

Songklanakarin J. Sci. Technol. 44 (4), 1000–1007, Jul. – Aug. 2022



Original Article

Image encryption using quantum spinning and trigonometric chaotic map

Kawinbhat Sirikantisophon¹, Mahwish Bano^{2*}, and Thammarat Panityakul¹

¹ Division of Computational Science, Faculty of Science, Prince of Songkla University, Hat Yai, Songkhla, 90110 Thailand

² Department of Mathematics, Air University, Islamabad, 44000 Pakistan

Received: 27 August 2021; Revised: 17 February 2022; Accepted: 21 March 2022

Abstract

The Quantization Process is having a huge and effective influence a wide range of mechanics problems. The influence of quantization doesn't only eases mechanical problems but also enlarges the cybersecurity standards. Quantization and cryptography are two sorts of quantum processing that utilize the concept of qubits rather than bits. The thought of fast computations with quite one difficulty stage is more practical within the era of quantum information. The advancement of quantization processes has given rise to the science of utilizing quantum mechanical properties to hold out cryptographic norms within the field of cybersecurity. In the present paper, we attempt to utilize the concepts of quantization in image encryption which ends up in quantum cryptography. We plan a state-of-the-art image encryption scheme for digital data-supported quantum spinning and rotation matrices. As an easy practice, we use a matrix-supported two-dimension rotation matrix with real entries. This rotation matrix together with Trigonometric Chaotic Map (TCM) is implanted further into a desired sizeable matrix to implement for image encryption. The benchmark images are employed for encryption alongside a rotation matrix of the specified size and rotation angle. Results are displayed for analysis.

Keywords: phase equation, rotation operators, TCM, RGB images, encrypted images

1. Introduction

Transfer of huge data, financial transactions, secure defense-related messages, secure bank communications, and other public and private information are now freely possible on fast computing machines. The transfer of data and knowledge by any mode brings significant harm to any organization. The world of communication has enormous issues which have been tremendously reduced by the invention of fast computing machines and improvement in various applications. That is why the secrecy and confidentiality of digital information have become one of the foremost unavoidable matters within this world; it is a neighborhood of continuous computer images. These images

*Corresponding author Email address: mahwish@mail.au.edu.pk have a crucial role in our daily working environment. Computer images have properties like repetition and various connectivity in between neighboring cells. This property makes it crucial for the traditional crypto algorithms to manage the online enciphering, thanks to necessarily high computational efficiency. Various methods have been developed to store many of these computer images; a number of them use chaotic theory to rearrange full crypto schemes with images that comprise confusion/diffusion through TCM and matric manipulations (Bano, Saleem, Shah, Thammarat, & Ronnason, 2020; Bano, Shah, & Shah, 2016a, 2016b, 2017; Hamza, & Titouna, 2016; Orawit, Thammarat, & Bano, 2021; Tong, Zhang, & Wang, 2016). A large number of innovative schemes have been developed to deal with the nonlinear part of block ciphers for the confusion within the blocks. The concept of quantum computers has been much enhanced which may be undermined to plain crypto algorithms. The essential rule of quantum computers is to re-addressed the input information condition that may be done by a linear combination of varied related inputs to conforming various related outputs. Quantum schemes are almost a kind of a circuit consisting of quantum gates that perform on qubits (Barranco, Bennett, Cleve, DiVincenzo, Margolus, Shor, Sleator, Smolin, & Weinfurter, 1995; Deutsch, 1985; Iliyasu, Dong, & Hirota, 2011). The applications of qubits and their related schemes are widely discussed (Monz, Kim, Hansel, Riebe, Villar, Schindler, Chawalla, Hennrich, & Blatt, 2009; Nielsen, & Chuang, 2000). At times, a quantum calculation has been attached with various branches of science and innovation, for example image processing, pattern recognition, speech recognition, and quantum games. The quantum machines, weaken the traditional cryptosystem. This utilizes mechanical characteristics as an example of superposition and entanglement. Quantum cryptography plans are likely to be helpful to the sole downsides of the traditional cryptosystem. This has given quantum physical standards a bit like the no-cloning hypothesis and Heisenberg theoretic (Trugenberger, 2002a, 2002b; Venegas-Andrea, & Bose, 2003a, 2003b; Yang, Xia, Jia, & Zhang, 2013). Quantum computers due to scientific theory are friendly to brute force attacks, so it's easily predictable. This creates an enormous threat to the national security level. Cryptography provides major and fixes standards of physics. These machines are supported by the 2 simple rules of practical physics, the Heisenberg uncertainty standard and thus the photon polarization. The sunshine photons can have enraptured especially ways. A Photon channel with the right value of polarization is typically segregated as captivated photons, and the Heisenberg uncertainty principle guideline

gives rise to quantum cryptosystem. This is often a substitute to form sure security and overcome secret intruders (Branson, 2013a, 2013b; Man, 2017; Sravan, Suneetha, & Sekhar, 2010; Sudha, Sekhar, & Reddy, 2007; Waseem, & Khan, 2018). Particles like electrons, neutrinos, and quarks which have half inner momentum are called spin. In the present paper, we develop half-spin matrices to support cryptography by the utilization of rotational operators of quantum electrodynamics. The half-rotating matrices are often used for input keys encryption also for encoding the digital images. The encryption process would be retrieved by decoding the keys first followed by utilizing stage data then by making use of keys with stage data of the knowledge to revive the message. If anybody gets one among the variables (keys or period of keys or period of the message), he would not be able to restore the message without knowing other components. The remaining sections comprise the quantum rotation matrices and TCM, an algorithm for the encryption, an experimental model, security and performance analysis, and differential analysis intrusions followed by a conclusion.

2. Rotation Matrices for Quantization

The most important linear transformations on R^2 and R^3 are people who produce Reflections, Projections, and Rotations. An operator that rotates each vector in R^2 by an angle α is named a Rotation operator. A detailed functional differential within the sort of angular spinning is given in Sudha, Sekhar, and Reddy (2007). A simplified form for angular operators that helps design in image encryption is considered below.

$$R_{a}(\alpha) = e^{i\frac{\alpha}{2}\sigma_{a}} = \begin{pmatrix} \sum_{m=0,2,4,\dots}^{\infty} \frac{\left(i\frac{\alpha}{2}\right)^{m}}{m!} & \sum_{m=1,3,5,\dots}^{\infty} \frac{\left(i\frac{\alpha}{2}\right)^{m}}{m!} \\ \sum_{m=1,3,5,\dots}^{\infty} \frac{\left(i\frac{\alpha}{2}\right)^{m}}{m!} & \sum_{m=0,2,4,\dots}^{\infty} \frac{\left(i\frac{\alpha}{2}\right)^{m}}{m!} \end{pmatrix}^{m} = \begin{pmatrix} \cos\frac{\alpha}{2} & i\sin\frac{\alpha}{2} \\ i\sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} \end{pmatrix}$$
(1)
$$R_{b}(\alpha) = e^{i\frac{\alpha}{2}\sigma_{b}} = \begin{pmatrix} \sum_{m=0,2,4,\dots}^{\infty} \frac{\left(i\frac{\alpha}{2}\right)^{m}}{m!} & -i\sum_{m=1,3,5,\dots}^{\infty} \frac{\left(i\frac{\alpha}{2}\right)^{m}}{m!} \\ i\sum_{m=1,3,5,\dots}^{\infty} \frac{\left(i\frac{\alpha}{2}\right)^{m}}{m!} & \sum_{m=0,2,4,\dots}^{\infty} \frac{\left(i\frac{\alpha}{2}\right)^{m}}{m!} \end{pmatrix}^{m} = \begin{pmatrix} \cos\frac{\alpha}{2} & \sin\frac{\alpha}{2} \\ -\sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} \end{pmatrix}$$
(2)
$$R_{c}(\alpha) = e^{i\frac{\alpha}{2}\sigma_{c}} = \begin{pmatrix} \sum_{m=0}^{\infty} \frac{\left(i\frac{\alpha}{2}\right)^{m}}{m!} & 0 \\ 0 & \sum_{m=0}^{\infty} \frac{\left(-i\frac{\alpha}{2}\right)^{m}}{m!} \end{pmatrix}^{m} = \begin{pmatrix} e^{i\frac{\alpha}{2}} & 0 \\ 0 & e^{-i\frac{\alpha}{2}} \end{pmatrix}$$
(3)

3. Proposed Image Encryption Technique based on Rotation Operator

Consider the matrices a, b, c, d are the defining parameters to be utilized in rotation matrices followed by a global matrix for encryption purposes.

K. Sirikantisophon et al. / Songklanakarin J. Sci. Technol. 44 (4), 1000-1007, 2022

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

$$c = \begin{pmatrix} \cos \frac{\alpha}{2} & \sin \frac{\alpha}{2} \\ -\sin \frac{\alpha}{2} & \cos \frac{\alpha}{2} \end{pmatrix} = R_b(\alpha) \qquad d = \begin{pmatrix} e^{\frac{\alpha}{2}} & 0 \\ 0 & e^{-\frac{\alpha}{2}} \end{pmatrix} = R_c(\alpha).$$
(4)

$$M = \begin{cases} M_i \in M_{4x4}(I, R_a(\alpha), R_b(\alpha), R_c(\alpha) | A_i \in \sigma_i(A_i), \sigma_i \in S_4, i = 1, 2, ..., 24 \text{ and} \\ A_i \in M_{2x2}(I, R_a(\alpha), R_b(\alpha), R_c(\alpha)) \end{cases}$$
(5)

We obtained 24 matrices $M = \{M_1, M_2, M_3, ..., M_{24}\}.$

The flow chart for the image encryption technique is explained in Figure 1.



Figure 1. Flow chart for image encryption

3.1 Image encryption using fixed rotation matrices

- Consider a target image as layers, then convert these layers of the image (RGB) into a 4×n order array.
- Select the phase for encryption that is understood by both the sender and the receiver.
- To obtain sub-matrices *M_i* from the set of matrices, *M*, we substitute the chosen phase above into Equation 5 and apply TCM.
- Select a key of any length [s, t, u, v, ...] with modulus 24 and consider it a matrix from a series of *M* in Equation (5).
- Apply encryption algorithm to every row layer of the target image like selected rotational matrices.

- After encryption is applied, change the size of the matrix layers to the first.
- Collect all the matrix layers into a matrix then extended into an encrypted image in RGB.
- Prescribe criteria to encrypt the key to be used for global encryption is given in Tong, Zhang, and Wang (2016).

3.2 Decryption processing using inverse rotation matrices

Decryption may be a reverse process started by employing the encrypted image within the previous section.

- Get the RGB encrypted image from previous steps and transform it into a matrix of size order.

1002

- Convert the matrix into layers. Choose all colored layers from them.
- Evaluate the phase data using Equation (5) and place them in a worldwide setting.
- Original keys as used for encryption should be decrypted using inverse matrices from the worldwide series M. Each matrix must have its inverses.
- On using these inverse matrices, decrypt each layer array.
- Transform the array layer's dimensions because it had been received in an encrypted image.
- Combine these layers to form a matrix image because it had been within the first image.

4. Application of the proposed algorithm into target images

The suggested algorithm is successfully implemented to the target images of 'Lena' and 'Fruits' for dimension 512×512 and produced corresponding encrypted images as it was done in our previous papers (Bano, Saleem, Shah, Thammarat, & Ronnason, 2020; Bano, Shah, & Shah, 2016a, 2016b, 2017; Orawit, Thammarat, & Bano, 2021). Extended performance analyses are administered (Fig.2a, 2b). Performance analysis of RGB layers of such images is also carried out and reported. The key equation to settle on the phase at each side is selected as:

$$y = 330 \text{ x} (2^{M}-1) \text{mod } 720,$$

where $M \in [1, 24]$ and $\theta = mean(y).$ (6)

The symmetric cryptography algorithm can be obtained by taking $\theta = 380.5$ in the above equation. A class of modular operations applied on selective matrices from the series M are changed regarding the size of a key by merging zeros and using the calculated phase. The encryption with selective keys is given in (Table 1, and Figures 3a, 3b).

5. Efficiency of the Proposed Algorithm

To test the efficiency of the proposed algorithm for strength and security, a series of conventional tests have been performed over encrypted images which contain sensibility, irregularity, and actual experiment. These are described here.

5.1 Random test on cipher images

The efficacy of any algorithm to a prescribed cryptosystem must have several assertions, like productivity,

Table 1. Cipher images obtained using fixed spinning operators



Figure 2. Target images of the Lena and fruits



Figure 3. a, Encrypted images of the Lena and b, Random mixing in picture (Lena641*Lena64)

acute intricacy, and smooth distribution. To test these, we used the quality NIST test for randomness of digital images, just like the Lena. The results of these tests are obtained and presented in Table 2. It is observed, given the achieved results, that the ciphers in our encryption algorithm are often asserted to be very irregular in their output.

5.2 Smoothness of pixels

To test the smoothness of the digital images, we evaluated the histograms of both cipher and plain images as given in (Trugenberger, 2002) and reported in Table 2.

Key	Key Matrices	Cipher images		
$1 \mod 24 = 1$	M_1	C_1	$M_1 \ge (I_{\rm R}, I_{\rm G}, I_{\rm B})$	
$3 \mod 24 = 3$	M_3	C_2	$M_3 \ge C_1$	
$7 \mod 24 = 7$	M_7	C_3	$M_7 \ge C_2$	
$14 \mod 24 = 14$	M_{14}	C_4	$M_{14} \ge C_3$	
$29 \mod 24 = 5$	M_5	C_4	$M_5 \ge C_4$	
$59 \mod 24 = 11$	M_{11}	C_5	$M_{11} \ge C_5$	

1004 K. Sirikantisophon et al. / Songklanakarin J. Sci. Technol. 44 (4), 1000-1007, 2022

Table 2. NIST results for the encrypted image

Taat		P	-values of encrypted image	es	Deculto
Test	-	Red	Green	Blue	- Results
Frequency distribution The rank of the matrix Iterations ($M = 10,000$) Long iterations of ones Overlapping templates No overlapping templates Radial DFT Entropy Universal Serial Serial Cumulative sums forward Cumulative sums reverse Random excursions	P values 1 P values 2 X = -4 $X = -3$ $X = -2$ $X = -1$ $X = 1$ $X = 1$ $X = 2$ $X = 3$	0.18410 0.28191 0.21762 0.67514 0.85988 0.92285 0.88464 0.16074 0.99445 0.17143 0.87464 0.3647 0.35221 0.57183 0.15716 0.099872 0.29907 0.0037788 0.0027926 0.10337	0.45703 0.28191 0.90595 0.71270 0.85988 0.54825 0.38399 0.33744 0.99292 0.039989 0.006063 0.34767 0.89099 0.0001427 0.40359 0.54469 0.47837 0.75769 0.43307 0.67278	0.24495 0.28191 0.54043 0.71270 0.85988 0.99989 0.029523 0.69469 0.99659 0.65972 0.98104 0.35256 0.77967 0.97465 0.95603 0.89146 0.88326 0.88326 0.885692 0.082712 0.68683	Success Success
	X = 4	0.2619	0.66907	0.1332	Success

We have computed the histograms of 3 256 digital images of size 256×256 . These images have various verifiable attributes. In Figures 3a and 3b, the histograms of plain pictures contain very sharp gradients thus the histograms of all encrypted images under the proposed scheme are genuinely smooth as compared to the primary image, which makes quantifiable assaults troublesome. Subsequently, it does not give any insight to be utilized during a test assault on the enciphered images (Figures 4a, 4b).



Figures 4. a, Histograms of original images Lena and b, histograms of original images fruits

5.3 Pixels correlation test

Neighboring pixels of any picture must be exceedingly associated either in horizontal, vertical, or corner to corner directions. Hence, a protected encrypted plan should evaluate this relationship to extend obstruction against measurable interrogation. To determine the connection between neighboring pixels during a transparent and encrypted image, the accompanying method has been completed. Initial, 10000 sets of two nearby pixels from the plain and encrypted image were chosen (Trugenberger, 2002). At that time correlation coefficients of every combined pair were ascertained utilizing the accompanying mathematical expression:

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

x and *y* are the two values of consecutive pixels within the image, $\sigma_{x, y}$ is the covariance, σ_{x}^{2} and σ_{y}^{2} are variances of a random variant. The correlation coefficients of cipher and plain images have different values as represented in Table 3 associated with plain and cipher images given in Figures 2, 3a, and 3b.

5.4 Intensity of plain and encrypted figures

The color intensity of a picture was monitored by the adjacency pixels of the image. The variance of color values is often taken as color depths or bit depth. The amount of pixels concerning the intensity of a picture is given in Figures 6a, 6b, 6c, 7a, 7b, 7c. The histograms contain sharp peaks within the pixels distributions of encrypted figures; the color intensities were quite smooth in RGB distributions. The resulting images obtained from the proposed algorithm are the best and have no clue to the intruders.

Table 2. Coefficient of correlation of the plain and the cipher figures

	Plain			Encrypted (present algorithm)			Ref		
Images	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena Fruits	0.9740 0.9753	0.9868 0.9757	0.9612 0.9567	-0.0113 -0.0129	-0.0093 -0.0155	0.0027 0.0012	0.041	0.0107	0.0097



Figures 5. a, Histograms of encrypted images Lena and b, histograms of encrypted images fruits



Figures 7. a, b, c, histograms of RGB images of Lena

5.5 Entropy evaluation

The leading characteristic of randomness is "entropy". Entropy may be a statistical measure of randomness that will characterize the feel of the input image or an encrypted image. The entropy of the image is often calculated by independent random events from a gaggle of discrete events and its probabilities of happenings over the whole image, then the sum of the merchandise of events and its probabilities over the whole pixels of a picture is that the entropy. The estimation of an ideal data entropy is 8. Different clear and encrypted image entropy obtained in Table 4 for the primary images of Figures 2. These entropies are on the verge of hypothetical estimation. In the encryption procedure leakage of data is not important because the method is protected from entropy intruders. A comparison of entropy of the proposed algorithm with those existing has for encrypted Lena image is better than the prevailing algorithm (Table 5).

Table 5. Comparative entropy of the Lena picture of size 256 x 256

Scheme	Entropy
Proposed algorithm	7.8988
Sun algorithm	7.9965
Baptista algorithm	7.9260
Wong algorithm	7.9690
Xiang algorithm	7.9950

5.6 Differential analysis

Differential analyses are required to form an encryption scheme robust against any differential attacks. It was done and we found the present scheme has enough suitability to any clear image. The sensitive analysis as was wiped out (Tong, Zhang, & Wang, 2016) has been administered for 2 target images, the Lena and the Fruits, and results are reported in Table 6.

Comparison of our proposed results with existing reported has been made and located a high resistance against differential and linear attacks.

6. Conclusions

A scheme was developed that supported quantum angular operators with TCM. Quantum half-spinning

 Table 4.
 Entropies of the original and the cipher images

techniques were used for the encryption of both the key and therefore the target image. Different possible key operations are investigated and located and it was almost impossible to break the modified key and the text because nobody knows what matrices have been chosen for multiplication from the given set M, this could be 2 matrices or more than 2 matrices. The proposed technique is predicated on the semi-spinning of the system, therefore the points lying in between -2pi to +2pi have infinite possible permutations of the rotation matrices. The proposed algorithm's features are an honest contender for image encryption purposes reported after statistical analysis has been done (Table 7).

Acknowledgements

This research work was partially supported by Chiang Mai University and the college of arts, media, and technology for funding.

References

- Bano, M., Saleem, A., Shah, T. M., Thammarat, P., & Ronnason, C., (2020). Extended image encryption with Markov processes in solutions images dynamical system of non-linear differential equations. Journal of Mathematical and Computational Science, 10(6).
- Bano, M., Shah, T., & Shah, T. M., (2017). Image reconstruction and text embedding using scan pattern with XOR in graph cut technique. *Journal* of Intelligent and Fuzzy Systems, 33(2), 1097-1104.
- Bano, M., Shah, T., & Shah, T. M., (2016). Genetic algorithm on piecewise linear chaotic map based on image encryption. *Indian Journal of Science and Technology*, 9(8).

Plain image							Cipher imag	e
Image	Plain Image	Red	Green	Blue	Encrypted image	Red	Green	Blue
Lena Fruits	7.7502 7.6868	7.2633 7.1466	7.5909 7.4330	6.9798 7.7588	7.9988 7.9984	7.9977 7.9980	7.9978 7.9980	7.9978 7.9979

Table 6. The sensitivity analysis of the proposed image encryption scheme

Standard images _		NPCR			MAF		
	Max	Min	Mean	Max	Min	Mean	
Lena Fruits	99.997 99.994	99.612 99.515	99.713 99.698	34.43 33.98	33.21 33.98	33.87 33.71	79.22 83.45

Table 7. Sensitivity analysis for color components

Test image		NPCR			UACI			MAE	
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Lena Fruits	99.88 99.67	99.73 99.89	99.79 99.65	33.33 33.04	33.88 33.21	32.78 76.36	82.78 76.36	77.88 86.34	81.78 88.98

- Bano, M., Shah, T., & Shah, T. M., (2016). Image reconstruction and text embedding using graph Cut. *Science International*, 28(2), 905-911.
- Barranco, A., Bennett C. H., Cleve R., Di Vincenzo, D. P., Margolus, N., Shor, P. W., . . . Weinfurter, H., (1995). Elementary gates for quantum computation. *Physics Review Part A*, 52, 3457.
- Branson, J., (2013). Derives the expression for rotation operator. *Quantum Physics*, 22(4).
- Branson, J., (2013). Spin (1/2) and derive spin (1/2) rotation matrices and operators. *Quantum Physics*, 22(4).
- Deutsch, D., (1985). Quantum theory, the Church-Turing principle, and the universal quantum computer. *Proceeding Royal Society, London A, 400*, 97–117.
- Hamza, R., & Titouna, F., (2016). A novel sensitive image encryption algorithm based on the Zaslavsky chaotic Map. *Information Security Journal Global Perspective*, 25,162–179.
- Iliyasu Le, P. Q., Dong, A. M., & Hirota, K., (2011). Efficient color transformations on quantum images. *Journal* of Advanced Computing and Intelligent Information, 15(10), 698–706.
- Man, P. P., (2017). Wigner active and passive rotation matrices applied to NMR tensor. *Concepts Magnetic Resonance, Part A*, 45(A(1)), 26.
- Monz, T., Kim, K., Hansel, W., Riebe, M., Villar, A. S., Schindler, P., . . Blatt, R., (2009). Realization of the quantum Toffoli gate with trapped ions. Physics Review Letter, 102(040501).
- Nielsen, M. A., & Chuang, I. L., (2000). *Quantum computation and quantum information*. Cambridge, England: Cambridge University Press.
- Orawit, T., Thammarat, P., & Bano, M., (2021). Double encryption using trigonometric chaotic map and XOR of an image. *Computers, Materials and Continua, 69*(3) doi:10.32604/cmc.2021.019153.

- Sravan, K. D., Suneetha, CH. & Sekhar, C. A., (2010). Encryption of data streams using Pauli spin ¹/2matrices. International Journal of Engineering Science and Technology, 2(6), 2020–2028.
- Sudha, K. R., Sekhar, C. A., & Reddy, P. V. G. D, (2007). Cryptography protection of digital signals using some recurrence relations. *International Journal of Computer Science and Network Security*, 7(5), 203– 207.
- Tong, XJ., Zhang, M. Wang, Z., & Ma, J., (2016). A joint color image encryption and compression scheme based on the hyperchaotic system. *Nonlinear Dynamics*, 84, 2333–2356.
- Trugenberger, C., (2002). Phase transitions in quantum pattern recognition. *Physics Review Letters*, 89(277903). doi:10.1103/PhysRevLett.89.277903 PMID: 12513243
- Trugenberger, C., (2002). Quantum pattern recognition. Quantum Information Process, 1(6), 471–493.
- Venegas-Andraca, S.E., & Bose, S., (2003). Quantum computation and image processing: New trends in artificial intelligence. *Proceedings of the International Conference on Artificial Intelligence*, *IJCAI-03*, 1563–1564.
- Venegas-Andraca, S. E., & Bose, S., (2003). Storing, processing, and retrieving an image using quantum mechanics. *Proceedings of SPIE Conference Quantum Information and Computation*, 5105, 137– 147.
- Waseem, H. M., & Khan, M., (2018). Information confidentiality using quantum spinning, rotation, and finite state machine. *International Journal of Theoretical Physics*, 57(11), 3584–3594.
- Yang, Y. G., Xia, J., Jia, X., & Zhang, H., (2013). Novel image encryption/decryption based on quantum Fourier transform and double phase encoding. *Quantum Information Process*, 1–17.