the transformation of the grayscale intensity of each pixel. The quantum circuits based on two chaotic keys depicting the random order of qubit permutation is given in Fig. 11a and Fig. 11b, respectively. After this step, the grayscale intesity of each pixel transforms from $|p_{yx}^7, p_{yx}^6, \ldots, p_{yx}^1, p_{yx}^0\rangle$ to $|p_{yx}^{7'}, p_{yx}^{6'}, \ldots, p_{yx}^{1'}, p_{yx}^{0'}, \rangle$. The transformed qubits obtained after applying the quantum circuits in Fig. 11a and Fig. 11b are given in 18 and 19, respectively.



(a) (b)

Fig. 7: Chaotic behaviour of the De Jong Fractal Map for: (a) $a = 1.645, b = 1.905, c = 0.320, d = 1.530$. (b) $a = 1.42, b = -2.28, c = 2.38, d = -2.08$.



(a) (b)

Fig. 8: Chaotic behaviour of the Van Der Pol Oscillator for: $h = 0.29$ and $\mu = 0.06$

$$\begin{aligned} p_{yx}^{7'} &= p_{yx}^0 \oplus p_{yx}^7, & p_{yx}^{6'} &= p_{yx}^{2'} \oplus p_{yx}^6, \\ p_{yx}^{5'} &= p_{yx}^{3'} \oplus p_{yx}^5, & p_{yx}^{4'} &= p_{yx}^{5'} \oplus p_{yx}^4, \\ p_{yx}^{3'} &= p_{yx}^{1'} \oplus p_{yx}^3, & p_{yx}^{2'} &= p_{yx}^{7'} \oplus p_{yx}^2, \\ p_{yx}^{1'} &= p_{yx}^{6'} \oplus p_{yx}^1, & p_{yx}^{0'} &= p_{yx}^0. \end{aligned} \tag{18}$$

$$\begin{aligned} p_{yx}^{7'} &= p_{yx}^{5'} \oplus p_{yx}^7, & p_{yx}^{6'} &= p_{yx}^6, \\ p_{yx}^{5'} &= p_{yx}^{2'} \oplus p_{yx}^5, & p_{yx}^{4'} &= p_{yx}^{7'} \oplus p_{yx}^4, \\ p_{yx}^{3'} &= p_{yx}^6 \oplus p_{yx}^3, & p_{yx}^{2'} &= p_{yx}^{0'} \oplus p_{yx}^2, \\ p_{yx}^{1'} &= p_{yx}^{4'} \oplus p_{yx}^1, & p_{yx}^{0'} &= p_{yx}^{3'} \oplus p_{yx}^0. \end{aligned} \tag{19}$$

C. Step-2: Block-wise Quantum Geometric Transformations

This block serves as the diffusion module in the Phase 1 of the proposed encryption scheme, named as $\mathbb{P}_1^{M2}$ in Fig. 9. In this step, the output of the preceding confusion module is divided in 1024 equal blocks of 8x8 size. On each block, three fast geometric transformations inspired from [30] are applied that result in the pixel-level scrambling of the image. Let Γ be the matrix form of a $2^k \times 2^k$ image, then, three operations Γ_I^{VF}, Γ_I^{HF}, and Γ_I^{CS} are given by:

$$\Gamma = \begin{bmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,2^k} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,2^k} \\ \vdots & \vdots & \ddots & \vdots \\ p_{2^k,1} & p_{2^k,2} & \cdots & p_{2^k,2^k} \end{bmatrix} \tag{20}$$

The operations are defined as follows:

- The vertical flip, i.e., flipping along the y-axis (Γ_I^{VF}):

$$\Gamma_I^{VF} = \begin{bmatrix} p_{2^k,1} & p_{2^k,2} & \cdots & p_{2^k,2^k} \\ p_{2^k-1,1} & p_{2^k-1,2} & \cdots & p_{2^k-1,2^k} \\ \vdots & \vdots & \ddots & \vdots \\ p_{1,1} & p_{1,2} & \cdots & p_{1,2^k} \end{bmatrix} \tag{21}$$

- The horizontal flip, flipping along the x-axis (Γ_I^{HF}):

$$\Gamma_I^{HF} = \begin{bmatrix} p_{1,2^k} & \cdots & p_{1,2} & p_{1,1} \\ p_{2,2^k} & \cdots & p_{2,2} & p_{2,1} \\ \vdots & \ddots & \vdots & \vdots \\ p_{2^k,2^k} & \cdots & p_{2^k,2} & p_{2^k,1} \end{bmatrix} \tag{22}$$

Authorized licensed use limited to: Edinburgh Napier University. Downloaded on June 26,2024 at 01:31:46 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. 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/TCE.2024.3415411

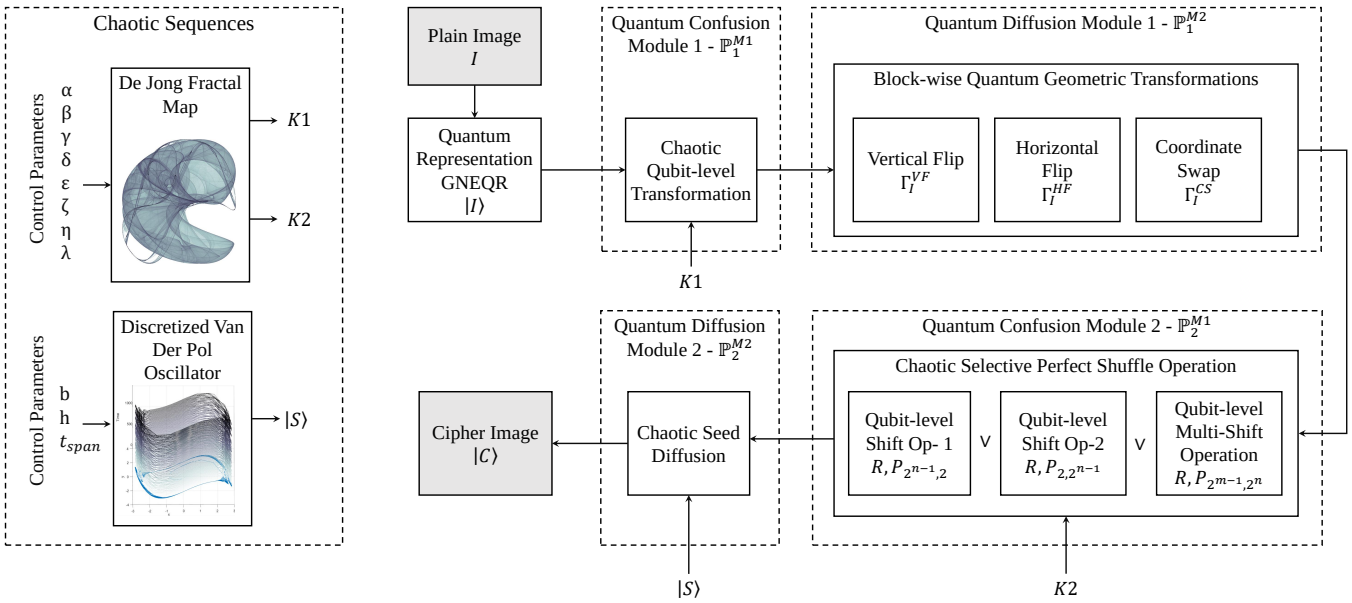


Fig. 9: The proposed quantum image encryption algorithm with Two-Phase Confusion Diffusion Acrhitecture.

- The coordinate swap (Γ_I^{CS}):

$$\Gamma_I^{CS} = \begin{bmatrix} p_{1,1} & p_{2,1} & \cdots & p_{2^k,1} \\ p_{1,2} & p_{2,2} & \cdots & p_{2^k,2} \\ \vdots & \vdots & \ddots & \vdots \\ p_{1,2^k} & p_{2,2^k} & \cdots & p_{2^k,2^k} \end{bmatrix} \tag{23}$$

The Quantum implementation circuits for these transformations are given in Fig. 12 and an exhibit of how these operations scramble the pixel in each block if given in Fig. 13. An 8x8 block is considered to illustrate the transformations.

D. Step-3: Chaotic Selective Shuffle Operation

This module incorporates a chaos-based selective perfect shuffle operation and is named as $\mathbb{P}_2^{M1}$ in Fig. 9. This module utilises three bit shift operations based on the perfect shuffle approach: 1) 2-bit left shift, 2) 2-bit right shift, 3) 4-bit left shift. Two of these operations, i.e., $R - P_{2^{n-1},2}$ and $P_{2,2^{n-1}}$ are developed by adding an extra bit reversal operation before shifting the qubits. The third operation $R - P_{2^{m-1},2^n}$, on the other hand, is a multi-bit shift operation. For the multi-bit shift operation, 4-bit left shift operation is utilized. The quantum circuit for the 4-bit left operation is depicted in Fig. 15b. The De Jong map is utilised to generate a selection key. This key dictates that the selection of operation for each pixel. The entry '0' in the key corresponds to first bit-shift operation, the entry '1' corresponds to second bit-shift operation, and similary '2' corresponds to third bit-shift operation. For example, for pixel 1, if the first entry in the key is '0', first shift operation will be applied on pixel 1. Similarly, for pixel 2 if the entry in

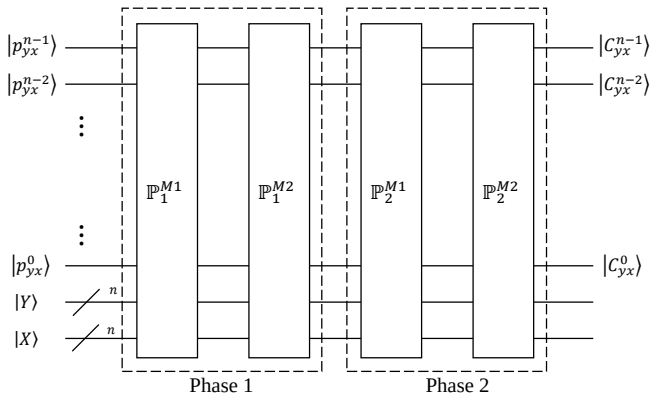


Fig. 10: Quantum circuit of the complete encryption scheme.

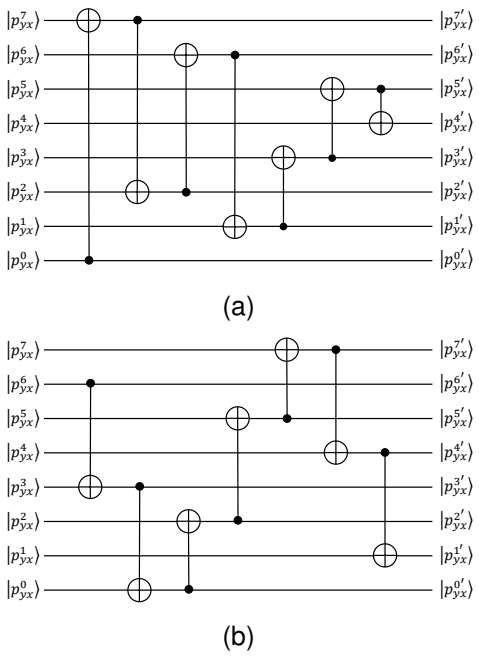


Fig. 11: Quantum circuits for Chaotic Qubit Transformations

Authorized licensed use limited to: Edinburgh Napier University. Downloaded on June 26,2024 at 01:31:46 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. 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/TCE.2024.3415411

the key is 1, then second operation will be applied on pixel 2. This key is highly random and ensures random selection of operation on each pixel.

The P_{2^n} is the perfect shuffle permutation that has two different forms defined as follows [26], [39], [40]:

$$P_{2^{n-1},2} = \left(P_{2^{n-2},2} \otimes I_2\right)\left(I_{2^{n-2}} \otimes P_{2,2}\right), \quad (24)$$

$$P_{2,2^{n-1}} = \left(I_2 \otimes P_{2,2^{n-2}}\right)\left(P_{2,2} \otimes I_{2^{n-2}}\right), \quad (25)$$

where $P_{2,2}$ represents a two qubit swap gate as shown in Fig. 3.

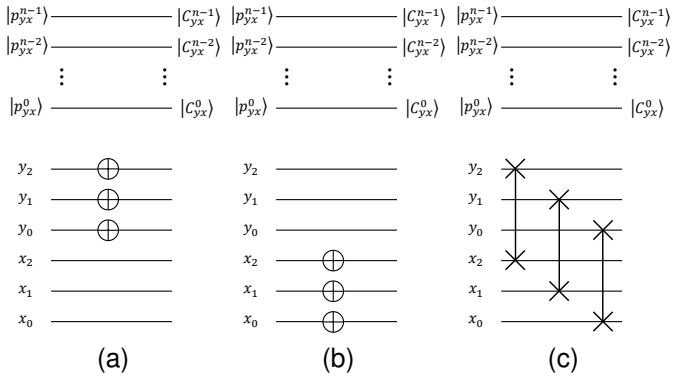


Fig. 12: Quantum circuits of geriatric transformations. (a) Γ_I^{VF}– vertical flip. (b) Γ_I^{HF}– horizontal flip. (c) Γ_I^{CS}– co-ordinate swap.

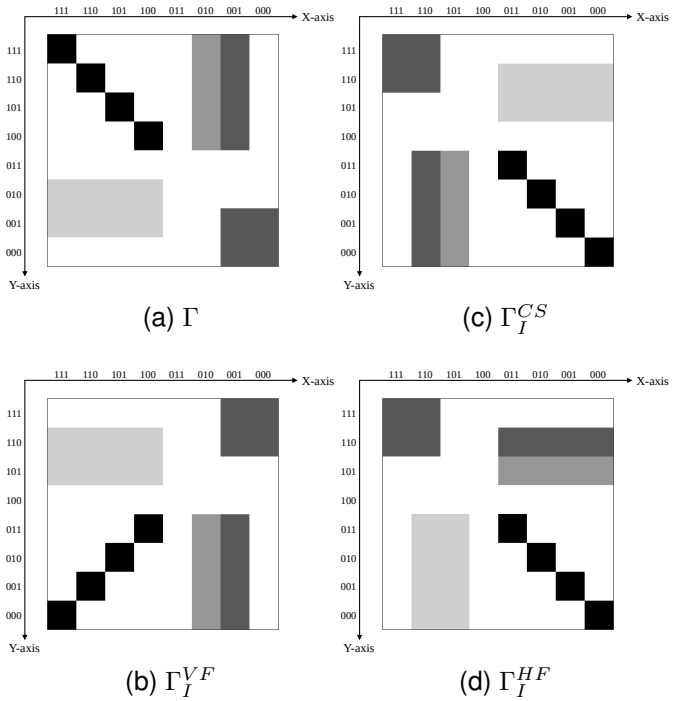


Fig. 13: Sample of geometric transformation operations on an 8x8 image block. (a) normal image. (b) output of Γ_I^{VF}– vertical flip. (c) output of Γ_I^{CS}– coordinate swap. (d) output of Γ_I^{HF}– horizontal flip.

Applying $P_{2^{n-1},2}$ and $P_{2,2^{n-1}}$ to the state $|j_n j_{n-1} \cdots j_2 j_1\rangle$, we have

$$\begin{aligned} P_{2^{n-1},2}\,|j_n j_{n-1} \cdots j_2 j_1\rangle &= |j_1 j_n j_{n-1} \cdots j_2\rangle\,, \\ P_{2,2^{n-1}}\,|j_n j_{n-1} \cdots j_2 j_1\rangle &= |j_{n-1} \cdots j_2 j_1 j_n\rangle\,. \end{aligned} \quad (23)$$

These operations represent a cyclic shift operator. To acheive multi-bit shift operations, the iterations of $P_{2^n,2^{m-1}}$ and $P_{2^{m-1},2^n}$ are given by

$$\begin{aligned} P_{2^n,2^{m-1}} &= (P_{2,2^{m-1}} \otimes I_{2^{n-1}})(I_2 \otimes P_{2^{n-1},2^{m-1}}), \\ P_{2^{m-1},2^n} &= (I_2 \otimes P_{2^{m-1},2^{n-1}})(P_{2^{m-1},2} \otimes I_{2^{n-1}}). \end{aligned} \quad (30)$$

The quantum circuits for the bit-shift operations $P_{2^{n-1},2}$ and $P_{2,2^{n-1}}$ are realised in Fig. 14.

Transformation function for the Bit Shift Approach

Extending the perfect shuffle approach to multi-bit shift operations, the realised quantum circuits via quantum swap gates are given in Fig. 15. The shift operation is performed on the gray value $\left|p_{yx}^{7'} p_{yx}^{6'} \cdots p_{yx}^{1'} p_{yx}^{0'}\right\rangle$, and new order is obtained as $\left|p_{yx}^{2'} p_{yx}^{3'} \cdots p_{yx}^{0'} p_{yx}^{1'}\right\rangle$.

To realise this bit-shift operation mathematically for a pixel (Y, X), the transformtion function is V_{YX} defined as follows [32], [41].

$$\begin{aligned} V_{YX}\left(|P_{YX}\rangle\right) &= V_{YX}\left(\left|p_{YX}^{7} p_{YX}^{6} \cdots p_{YX}^{1} p_{YX}^{0}\right\rangle\right) \\ &= \left|p_{YX}^{2'} p_{YX}^{3'} \cdots p_{YX}^{0'} p_{YX}^{1'}\right\rangle \end{aligned} \quad (26)$$

Then define the sub-operation $\mathbf{W}_{YX}$ by using permutation operator V_{YX}.

$$\mathbf{W}_{YX} = \left(\mathbf{I}^{\otimes 8} \otimes \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |yx\rangle\langle yx|\right) + V_{YX} \otimes |YX\rangle\langle YX| \quad (27)$$

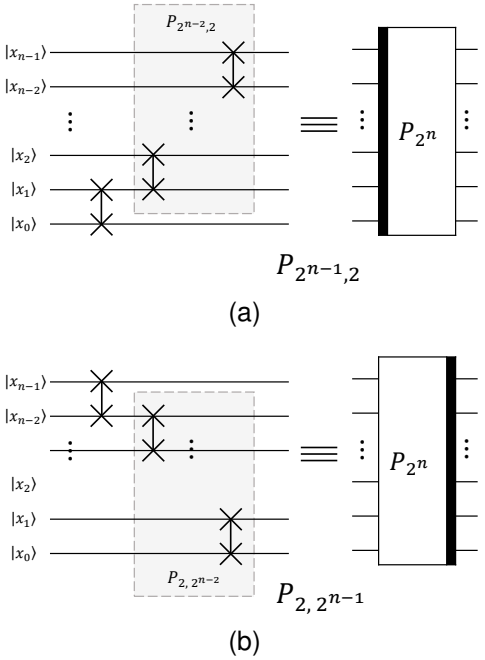


Fig. 14: Quantum circuits for perfect shuffle $P_{2^{n-1},2}$ and $P_{2,2^{n-1}}$

Authorized licensed use limited to: Edinburgh Napier University. Downloaded on June 26,2024 at 01:31:46 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. 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/TCE.2024.3415411

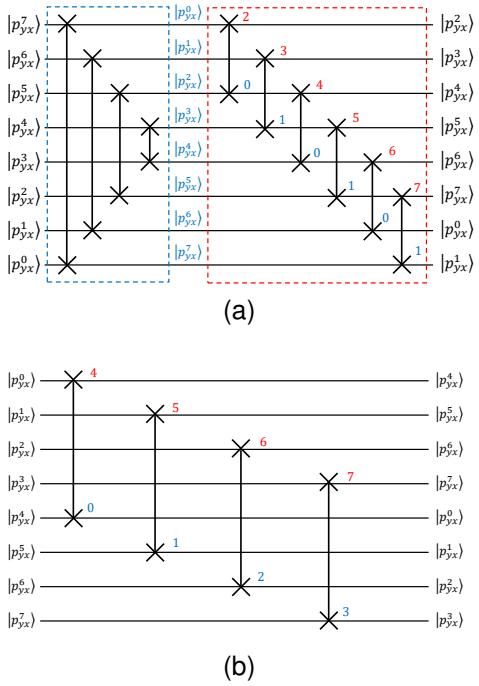


Fig. 15: Quantum circuits for multi-bit shift operations. (a) 2 bit left shift. (c) 4 bit left shift.

where the quantum sub-operation $\mathbf{W}_{YX}$ is unitary. The bit-level permutation of pixel (Y_0, X_0) can be accomplished by applying the sub-operation $\mathbf{W}_{Y_0X_0}$ on quantum state $|I_1\rangle$ and obtain the following resultant.

$$W_{Y_0X_0}\left(|I_1\rangle\right) = W_{Y_0X_0}\left(\frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|P_{yx}\rangle\,|y'\rangle\,|x'\rangle\right)$$

$$= \frac{1}{2^n}\left(\sum_{\substack{y=0\\x=0\\yx\neq Y_0X_0}}^{2^n-1}|P_{yx}\rangle\,|y'\rangle\,|x'\rangle + V_{YX}\left(|P_{Y_0X_0}\rangle\right)|Y_0X_0\rangle\right)$$

$$= \frac{1}{2^n}\left(\sum_{\substack{y=0\\x=0\\yx\neq Y_0X_0}}^{2^n-1}|P_{y'x'}\rangle\,|y'\rangle\,|x'\rangle + \left|p^{2'}_{Y_0X_0}p^{3'}_{Y_0X_0}\cdots p^{7'}_{Y_0X_0}p^{0'}_{Y_0X_0}p^{1'}_{Y_0X_0}\right\rangle|Y_0X_0\rangle\right) \tag{28}$$

The procedure involves the application of the transformation $\mathbf{W}_{Y_1X_1}$ to the existing state, aiming to adjust the grayscale level of the pixel situated at coordinates (Y_1, X_1).

$$W_{Y_1X_1}W_{Y_0X_0}\left(|I_1\rangle\right) = W_{Y_1X_1}W_{Y_0X_0}\left(\frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|P_{yx}\rangle\,|y'\rangle\,|x'\rangle\right)$$

$$= \frac{1}{2^n}\Bigg(\sum_{\substack{y=0\\x=0\\yx\neq Y_0X_0,Y_1X_1}}^{2^n-1}|P_{yx}\rangle\,|y'\rangle\,|x'\rangle + \left|p^{2'}_{Y_0X_0}p^{3'}_{Y_0X_0}\cdots p^{0'}_{Y_0X_0}p^{1'}_{Y_0X_0}\right\rangle|Y_0X_0\rangle + \left|p^{2'}_{Y_1X_1}p^{3'}_{Y_1X_1}\cdots p^{0'}_{Y_1X_1}p^{1'}_{Y_1X_1}\right\rangle|Y_1X_1\rangle\Bigg) \tag{29}$$

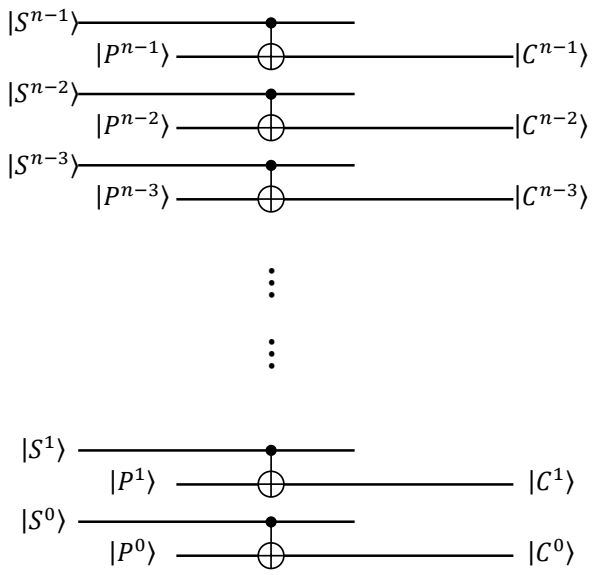


Fig. 16: Quantum circuit for the chaotic seed diffusion module.

E. Step 4: Chaotic Seed Diffusion

The final module of this encryption scheme is the chaotic seed diffusion module and is named as $\mathbb{P}_2^{M2}$ in Fig. 9. It involves generating a 256×256 random matrix using the discretized Van Der Pol Oscillator. This matrix is then combined with the output of a confusion module through a bitwise XOR operation, that is realised via combination of CNOT gates depicted in Fig. 16 and the encrypted image can be represented by:

$$\begin{aligned}|C\rangle &= |S\rangle \oplus |I_2\rangle \\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left(|S_{YX}\rangle \oplus \left|P'_{YX}\right\rangle\right)|YX\rangle \\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|C_{YX}\rangle\,|YX\rangle\end{aligned} \tag{30}$$

V. Results and Analysis

The proposed two-phase QIE scheme has been extensively evaluated for several security evaluation parameters, histogram analysis, correlation analysis, entropy, the Number of Pixel Change Rate (NPCR), the Unified Average Changed Intensity (UACI), etc. All tests are performed on five grayscale test images,i.e., Baboon, Apple (binary), Jupiter, Medical Imaging, and Cameraman. The proposed scheme is simulated and evaluated in MATLAB using classical equivalents of quantum gates. Fig 17 shows the visual encryption and decryption results for the proposed two-phase QIE scheme. It can be observed that the input images are effectively encrypted, concealing all visual information.

A. Histogram Analysis

A histogram usually represents the frequency of occurrence of each intensity level within the image. This information

Authorized licensed use limited to: Edinburgh Napier University. Downloaded on June 26,2024 at 01:31:46 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. 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/TCE.2024.3415411

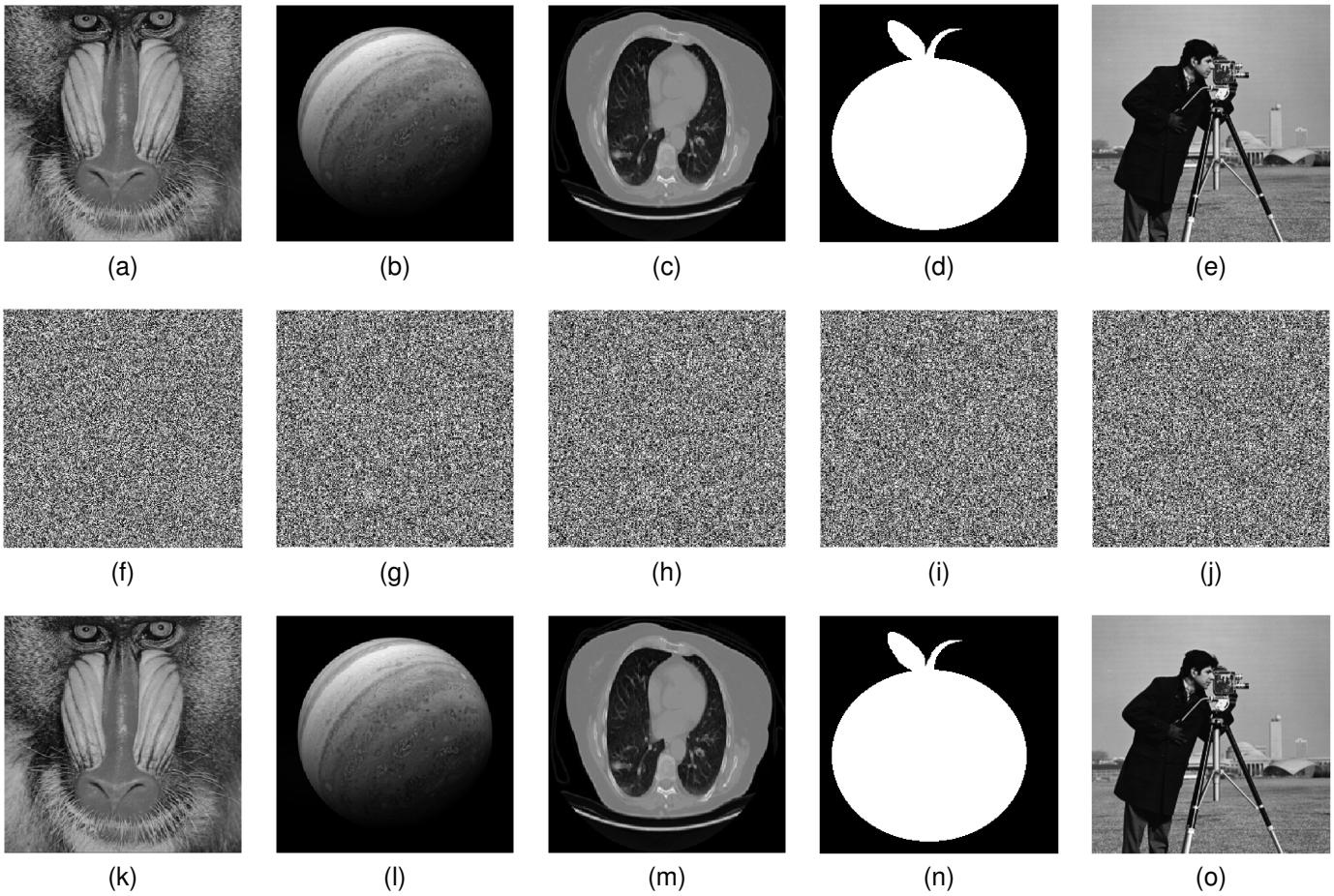


Fig. 17: Visual Encryption Analysis of the proposed scheme. (a-e) Plaintext images. (f-j) Encrypted Images. (k-o) Decrypted Images.

is crucial in term of image encryption, as it can be used to retrieve the original information in the image. Ideally, an encrypted image's histogram should resemble a uniform distribution, where each pixel intensity has roughly the same frequency of occurrence. Fig. 18 shows that the histogram analysis, depicting the equally distributed frequency of occurrence for all test images. This means that the encrypted image has equal frequency of occurrence for all pixel intensities, thereby making it difficult for the attackers to predict the frequency of occurrence of any specific pixel intensity in the original image.

B. Correlation Analysis

Correlation is the relationship between the adjacent pixels of an image. In a plaintext image, adjacent pixels tend to have correlated or similar values in certain regions due to shapes and structure of objects in the image. An effective encryption algorithm should reduce or ideally break this correlation, making the encrypted image appear as random noise and the ideal value of correlation for an encrypted image should be zero. The correlation coefficient is found by:

$$\text{Corr}_C = \frac{\sum_{p=1}^{M}\sum_{q=1}^{N}\left(P(p,q)-O(P)\right)\left(C(p,q)-O(C)\right)}{\sqrt{\sum_{p=1}^{M}\sum_{q=1}^{N}\left(P(p,q)-O(P)\right)^2\sum_{p=1}^{H}\sum_{q=1}^{N}\left(C(p,q)-O(C)\right)^2}} \tag{31}$$

where,

- $\sum_{p=1}^{M}\sum_{q=1}^{N}(\cdots)$ and $\sum_{p=1}^{H}\sum_{q=1}^{N}(\cdots)$ represent double summations over the pixels, iterating through rows p and columns q.
- $P(p,q)$ and $C(p,q)$ denote the pixel intensities at a particular row-column position in their respective images.
- $O(P)$ and $O(C)$ refer to the expected values for their corresponding images.

All images were analyzed for the effective dispersion of correlation coefficients and the results are displayed in Fig. 19. The widely dispersed correlation coefficients validates that the encryption algorithm has successfully broken the inherent correlations between adjacent pixels. This is why the vertical, horizontal, and diagonal correlation coefficients for the encrypted Baboon image showing near to zero values are given in Table I.

C. Entropy Analysis

Entropy serves as an indicator of the unpredictability or disorder within a system. In information theory, it is utilized to gauge the level of uncertainty in forecasting the outcome of a random variable. For a discrete random variable X with

Authorized licensed use limited to: Edinburgh Napier University. Downloaded on June 26,2024 at 01:31:46 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. 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/TCE.2024.3415411

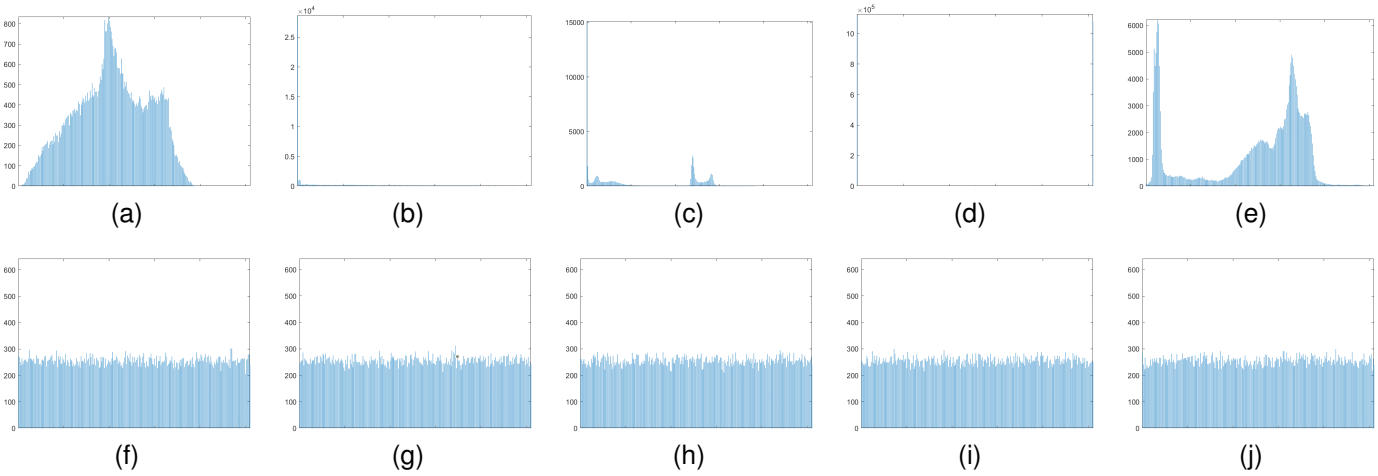


Fig. 18: Histogram Analysis of encrption scheme. (a-e) histograms of plaintext images. (f-j) histograms of the ciphertext images.

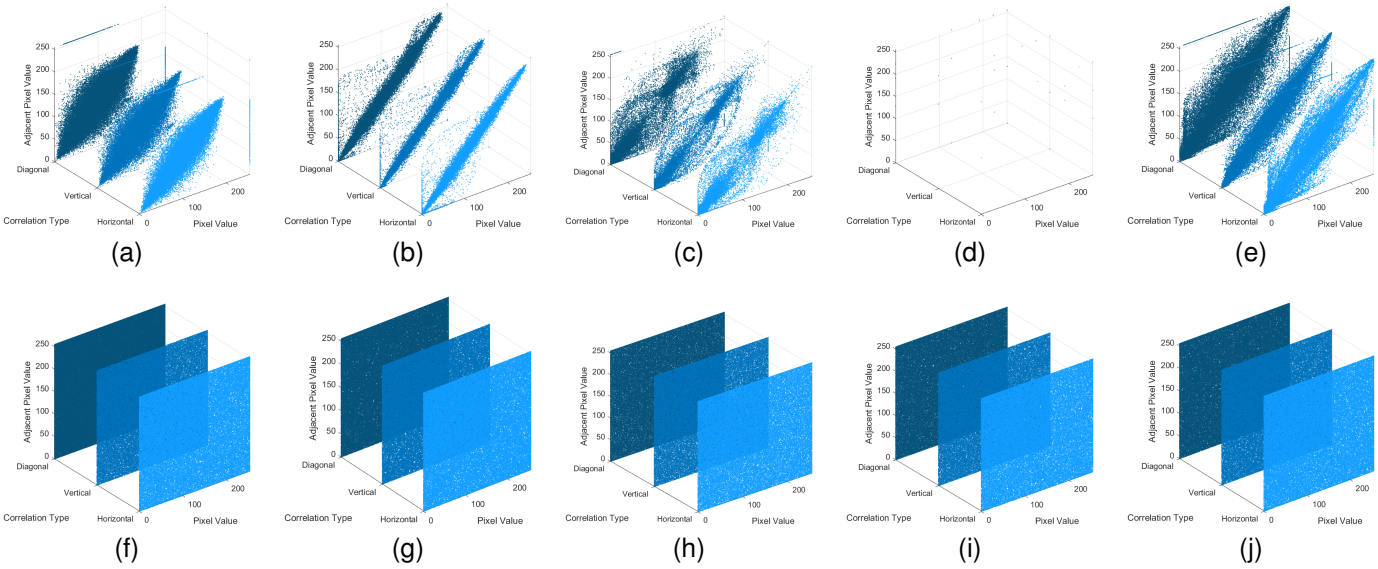


Fig. 19: Correlation analysis of encryption scheme. (a-e) correlation coefficients of plaintext images. (f-j) correlation coefficients of ciphertext images.

probability mass function $p(|x\rangle)$, the entropy $H(X)$ is defined as:

$$H(X) = -\sum_{|x\rangle \in X} p(|x\rangle) \log_2 p(|x\rangle) \tag{32}$$

Where:

- $|x\rangle$ is an outcome of the random variable X.
- $p(|x\rangle)$ is the probability of occurrence of $|x\rangle$.

As Grayscale images typically have pixel intensities in a range of 0 and 255. The ideal entropy for such an image is given by:

$$H_{\max} = \log_2 L \tag{33}$$

Where L is the number of distinct grayscale levels (i.e., 256 for 8-bit images). Thus, the ideal entropy for an 8-bit grayscale image is:

$$H_{\text{ideal}} = \log_2 256 = 8 \tag{34}$$

So, the maximum entropy of a 256×256 grayscale image is 8 bits/pixel, indicating complete randomness.

The results of the entropy for the test images is given in Table II. The entropy values of encrypted images are ideally

TABLE I: Correlation Analysis of Cipher Images

Sr.	Image	Correlation	Correlation Coefficients		
			Horiz	Vert	Diag
1	Baboon	0.00024	0.0012	0.0065	-0.0071
2	Jupiter	0.00047	0.0027	0.0029	0.0026
3	Medical Imaging	0.00036	-0.0070	-0.0032	0.0031
4	Apple Binary	0.0024	-0.0089	0.0015	0.0055
5	Cameraman	0.0001	0.0089	0.0044	0.0054

Authorized licensed use limited to: Edinburgh Napier University. Downloaded on June 26,2024 at 01:31:46 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. 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/TCE.2024.3415411

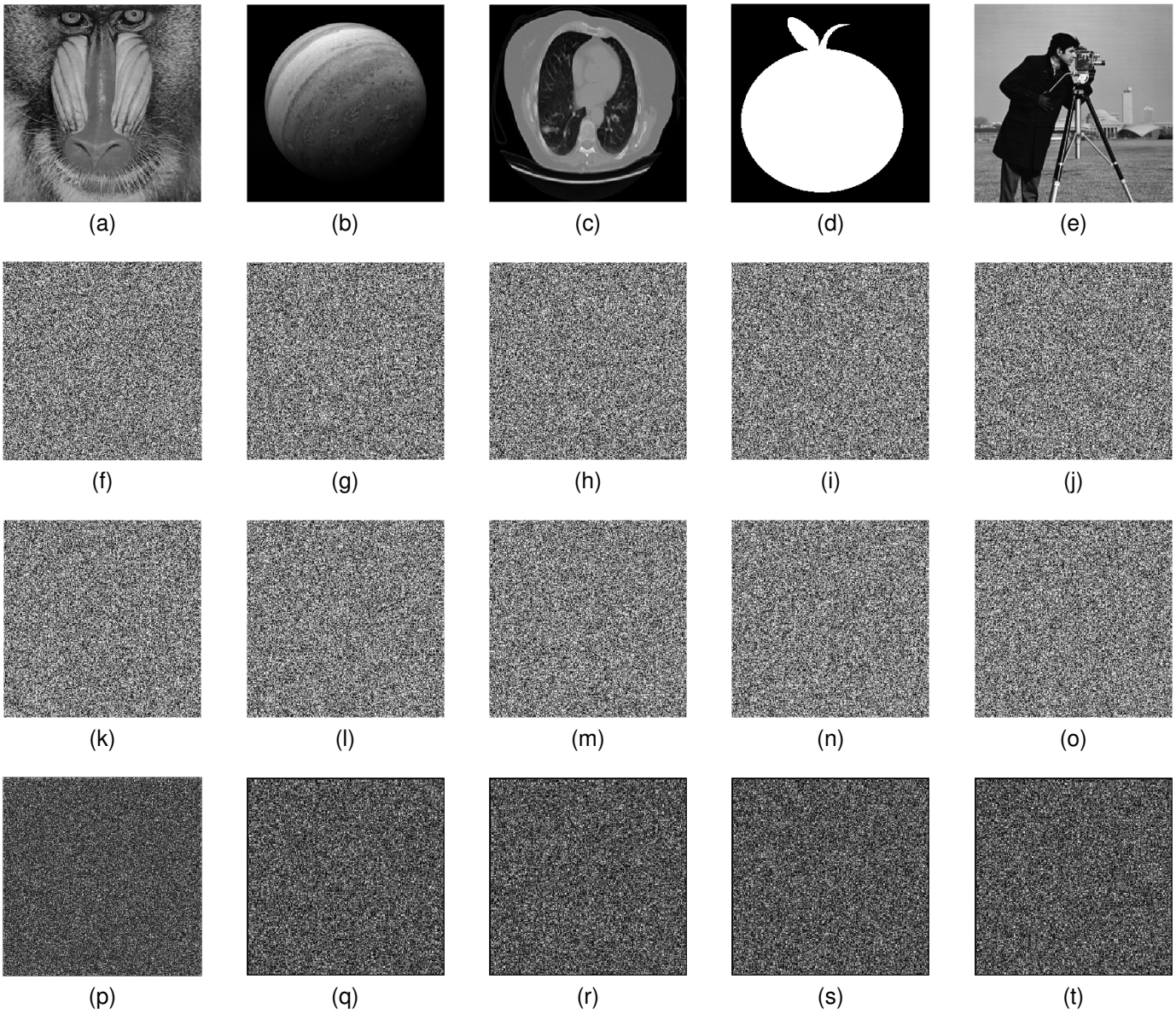


Fig. 20: Results of differential attack on test images. (a-e) Plaintext Images. (f-j) Ciphertexts of original palintext images. (k-o) Ciphertexts of corrupted plaintext Images with 1-bit change. (p-t) difference between both ciphertext images.

close to 8, indicating a high level of randomness within these images. This high randomness is a key factor in ensuring the robustness and security of the encryption method used.

D. Resistance to Differential Attacks

Differential attacks aim to find differences between two encrypted images that result from slight differences in their plaintext versions. The proposed two-phase QIE scheme was tested for differential attacks and the results are shown in Fig. 20. The plaintext test image by altered by changing just one bit in the plaintext image and then encrypted these 1-bit-altered images. Row 3 in Fig. 20 depict the encrypted images of the 1-bit altered plaintext images. The difference between the original ciphertext and the 1-bit altered ciphertext is depicted in Row 4 of Fig. 20. If the encryption was invariant to the change of a single pixel, the difference between the two encrypted images woulfd be 0, resulting in a completely black difference image. However, as can be observed, the difference images are not black.

TABLE II: Entropy of the plaintext and cipher images

Sr.	Image	Plaintext Image	Cipher Image
1	Baboon	7.29	7.99
2	Jupiter	5.26	7.99
3	Medical Imaging	5.8	7.99
4	Apple Binary	1.03	7.99
5	Cameraman	7.04	7.99

Authorized licensed use limited to: Edinburgh Napier University. Downloaded on June 26,2024 at 01:31:46 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. 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/TCE.2024.3415411

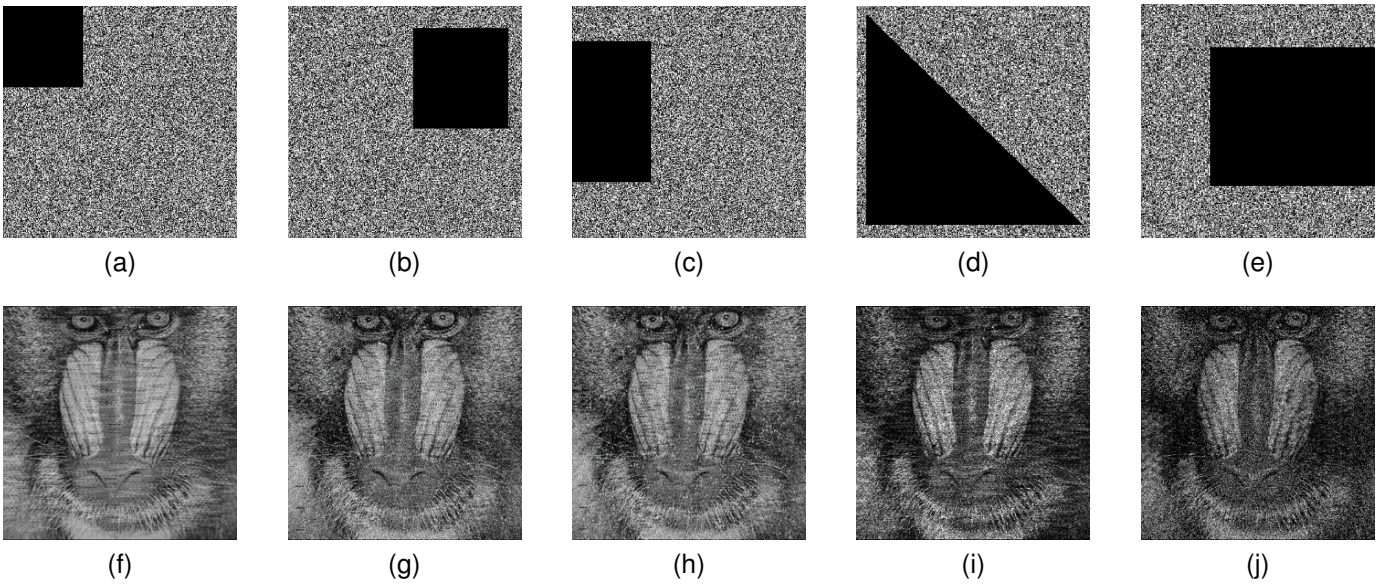


Fig. 21: Resilience against occlusion attacks. (a to e) ciphertext images with occlusion attacks. (f-j) decrypted images.

E. Analysis of Number of Pixels Changing Rate (NPCR)

NPCR is often utilized to compare two encrypted images that arise from minute variations in the original plaintext images. NPCR is a metric primarily used in the context of image encryption to measure how sensitive an encryption scheme is to slight changes in its input. NPCR can be computed for two images C_1 and C_2 by:

1) Determine Differing Pixels: For each pixel position (p, q), check if the pixel value in C_1 is different from the pixel value in C_2. If they're different, mark that position.
2) Compute the NPCR: The formula for NPCR is:

$$\text{NPCR} = \frac{1}{2^{2n}} \sum_{p,q} |\Delta(p, q)| \times 100\% \tag{35}$$

.

Here: Δ is the difference in pixel positions between C_1 and C_2.
H denotes the height of the image and W denotes the width of the image.

A high NPCR value (close to 100%) indicates that nearly all the pixels between the two compared images differ from each other. It can be seen in Table 11 that the NPCR values for all three test images are close to 100% depicting the resilience of the proposed scheme.

F. Analysis of Unified Average Changing Intensity (UACI)

The Unified Average Changing Intensity (UACI) metric measures the average difference in pixel intensities between two images. In image encryption, UACI is particularly useful for assessing how minute changes in the original images (plaintexts) affect the pixel values in their encrypted counterpart. While NPCR focuses on the number of pixel positions that change, UACI assesses the magnitude or intensity of those changes. To compute the UACI between two images C_1 and C_2, the following steps are followed:

1) Determine the Intensity Differences: For each pixel position (p, q), compute the absolute difference between the pixel values in C_1 and C_2.
2) Compute the UACI: The formula for UACI is:

$$\text{UACI} = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} \left(\frac{|C_1(p, q) - C_2(p, q)|}{L - 1} \right) \times 100\%$$

Where:

- H and W are the height and width of the images, respectively.
- L is the maximum possible pixel value. For an 8-bit grayscale image, $L = 256$.

A high value of UACI value indicates a considerable average change in pixel brightness levels between two images. In image encryption, this denotes that minute changes in the original image result in significant changes in the pixel values of the encrypted output, highlighting the encryption algorithm's sensitivity to input changes. On the other hand, a low UACI might indicate that the encryption algorithm isn't introducing enough variability in pixel intensities, which could be a potential security concern.

In the literature, a commonly cited ideal or threshold value for UACI is approximately 33.46% for an 8-bit grayscale image [42, 43]. This percentage means that the difference in the pixel intensities of two images should be around 255/2 or 127.5. The calculation for this ideal value, considering the maximum pixel value to be 255, is:

$$\text{UACI} = \frac{127.5}{255} \times 100\% \approx 33.46\%$$

A UACI value close to 33.46% indicates that the encryption scheme effectively introduces variability in pixel intensities. Table **??** shows that UACI for all test images is greater than 33.5%.

Authorized licensed use limited to: Edinburgh Napier University. Downloaded on June 26,2024 at 01:31:46 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. 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/TCE.2024.3415411

TABLE III: Comparison of NPCR and UACI analysis

Image	NPCR	UACI
Baboon	99.7045%	33.5689%
Jupiter	99.7921%	33.5107%
Medical Imaging	99.7001%	33.5991%
Apple Binary	99.5069%	33.5001%
Cameraman	99.7092%	33.5994%
Average	**99.6826%**	**33.5556%**
Ref [42]	99.6573%	33.56%
Ref [43]	99.65%	33.5504%
Ref [44]	99.57%	33.51%

G. Resilience Against Data Loss

For the transmission of digital images over networks, a primary concern is the susceptibility of these images to noise and data loss, which could substantially compromise the integrity of an encrypted image. Occlusion attacks, also known as data loss attacks, represent a notable threat. An occlusion attack involves an adversary maliciously removing sections of a cipher image with the intent to invalidate the decryption process. The proposed scheme has been evaluated for both the data loss attacks and noise attacks. Fig. 21 offers a visual representation of this test, showcasing the cipher image 'Baboon' subjected to occlusion attacks of different severities. The results show that even after 60% cropping of the encrypted images, the algorithm successfully decrypted the image revealing maximum information.

VI. Conclusion

This paper developed and evaluated a quantum image encryption scheme designed to secure image data in the quantum-enabled consumer technology. Through the introduction of a two-phase chaotic confusion-diffusion architecture, the scheme encrypts both the position and intensity information of quantum image pixels at multiple levels. The implementation of novel quantum circuits for qubit-level transformations and chaos-based operations further strengthened the designed confusion-diffusion modules. The comprehensive evaluation of the scheme in terms of statistical security parameters, like entropy, correlation, etc, demonstrated its effectiveness. Furthermore, the results also demonstrated the proposed scheme's resilience to differential attacks. Even a minute change in the plaintext led to a considerably different encrypted image, highlighting the method's sensitivity and non-linearity.

References

[1] W.-W. Hu, R.-G. Zhou, S. Jiang, X. Liu, and J. Luo, "Quantum image encryption algorithm based on generalized arnold transform and logistic map," *CCF Transactions on High Performance Computing*, vol. 2, pp. 228–253, 2020.

[2] R. Sotelo, "Quantum in consumer technology," *IEEE Consumer Electronics Magazine*, vol. 12, no. 5, pp. 4–7, 2023.

[3] K. N. Singh, N. Baranwal, O. P. Singh, and A. K. Singh, "Sielnet: 3-d chaotic-map-based secure image encryption using customized residual dense spatial network," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 4, pp. 862–868, 2023.

[4] H. K. Singh and A. K. Singh, "Using deep learning to embed dual marks with encryption through 3-d chaotic map," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 3056–3063, 2024.

[5] J. He, H. Zhu, and X. Zhou, "Quantum image encryption algorithm via optimized quantum circuit and parity bit-plane permutation," *Journal of Information Security and Applications*, vol. 81, p. 103698, 2024.

[6] Y. Zhou, L. Liu, and H. Shen, "Digital media steganography based on spatial distortion model is used to encrypt consumer electronic product data," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 4490–4498, 2024.

[7] M. Singh, N. Baranwal, K. N. Singh, and A. K. Singh, "Using gan-based encryption to secure digital images with reconstruction through customized super resolution network," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 3977–3984, 2024.

[8] H. K. Singh, N. Baranwal, K. N. Singh, and A. K. Singh, "Using multimodal biometric fusion for watermarking of multiple images," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 3487–3494, 2024.

[9] R. Chaurasia and A. Sengupta, "Retinal biometric for securing jpeg-codec hardware ip core for ce systems," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 3, pp. 441–457, 2023.

[10] B. B. Gupta, A. Gaurav, and V. Arya, "Secure and privacy-preserving decentralized federated learning for personalized recommendations in consumer electronics using blockchain and homomorphic encryption," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 2546–2556, 2024.

[11] I. Aribilola, M. N. Asghar, N. Kanwal, M. Fleury, and B. Lee, "Securecam: Selective detection and encryption enabled application for dynamic camera surveillance videos," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 2, pp. 156–169, 2023.

[12] S. Mehraj, S. Mushtaq, S. A. Parah, K. J. Giri, J. A. Sheikh, A. H. Gandomi, M. Hijji, B. B. Gupta, and K. Muhammad, "Rbwci: robust and blind watermarking framework for cultural images," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 2, pp. 128–139, 2022.

[13] K. K. Singamaneni, G. Muhammad, and Z. Ali, "A novel multi-qubit quantum key distribution ciphertext-policy attribute-based encryption model to improve cloud security for consumers," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1092–1101, 2024.

[14] F. Yan, S. E. Venegas-Andraca, F. Yan, and S. E. Venegas-Andraca, "Quantum image representations," *Quantum Image Processing*, pp. 19–48, 2020.

[15] F. Yan, A. M. Iliyasu, and S. E. Venegas-Andraca, "A survey of quantum image representations," *Quantum Information Processing*, vol. 15, pp. 1–35, 2016.

[16] S. E. Venegas-Andraca and J. Ball, "Processing images in entangled quantum systems," *Quantum Information Processing*, vol. 9, no. 1, pp. 1–11, 2010.

[17] P. Q. Le, F. Dong, and K. Hirota, "A flexible representation of quantum images for polynomial preparation, image compression, and processing operations," *Quantum Information Processing*, vol. 10, pp. 63–84, 2011.

[18] H.-S. Li, Z. Qingxin, S. Lan, C.-Y. Shen, R. Zhou, and J. Mo, "Image storage, retrieval, compression and segmentation in a quantum system," *Quantum information processing*, vol. 12, no. 6, pp. 2269–2290, 2013.

[19] B. Sun, P. Q. Le, A. M. Iliyasu, F. Yan, J. A. Garcia, F. Dong, and K. Hirota, "A multi-channel representation for images on quantum computers using the rgbα color space," in *2011 IEEE 7th International Symposium on Intelligent Signal Processing*. IEEE, 2011, pp. 1–6.

[20] Y.-G. Yang, X. Jia, S.-J. Sun, and Q.-X. Pan, "Quantum cryptographic algorithm for color images using quantum fourier transform and double random-phase encoding," *Information Sciences*, vol. 277, pp. 445–457, 2014.

[21] B. Sun, A. Iliyasu, F. Yan, F. Dong, and K. Hirota, "An rgb multi-channel representation for images on quantum computers," *J. Adv. Comput. Intell. Intell. Inform*, vol. 17, no. 3, 2013.

[22] S. E. Venegas-Andraca and S. Bose, "Storing, processing, and retrieving an image using quantum mechanics," in *Quantum information and computation*, vol. 5105. SPIE, 2003, pp. 137–147.

[23] P. Q. Le, A. M. Iliyasu, F. Dong, and K. Hirota, "Fast geometric transformations on quantum images." *IAENG International Journal of Applied Mathematics*, vol. 40, no. 3, 2010.

[24] P. Q. Le, A. Iliyasu, F. Dong, and K. Hirota, "Strategies for designing geometric transformations on quantum images," *Theoretical Computer Science*, vol. 412, no. 15, pp. 1406–1418, 2011.

[25] Y. Zhang, K. Lu, Y. Gao, and M. Wang, "Neqr: a novel enhanced quantum representation of digital images," *Quantum information processing*, vol. 12, pp. 2833–2860, 2013.

[26] H.-S. Li, P. Fan, H.-Y. Xia, H. Peng, and S. Song, "Quantum implementation circuits of quantum signal representation and type conversion," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 1, pp. 341–354, 2018.

Authorized licensed use limited to: Edinburgh Napier University. Downloaded on June 26,2024 at 01:31:46 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. 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/TCE.2024.3415411

[27] N. Sharma, P. Kumar, and S. K. Rai, "Chua's oscillator-based rsa algorithm with authenticated masked public key for secure communication," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 4, pp. 1124–1132, 2023.
[28] F. Yan, A. M. Iliyasu, and P. Q. Le, "Quantum image processing: a review of advances in its security technologies," *International Journal of Quantum Information*, vol. 15, no. 03, p. 1730001, 2017.
[29] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 10 1949.
[30] N. Jiang, L. Wang, and W.-Y. Wu, "Quantum hilbert image scrambling," *International Journal of Theoretical Physics*, vol. 53, pp. 2463–2484, 2014.
[31] N. Jiang, W.-Y. Wu, and L. Wang, "The quantum realization of arnold and fibonacci image scrambling," *Quantum information processing*, vol. 13, no. 5, pp. 1223–1236, 2014.
[32] X. Liu, D. Xiao, and C. Liu, "Quantum image encryption algorithm based on bit-plane permutation and sine logistic map," *Quantum Information Processing*, vol. 19, pp. 1–23, 2020.
[33] J. Zhang, Z. Huang, X. Li, M. Wu, X. Wang, and Y. Dong, "Quantum image encryption based on quantum image decomposition," *International journal of theoretical physics*, vol. 60, pp. 2930–2942, 2021.
[34] F. Yan, Y. Guo, A. M. Iliyasu, Z. Jiang, and H. Yang, "Multi-channel quantum image scrambling," *Journal of Advanced Computational Intelligence and Intelligent Informatics*, vol. 20, no. 1, pp. 163–170, 2016.
[35] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge university press, 2010.
[36] H.-S. Li, P. Fan, H.-Y. Xia, H. Peng, and S. Song, "Quantum implementation circuits of quantum signal representation and type conversion," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 1, pp. 341–354, 2019.
[37] A. Dewdney, "Probing the strange attractions of chaos," p. 108, 1987.
[38] B. Van der Pol, "theory of the amplitude of frfee. forced triode vibrations," *Radio review*, vol. 1, pp. 701–710, 1920.
[39] H.-S. Li, X. Chen, S. Song, Z. Liao, and J. Fang, "A block-based quantum image scrambling for gneqr," *IEEE Access*, vol. 7, pp. 138 233–138 243, 2019.
[40] H.-S. Li, P. Fan, H.-y. Xia, and S. Song, "Quantum multi-level wavelet transforms," *Information Sciences*, vol. 504, pp. 113–135, 2019.
[41] M. Hu, J. Li, and X. Di, "Quantum image encryption scheme based on 2d s ine 2-l ogistic chaotic map," *Nonlinear Dynamics*, vol. 111, no. 3, pp. 2815–2839, 2023.
[42] Y.-G. Yang, J. Tian, H. Lei, Y.-H. Zhou, and W.-M. Shi, "Novel quantum image encryption using one-dimensional quantum cellular automata," *Information Sciences*, vol. 345, pp. 257–270, 2016.
[43] S. Etemadi Borujeni and M. Eshghi, "Chaotic image encryption system using phase-magnitude transformation and pixel substitution," *Telecommunication Systems*, vol. 52, pp. 525–537, 2013.
[44] S. Zhou, "A quantum image encryption method based on dnacnot," *IEEE Access*, vol. 8, pp. 178 336–178 344, 2020.

Muhammad Shahbaz Khan is an experienced academic and researcher with more than 10 years of experience in teaching and research. He received his B.S. and M.S. degrees in Electronics and Electrical Engineering from NFC IET, Multan, and HITEC University, Taxila Pakistan in 2011 and 2015, respectively. He has served as a Lecturer in the Department of Electrical Engineering, HITEC University for more than 8 years. He is currently pursuing his PhD degree in Cyber Security and Artificial Intelligence at the School of Computing, Engineering and the Built Environment, Edinburgh Napier University, Edinburgh, UK. His research interests include chaotic systems, chaotic image encryption, post-quantum cryptography, intrusion detection, and AI for cyber security and healthcare.

Jawad Ahmad (Senior Member, IEEE) is currently an experienced Researcher with more than ten years of cutting-edge research and teaching experience in prestigious institutes, including Edinburgh Napier University, U.K.; Glasgow Caledonian University, U.K.; Hongik University, South Korea; and HITEC University Taxila, Pakistan. He has taught various courses both at undergraduate (UG) and postgraduate (PG) levels during his career. He has coauthored more than 100 research papers in international journals and peer-reviewed international conference proceedings. His research interests include cybersecurity, multimedia encryption, and machine learning. He regularly organizes timely special sessions and workshops for several flagship IEEE conferences. He is an invited reviewer of numerous world-leading high-impact journals (reviewed more than 100 journal articles to date).

Ahmed Al-Dubai (Senior Member, IEEE) received the Ph.D. degree in computing from the University of Glasgow in 2004. He is currently a Professor in networking and communication algorithms with the School of Computing, Edinburgh Napier University, U.K. His research interests include communication algorithms, mobile communication, the Internet of Things, and future internet. He received several international awards.

Nikolaos Pitropakis received his degree in Computer Science from the University of Athens, Greece in 2009. He completed an MSc in Advanced Information Systems at the Athens University of Economics and Business in 2011. Currently, he is an Associate Professor of cybersecurity at the School of Computing of Edinburgh Napier University, and a Fellow of the HEA and a core member of the Blockpass Identity Lab. Dr Pitropakis has a strong research background in attacks against machine learning. His current research interests include adversarial machine learning, trust and privacy using distributed ledger technology, advanced cyber attack attribution, and data science applied to cyber security and IoT device security.

Baraq Ghaleb received the B.Sc. degree in computer science from The University of Jordan, Amman, Jordan, in 2009, the M.Sc. degree from the Jordan University of Science and Technology, Irbid, Jordan, in 2013, and the Ph.D. degree in applied computing from Edinburgh Napier University, Edinburgh, U.K. Currently he is an Associate Professor with the School of Computing, Engineering and the Built Environment, Edinburgh Napier University, Edinburgh, UK. He holds one patent in the field of the IoT routing. His current research interests include routing protocols in low-power and lossy networks and the Internet of Things (IoTs), security of LLNs, and the IoT in addition to data mining.

Authorized licensed use limited to: Edinburgh Napier University. Downloaded on June 26,2024 at 01:31:46 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Consumer Electronics. 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/TCE.2024.3415411

Amjad Ullah is a Lecturer in Software engineering at the Edinburgh Napier University, UK. He has 15+ years of professional experience in the field of computing with a focus on software engineering, and distributed systems. So far, he has actively contributed and involved in cutting-edge research and development of innovation and research-based Horizon projects including COLA, CloudiFacturing, ASCLEPIOS, PITHIA, and DIGITbrain. He has the experience of co-authoring research papers in leading international journals and peer-reviewed international conference proceedings. He also has a strong interest in contributing to the open-source development community and has so far contributed to various open-source projects.

Muhammad Attique Khan (Member IEEE) received the master's degree in action recognition and Ph.D. degree in medical imaging using deep learning using deep learning from COMSATS University Islamabad, Islamabad, Pakistan.,He is currently an Assistant Professor with the Computer Science Department, HITEC University, Taxila, Pakistan. His primary research focus in recent years is medical imaging, COVID-19, MRI analysis, video surveillance, human gait recognition, and agriculture plants using deep learning. He has more than 280 publications that have more than 10 000+ citations and an impact factor of 850+ with h-index 61 and i-index 165.,Dr. Khan is a Reviewer of several reputed journals such as IEEE Transaction on Industrial Informatics, IEEE Transaction of Neural Networks, Pattern Recognition Letters, Multimedia Tools and Application, Computers and Electronics in Agriculture, IET Image Processing, Biomedical Signal Processing Control, IET Computer Vision, Eurasipe Journal of Image and Video Processing, IEEE Access, MDPI Sensors, MDPI Electronics, MDPI Applied Sciences, MDPI Diagnostics, and MDPI Cancers.

William J. Buchanan is a Professor with the School of Computing, Edinburgh Napier University, Edinburgh, U.K. He currently leads the Blockpass ID Lab and the Centre for Cybersystems and Cryptography. He has published over 30 academic books, and over 300 academic research papers. He works in the areas of blockchain, cryptography, trust, and digital identity. He has one of the most extensive cryptography sites in the World (asecuritysite.com), and is involved in many areas of novel research and teaching. Along with this, his work has led to many areas of impact, including three highly successful spin-out companies, along with awards for excellence in knowledge transfer, and for teaching.,Prof. Buchanan was awarded an "Outstanding Contribution to Knowledge Exchange" award and an OBE. He is a Fellow of BCS.

Authorized licensed use limited to: Edinburgh Napier University. Downloaded on June 26,2024 at 01:31:46 UTC from IEEE Xplore. Restrictions apply.
© 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.