Quantum Image Encryption using Quantum Image Representations

Achraf Abdelghafour Zemate[1*], *Moulay Brahim Sedra*[1]

[1]LMPS, Department of Physics, Ibn Tofail University, Kenitra, Morocco

Abstract. Since their introduction, numerous quantum image encryption methods have been developed. As we shall demonstrate, protecting visual information against classical and quantum threats depends on representations. In this paper, we identify the essential components of quantum encryption algorithms and explain a variety of quantum image representations with different levels of qubit efficiency, computational complexity, and security. The paper also explores the favourable and unfavourable aspects of hybrid, chaos-based, quantum transform-based, and DNA-based quantum image encryption schemes. The security analysis focuses on noise tolerance and scalability. This involves aspects such as key space size, resistance to various attacks, and calculation efficiency. Meanwhile, potential areas for investigation include robust algorithms, hybrid systems and reducing decoding errors. We also address the implementation difficulties involved, including the necessary hardware and decoding error reduction. Classical and quantum techniques, as well as more advanced quantum equipment, are considered too. The evaluation calls for uniform policies and realistic responses and emphasises how quantum image encryption could transform information security in the quantum era. and realistic answers and highlights how quantum image encryption may change information safety within the quantum generation.

Keywords: Quantum image encryption , quantum image representation , NEQR , FRQI , GQIR

1 Introduction

Quantum technologies enhance cryptography and communication by utilizing quantum mechanics. Images that contain sensitive information may potentially be shared with others via modern communication techniques. Preservation of personal data is crucial to prevent misuse, and one of the main challenges is to ensure comprehensive protection of multimedia data. This article provides an in-depth analysis of Quantum Image Encryption (QIE) techniques, focusing on certain commonly used Quantum Image Representations (QIR).

We discuss what motivated the transition toward QIE and why traditional techniques are not secure given the advent of quantum computers [1]. Visual data is used in an increasing

* Corresponding author: zemate.achraf@gmail.com

number of fields, but classical encryption can be broken by quantum computers, how to protect visual data using some advanced technologies that are immune from the effects of quantum boats [1-2]. The goal of this paper is to present an analysis on conventional QIRs, their pros/cons and how they have been utilized in various QIE algorithms. We will analyze, especially, its security properties in terms of key space, resistance to different types of attacks (known plaintext attack, chosen plaintext attack, statistical test and differential analyses [2- 4]), statistics distributions of cryptographic transformed and complexity computational. The increasing sophistication of cyberattacks and the possibility that quantum computers could break current encryption standards highlight the need to develop quantum-resistant alternatives [1]. To do so, it is necessary to analyze existing QIE techniques and their underlying QIRs to identify their strengths, weaknesses, and potential avenues for future development.

2 Quantum image representations: a comparative analysis

2.1 Overview of QIRs

There are a lot of proposals for QIRs, each having its own specific properties. They also convert classical information into quantum states, and support quantum-level algorithms for encryption and data processing [5]. The dominant QIRs were the Novel Enhanced Quantum Representation (NEQR) [6], Flexible Representation of Quantum Images (FRQI) [7] and the Generalized Quantum Image Representation (GQIR) [2]. Other representations such as Quantum Representation of Images using Cluster States (QIRC) [8] and approaches using qutrits [9] have also been investigated. Each of them considers the qubit requirements, computational overhead and ease of implementing different quantum operations in a compromise [10]. The QIR is a critical factor for the performance and security of this QIE algorithm. It is necessary to perform a deep comparison between these representations in evaluating their appropriateness for various QIE applications.

2.2 NEQR: encoding and applications

NEQR for an image of size $2^n \times 2^n$, is defined by [10]:

$$|I\rangle = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|f(y,x)\rangle|yx\rangle = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\otimes|C_{yx}^{i}\rangle|yx\rangle \quad (1)$$

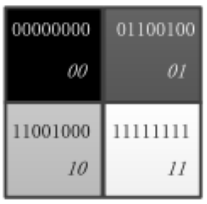
With

$$f(x,y) = C_{yx}^{0}\dots C_{yx}^{q-2}C_{yx}^{q-1} \quad ; \quad C_{yx}^{k} \in [0,1] \quad ; \quad f(x,y) \in [0, 2^q - 1]$$

I : image ; $f(x,y)$: color ; xy : position coordinates

In NEQR, image pixels are encoded using a sequence of qubits [7-9]. It is popular because it is relatively simple to implement and uses fewer qubits than other methods. In some QIE schemes, NEQR's structure can also be applied to encryption, permutation, and diffusion operations [7-9]. As an example, [7] uses NEQR and a chaotic Henon map together with quantum coding for color image encryption. For diffusion, the algorithm uses bit-level adjacent exchange operations and key streams generated from the Henon map. [8] proposes a method by DNA Controlled-Not (DNACNot) gates, which relies on parameters used from a chaotic key generator to modify a sequence prior to a controlled-NOT operation on the scrambled bit-plane. [9] proposes an evolutionary quantum scrambling scheme employing a genetic algorithm to optimize the rate of scrambling from NEQR

representation to find the best scheme on cost, complexity, and image type. Nevertheless, the qubit efficiency and computational complexity of NEQR, particularly for higher resolution images, is a matter of concern [10]. Additionally, the defense against superior quantum attack by NEQR-based QIE schemes should be addressed. Figure 1 shows an example of a NEQR 2×2 quantum image and its quantum state [10].



$$|I\rangle = \frac{1}{2}(|0\rangle\otimes|00\rangle + |100\rangle\otimes|01\rangle + |200\rangle\otimes|10\rangle + |255\rangle\otimes|11\rangle)$$
$$= \frac{1}{2}(|00000000\rangle\otimes|00\rangle + |01100100\rangle\otimes|01\rangle + |11001000\rangle\otimes|10\rangle + |11111111\rangle\otimes|11\rangle)$$

Fig. 1. A 2×2 NEQR quantum image and its quantum state.

2.3 FRQI: flexibility and limitations

FRQI is defined by [11]:

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

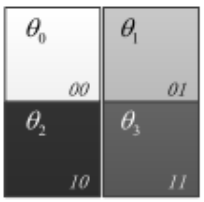
With

$$|c_i\rangle = \cos\theta_i|0\rangle + \sin\theta_i|1\rangle$$

$i = 0,1,2\ldots..2^{2n}\text{-}1$; $\theta_i \in [0, \pi/2]$; $\theta = (\theta_0, \theta_1, \theta_2 \ldots \theta_{2^{2n}-1})$

θ is the angle vector corresponding to the color information. $|0\rangle$ and $|1\rangle$ are two-dimensional quantum ground states. $|i\rangle$ is a 2n-dimensional quantum state.

FRQI is flexible in how images are represented, allowing various transformations and manipulations to be applied [10-11]. Due to its adaptability, it can be used with a variety of QIE algorithms. Nonetheless, the probabilistic nature of quantum measurements, which stems from their intrinsic uncertainty, can lead to ambiguities in both encryption and decryption [11]. This means that the probabilistic representation of a quantum state of the image is not precisely described. [10] examines FRQI in relation to quantum watermarking as well as the authentication process for images and videos, demonstrating its applicability, while also noting the want for stronger error correction methods. [11] studies FRQI as a data encoder in image classification tasks using quantum neural networks and observes that classification accuracy is reasonably high even though FRQI is a probabilistic encoder. As noted in reference [11], the adaptation of FRQI in QIE has its constraints in terms of its flexibility, potential for noise, and the need for effective error correction strategies. An example of an FRQI representation for a 2x2 image is shown in Figure 2.



$$|I\rangle = \frac{1}{2}\Big[\big(\cos\theta_0|0\rangle + \sin\theta_0|1\rangle\big)\otimes|00\rangle + \big(\cos\theta_1|0\rangle + \sin\theta_1|1\rangle\big)\otimes|01\rangle +$$
$$+\big(\cos\theta_2|0\rangle + \sin\theta_2|1\rangle\big)\otimes|10\rangle + \big(\cos\theta_3|0\rangle + \sin\theta_3|1\rangle\big)\otimes|11\rangle\Big]$$

Fig. 2. A 2×2 FRQI quantum image and its quantum state.

2.4 GQIR and other representations

To represent the Y coordinates and X coordinates of an image, GQIR successively uses the parameters h and w such that h=[log$_2$H] qubits and w=[log$_2$W] qubits. Information about color and location is captured in normalized quantum states as follows: |0⟩ and |1⟩. In GQIR, images are written [12] as:

$$|I\rangle = \frac{1}{\sqrt{2}^{h+w}} \left(\sum_{Y=0}^{H-1} \sum_{Y=0}^{W-1} |c_{YX}\rangle \otimes |XY\rangle \right) \quad (3)$$

Where

$$|YX\rangle = |Y\rangle|X\rangle = |y_{h-1}y_{h-2} \dots y_0\rangle|x_{w-1}x_{w-2} \dots x_0\rangle \quad ; \quad y_i, x_i \in \{0,1\}$$
$$|C_{YX}\rangle = |C_{YX}^{q-1} C_{YX}^{q-2} \dots C_{YX}^{0}\rangle \quad ; \quad C_{YX}^{i} \in \{0,1\}$$

q is color depth. And

$$h = \begin{cases} [log_2 H], H > 1 \\ 1, H = 1 \end{cases} \quad ; \quad w = \begin{cases} [log_2 W], W > 1 \\ 1, W = 1 \end{cases}$$

GQIR offers a more generalized framework for QIR, and it also treats other techniques as special cases [3]. Together, the results streamline the QIRs analysis process and allow comparisons between multiple QIE schemes. In a study in [3] a QIE method is developed that uses GQIR mixed with a four-dimensional chaotic system and Arnold transformation for pixel position scrambling. With problems in periodicity, small key space, and other problems seen in many traditional algorithms addressed, this approach seeks to improve the security and usability of the encryption. QIRC utilizes cluster states with advantages in terms of entanglement and experimental feasibility [12], therefore, it is a potential implementation in practice. [12] proposes a secure image encryption scheme embedded with a QIRC model, and describes the concept of cluster states, which are utilized for either representation or encryption purpose. The use of qutrits [13] allows new methods to explore higher-dimensional quantum states that would offer a potentially larger key space and increased security compared to lower-dimensional quantum states. However, exploration of this non-standard approach still needs to conduct additional research to establish their usefulness in QIE such as scalability and robustness towards a variety of attack modes. A comprehensive comparative study of these different quantum state transformers (QIRs) across the various aspects of their strengths and limitations is essential for choosing the optimal representation for various QIE applications. An illustration of a GQIR representation is shown in figure 3 [13].

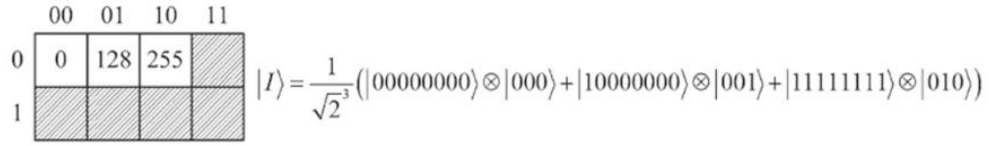


Fig. 3. An example image and its representative expression in GQIR.

3 Quantum image encryption algorithms: a taxonomy

This part groups the various QIE algorithms according on their underlying techniques, noting their main characteristics, benefits, and drawbacks. The security, effectiveness, and usability of the QIE system depend much on the algorithm selected.

3.1 Chaos-based QIE

Many QIE algorithms utilize chaotic systems to generate pseudo-random sequences for encryption keys [3, 4, 14, 15]. The unpredictable nature of chaotic systems enhances the security of QIE by making it difficult to predict the encryption keys. Different chaotic systems, such as the Lorenz system [3], Lotka-Volterra system [4], and Chen system [14,16], have been employed in various QIE schemes. For example, [3] uses a four-dimensional chaotic system to generate keys for pixel value encryption and Arnold transformation for pixel position scrambling. [4] employs a multilayer short memory fractional order Lotka-Volterra system and a dual-scale triangular map for a fast QIE scheme. [14] proposes a dual chaos system based on quantum logistic mapping and the Chen chaos system for generating chaotic sequences. [15] introduces a three-layer encryption scheme for quantum color images based on a 6D hyperchaotic system. The choice of chaotic system impacts the complexity and security of the algorithm, with higher-dimensional systems potentially offering greater randomness and improved resistance to attacks [3, 4, 14, 15]. However, the computational cost of generating and utilizing chaotic sequences needs to be considered.

3.2 Quantum transform-based QIE

Many QIE algorithms have Quantum Arnold Transform (QAT) [17-19] and Quantum Fourier Transform (QFT) [17]. These transforms offer fast ways to scramble pixel positions or translate pixel values in one method that enhances the confusion and diffusion properties of the encryption process [17-19]. [17] adopts the double quantum image encryption algorithm that uses QAT to scramble pixel positions, and then qubit random rotation in both spatial and frequency domains (with the help of QFT) to modify gray information. In [18], a quantum image encryption scheme is presented by combining both Arnold transform with S-box scrambling and uses SHA-256 hashing of plain images to provide this key. [19] employs Quantum Random Phase Encoding along with Arnold Transform to provide security enhancement. With a combination of quantum transforms and others such as chaotic systems, security can be fortified further in imaging encryption. These transforms are extremely efficient, as well as having quantum properties that are useful for their purpose, which makes them useful to make QIE algorithms for safe and efficient operations. However, translating these transformations to existing quantum computers is resource-intensive and the need of optimization of quantum circuits would go some way forward.

3.3 DNA-based QIE

DNA computing is one possible method for DNA-based QIE because it makes use of the biological properties of DNA by encoding and manipulating image data [5]. Inherently random and complex, the way DNA sequences are made provide a great basis for a number of ways of securing encryption on a high level. Therefore, the integration of DNA encoding alongside quantum manipulation increases the strength and security of QIE [5]. [5] combines quantum DNA codec with quantum Hilbert scrambling for pixel-level diffusion and position scrambling. The use of DNA-based techniques will provide large key space potential and also have their own inherent resilience to certain types of attacks. But the practical implementation of DNA-based QIE remains a daunting task due to some of the complexities and limitations of today's DNA computing methods. Further investigations are required to examine the feasibility and efficiency of DNA-based QIE in practice.

3.4 Hybrid approaches

Thus, combining techniques of the chaotic nature, quantum transform, and DNA computing, hybrid QIE algorithms offer enhanced security and efficiency. These hybrid methods utilize the advantages of multiple methods to overcome the limitations of individual techniques. [20] integrates the B92 QKD protocol, Galois Field operations, and a Hyper 3D Logistic Map for secure image communication. Hybrid QIE algorithms must carefully balance security, efficiency, and implementation complexity in order to be effective. The integration of different methods must be done thoroughly based on their individual characteristics and potential synergies. Future research in QIE will focus on developing efficient hybrid algorithms.

4 Security analysis of QIE schemes

In order to evaluate the robustness of a QIE scheme, it is necessary to undertake an overall security analysis. This section is aimed at covering some essential components in security analysis, with a focus on key space analysis and the complexities involved in calculations.

4.1 Key space analysis

The size of a cryptographic system's key space is one of the most fundamental factors. It is much more challenging for attackers to succeed with brute-force methods when there's a larger key space. Many QIE algorithms exploit chaotic systems and quantum operations to create these expansive key spaces. For example, one study claims that a particular QIE algorithm has a key space of 10140, which is much larger than 2128. The above shows the potential for large key spaces in the realm of QIE.

4.2 Computational complexity

Another crucial factor to think about with QIE algorithms is their computing complexity [17-18]. Good algorithms increase QIE's utility and decrease computational overhead. Computational complexity [17-18] is much affected by the selection of encryption methods and QIR. High computational complexity algorithms might not be appropriate for live applications or big image processing. Moreover, the computational power needed for QIE algorithms may be rather more than that of classical algorithms, particularly when processing high-resolution images. Therefore, the creation of fast quantum circuits and algorithms is necessary if QIE is to become a feasible actuality. The trade-off between security and efficiency demands close optimization to guarantee that the picked QIE algorithm balances available computer resources with security needs.

5 Conclusions

Quantum image encryption system is fast developing and has great potential to protect data. Quantum Information Engineering will evolve, leading towards a focus on algorithms that are more solid and environmentally friendly and resistant to classical as well as quantum attacks. New QIRs and advanced errors correction technologies, and new quantum computing hardware are also significant to advance QIE. Integrating QIE with alternate quantum facts processing mechanisms, such as quantum key distribution, may also contribute to information security. It discusses the progress of QIE and makes suggestions for future studies. In quantum technology, visible record protection ensures practical and

scalable QIE outcomes. Quantifying the global validity of QIE will also depend heavily upon hybrid strategies and tuned algorithms. Hardware and software development for quantum computers could also be fundamental in this regard: altering hardware and software of quantum computers could perhaps be essential to realising QIE economically. QIE will be necessary to safeguard such critical visual data as the world of quantum computers transitions into adulthood. It will thus become paramount to establish standardized safety metrics and benchmarking frameworks for QIE algorithms for honest comparisons and driving progress in this topic area.

References

1. A. Mehmood, A. Shafique, M. Alawida, A.-N. Khan, Advances and Vulnerabilities in Modern Cryptographic Techniques: A Comprehensive Survey on Cybersecurity in the Domain of Machine/Deep Learning and Quantum Techniques. IEEE Access **12**, 27530 (2024).
   https://doi.org/10.1109/ACCESS.2024.3367232
2. X.-D. Liu, Q.-H. Chen, R.-S. Zhao, G.-Z. Liu, S. Guan, L.-L. Wu, X.-K. Fan, Quantum image encryption algorithm based on four-dimensional chaos. Front. Phys. **12**, 1230294 (2024).
   https://doi.org/10.3389/fphy.2024.1230294
3. Y. Ma, F.-F. Yu, L.-H. Gong, W.-P. Zou, Fast quantum image encryption scheme based on multilayer short memory fractional order Lotka-Volterra system and dual-scale triangular map. Front. Phys. **10**, 1028630 (2022).
   https://doi.org/10.3389/fphy.2022.1028630
4. J. Gao, Y. Wang, Z. Song, S. Wang, Quantum Image Encryption Based on Quantum DNA Codec and Pixel-Level Scrambling. Entropy **25**, 865 (2023).
   https://doi.org/10.3390/e25060865
5. F. Yan, A.-M. Iliyasu, P.-Q. Le, Quantum image processing: A review of advances in its security technologies. Int. J. Quantum Inform. **15**, 1730001 (2017).
   https://doi.org/10.1142/S0219749917300017
6. Y.-K. Hamad, A.-Y. Yousuf, T.-S. Atia, An Evolutionary Quantum Scrambling Scheme for Medical Image with NEQR Representation. IJCDS **13**, 1383 (2023).
   https://doi.org/10.12785/ijcds/1301112
7. A. Iliyasu, Towards Realising Secure and Efficient Image and Video Processing Applications on Quantum Computers. Entropy **15**, 2874 (2013).
   https://doi.org/10.3390/e15082874
8. A. Mandal, S. Banerjee, P.-K. Panigrahi, Quantum Image Representation on Clusters, in 2021 IEEE International Conference on Quantum Computing and Engineering, IEEE, Broomfield, CO, USA, October (2021).
9. A. Khandelwal, M.-G. Chandra, Quantum Image Representation Methods Using Qutrits, arXiv:2207.09096, (2022).
   https://doi.org/10.48550/arXiv.2207.09096
10. Y. Zhang, K. Lu, Y. Gao, M. Wang, NEQR: a novel enhanced quantum representation of digital images. Quantum Inf Process **12**, 2833 (2013).
    https://doi.org/10.1007/s11128-013-0567-z
11. P. Q. Le, A. M. Iliyasu, F. Dong, and K. Hirota, A Flexible Representation and Invertible Transformations for Images on Quantum Computers, in New Advances in Intelligent Signal Processing, Springer Berlin Heidelberg, Berlin, Heidelberg, (2011).

12. N. Jiang, X. Lu, H. Hu, Y. Dang, Y. Cai, A Novel Quantum Image Compression Method Based on JPEG. Int J Theor Phys **57**, 611 (2018). https://doi.org/10.1007/s10773-017-3593-2
13. R.-G. Zhou, X. Liu, J. Luo, Quantum Circuit Realization of the Bilinear Interpolation Method for GQIR. Int J Theor Phys **56**, 2966 (2017). https://doi.org/10.1007/s10773-017-3463-y
14. Y. Dong, C. Yin, C. Xu, R. Yan, A quantum image encryption method for dual chaotic systems based on quantum logistic mapping. Phys. Scr. **99**, 015103 (2024). https://doi.org/10.1088/1402-4896/ad1020
15. Y. Dong, C. Xu, C. Yin, Three-layer quantum image encryption algorithm based on 6D hyperchaos. Journal of Applied Physics **134**, 224401 (2023). https://doi.org/10.1063/5.0176657
16. L. Wu, M. Li, J. Jia, X. Sun, Quantum image encryption based on hyper-chaotic system and double-random phase encoding, in Third International Conference on Advanced Algorithms and Signal Image Processing, SPIE, Kuala Lumpur, Malaysia, October 10 (2023).
17. X. Liu, D. Xiao, C. Liu, Double Quantum Image Encryption Based on Arnold Transform and Qubit Random Rotation. Entropy **20**, 867 (2018). https://doi.org/10.3390/e20110867
18. H. Liu, B. Zhao, L. Huang, Quantum Image Encryption Scheme Using Arnold Transform and S-box Scrambling. Entropy **21**, 343 (2019). https://doi.org/10.3390/e21040343
19. D. Hermanto, Z. Pratama, Moch. S.-Hidajat, Embedding Quantum Random Phase Encoding Arnold Transform for Advanced Image Security. Sji **11**, 831 (2024). https://doi.org/10.15294/sji.v11i3.12256
20. D. R.-I. Moses Setiadi, N. Rijati, A.-R. Muslikh, B.-Vicky Indriyono, A. Sambas, Secure Image Communication Using Galois Field, Hyper 3D Logistic Map, and B92 Quantum Protocol. CMC **81**, 4435 (2024). https://doi.org/10.32604/cmc.2024.058478