JOURNAL OF INFORMATION TECHNOLOGY, CYBERSECURITY, AND ARTIFICIAL INTELLIGENCE

(ARTICLE)

A Gray Image Quantum Encryption using GNEQR Representation

Achraf Abdelghafour Zemate
LPMS, Department of Physics
Ibn Tofail University
Kenitra, Morocco

Moulay Brahim Sedra
LPMS, Department of Physics
Ibn Tofail University
Kenitra, Morocco

Journal of Information Technology, Cybersecurity, and Artificial Intelligence, 2025, 2(1), 8–17

Publication history: December 14 2024; Revised January 11 2024, Accepted January 14, 2024

Article DOI: https://doi.org/10.70715/jitcai.2024.v2.i1.002

Abstract

In the digital era, characterized by extensive online data exchange, information security has become a priority. While traditional encryption methods have proven effective in protecting data transfers, the advent of advanced quantum computing has increased susceptibility to security breaches. Quantum encryption provides a revolutionary solution to this problem by using quantum mechanics principles to establish algorithms that are impermeable to decryption. Using these quantum properties, cryptographic protocols are developed to provide superior security, unlike traditional encryption methods. The image plays an important role in transmitting information in all areas. Therefore, quantum image encryption methods are specifically designed to counter the potential risks posed by quantum computers, which can compromise conventional encryption protocols. This ensures the preservation of data security despite advances in quantum computing technology. In addition, quantum image encryption improves data transmission efficiency by establishing secure communication channels using quantum stats, thereby reducing the need for bandwidth and improving transmission speed. This paper proposes a new method of quantum encryption based on GNEQR representation and the modification of pixel values and positions in an image. After converting the image into a quantum form, we applied an algorithm to modify the values and positions of the pixels using a succession of quantum gates. We concluded this study with a statistical analysis showing the robustness of our quantum image encryption method.

Keywords : Quantum image encryption; GNEQR representation; quantum image processing; quantum gate; quantum encryption circuit.

1. Introduction

Data and communication systems are facing serious security challenges due to the growing popularity of multimedia technologies and the emergence of smart electronic devices. Current communication requires the use of image encryption techniques as effectively as possible to preserve the confidentiality of sensitive images Digital images are essential to modern communication, enabling ideas to be conveyed concisely and effectively. Sending images with maximum security remains a major challenge and is becoming increasingly difficult with the relentless advancement of quantum computing [1]. Quantum image cryptography is currently one of the best techniques for protecting multimedia data [2]. Quantum image representation allows image data to be represented using quantum states [3].FRQI [4], NAQSS [5], QUALPI [6], SQR [7], NEQR [8], GNEQR[9], QRCI [10], QRMW [11], QMCR [12], QBIR [13], QIIR [14], OQIM [15] and others [16] and other methods are used to represent image data in the form of qubits.

The development of algorithms for quantum image cryptography is crucial due to the sensitive and complex nature of visual data. Images contain a huge amount of information that requires special methods to secure their exchange. Research in this area is essential to ensure the privacy of visual data in an ever-changing digital world.

Many studies have been conducted to find a more secure and efficient quantum image encryption algorithm. An algorithm that can ensure that all image data are secure and protected from unauthorized access. It must be able to encrypt large sets of image data quickly and efficiently [17].

The GNEQR quantum representation is emerging as a novel approach in the field of quantum cryptography, offering significant advantages in terms of security and efficiency [9]. It relies on advanced quantum principles to transform visual data into a quantum form, thus exploiting the unique properties of quantum mechanics to guarantee information confidentiality.

In this work, we examine in detail the theoretical foundations of the GNEQR quantum representation and explore its specific application to image encryption. We highlight the potential advantages of this approach, including its resistance to both classical and quantum attacks, as well as its ability to guarantee the confidentiality of visual data in an emerging quantum computing context.

This study helps broaden our understanding of the possibilities offered by quantum cryptography in image processing, paving the way for new secure applications in various fields that require image transmission.

2. The GNEQR representation

The GNEQR quantum representation is important in various areas of quantum information processing. It allows for the storage and processing of quantum images, facilitating tasks such as quantum image transformations and transparency information processing. Additionally, the GNEQR representation method solves the problem of image scrambling for rectangular images, requiring fewer quantum bits to represent images of different sizes [9]. Furthermore, the GNEQR representation is used in encryption protocols to secure the exchange of facial images, perturbing pixel locations per block in grayscale images. Overall, the GNEQR quantum representation provides a valuable tool for quantum image processing, enabling efficient storage, manipulation, and encryption of quantum images [18].

This representation is described in [19],[20]. For a gray image, color α with m qubits is presented by (1) :

$$|\alpha\rangle = |\alpha_{m-1}\alpha_{m-2}.....\alpha_1\alpha_0\rangle = |\alpha_{m-1}\rangle\,|\alpha_{m-2}\rangle \ldots |\alpha_1\rangle\,|\alpha_0\rangle \qquad (1)$$

With $\alpha_{m-1}\alpha_{m-2}\ldots\alpha_0$ is the binary extension of α

The expression of a quantum image for a $2^n \times 2^n$ image is described by (2)

$$|\Psi\rangle = \frac{1}{\sqrt{2^{n+n}}}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}|f(x,y)\rangle\,|x\rangle|y\rangle \qquad (2)$$

Where

f(x, y) : pixel color

(x, y) : position of the pixel

The following figure “Fig. 1” presents an example of the GNEQR representation for a $2^1\times2^2$ size image and its quantum state [18].

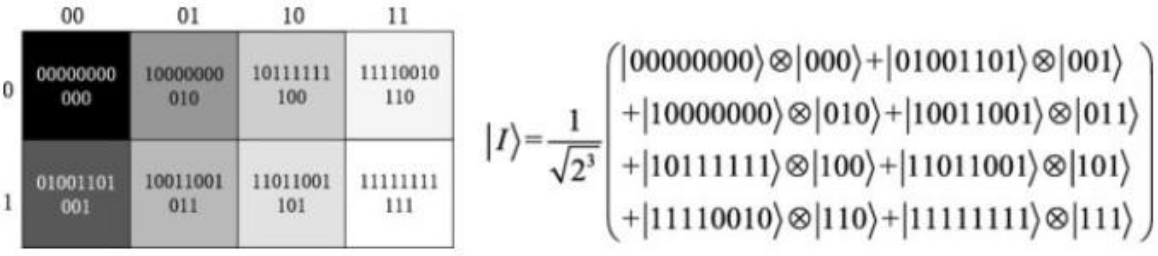


Fig.1 Example of the GNEQR representation for a 2×4 size image and its quantum state.

3. Steps of quantum encryption

3.1. **Step 1**

We took a sample color image (Lena's image), 128 x 128. “Fig 2”.

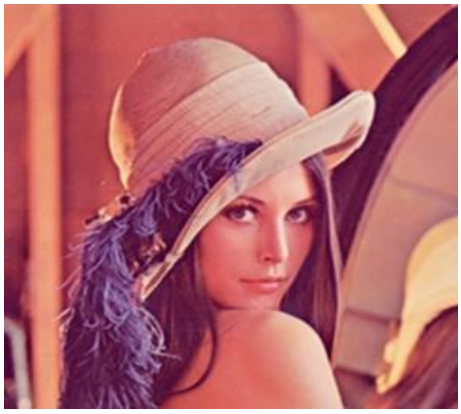


Fig.2 Original image.

We transform it into a gray image “Fig. 3”.

Fig.3 Gray image of Lena.

Then, we extract the first block 4x4 of the gray image matrix (3).

$$\begin{pmatrix} 156 & 148 & 145 & 148 \\ 147 & 152 & 149 & 146 \\ 146 & 153 & 150 & 147 \\ 153 & 152 & 151 & 154 \end{pmatrix} \quad (3)$$

3.2. **Step 2**

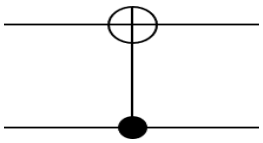
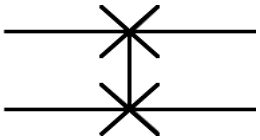
Next, we transform the pixel values into 8-bit binary, and we use GNEQR to represent the pixels in the first block 2^2x2^2 (4).

$$|\Psi\rangle = \frac{1}{2^2}[\ |10011100\rangle\otimes|00\rangle|00\rangle + |10010011\rangle\otimes|00\rangle|01\rangle + +|10010010\rangle\otimes|00\rangle|10\rangle + |10011001\rangle\otimes|00\rangle|11\rangle$$
$$+ |10010100\rangle\otimes|01\rangle|00\rangle + |10011000\rangle\otimes|01\rangle|01\rangle + |10011001\rangle\otimes|01\rangle|10\rangle + |10011000\rangle\otimes|01\rangle|11\rangle$$
$$+ |10010001\rangle\otimes|10\rangle|00\rangle + |10010101\rangle\otimes|10\rangle|01\rangle + |10010110\rangle\otimes|10\rangle|10\rangle + |10010111\rangle\otimes|10\rangle|11\rangle$$
$$+ |10010100\rangle\otimes|11\rangle|00\rangle + |10010010\rangle\otimes|11\rangle|01\rangle + |10010011\rangle\otimes|11\rangle|10\rangle + |10011010\rangle\otimes|11\rangle|11\rangle] \quad (4)$$

3.3. **Step 3**

Table 1 exhibits the quantum logic gates that are used in the encryption circuit [1],[21],[22],[23].

Table 1 Quantum logic gates used

Gate	Action	Notation
Pauli X or NOT	X|0⟩=|1⟩ X|1⟩=|0⟩	
Controlled NOT (CNOT)	CNOT|00⟩=|00⟩ CNOT|01⟩=|01⟩ CNOT|10⟩=|11⟩ CNOT|11⟩=|10⟩	
SWAP	SWAP|00⟩=|00⟩ SWAP|01⟩=|10⟩ SWAP|10⟩=|01⟩ SWAP|11⟩=|11⟩	

Our quantum encryption algorithm is established by the succession of logic gates (5):

$$SWAP_{1,2}\ SWAP_{3,4}\ SWAP_{5,6}\ SWAP_{7,8}\ C_1NOT_2\ C_7NOT_8\ NOT_9\ NOT_{10}\ NOT_{11}\ NOT_{12} \quad (5)$$

And the quantum circuit of encryption applied to each 4x4 block is “Fig. 4”.

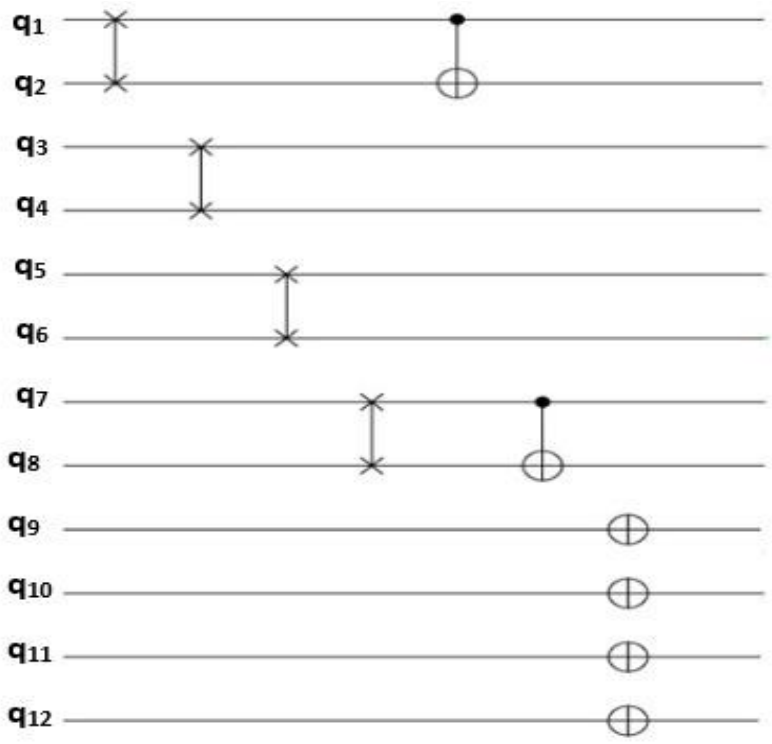


Fig.4 Proposed quantum encryption circuit.

4. RESULTS

Thus, the first block becomes (6)

$$\begin{pmatrix} 101 & 106 & 100 & 103 \\ 98 & 105 & 103 & 97 \\ 97 & 107 & 100 & 98 \\ 104 & 99 & 104 & 108 \end{pmatrix} \quad (6)$$

The first block's encrypted state $|\Psi c\rangle$ is represented by (7)

$$|\Psi_c\rangle = \frac{1}{2^2}[|01100101\rangle\otimes|00\rangle|00\rangle + |01100010\rangle \otimes |00\rangle|01\rangle + |01100001\rangle \otimes |00\rangle|10\rangle + |01101000\rangle \otimes |00\rangle|11\rangle$$

$$+|01101010\rangle\otimes|01\rangle|00\rangle + ||01101001\rangle \otimes |01\rangle|01\rangle + |01101011\rangle \otimes |01\rangle|10\rangle + |01100011\rangle \otimes |01\rangle|11\rangle$$

$$+|01100100\rangle\otimes|10\rangle|00\rangle +|01100111\rangle\otimes|10\rangle|01\rangle + |01100100\rangle\otimes|10\rangle|10\rangle + |01101000\rangle\otimes|10\rangle|11\rangle$$

$$+|01100111\rangle \otimes |11\rangle|00\rangle + |01100001\rangle \otimes |11\rangle|01\rangle + |01100010\rangle \otimes |11\rangle|10\rangle + |01101100\rangle \otimes |11\rangle|11\rangle] \quad (7)$$

Finally, we can construct the encrypted gray image by concatenation of all the blocks “Fig. 5”.

Fig.5 Encrypted Lena image.

5. Statistical Analysis and Discussion

5.1. **Histogram**

It represents the distribution of pixels in an image.

The Encrypted image histogram is almost uniform. This is a completely different histogram than the one of the original image “Fig. 6”. This indicates that the encryption process is strong and can resist attacks [23].

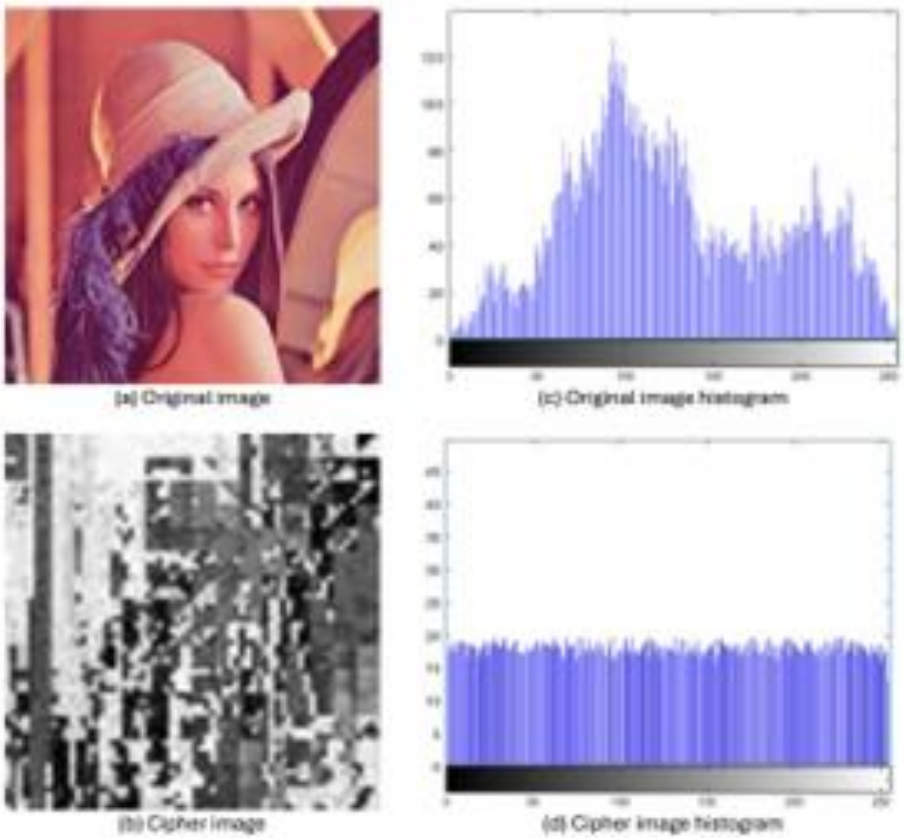


Fig.6 Histograms of the original and encrypted image.

5.2. Correlation coefficient

In general, this coefficient is used to measure the similarity between two pixels. This is an important indicator of image encryption effectiveness [24]. By calculating the correlation coefficient, we can determine the correlation between the original and encrypted images[25], [26]. It is presented by (8)

$$\mathbf{r} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(\beta_{ij} - \bar{\beta})(\gamma_{ij} - \bar{\gamma})}{\sqrt{\left(\sum_{i=1}^{M}\sum_{j=1}^{N}(\beta_{ij} - \bar{\beta})^2\right)\left(\sum_{i=1}^{M}\sum_{j=1}^{N}(\gamma_{ij} - \bar{\gamma})^2\right)}} \qquad (8)$$

Where

β_{ij} represent the pixels of the original.

γ_{ij} represent the pixels of the cipher image.

$\bar{\beta}$ and $\bar{\gamma}$ are average values of β_{ij} and γ_{ij} .

To make it difficult to guess the value of a pixel's neighbors, an encrypted image must have a low correlation between two neighboring pixels [27],[28].

Table 2 compares our correlation results along directions with previous work using the Lena image.

Table 2 Correlation coefficients for our method and those of other studies

	Correlation directions		
	Vertical	**Horizontal**	**Diagonal**
Image (Lena)	0.90503	0.78617	0.71676
Cipher image	-0.01336	-0.01336	-0.00910
Cipher image in Ref. [29]	0.01308	0.0271	-0.00427
Cipher image in Ref. [30]	-0.0039	0.0229	-0.0106
Cipher image in Ref. [31]	0.013787	-0.010578	0.015208

The correlation coefficients of the proposed method are near zero compared with those of previous studies. This means that there is little linear correlation between the pixels of the original image and those of the encrypted image. Therefore, the encryption is robust and secure against correlation analysis attacks [32],[33].

5.3. MSE

The Mean Squared Error measures how closely the original image and encrypted image are similar [7]. It is presented by (9)

$$\mathrm{MSE} = \frac{1}{\mathrm{M}\times\mathrm{N}} \sum_{x=1}^{M} \sum_{y=1}^{N} (\mathrm{I}(x,y)\text{-}\mathrm{I}'(x,y))^2 \qquad (9)$$

I(x, y) : original image

I’(x, y) : encrypted image

M×N: image size

x,y: pixel position

Table 3 presents the MSEs found and those of the two previous results.

Table 3 MSE of grey images for our method and those of other studies

Method	**MSE per Channel**		
	Red	**Green**	**Blue**
Ref. [33]	9.117E3	9.810E3	1.068E4
Ref. [20]	9.827E3	1.0481E4	4.108E4
Proposed	1.0438E4	1.1057E4	9.1731E3

As a criterion for encryption level, the MSE value can be used to determine the security of cryptosystems. A higher MSE value indicates a stronger encryption method[34].

5.4. Discussion

Our histogram of the encrypted image is uniform, meaning that it has pixel values distributed evenly across the range, making it difficult to detect visual patterns in encrypted images. Therefore, it is difficult to determine what the original image looked like. This makes the task of analyzing encrypted images much more difficult than that of analyzing unencrypted images.

The correlation coefficients found are very close to zero. In this way, the encryption technique eliminates the correlation between pixels adjacent to the original image, making any attack based on correlation difficult.

The MSE values we found are high, which shows that the similarity is almost zero between the original image and the encrypted image. This indicates that our method can withstand attacks.

6. CONCLUSION

This study presents a new encryption method based on the use of the GNEQR representation and the modification of pixel positions and values. Based on the results, we conclude that the proposed quantum encryption method is both secure and resilient to common attacks. We are convinced that our method can be improved to provide an efficient and secure solution for broad image encryption applications. Future research could focus on developing more efficient encryption algorithms, using multi-factor authentication for improved security, and exploring the use of quantum computation for secure encryption.

7. Acknowledgments

The authors would like to express their best acknowledgments to Dr. Issam Andaloussi for useful remarks and discussions.

8. References

[1] F. Yan and S. E. Venegas-Andraca, *Quantum Image Processing*. Singapore: Springer Singapore, 2020. doi: 10.1007/978-981-32-9331-1.

[2] M. Naseri *et al.*, "A new cryptography algorithm for quantum images," *Optik*, vol. 171, pp. 947–959, Oct. 2018, doi: 10.1016/j.ijleo.2018.06.113.

[3] J. Wang, Y.-C. Geng, L. Han, and J.-Q. Liu, "Quantum Image Encryption Algorithm Based on Quantum Key Image," *Int J Theor Phys*, vol. 58, no. 1, pp. 308–322, Jan. 2019, doi: 10.1007/s10773-018-3932-y.

[4] P. Q. Le, F. Dong, and K. Hirota, "A flexible representation of quantum images for polynomial preparation, image compression, and processing operations," *Quantum Inf Process*, vol. 10, no. 1, pp. 63–84, Feb. 2011, doi: 10.1007/s11128-010-0177-y.

[5] H.-S. Li, Q. Zhu, R.-G. Zhou, L. Song, and X. Yang, "Multi-dimensional color image storage and retrieval for a normal arbitrary quantum superposition state," *Quantum Inf Process*, vol. 13, no. 4, pp. 991–1011, Apr. 2014, doi: 10.1007/s11128-013-0705-7.

[6] Y. Zhang, K. Lu, Y. Gao, and K. Xu, "A novel quantum representation for log-polar images," *Quantum Inf Process*, vol. 12, no. 9, pp. 3103–3126, Sep. 2013, doi: 10.1007/s11128-013-0587-8.

[7] S. Yuan, X. Mao, Y. Xue, L. Chen, Q. Xiong, and A. Compare, "SQR: a simple quantum representation of infrared images," *Quantum Inf Process*, vol. 13, no. 6, pp. 1353–1379, Jun. 2014, doi: 10.1007/s11128-014-0733-y.

[8] Y. Zhang, K. Lu, Y. Gao, and M. Wang, "NEQR: a novel enhanced quantum representation of digital images," *Quantum Inf Process*, vol. 12, no. 8, pp. 2833–2860, Aug. 2013, doi: 10.1007/s11128-013-0567-z.

[9] H.-S. Li, P. Fan, H.-Y. Xia, H. Peng, and S. Song, "Quantum Implementation Circuits of Quantum Signal Representation and Type Conversion," *IEEE Trans. Circuits Syst. I*, vol. 66, no. 1, pp. 341–354, Jan. 2019, doi: 10.1109/TCSI.2018.2853655.

[10] L. Wang, Q. Ran, J. Ma, S. Yu, and L. Tan, "QRCI: A new quantum representation model of color digital images," *Optics Communications*, vol. 438, pp. 147–158, May 2019, doi: 10.1016/j.optcom.2019.01.015.

[11] E. ŞahiN and İh. Yilmaz, "QRMW: quantum representation of multi wavelength images," *Turk J Elec Eng & Comp Sci*, vol. 26, no. 2, pp. 768–779, Mar. 2018, doi: 10.3906/elk-1705-396.

[12] M. Abdolmaleky, M. Naseri, J. Batle, A. Farouk, and L.-H. Gong, "Red-Green-Blue multi-channel quantum representation of digital images," *Optik*, vol. 128, pp. 121–132, Jan. 2017, doi: 10.1016/j.ijleo.2016.09.123.

[13] X. Liu, D. Xiao, W. Huang, and C. Liu, "Quantum Block Image Encryption Based on Arnold Transform and Sine Chaotification Model," *IEEE Access*, vol. 7, pp. 57188–57199, 2019, doi: 10.1109/ACCESS.2019.2914184.

[14] B. Wang, M. Hao, P. Li, and Z. Liu, "Quantum Representation of Indexed Images and its Applications," *Int J Theor Phys*, vol. 59, no. 2, pp. 374–402, Feb. 2020, doi: 10.1007/s10773-019-04331-0.

[15] G. Xu, X. Xu, X. Wang, and X. Wang, "Order-encoded quantum image model and parallel histogram specification," *Quantum Inf Process*, vol. 18, no. 11, p. 346, Nov. 2019, doi: 10.1007/s11128-019-2463-7.

[16] J. Su, X. Guo, C. Liu, and L. Li, "A New Trend of Quantum Image Representations," *IEEE Access*, vol. 8, pp. 214520–214537, 2020, doi: 10.1109/ACCESS.2020.3039996.

[17] N. A. E.-S. Mohamed, H. El-Sayed, and A. Youssif, "Mixed Multi-Chaos Quantum Image Encryption Scheme Based on Quantum Cellular Automata (QCA)," *Fractal Fract*, vol. 7, no. 10, p. 734, Oct. 2023, doi: 10.3390/fractalfract7100734.

[18] K. Liu, Y. Wei, and H.-S. Li, "The quantum realization of image linear gray enhancement," *Quantum Machine Intelligence*, vol. 5, no. 1, p. 15, Mar. 2023, doi: 10.1007/s42484-023-00102-7.

[19] H.-S. Li, Y. Xu, Y. Qin, D. Fu, and H.-Y. Xia, "The addition and subtraction of quantum matrix based on GNEQR," *Int. J. Quantum Inform.*, vol. 17, no. 07, p. 1950056, Oct. 2019, doi: 10.1142/S0219749919500564.

[20] S. Rfifi, A. Maafiri, K. Chougdali, and A. Gueddana, "A new efficient model of quantum image cryptography based on sampled GNEQR storage presentation," *J. Korean Phys. Soc.*, vol. 78, no. 7, pp. 618–626, Apr. 2021, doi: 10.1007/s40042-021-00065-7.

[21] J. C. Garcia-Escartin and P. Chamorro-Posada, "A SWAP gate for qudits," *Quantum Inf Process*, vol. 12, no. 12, pp. 3625–3631, Dec. 2013, doi: 10.1007/s11128-013-0621-x.

[22] Z. Wang, M. Xu, and Y. Zhang, "Review of Quantum Image Processing," *Arch Computat Methods Eng*, vol. 29, no. 2, pp. 737–761, Mar. 2022, doi: 10.1007/s11831-021-09599-2.

[23] 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. 138233–138243, 2019, doi: 10.1109/ACCESS.2019.2942986.

[24] J. Shang and X. Xu, "Research on a double image security transmission algorithm of image encryption and hiding," *Measurement: Sensors*, vol. 31, p. 100942, Feb. 2024, doi: 10.1016/j.measen.2023.100942.

[25] M. Planat and P. Solé, "Clifford groups of quantum gates, BN-pairs and smooth cubic surfaces," *J. Phys. A: Math. Theor.*, vol. 42, no. 4, p. 042003, Jan. 2009, doi: 10.1088/1751-8113/42/4/042003.

[26] M. Khan and H. M. Waseem, "A novel image encryption scheme based on quantum dynamical spinning and rotations," *PLoS ONE*, vol. 13, no. 11, p. e0206460, Nov. 2018, doi: 10.1371/journal.pone.0206460.

[27] M. Kumar, A. Aggarwal, and A. Garg, "A Review on Various Digital Image Encryption Techniques and Security Criteria," *IJCA*, vol. 96, no. 13, pp. 19–26, Jun. 2014, doi: 10.5120/16854-6720.

[28] K. Loukhaoukha, J.-Y. Chouinard, and A. Berdai, "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle," *Journal of Electrical and Computer Engineering*, vol. 2012, pp. 1–13, 2012, doi: 10.1155/2012/173931.

[29] J. Yu, C. Li, X. Song, S. Guo, and E. Wang, "Parallel Mixed Image Encryption and Extraction Algorithm Based on Compressed Sensing," *Entropy*, vol. 23, no. 3, p. 278, Feb. 2021, doi: 10.3390/e23030278.

[30] M. Shi, S. Guo, X. Song, Y. Zhou, and E. Wang, "Visual Secure Image Encryption Scheme Based on Compressed Sensing and Regional Energy," *Entropy*, vol. 23, no. 5, p. 570, May 2021, doi: 10.3390/e23050570.

[31] W. Song, C. Fu, M. Tie, C.-W. Sham, J. Liu, and H. Ma, "A fast parallel batch image encryption algorithm using intrinsic properties of chaos," *Signal Processing: Image Communication*, vol. 102, p. 116628, Mar. 2022, doi: 10.1016/j.image.2021.116628.

[32] Y. Ma, "Research and application of Big data encryption technology based on quantum lightweight image encryption," *Results in Physics*, vol. 54, p. 107057, Nov. 2023, doi: 10.1016/j.rinp.2023.107057.

[33] L. Wang, Q. Ran, and J. Ma, "Double quantum color images encryption scheme based on DQRCI," *Multimed Tools Appl*, vol. 79, no. 9–10, pp. 6661–6687, Mar. 2020, doi: 10.1007/s11042-019-08514-z.

[34] H. Ogras, "An efficient color image encryption scheme based on a matrix scrambling method and a new hybrid chaotic map," *Cogent Engineering*, vol. 8, no. 1, p. 1940638, Jan. 2021, doi: 10.1080/23311916.2021.1940638.