# A Geometric transformation applied to Quantum Cryptography

Sadia Yasmeen[1] and Muhammad Hashim[2]

[1]Preston University Kohat, Islamabad Campus, H-8, Islamabad, Pakistan,

[2]Comsats University, Islamabad, Pakistan

*Corresponding author

E-mail address: sadia.yasmeen1995@gmail.com

## Abstract

Quantum cryptography leverages the principles of quantum mechanics to provide unprecedented security in communication systems. A novel approach to enhancing the robustness and efficiency of quantum cryptographic protocols involves the application of geometric transformations. This paper explores the integration of geometric transformations, specifically unitary transformations, into the quantum key distribution (QKD) process. By employing such transformations, we aim to optimize the manipulation of quantum states, thereby improving the resilience of cryptographic keys against potential eavesdropping attacks. The study investigates the theoretical framework of applying geometric transformations to quantum states, demonstrating how they can be used to encode, transmit, and decode quantum information with heightened security. Simulation results indicate that these transformations can significantly increase the fidelity of transmitted quantum states, reduce error rates, and bolster the overall security of quantum communication channels. This work lays the foundation for further exploration of geometric methods in quantum cryptography, potentially leading to more secure and efficient quantum communication systems.

The goal of this paper is to apply the ideas of quantum dynamics to cryptography, potentially leading to quantum cryptography. We developed a novel encryption system based on quantum rotation and spinning operators for digital data. In this straightforward exercise, we create a matrix using a two-dimensional rotation matrix with real entries. The rotation matrix is further integrated into the sizeable matrix needed for image encryption. In addition to a rotation matrix of the necessary size and rotation angle, the benchmark images are used for encryption. The analysis and results are shown.

## 1.0 Introduction

Huge amounts of data are being sent over unreliable communication lines thanks to the development of fast computing machines. Large databases are now used to store and manage the information of all social media servers, banks, military institutions, and other private sectors. Any organization suffers significant harm when information is shared via digital media. The world of today faces a great deal of challenges as a result of the widespread use of digital technology. Thus, one of the inevitable problems now is the security and confidentiality of digital contents. The modern world is essentially a continuous digital image era.

These digital materials are very important to us. Because digital images require high computational efficiency, their precise properties, such as redundancy and resilient connections between adjacent pixels, make it difficult for outdated conventional encryption algorithms to handle real-time enciphering. Various methods have emerged in the literature to safeguard these digital images. Certain methods employ chaos theory to create comprehensive encryption schemes that include diffusion and confusion across multiple rounds [27,46]. Additionally, some researchers created novel and inventive techniques to build a nonlinear component of block ciphers, which is undoubtedly the cause of any block cipher's confusion [14–16].

Classical cryptographic algorithms face a serious threat from the emerging concept of quantum computers. The basic idea behind quantum computing is the transformation of input information states, represented by a linear combination of various related inputs, into outputs that conform to various related outputs. A circuit made up of quantum gates that operate on qubits is analogous to a quantum scheme [5–18].

There have been physical demonstrations of the qui-bits and the associated entryways in [24, 26]. Currently, quantum computation is linked to many areas of science and innovation, including computational geometry, quantum games, image processing, and pattern recognition. The potential quantum computers will use mechanical properties like superposition and entanglement to weaken the conventional cryptosystem from the ground up. Given quantum physical properties like the Heisenberg vulnerability and the no cloning hypothesis, quantum cryptography schemes have been thought to be helpful in mitigating the worst aspects of traditional cryptosystems [39–43].

Since quantum computers are based on quantum information theory, brute force attacks can be carried out on them with relative ease thanks to technological advancements in the modern computer world. This vulnerability presents a risk to the ideal security needed for both protected innovation and national security. Using the fundamental and consistent principles of quantum mechanics, quantum cryptography provides an alternative to depending on the complex nature of factoring large numbers. It is predicated on the photon polarization and the Heisenberg uncertainty standard, two fundamental ideas in theoretical physics. It illustrates the various ways in which light photons can become enraptured. A captivated photon can only be distinguished by a photon channel with the appropriate polarization.

A single photon's path combined with the Heisenberg uncertainty principle, which gave rise to quantum cryptography, offers an enticing substitute for ensuring security and defeating spies [35–48]. Few particles have half inner angular momentum, also known as spin, such as electrons, quarks, and neutrinos. In order to provide additional insight into cryptography, we develop a spinner portrayal for half spin in this paper using spinning operators of quantum dynamics. The half spinning operator serves two purposes: first, it encrypts the keys; second, it can be used to encode digital images through the use of this innovative mechanism. Phase data is the key component of our scheme; we use it to encode and decode the picture parameters.

We can use different stages for keys and messages to achieve the highest level of security. In order to unscramble the message, we must first use stage data to decode the keys, and then we must use the message's stage data along with the keys to unscramble the message. Again, if someone were to take one of the variables—keys, the duration of the keys, or the message—he should not be able to decipher the message without being aware of the other components.

## 1.1 Mathematical expression for rotation operators

You can find the detailed derivations of spinning and rotation in [11–41]. The following mathematical expression for rotation operators will be useful when creating an image encryption technique:

$$R_a(\gamma) = e^{i\frac{\gamma}{2}\sigma_a} = \begin{bmatrix} \sum\limits_{m=0,2,4..}^{\infty} \frac{\left(i\frac{\gamma}{2}\right)^m}{m!} & \sum\limits_{m=1,3,5..}^{\infty} \frac{\left(i\frac{\gamma}{2}\right)^m}{m!} \\ \sum\limits_{m=1,3,5..}^{\infty} \frac{\left(i\frac{\gamma}{2}\right)^m}{m!} & \sum\limits_{m=0,2,4..}^{\infty} \frac{\left(i\frac{\gamma}{2}\right)^m}{m!} \end{bmatrix} = \begin{pmatrix} \cos\frac{\gamma}{2} & i\sin\frac{\gamma}{2} \\ i\sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix} \quad (1)$$

$$R_b(\gamma) = e^{i\frac{\gamma}{2}\sigma_b} = \begin{bmatrix} \sum\limits_{m=0,2,4..}^{\infty} \frac{\left(i\frac{\gamma}{2}\right)^m}{m!} & -i\sum\limits_{m=1,3,5..}^{\infty} \frac{\left(i\frac{\gamma}{2}\right)^m}{m!} \\ i\sum\limits_{m=1,3,5..}^{\infty} \frac{\left(i\frac{\gamma}{2}\right)^m}{m!} & \sum\limits_{m=0,2,4..}^{\infty} \frac{\left(i\frac{\gamma}{2}\right)^m}{m!} \end{bmatrix} = \begin{pmatrix} \cos\frac{\gamma}{2} & \sin\frac{\gamma}{2} \\ -\sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix} \quad (2)$$

$$R_c(\gamma) = e^{i\frac{\gamma}{2}\sigma_c} = \begin{bmatrix} \sum\limits_{m=0}^{\infty} \frac{\left(i\frac{\gamma}{2}\right)^m}{m!} & 0 \\ 0 & \sum\limits_{m=0}^{\infty} \frac{\left(-i\frac{\gamma}{2}\right)^m}{m!} \end{bmatrix} = \begin{pmatrix} e^{i\frac{\gamma}{2}} & 0 \\ 0 & e^{i\frac{\gamma}{2}} \end{pmatrix} \quad (3)$$

## 1.2 Proposed Image Encryption Scheme

For encryption purposes, defining parameter to be used in rotation matrices followed by a global matrix,

$$a=\begin{pmatrix}1&0\\0&1\end{pmatrix}=I \qquad b=\begin{pmatrix}\cos\frac{\gamma}{2}&\sin\frac{\gamma}{2}\\ \sin\frac{\gamma}{2}&\cos\frac{\gamma}{2}\end{pmatrix}=R_a(\gamma)$$

$$c=\begin{pmatrix}\cos\frac{\gamma}{2}&\sin\frac{\gamma}{2}\\ -\sin\frac{\gamma}{2}&\cos\frac{\gamma}{2}\end{pmatrix}=R_b(\gamma) \qquad d=\begin{pmatrix}e^{\frac{\gamma}{2}}&0\\0&e^{-\frac{\gamma}{2}}\end{pmatrix}=R_c(\gamma)$$

(4)

$$M=\left\{\begin{matrix}M_i\in M_{4\times4}\big(I,R_a(\gamma),R_b(\gamma),R_c(\gamma)\big)\,|\,A_i\in\sigma_i(A_i),\\ \sigma_i\in S_4,\ i=1,2,\dots,24\ and\\ \\ A_i\in M_{2\times2}(I,R_a(\gamma),R_b(\gamma),R_c(\gamma)\end{matrix}\right\}$$

(5)

We get 24 matrices $M=\{M_1,M_2,M_3,\dots,M_{24}\}$. The image encryption scheme is defined as follows,

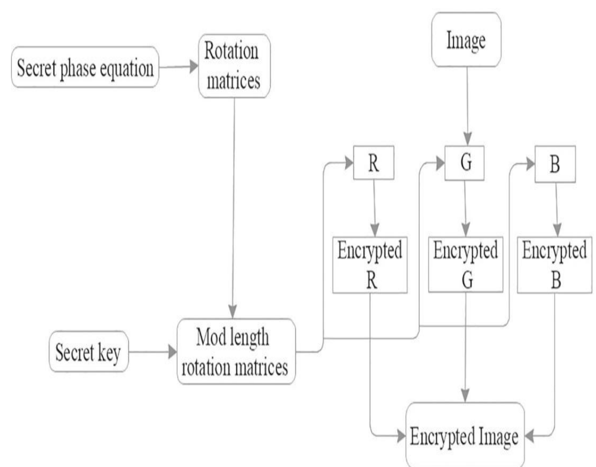



**Fig.1. Flow chart for Image encryption**

### 1.2.1 Image Encryption

- After reading an image, convert each RGB layer to a 4×n order.
- Establish criteria for the encryption phase that the sender and recipient are aware of.
- To obtain matrices from the set of matrices, enter phase in Eq. (5).
- Choose key of any length $[a\ \ b\ \ c\ \ d\ \ \dots]$ under mod 24 and take it as regarding matrix / matrices from set $M$ of Eq. (5).
- Using the chosen rotational matrices, encrypt every layer of the digital image.
- Convert the encrypted layers' dimensions back to their original size.
- Combine all the encrypted layers to form an encrypted image in RGB.
- We can also choose the following criteria for encrypting the key: Assume that the key digits are odd.

Then, compute what this equals, convert to binary, and see if the last bit is 0. If not, select the matrix to encrypt the key. If not, select the matrix to encrypt the key. If the key digits are even, calculate the value, which in this case is c. Then, convert c to binary and see if the last bit is 0. If not, choose matrices related to encrypting the key.

### 1.2.2 Image Decryption

- Read an RGB-encrypted image and convert it to an ordered format.
- Extract the RGB layers from encrypted Image.
- Calculate the phase decided by equation and put in set $M$ of Eq. (5).
- Next, take the corresponding matrix or matrices from set M and find their inverse. Extract the original keys from the encrypted keys.
- Decrypt each layer with inverse matrix/ matrices.
- Modify the layer dimensions as they are received in encrypted format.
- Combine all the layers to form an image as was in original.

## 1.3 Experimentation of Proposed Algorithm

The suggested algorithm is used to encrypt the 512x512 image of "Lena" and "Fruits," after which different analyses are carried out (Fig. 2a, 2b).

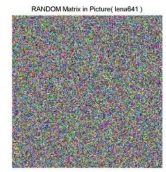
Choose the image of 'Lena' and 'Fruits' extract its RGB layers and perform analysis.

Select the secret equation to choose the phase at both sides as:

$$y = 330x(2^M - 1) mod 720, where\ M \in [1,24] and\ \gamma = mean(y) \qquad (6)$$

By using this equation, take $\gamma$ = 382.5, as the described algorithm refers symmetric cryptography. Therefore, we select different matrices from set M based on the modulus operations are: $14 \bmod 24 = A_{14}$ $29 \bmod 24 = A_5$ , $59 \bmod 24 = A_{11}$ . Now transform the matrices $A_{14}, A_5, A_{11}$ regarding dimension of key by appending zeros and apply calculated phase. The image encryption with given key as follow (see Table 1).

Fig .(2a, 2b). Target Images of Lena and Fruits



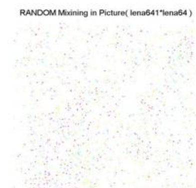




**Fig. (3a, 3b). Encrypted Images of Lena and Fruits**

## 1.4 Performance Analysis of Proposed Algorithm

In order to verify the security and functionality of the recommended encryption algorithm, we have carried out a few tests on common digital photos. These measures include an irregularity test for the encrypted images, a factual examination, and a sensibility investigation. The corresponding subsections provide a detailed discussion of each of these measures.

### 1.4.1 Randomness Test for Cipher

A few characteristics, such as long duration, uniform distribution, high intricacy, and productivity, are necessary for the security of a cryptosystem. We tested the haphazardness of digital images using NIST SP 800-22 with the specific aim of meeting these requirements. Some of these tests consist of different subsets. To complete all NIST tests, a 24-bit scrambled digital image of Lena is used. Many beginning keys are used in order to test the figure haphazardness. Table 2 displays the test results' aftereffects. By dissecting these results, we can determine that our predicted method for digital picture encryption successfully passes the NIST tests. As a result, given the achieved results, it can be said that the random ciphers generated by our encryption algorithm have highly irregular outputs.

| **Key** | **Key Matrices** | **Cipher Images** | |
|---|---|---|---|
| $1 \bmod 24 = 1$ | $M_1$ | $C_1$ | $M_1$ x $(I_R, I_G, I_B$ |
| $3 \bmod 24 = 3$ | $M_3$ | $C_2$ | $M_3$ x $C_1$ |
| $7 \bmod 24 = 7$ | $M_7$ | $C_3$ | $M_7$ x $C_2$ |
| | | | |
| $14 \bmod 24 = 1$ | $M_{14}$ | $C_4$ | $M_{14}$ x $C_3$ |
| $29 \bmod 24 = 5$ | $M_5$ | $C_4$ | $M_5$ x $C_4$ |
| $59 \bmod 24 = 1$ | $M_{11}$ | $C_5$ | $M_{11}$ x $C_5$ |

**Table 1. Key matrices for image encryption by using rotation and spinning operators**

## 1.5 Uniformity of Pixels

Histograms uniformity of enciphered contents is one of the most notable features for assessing the security of digital content encryption frameworks [26]. We've taken

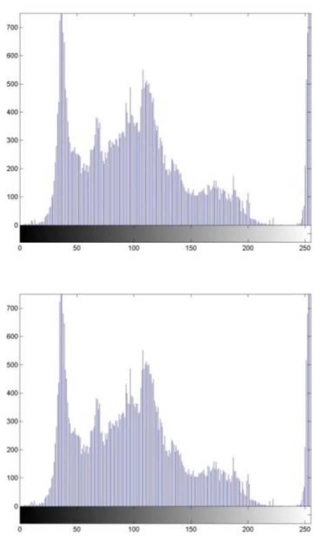
| **Test** | | **P-values for color encryption of encrypted images** | **Results** |
|---|---|---|---|
| | | **Red Green Blue** | Pass |
| Frequency | | 0.16410 0.46703 0.25495 | Pass |
| Block frequency | | 0.64862 0.53145 0.17899 | Pass |
| Rank | | 0.29191 0.29191 0.29191 | Pass |
| Runs $(M = 10{,}000)$ | | 0.21762 0.90595 0.54043 | Pass |
| Long runs of ones | | 0.67514 0.71270 0.71270 | Pass |
| Overlapping templates | | 0.85988 0.85988 0.85988 | Pass |
| No overlapping templates | | 0.92285 0.54825 0.99989 | Pass |
| Spectral DFT | | 0.88464 0.38399 0.029523 | Pass |
| Approximate entropy | | 0.16074 0.33744 0.69469 | Pass |
| Universal | | 0.99445 0.99292 | Pass |

| | | | |
|---|---|---|---|
| | | 0.99659 | |
| Serial | P values 1 | 0.17143 0.039989 0.65972 | Pass |
| Serial | P values 2 | 0.87464 0.006063 0.98104 | Pass |
| Cumulative sums forward | | 0.3647 0.34767 0.35256 | Pass |
| Cumulative sums reverse | | 0.35221 0.89099 0.77967 | Pass |
| Random excursions | $X=-4$ | 0.57183 0.0001427 0.97465 | Pass |
| | $X=-3$ | 0.15716 0.40359 0.95603 | Pass |
| | $X=-2$ | 0.099872 0.54469 0.89146 | Pass |
| | $X=-1$ | 0.29907 0.47837 0.88326 | Pass |
| | $X=1$ | 0.0037788 0.75769 0.85692 | Pass |
| | $X=2$ | 0.0027926 0.43307 0.082712 | Pass |
| | $X=3$ | 0.10337 0.67278 0.68683 | Pass |
| | $X=4$ | 0.2619 0.66907 0.1332 | Pass |
| Random excursions variants | $X=-5$ | 0.4330 0.45637 0.53288 | Pass |
| | $X=-4$ | 0.48074 0.90043 0.47950 | Pass |
| | $X=-3$ | 0.4907 0.081938 0.402778 | Pass |
| | $X=-2$ | 0.57415 0.035518 0.28009 | Pass |
| | $X=-1$ | 0.29168 0.21445 0.18145 | Pass |
| | $X=1$ | 0.00066 0.24660 0.78927 | Pass |
| | $X=2$ | 0.001451 0.47354 0.87737 | Pass |
| | $X=3$ | 0.01364 0.31764 0.90486 | Pass |
| | $X=4$ | 0.039974 0.15018 0.91954 | Pass |

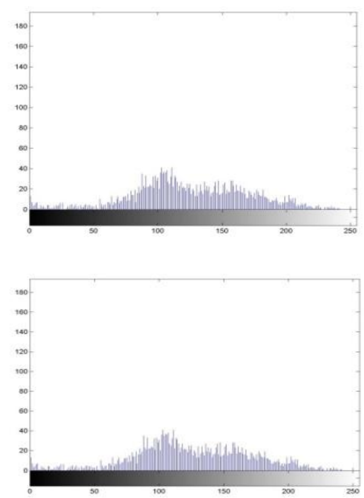
| | | | |
|---|---|---|---|
| | $X = 5$ | 0.065987 0.19477 0.47603 | Pass |

**Table 2. NIST test results for encrypted image**

Three 512x512, dark-level digital images with different substances are computed, along with their histograms. Regarding Figs. (3a, 3b), all of the encipher images' histograms under the projected scheme are genuinely uniform and fundamentally different from the original image, which makes measurable assaults problematic. The plain-picture histograms feature extensive, sharp ascents followed by sharp decreases. Consequently, it provides no information that could be applied to a quantifiable analysis attack against the encrypted image (refer to Figs. 4a, 4b).



**Figs. (3a, 3b). Histograms of original Images Lena and Fruits**



**Figs. (4a, 4b). Histograms of Encrypted Images Lena and Fruits**

## 1.6 Pixels Correlation Test

It is noteworthy that adjacent pixels in the image have a strong association in the horizontal, vertical, or corner-to-corner directions. Therefore, in order to strengthen the barrier against quantifiable investigation, the protected encrypted plan should remove this relationship. The accompanying method was finished in order to test the relationship between neighboring pixels in a plain and encrypted image. In the beginning, 10,000 pairs of adjacent pixels from the plain and encrypted images were selected at random [38, 39]. At that point, each combine pair's correlation coefficients were determined using the accompanying mathematical expression:

$$r_{x,y} = \frac{\sigma_{x,y}}{\sqrt{\sigma_x^2 \sigma_y^2}}$$

where $x$ and $y$ are values of two adjacent pixels at gray scale in the image, $\sigma_{x,y}$ is the covariance, $\sigma_x^2$ and $\sigma_y^2$ are variances of random variable $x$ and $y$ respectively. The correlation coefficients of plain and cipher images have different contents conveyed in Tables 3 and 4 related to plain and cipher images given in Figs (2a, 2b, 3a, 3b). Moreover, the quantitative analysis for correlation coefficient is discussed in Table 3, which shows the correlation distribution of original and encrypted images in horizontal, vertical and diagonal directions.

| Standard images | Plain | | | Encrypted (proposed scheme) | | | Ref |
|---|---|---|---|---|---|---|---|
| | Horizontal | Vertical | Diagonal | Horizontal | Vertical | Diagonal | Horizontal Vertical Diagonal |
| Lena | 0.9740 | 0.9868 | 0.9612 | -0.0113 | -0.0093 | 0.0027 | 0.041 0.0107 0.0097 |
| Fruits | 0.9753 | 0.9757 | 0.9567 | -0.0129 | -0.0155 | 0.0012 | - - - |
| Parrot | 0.9566 | 0.9434 | 0.9260 | -0.0108 | -0.0141 | 0.0054 | - - - |

**Table 3. Correlation coefficients of plain cipher images**

### 1.6.1 Correlation Between Original and Encrypted Images

.By calculating the 2D coefficients of correlation between original and encrypted images, the correlation between numerous pairs of original/encrypted images is examined here [28]. The correlation coefficients are computed using the following equation.

$$r = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{ij}-\bar{X}\right)\left(Y_{ij}-\bar{Y}\right)}{\sqrt{\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{ij}-\bar{X}\right)^2\right)\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\left(Y_{ij}-\bar{Y}\right)^2\right)}}$$

where X and Y represents the plain and cipher image,

$\bar{X}$ and $\bar{Y}$ are the mean values of $X$ and $Y$ , $M$ is the he correlation coefficients among various pairs of plain and cipher images are very small or practically zero, therefore the plain and cipher images are significantly different. Additionally, the evaluation of the correlation coefficient of anticipated process with modern approaches using Lena image given in Table 4. The results of our offered scheme have lower values of correlation coefficient which qualify for an efficient technique for image enciphering in real time applications.

| | Correlation directions | | |
|---|---|---|---|
| | Horizontal | Vertical | Diagonal |
| Plain image | 0.9740 | 0.9868 | 0.9612 |
| Proposed encryption | -0.0113 | -0.0093 | 0.00270 |
| scheme | | | |
| Ref. | 0.01089 | 0.01811 | 0.00610 |
| Zhang et. Al | 0.08200 | 0.04000 | 0.00500 |
| Zhou et al | 0.012 | 0.02700 | 0.00700 |
| Ref | 0.01589 | 0.06538 | 0.03231 |
| Mao et. Al | 0.04500 | 0.02800 | 0.02100 |
| Etimadi et. Al | 0.005 | 0.01100 | 0.02300 |

**Table 4. Comparison of the correlation coefficient of proposed scheme with recent techniques using Lena image**

## 1.7 Pixel Difference Analysis

By computing the PSNR and MSE values, the pixel difference method-based image quality assessment has been completed. These error metrics are employed in the comparison of various images.

### 1.7.1 MSE and PSNR Analysis

A digital image that has been jumbled up should not be exactly the same as the original. To gauge the degree of enciphering, we calculate the mean square error (MSE) between the unencrypted and encrypted images. MSE can be described as follows:

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(P_{ij} - C_{ij}\right)^2}{M \text{ x } N}$$

where $P_{ij}$ and $C_{ij}$ allude to pixels situated at $i^{th}$ row and $j^{th}$ column of unique digital and scram- bled image separately. Larger the MSE esteem, better the encryption security. The encrypted image quality is assessed utilizing PSNR (peak signal to noise ratio) which is depicted by the following expression.

$$PSNR = 20\log_{10}\left[\frac{I_{\max}}{\sqrt{MSE}}\right]$$

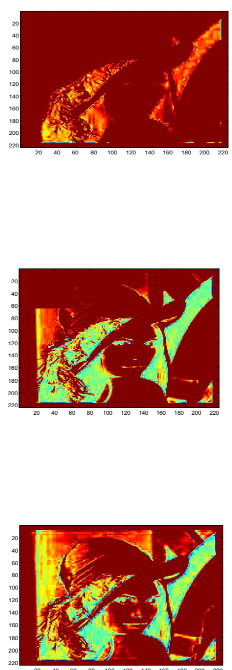
where $I_{max}$ is the greatest pixel estimation of image. The PSNR ought to be low esteem when compares to the immense distinction between plain and ciphered image. The viability of pro- posed strategy, assessed as far as MSE and PSNR for every one of the three digital images, is presented in Table 5.

| **Images** | **Encrypted (proposed scheme)** | |
|---|---|---|
| | MSE | PSNR |
| Lena | 4859.03 | 11.30 |
| Fruits | 6399.05 | 10.10 |
| Parrot | 7274.44 | 9.55 |

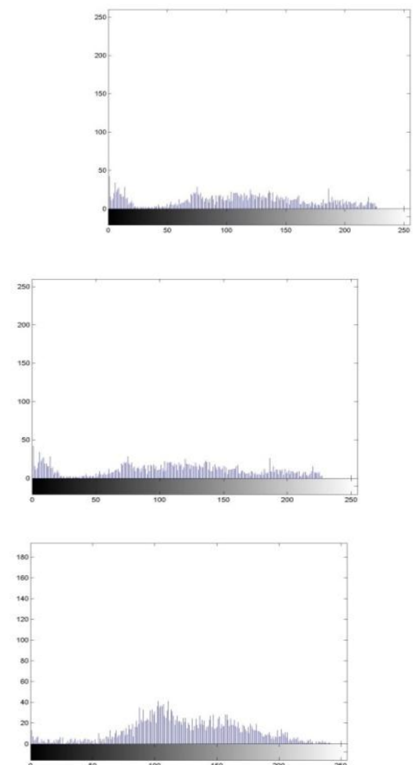
**Table 5. pixel difference based measures of proposed scheme**

## 1.8 Three Dimensional Color intensity of Plain and Encrypted Images

The RGB color coordinates' intensity determines how each pixel looks. The amount of data that is stored in a pixel determines the color depth. Bit depth is another name for color depth, which regulates pixel colors. Here, we display the total number of pixels that correspond to the image's intensity level (see Figs. (5a, 5b, 5c, 6a, 6b, and 6c)). The 3D color intensities in encrypted images are fairly uniform, resulting in a flat plan in RGB coordinates, in contrast to the sharp peaks that make up the 3D histograms for plain images. These three-dimensional figures indicate that our expected image encryption scheme is quite strong and that an eavesdropper would not be able to access or estimate any information from the uniform distribution of encrypted image pixels.



**Figs. (5a, 5b, 5c). RGB Images of Lena**



**Figs. (6a, 6b, 6c). Histograms of RGB Images of Lena**

## 1.9 Entropy Investigation

Entropy is the most leading feature of randomness [2, 17, 36]. Specified a source of independent random events from set of possible discrete events $\{y_1, y_2, . . ., y_i\}$ with associated probabilities $\{p(y_1), p(y_2), . . ., p(y_i)\}$, the average per source output information called entropy of source.

The $y_i$ in this condition is called source images and 2N is the aggregate conditions of data. For absolutely irregular source emanating 2N signs, entropy ought to be N.

For perfectly indiscriminate digital content, the estimation of ideal data entropy is 8. Various plain and cipher images entropies accounted in Table 6 as indicated by the original images of Figs. (2a, 2b).

| | | Color component of plain image | | | | Color component of encrypted image |
|---|---|---|---|---|---|---|
| **Image** | **Plain Image** | **Red** | **Green** | **Blue** | **Encrypted image** | **Red Green Blue** |
| Lena | 7.7502 | 7.2633 | 7.5909 | 6.9798 | 7.9988 | 7.9977 7.9978 7.9978 |
| Fruits | 7.6868 | 7.1466 | 7.4330 | 7.7588 | 7.9984 | 7.9980 7.9980 7.9979 |
| Parrot | 7.1412 | 7.1803 | 7.7031 | 5.9653 | 7.9998 | 7.9981 7.9975 7.9976 |

**Table 6. Information entropies of original and encrypted images**

These entropy esteems are near the hypothetical esteem 8. This implies data leakage in encryption procedure is irrelevant and the mechanism is protected upon entropy attacks. We have compared information entropy of our suggested encryption technique with already developed schemes. The entropy of the proposed scheme for encrypted Lena image is superior to existing algorithm on comparing; see Table 7 [44].

| Algorithm | Entropy |
|---|---|
| Proposed | 7.9988 |
| Sun's algorithm | 7.9965 |
| Baptista's algorithm | 7.9260 |
| Wong's algorithm | 7.9690 |
| Xiang's algorithm | 7.9950 |

**Table 7. Comparison results for information entropies of Lena image of size 512 x 512**

## 1.10 Robustness against differential attack

We need to modify the digital plain image (for example, one pixel) in order to strengthen our image encryption technique against differential attack. This modification affects the entire comparing encrypted image, with a possibility of a half pixel changing. We show that our scheme is sufficiently affectable to a plain image. A modification in the ith block of a permuted digital image directly affects the ith block of an encrypted image. In any case, the modification has little effect on the previously jumbled blocks, negates its effect gradually, and gradually disappears in the subsequent blocks. Due to the fact that the ith block only affects one pixel of the (i+1)th block, or Di+1, it does not immediately affect the subsequent blocks. The number of pixels change rate (NPCR) is coupled with the mean absolute error (MAE) and UACI (unified average intensity) in order to determine the impact of a small variation in the digital plain contents on its encrypted. The MAE is defined as follows: let C(i, j) and P(i, j) be the gray level pixels at the ith row and jth column of M×N plain and cipher images, respectively:

$$MAE = \frac{\sum_{i,j} \left| C(i,j) - P(i,j) \right|}{M \text{ x } N}.$$

increased the MAE esteem, which improved the encryption security. NPCR and UACI are the two fundamental measures that can be used to testify the impact of changing a single pixel in a plain image and an encrypted image overall with the proposed scheme. We examine two encoded images with a single pixel difference in their source image. The following mathematical expressions can be used to determine the NPCR and UACI if the first image is represented as C1 (i, j) and the second image as C2 (i, j).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \text{ x } H} \text{ x } 100\%$$

where

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases}$$

$$UACI = \frac{1}{W \text{ x } H} \sum_{i=0}^{M-1} \sum_{jj=0}^{N-1} \left| \frac{C_1(i,j) - C_2(i,j)}{255} \right| \text{ x } 100\%$$

| **Standard images** | **NPCR** | | | **UACI** | | | **MAE** |
|---|---|---|---|---|---|---|---|
| | Max | Min | Mean | Max | Min | Mean | |
| Lena | 99.997 | 99.612 | 99.713 | 34.43 | 33.21 | 33.87 | 79.22 |
| Fruits | 99.994 | 99.515 | 99.698 | 33.98 | 33.98 | 33.71 | 83.45 |
| Parrot | 99.998 | 99.597 | 99.869 | 33.53 | 33.11 | 33.24 | 75.3 |

**Table. 8. The estimate of sensitivity analysis of proposed image encryption scheme**

The higher the UACI value, the better the encryption security. To assess the plain image sensitivity, the plain image is first encrypted. After that, a single pixel is arbitrarily chosen and altered in the plain image. The experimental results of our proposed scheme are presented in Tables 8–10, with the MAE values displayed in the final column of Tables 8 and 9.

The sources of MAE, MPCCR, and UACI across different plans are examined in Tables 8–10. It shows that the UACI esteem is greater than 34% and that the NPCR esteems are consistently equal to the ideal estimate of 1. This result demonstrates that the expected scheme is highly sensitive to even small changes in the original image; for example, even if there is a 1-bit difference between the two scrambled plain images, the two unscrambled enciphered images differ significantly from one another. As such, when compared to alternative schemes, the projected design has a higher ability to withstand differential attacks. The described algorithm's magnificence and flexibility allow it to modify the cipher image at any time, and its encrypted image cannot be decrypted using only one matrix and one phase. Phase θ and the two matrices should be known in order to decode the encrypted image. Since θ has large foci, an enciphered image would change with even a slight shift in stage, such as 0.01. Additionally, we have contrasted our NPCR and UACI results with some previously published, well-known results [2–6]. The suggested scheme is highly resistant to both linear and differential attacks, and it closely aligns with the findings in the references [42–45].

## Conclusion

We developed a novel encryption method based on quantum rotation operators in this research article. We have added confusion and diffusion capabilities to our proposed schemes by utilizing the quantum half spinning. To confuse cryptanalysts, we could compress or expand the key by simply multiplying it with any nonsingular matrix of [4×n] that is known to both the sender and the recipient. Since no one knows which matrices from set M are being multiplied—two or more—cryptanalysts will have a difficult time deciphering the key and message (a challenge for crackers).Since the algorithm being described deals with half spinning, there are an infinite number of points between -720˚ and +720^, and there are four possible combinations of rotation matrices. It is suggested that the suggested algorithm is a strong contender for picture encryption by employing statistical analysis for our expected algorithm.

| | **NPCR** | | | **UACI** | | | **MAE** | | |
|---|---|---|---|---|---|---|---|---|---|
| **Test Image** | **Red** | **Green** | **Blue** | **Red** | **Green** | **Blue** | **Red** | **Green** | **Blue** |
| Lena | 99.88 | 99.73 | 99.79 | 33.33 | 33.88 | 32.78 | 82.78 | 77.88 | 81.78 |
| Fruits | 99.67 | 99.89 | 99.65 | 33.04 | 33.21 | 76.36 | 76.36 | 86.34 | 88.98 |
| Parrot | 99.82 | 99.91 | 99.87 | 33.16 | 33.45 | 79.87 | 79.87 | 65.23 | 69.88 |

**Table . 9. The assessment of sensitivity analysis for color components.**

## References


[1]. Abal G., Donangelo R., Fort H.: Conditional strategies in iterated quantum games. Physica A 387, 5326–5332 (2008).

[2]. Barenco A., Bennett C.H., Cleve R., DiVincenzo D.P., Margolus N., Shor P.W., Sleator T., Smolin J.A., Weinfurter H. Elementary gates for quantum computation. Phys. Rev. Part A 52, 3457 (1995).

[3]. Borujeni S.E.; Eshghi M. Chaotic image encryption design using tompkins-paige algorithm. Hindawi Publishing Corporation Mathematical Problem in Engineering vol. 200, p. 22 (2009).

[4]. Chandra Sekhar A., Prasad Reddy P.V.G.D, Murthy A.S.N., Krishna Gandhi B., Self-Encrypting Data Streams Using Graph Structures, IETECH Journal of Advanced Computations, 2(1) (2008) 2007–2009.

[5]. Deutsch D.: Quantum theory, the Church-Turing principle and the universal quantum computer, Proc. R. Soc. London A( 400), 97–117 (1985).

[6]. Enayatifar R, Abdullah AH, Isnin IF, Altameem A, Lee, Image encryption using a synchronous permutation-diffusion technique. Opt Lasers Engg. 90:146–154 (2017).

[7]. Gao H.; Zhang Y.; Liang S.; Li D.: A new chaotic algorithm for image encryption. Chaos Solitons Frac- tals 29(2), 393–399 (2006).

[8]. Hamza R, Titouna F, A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. Inf. Secur J Global Perspective 25:162–179 (2016).

[9]. J. Aditya, P. Shankar Rao. Quantum Cryptography, https://cs.stanford.edu/people/adityaj/ QuantumCryptography.pdf.

[10]. Jim Branson 2013-04-22, Quantum physics, derive the expression for rotation

operator.

[11]. Jim Branson 2013-04-22, Quantum Physics, Spin (1/2) and Derive Spin (1/2) Rotation Matrices and operators.

[12]. Khan Majid, An image encryption by using Fourier series. Journal of Vibration and

Control, 21 (2015) 3450–3455.

[13]. Khan Majid, Shah Tariq, An efficient chaotic image encryption scheme, Neural

Comput. & Application, 26 (2015) 1137–1148.

[14]. Khan Majid, Shah Tariq, Construction and applications of chaotic S-boxes in image encryption, Neural Comput. & Application, 27 (2016) 677–685.

[15]. Khan Majid, Shah Tariq, A novel image encryption technique based on Henon chaotic map and S8 symmetric group, Neural Comput. & Application, 25 (2014) 1717–1722.

[16]. Khan Majid, Tariq Shah and Syeda Iram Batool, Texture analysis of chaotic coupled map lattices based image encryption algorithm, 3D Research, 15(3) (2015) 1–5.

[17]. Lanzagorta M.,Uhlmann J. Quantum algorithmic methods for computational geometry. Math. Struct. Comput. Sci. 20(6), 1117–1125 (2010).

[18]. Le P.Q., Iliyasu A.M., Dong F., Hirota K. Efficient color transformations on quantum images.

J. Adv. Comput. Intell. Inform. 15(10), 698–706 (2011).

[19]. Liboff Richard, Introductory Quantum Mechanics, IV Edition, Addison Wesley, 2002.

[20]. Linhua Z; Liao X.; Wang X.: An image encryption approach based on chaotic maps. Chaos Solitons Fractals 24(3), 759–765 (2005).

[21]. Majid Khan A novel image encryption scheme based on multi-parameters chaotic S-boxes, Nonlinear Dynamics, 82 (2015) 527–533.

[22]. Man P.P.: Wigner active and passive rotation matrices applied to NMR tensor. Concepts Magn. Reson. Part A 45 A(1), 26 (2017).

[23]. Mao Y.; Chen G.; Lian S.: A novel fast image encryption scheme based on 3D chaotic bakermaps. Int. J. Bifurcation Chaos 14(10), 3613–3624 (2004).

[24]. Monz T., Kim K., Hansel W., Riebe M., Villar A.S., Schindler P., Chwalla M., Hennrich M., Blatt R.: Realization of the quantum Tofoligate with trapped ions. Phys. Rev. Let. 102, 040501 (2009).

[25]. Nicholas Wheeler, Spin matrices for arbitrary spin, http://www.reed.edu/physics/faculty/wheeler/ documents/Quantum%20Mechanics/ Miscellaneous%20Essays/Angular%20Momentum,%20Spin/D3.%20Spin%20Matrices.pdf.

[26]. Nielsen M.A., Chuang I.L.: Quantum Computation and Quantum Information.

Cambridge University Press, Cambridge (2000).

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

[28]. Planat Michel and Solse Patric, "Clifford groups of Quantum gates, BN-pairs and smooth cubic surfaces-Journal of Physics A: Mathematical and theoretical 19th December 2008.

[29]. Sakurai J., Modern Quantum Mechanics, Addidon Wesley, 1985.

[30]. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and

factoring. Proceedings of 35th Annual Symposium Foundations of 751

Computer Science, IEEE Computer Society. Press, Los Almitos, CA, 124 C134

(1994).

[31]. Sravan Kumar D., CH.Suneetha and A.Chandra Sekhar, Encryption of data

streams using Pauli spin ½ matrices, International Journal of Engineering

Science and Technology, 2(6) (2010) 2020–2028

[32]. Stakhov A.P., The golden matrices and a new kind of cryptography", Chaos, Solutions and Fractals 32 (2007) 1138–1146.

[33]. Sudha K.R., chandra Sekhar A., Prasad Reddy P.V.G.D. Cryptography Protection of Digital Signals using Some recurrence relations, International Journal of Computer Science and Network security, 7 (5) (2007) 203–207.

[34]. Tong XJ, Zhang M, Wang Z, Ma J, A joint color image encryption and compression scheme based on hyperchaotic system. Nonlinear Dyn. 84:2333–2356 (2016).

[35]. Trugenberger C.: Phase transitions in quantum pattern recognition. Phys. Rev. Lett. 89, 277903 (2002). https://doi.org/10.1103/PhysRevLett.89.277903 PMID: 12513243

[36]. Trugenberger C.: Probabilistic quantum memories. Phys. Rev. Lett. 87, 067901 (2001). https://doi.org/10.1103/PhysRevLett.87.067901 PMID: 11497863

[37]. Trugenberger C.: Quantum pattern recognition. Quantum Inf. Process. 1(6), 471–493 (2002).

[38]. Venegas-Andraca, S.E., Bose, S.: Storing, processing and retrieving an image using quantum mechanics. Proceedings of SPIE Conference Quantum Information and Computation, 5105, pp. 137–147 (2003)

[39]. Venegas-Andraca, S.E., Bose, S. Quantum computation and image processing: new trends in artificial intelligence. Proceedings of the International Conference on Artificial Intelligence, IJCAI-03, pp. 1563– 1564 (2003).

[40]. Wang X., Teng L., Qin X.: A novel colour image encryption algorithm based on chaos. Signal Process. 92, 1101–1108 (2012)

[41]. Waseem H.M. and Khan M., 2018. Information Confidentiality Using Quantum Spinning, Rotation and Finite State Machine. International Journal of Theoretical Physics, 57(11), pp.3584–3594.

[42]. Yang Bo, Liao Xiaofeng, A new color image encryption scheme based on logistic map over the finite field ZN, Multimed Tools Appl, https://doi.org/10.1007/s11042-017-5590-0.

[43]. Yang Y.G., Xia J., Jia X., Zhang H.: Novel image encryption/decryption based on quantum Fourier transform and double phase encoding. Quantum Inf. Process., pp. 1–17 (2013).

[44]. Zhang Guoji, Liu Qing, A novel image encryption method based on total shuffling scheme, Optics Communications 284 (2011) 2775–2780.

[45]. Zhang YS, Xiao D, Self-adaptive permutation and combined global diffusion for chaotic color image

encryption. AEU Int. J Electron Comm. 68:361–368 (2014).

[46]. Zhou N., Liu Ye: Novel qubit block encryption algorithm with hybrid keys. Physica A 375, 693–698 (2007).

[47]. Zhou Q.; WoWong K.; Liao X.; Xiang T.; Hu Y.: Parallel image encryption algorithm based on discretized chaotic map. Chaos Solitons Fractals 38(4), 1081–1092 (2008).

[48]. Zwiebach B.: Spin one-half, bras, kets and operators, MIT Physics Department (2013).