Scientific Journal of Informatics
Vol. 11, No. 3, Aug 2024
p-ISSN 2407-7658 https://journal.unnes.ac.id/journals/sji/index e-ISSN 2460-0040

Embedding Quantum Random Phase Encoding Arnold Transform for Advanced Image Security

Didik Hermanto[1*], Zudha Pratama[2], Moch. Sjamsul Hidajat[3]
[1,2,3]Department of Informatics Engineering, Faculty of Computer Sciences, Universitas Dian Nuswantoro, Indonesia

Abstract.
Purpose: This research purpose an improvised version of the image encryption technique by incorporating Quantum Random Phase Encoding with the Arnold Transform to help enhance the strength and non-predictability of the encryption process. In this research work, some ideas gained from quantum-based methods have been brought to use with conventional approaches in image encryption techniques for enhancing their security.
Method: This model represents the basic methodology that underlies the Arnold Transform for scrambling the arrangement of image pixels to mask recognizable structures within quantum random phase encoding to introduce complexity through quantum-generated random phases.
Result: The experimental results show much improvement in encryption efficiency. For example, in the case of "Cameraman" and "Lena", MSE parameters are 98.134 and 104.76, respectively; these now go up to 832.01 and 888.78. This implies that the higher decrement of these values-from 21.17 dB and 23.98 dB to 13.41 dB and 13.33 dB translates into higher distortion with higher security. Meanwhile, UACI and NPCR are also very steady and the mean value is about 0.3356 to 0.3358 and 99.60 to 99.61, which proves that this method has been effective in changing the pixel's value, sensitive input changes.
Novelty: This work is novel due to the introduction of quantum technologies in the classical methodology of image encryption. While classical techniques make use of conventional transforms for scrambling, like the Arnold Transform, this work embeds quantum randomness and intricacy in the process as a means of encoding; namely, Quantum Random Phase Encoding.

Keywords: Arnold transform, Digital security, Image security, Quality measurement, Quantum encryption
Received August 2024 / **Revised** September 2024 / **Accepted** October 2024

INTRODUCTION

Security can be defined as preventing sensitive information or data from falling into unauthorized hands [1], [2], [3]. Data protection supports the prevention of unauthorized access, integrity, and confidentiality of information. Backups for digital images are among the most frequent types of data [4]. Recent developments have led to a situation whereby misappropriation of image data-that is stealing of photographs, illegal claims to image ownership, and unauthorized posting of an individual's photographed images on the internet with no permission-can be done. [5]. This is done as a result of lax security measures that should be put in place to protect images in the digital platform. Cryptography is a means to go about this. Cryptography is a science that deals with the methods of computational message confidentiality [6]. Harahap [7] mentions that there are three basic functions of cryptography: encryption - it is supposed to protect the data being sent and keep the confidentiality of the message; decryption - it is opposite to encryption and aims at restoring messages; keys - they are used in the processes of encryption and decryption. There are several encryption algorithms associated with it; all of the algorithms have their respective attributes along with advantages concerning security and efficiency. Which algorithm to use entirely depends upon the requirements of the encryption system. Encryption algorithms can also be used on texts and images to keep the data protected [1].

An effective high-level encryption algorithm could solve the problem of security in digital photo data by embedding quantum random phase encoding Arnold transform. Also, the digital images have to be

*Corresponding author.
Email addresses: didik.hermanto@dsn.dinus.ac.id (Hermanto)*, zudha.pratama@dsn.dinus.ac.id (Pratama), moch.sjamsul.hidajat@dsn.dinus.ac.id (Hidajat)
DOI: 10.15294/sji.v11i3.9440

encrypted with cryptography to ensure that only the people who have the correct decryption keys could access them for confidentiality and integrity and authenticity of image data. Secure symmetric/asymmetric encryption methods, such as AES/RSA, respectively, are considered a few of the solutions against the challenge [2], [3], [8]. More importantly, the supplementation with techniques such as digital watermarking can even support the image for copyright protection and authenticity. This will ensure that by incorporating encryption and watermarking into one, the photographers' works would, to a great extent, be protected from theft, unauthorized identification of ownership of an image, and its illicit dissemination online. However, to achieve such a solution, deep knowledge is needed in various encryption algorithms and further in how to adapt those peculiarities to the system used. This point is of utmost importance if the maximum security of digital image data is being pursued.

Researchers have used different encryption algorithms to protect images. In the latest work, by Yusri et al. in 2022 [9] one can notice the work done on improvement in digital image encryption with variation in Arnold Cat Map in integration with DNA encoding. This would allow bringing out a significant variation in the result of encryption. Moreover, the resultant histogram spread uniformly. It can be concluded hereby that the methodology for encryption is indeed quite well-designed and invertible. The work of Liu et al., in 2021 [10] presents a three-level quantum image encryption algorithm using the Arnold transform and logistic map. It was done by performing permutations at block, bit, and pixel levels. Empirical results show the proposed quantum encryption algorithm improves the security and computational efficiency of conventional algorithms. Reasearch by Hu et al. in 2020 [11] propose an advanced quantum architecture of serial structure for the performance of the general Arnold transformation, for the general Arnold transformation of the key image and for quantum keys-based pixel encryption. Obviously, this quantum algorithm improves the computational efficiency greatly when compared with the traditional. The reliability of this quantum algorithm in terms of secure and high visual quality performances was also shown from both experimental and numerical analyses. This becomes a basis for the technique developed in research by Tian and Su's in 2022 [12] to optically encrypt an image using Double Random Phase Encoding (DRPE) along with Chaotic S-box for image substitution and an Improved Arnold Transform-IAT, which augments the security of the DRPE system. High complexity and low differential uniformity of the Chaotic S-box used provide mitigations against the linear security issues. These simulated results proved that the developed encryption scheme was efficient and secure. In 2017, Wang et al. [13] proposed a quantum color image encryption method based on a noncollinear 3D Arnold transformation with 3D Logistic chaos for the QRCI image model. With regard to simulation results and performance evaluation, the presented encryption method would have good efficiency because it was highly efficient in terms of computational complexity and had good ability in terms of strong security.

The new approach undertaken for the improvement of security in images, based on above-related research, is presented in this paper. Security of the high-resolution images in this work was developed through an encryption scheme by bringing together the aspects of Arnold Transformation and quantum random phase encoding. Arnold Transformation is one of the techniques pertaining to image encryption, relating to pixel scrambling. With its periodic nature, however, it has been thought not robust enough in security terms to act as an independent cryptographic system [14]. On the other hand, under volume holography, random phase encoding is devoted to the multiplexing of holographic storage, image encryption, and optical sensors. Based on diffraction attributes and alignment of the decryption keys, this technique enables encrypted image retrieval out of holographic memory systems [15]. The proposed approach can be further developed into a robust and secure image encryption system that integrates the Arnold Transform into the quantum random phase encoding, for the overcoming of defects of each single approach.

METHODS

In the proposed approach for image encryption, quantum circuits will apply in generating random phase values. More precisely, a quantum circuit in the first stage generates random phase values applied to the randomizing of the pixel values of a plain image. Later, the image, carrying these quantum-generated phases, performs an XOR operation with these random values, embedding the quantum randomness in the image. First, this image is converted into the image matrix, which undergoes the Arnold Transform to scramble the pixel positions even further. Again, with a view to introducing more security in the resultant encrypted image, the XOR operation between the transformed image and random-phase values needs to be executed. This two-tier encryption technique combines quantum random phase encoding with the Arnold Transform, so that it ensures a high level of integration of security by quantum randomness with iterative

pixel scrambling, making the unauthorized decryption very difficult. The flowchart of the proposed encryption is depicted in Figure 1.

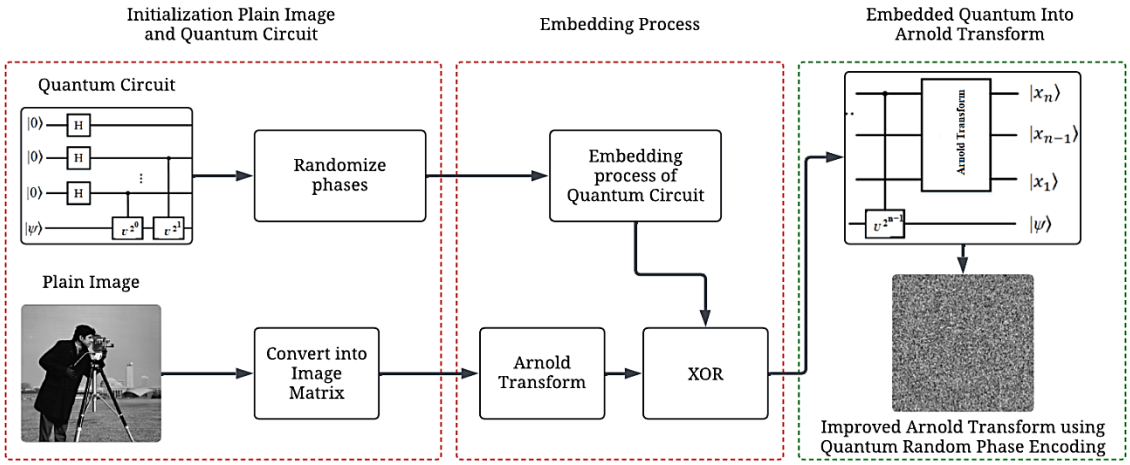


Figure 1. Proposed encryption

Arnold transform

Amongst all encryption techniques, probably the most famous technique in image encryption is the Arnold transform [16], [17]. It simply enhances the security of an image by reordering the position of the pixels. In this iteration transformation, each and every pixel of the image will be reordered concerning a mathematical formula [18]. Lots of irregular and unidentifiable pixels will be contained in the rearranged image. The Arnold transform, performed at every step, acts to shift the position of the pixels, spreading the picture data over the matrix. This randomization obscures the actual content, and decoding is not as easy for the unauthorized user, as he/she would not know the parameters used for conversion. Among other encryption techniques, Arnold's transformation adds an extra layer of complication in increasing the level of security in the process of encrypting images [19]. The Arnold transform is generally considered a mathematical method for scattering the positions of pixels in an image. The equation is shown in equation (1).

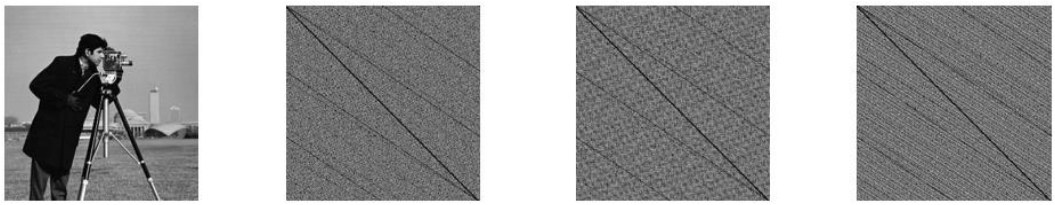
$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \ mod\ N \tag{1}$$

For the Arnold transform, let the original coordinates of an image pixel be denoted by (x, y) and its coordinates after transformation be defined by (x', y'). In its computation for the new position of pixels, the transformation takes up matrix parameters a, b, c, and d to calculate the new pixel positions, and the dimensions of the image are indicated by N (for an $N \times N$ image). for the Arnold Cat Map, the parameters are set as seen in eq (2), Thus, the transform can be simplified to eq (3).

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \tag{2}$$

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x + y \\ x + 2y \end{pmatrix} mod\ N \tag{3}$$

This formula rearranges the pixel positions in a way that creates a seemingly random distribution, enhancing the security of the encrypted image. The results of Arnold transform without embedding quantum random phases can be seen in Figure 2.



(a) Plain image (b) Results of 1 iteration (c) Results of 3 iteration (d) Results of 5 iteration

Figure 2. Results of arnold transform each iteration

Quantum random phases

Quantum Random Phases indeed creates truly random phases, per the basic principles of quantum mechanics for cryptography technique [19]. Unlike the classic random number generator, these generators produce nonpredictable or reproducible quantum random phase generators due to the stochastic nature of quantum processes like the Superposition and Entanglement [20], [21]. The phases generated in quantum systems allow encoding of information, employing the intrinsic indeterminacy of quantum mechanics for the elaboration of robust barriers to decryption and unauthorized access in full safety [22]. This is one way to enhance protocol encryption security by making use of the singular properties of quantum systems for elaborating appropriate and reliable cryptography solutions. This can be interpreted in quantum mechanics as indeterminacy in the phases generated, mathematically described by quantum state superposition and the action of a unitary operation. For a quantum system, the phase factor ϕ is represented in the context of quantum states as seen in eq (4).

$$| \psi\rangle = e^{i\phi} | \phi\rangle \tag{4}$$

where $| \psi\rangle$ is the quantum state after the phase shift, $| \phi\rangle$ is the base quantum state, and ϕ is the phase shift. Normally, most quantum processes, including the measurement of quantum states in superposition or even the output of quantum interference experiments, apply in order to create truly random phases. In principle, phase randomness relates to quantum uncertainty and the probabilistic nature of quantum mechanics. A commonly used equation in quantum random phase generation can be seen in eq (5).

$$\phi = \frac{arg(U | \phi\rangle)}{N} \tag{5}$$

Where U represents a unitary operator that introduces a phase shift to a quantum state. The phase ϕ is determined by the argument of the resulting quantum state after applying U, denoted as $arg(U | \phi\rangle)$. This phase is uniformly distributed over the interval $[0,2\pi)$, with N serving as the normalization factor to ensure this uniform distribution. The unitary operator U and the resulting phase shift ϕ are key to generating truly random phases used in various quantum cryptographic applications. The encryption process that utilizes a combination of Quantum Random Phase Encoding and Arnold Transform is carried out using eq (6) - (9).

$$M(x,y) = I(x,y) \oplus \Phi(x,y) \tag{6}$$

After applying the Arnold Transform based on eq (1), the pixel values at the new coordinates (x', y') in the transformed image matrix can be seen in eq (7).

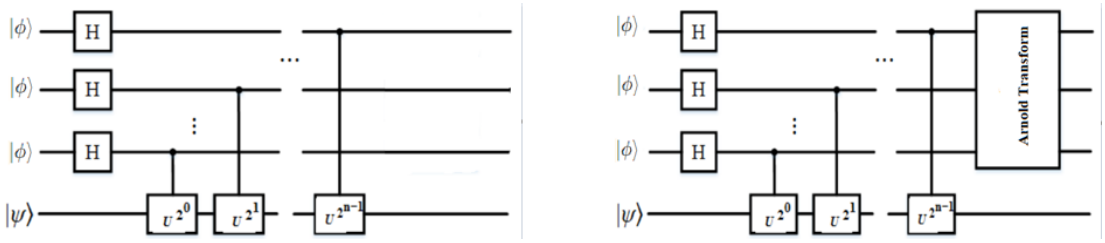
$$I_{encrypted}(x', y') = M(x,y) = I(x,y) \oplus \Phi(x,y) \tag{7}$$

The complete process combines both the embedding of quantum random phases and the Arnold Transform into a single encryption framework. The formula for the encrypted image matrix can be seen in eq (8).

$$I_{encrypted}(x', y') = M(x,y) = (I(x,y) \oplus \Phi(x,y)) \tag{8}$$

where $\oplus$ denotes the XOR operation performed between the pixel value and the phase value, $I_{encrypted}$ represents the final encrypted image matrix where pixel values have been modulated by quantum random phases and then scrambled by the Arnold Transform. So that from the combination of these two methods, the quantum circuit results are obtained as illustrated in Figure 3. where (a) is the quantum circuit before

the integration of the Arnold transform, while (b) is after integrating the quantum random phase into the Arnold transform.



(a) Quantum circuit without embedding Arnold transform

(b) Quantum circuit with embedding Arnold transform

Figure 3. Embedding quantum into arnold transform

RESULTS AND DISCUSSIONS

The study starts with the initialization of the original images, specifically "cameraman," "lena," "mandrill," and "plane," each with a resolution of 512 x 512 pixels. The encryption process is executed with a single iteration of the Arnold Transform, combined with Quantum Random Phase Encoding. The program is run on a Ryzen 7 7800X3D processor with 32 GB RAM and an RTX 3070 Ti GPU. The outcomes of the proposed encryption method are demonstrated in Figure 4, where (a) – (d) shows the plain images, (e) – (h) depicts the encryption result using only Arnold Transform, (i) – (l) demonstrates the proposed encryption combining Arnold Transform with Quantum Random Phase Encoding, and (m) – (p) shows decryption results.

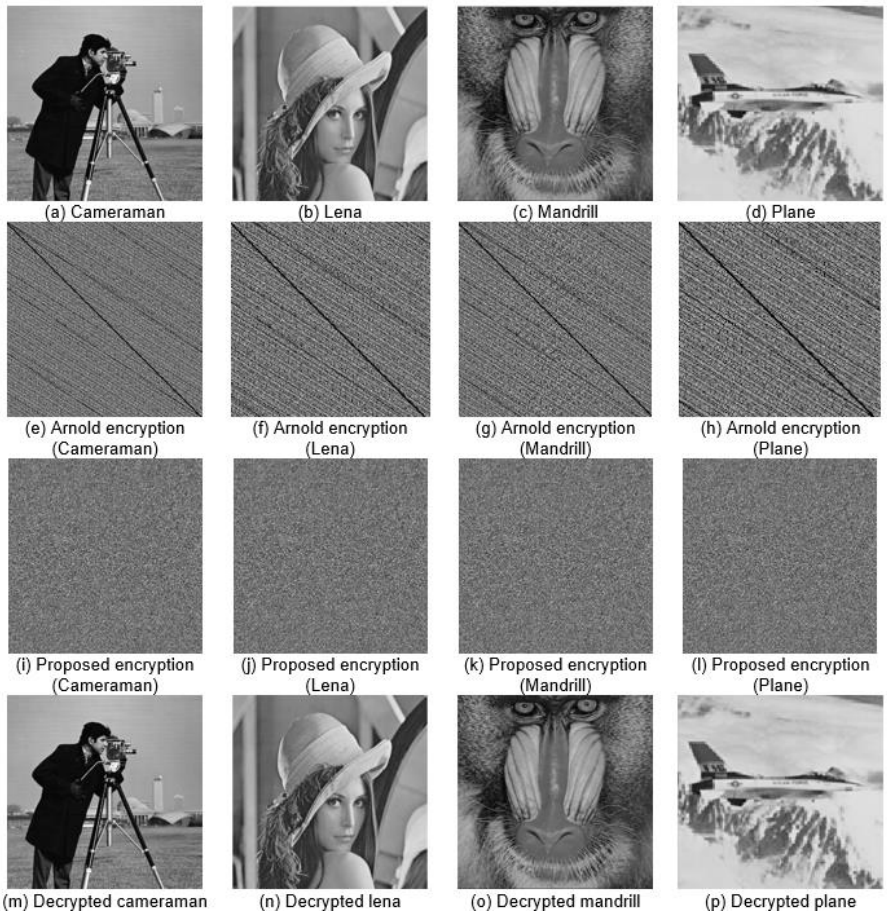


Figure 4. Experiment results each plain image

MSE and PSNR measurement

MSE calculates the average squared deviation between the original image and the modified (or encrypted) image [23]. It quantifies how much the distorted image deviates from the original image. On other hand, PSNR assesses the ratio between the highest possible power of a signal (image) and the power of the noise (error). It is expressed in decibels (dB) [23]. Based on MSE and PSNR Measurement as shown in Table 1.

Table 1. MSE and PSNR Measurement

Encrypted Image	Arnold Transform without Quantum		Arnold Transform with Quantum	
	MSE	PSNR	MSE	PSNR
Cameraman	98.134	21.17 dB	832.01	13.41 dB
Lena	104. 76	23.98 dB	888.78	13.33 dB
Mandrill	81.107	21.34 dB	796.31	14.11 dB
Plane	88.765	19.64 dB	848.73	15.79 dB

UACI and NPCR measurement

UACI measures the average change in intensity for each pixel when a small change is made to the original image [24]. It evaluates how well the encryption algorithm can differentiate between slightly different images, NPCR evaluates the percentage of pixels that alter when a minor modification is applied to the original image [23]. It measures the proportion of pixels that vary between two encrypted images. UACI and NPCR measurements are presented in Table 2.

Table 2. UACI and NPCR measurement

Encrypted Image	Arnold Transform without Quantum		Arnold Transform with Quantum	
	UACI	NPCR	UACI	NPCR
Cameraman	0.3347	99.22	0.3356	99.60
Lena	0.3346	99.28	0.3357	99.60
Mandrill	0.3343	99.26	0.3357	99.61
Plane	0.3343	99.26	0.3358	99.61

Entropy measurement

Entropy is a fundamental concept in information theory used to gauge the randomness or unpredictability of the information contained in an image [23]. The results based on entropy measurements are shown in Table 3.

Table 3. Entropy measurement

Encrypted Image	Arnold Transform without Quantum	Arnold Transform with Quantum
	Entropy	Entropy
Cameraman	7.9998	7.9999
Lena	7.9997	7.9999
Mandrill	7.9998	7.9999
Plane	7.9997	7.9999

Table 4. Comparison results with related reseach

Researcher	Method and Novelty	Tested Image	UACI	NPCR
[25]	Quantum Bit-Plane Scrambling	Cameraman	33.57	99.58
		Plane	33.36	99.60
[26]	Quantum S-Box Scrambling	Cameraman	33.43	99.60
		Lena	33.40	99.60
		Mandrill	33.45	99.60
Our	Quantum Arnold Scrambling	Cameraman	3356	99.60
		Lena	3357	99.60
		Mandrill	3357	99.61
		Plane	3358	99.61

Table 4 presents a comparative analysis of the proposed Quantum Arnold Scrambling method in relation to pertinent research. Prior research has demonstrated favorable outcomes utilizing the Quantum Bit-Plane Scrambling technique as reported by [25] and the Quantum S-Box Scrambling method as mentioned by [26]. These methods have yielded UACI values ranging from 33.4 to 33.6 and NPCR values consistently around 99.58 to 99.60. Our research presents the Quantum Arnold Scrambling technique, showing a notable enhancement in UACI values ranging from 3356 to 3358. Additionally, this method consistently maintains

high NPCR values, which range between 99.60 and 99.61. These findings suggest that our method results in a significant increase in pixel intensity changes, indicating improved encryption effectiveness. At the same time, pixel sensitivity robustness remains consistent based on NPCR analysis.
In the last phase of this study, decryption is carried out as shown in Figure 5. The decryption process using the correct iteration key (a) results in the successful recovery of the original image. The image in Figure (b) demonstrates decrypting with an inaccurate iteration key, resulting in the improper reconstruction of the original image. (c) introduces decryption by slightly adjusting quantum phases, resulting in a modified yet partially recognizable image. In conclusion, section (d) illustrates decryption with inaccurate quantum phases, leading to considerable distortion and an unidentifiable image.

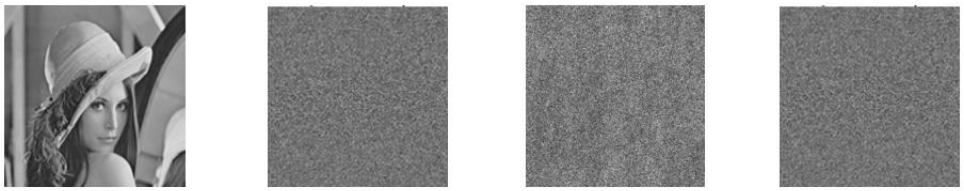

(a) (b) (c) (d)

Figure 5. Decryption phase

CONCLUSION

The integration of Quantum Random Phase Encoding into the Arnold Transform enhances the encryption process, as demonstrated by the enhanced metrics. For MSE and PSNR, the Arnold Transform alone yields MSE values of 98.134 for "Cameraman" and 104.76 for "Lena," with corresponding PSNR values of 21.17 dB and 23.98 dB. When Quantum Random Phase Encoding is employed, the MSE values witness a notable rise, reaching 832.01 for "Cameraman" and 888.78 for "Lena." Concurrently, the PSNR values show a decline to 13.41 dB and 13.33 dB for the corresponding images, signaling enhanced distortion and heightened encryption strength. In Quantum Random Phase Encoding, the UACI value is approximately 0.33, while NPCR ranges between 99.51 and 99.55. This suggests that the method retains its effectiveness in modifying pixels and adapting to alterations. The entropy values for both methods approach their maximum, ranging from 7.9997 to 7.9999, demonstrating a consistent level of randomness. Integrating Quantum Random Phase Encoding with Arnold Transform enhances the security and robustness of the encryption scheme. This is evidenced by the increased effectiveness of encryption and heightened randomness of images. It is recommended that future research be conducted to explore different methods for enhancing the integration of Quantum Random Phase Encoding with the Arnold Transform. Optimizing the Quantum Random Phase Encoding process may necessitate the advancement of more efficient quantum circuits or alternate phase encoding strategies in order to adequately manage the trade-off between computational complexity and encryption strength.

REFERENCES

[1] I. Riadi, A. Fadlil, and F. A. Tsani, "Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher," *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 7, no. 1, pp. 33–45, Jan. 2022, doi: 10.14421/jiska.2022.7.1.33-45.

[2] M. Bedoui, H. Mestiri, B. Bouallegue, B. Hamdi, and M. Machhout, "An improvement of both security and reliability for AES implementations," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, pp. 9844–9851, 2022.

[3] V. Kolate and R. B. Joshi, "An information security using DNA cryptography along with AES algorithm," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 1S, pp. 183–192, 2021.

[4] E. Ndruru and T. Zebua, "Pembangkitan Kunci Beaufort Cipher Dengan Teknik Blum-blum Shub pada Pengamanan Citra Digital," *Bulletin of Information Technology (BIT)*, vol. 3, no. 2, pp. 149–154, Jun. 2022, doi: 10.47065/BIT.V3I2.302.

[5] A. Sujjada and E. Juniar, "IMPLEMENTASI ALGORITMA HILL CIPHER UNTUK PROSES ENKRIPSI DATA MENGGUNAKAN MEDIA CITRA DIGITAL," *Jurnal RESTIKOM : Riset Teknik Informatika dan Komputer*, vol. 3, no. 1, pp. 1–17, Jun. 2021, doi: 10.52005/RESTIKOM.V3I1.76.

[6] N. W. Hidayatulloh, M. Tahir, H. Amalia, N. A. Basyar, A. F. Prianggara, and M. Yasin, "Mengenal Advance Encryption Standard (AES) sebagai Algoritma Kriptografi dalam Mengamankan Data,"

Digital Transformation Technology, vol. 3, no. 1, pp. 1–10, May 2023, doi: 10.47709/DIGITECH.V3I1.2293.
[7] L. Harahap, J. Franky, R. Panggabean, and S. Situmorang, "IMPLEMENTASI METODE KRIPTOGRAFI STREAM CIPHER GIFFORD UNTUK ENKRIPSI INTENSITAS WARNA PIKSEL PADA CITRA DIGITAL RAHASIA," *Jurnal Sains dan Teknologi ISTP*, vol. 15, no. 2, pp. 203–210, Sep. 2021, doi: 10.59637/JSTI.V15I2.94.
[8] M. N. Alenezi, H. Alabdulrazzaq, H. M. Alhatlani, and F. A. Alobaid, "On the performance of AES algorithm variants," *International Journal of Information and Computer Security*, vol. 23, no. 3, pp. 322–337, 2024.
[9] T. A. S. yusri and D. Rudhistiar, "ENKRIPSI CITRA DIGITAL BERBASIS KOMBINASI ARNOLD CAT MAP TERMODIFIKASI DAN DNA ENCODING," *Jurnal Mnemonic*, vol. 5, no. 2, 2022, Accessed: Jul. 13, 2024. [Online]. Available: https://garuda.kemdikbud.go.id/documents/detail/3103383
[10] X. Liu, D. Xiao, and C. Liu, "Three-level quantum image encryption based on Arnold transform and logistic map," *Quantum Inf Process*, vol. 20, no. 1, pp. 1–22, Jan. 2021, doi: 10.1007/S11128-020-02952-7/METRICS.
[11] W. W. Hu, R. G. Zhou, J. Luo, S. X. Jiang, and G. F. Luo, "Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms," *Quantum Inf Process*, vol. 19, no. 3, Mar. 2020, doi: 10.1007/s11128-020-2579-9.
[12] P. Tian and R. Su, "A Novel Virtual Optical Image Encryption Scheme Created by Combining Chaotic S-Box with Double Random Phase Encoding," *Sensors 2022, Vol. 22, Page 5325*, vol. 22, no. 14, p. 5325, Jul. 2022, doi: 10.3390/S22145325.
[13] H. Wang, J. Wang, Y. C. Geng, Y. Song, and J. Q. Liu, "Quantum Image Encryption Based on Iterative Framework of Frequency-Spatial Domain Transforms," *International Journal of Theoretical Physics*, vol. 56, no. 10, pp. 3029–3049, Oct. 2017, doi: 10.1007/s10773-017-3469-5.
[14] J. Wu, Z. Liu, J. Wang, L. Hu, and S. Liu, "A compact image encryption system based on Arnold transformation," *Multimed Tools Appl*, vol. 80, no. 2, pp. 2647–2661, Jan. 2021, doi: 10.1007/S11042-020-09828-Z/METRICS.
[15] J. O'Sullivan *et al.*, "Random-Access Quantum Memory Using Chirped Pulse Phase Encoding," *Phys Rev X*, vol. 12, no. 4, p. 041014, Oct. 2022, doi: 10.1103/PHYSREVX.12.041014/FIGURES/15/MEDIUM.
[16] "Color Image Encryption Scheme Based on Key Dependent S-box and Arnold's Cat Map." [Online]. Available: www.ijert.org
[17] H. Tora, E. Gokcay, M. Turan, and M. Buker, "A generalized Arnold's Cat Map transformation for image scrambling," *Multimed Tools Appl*, vol. 81, no. 22, pp. 31349–31362, 2022.
[18] D. Das and C. Pradhan, "Image Encryption Based on Cyclic Chaos, PRNG and Arnold's Cat Map," in *Proceedings of Data Analytics and Management*, A. Khanna, Z. Polkowski, and O. Castillo, Eds., Singapore: Springer Nature Singapore, 2023, pp. 281–291.
[19] A. Shen *et al.*, "Experimental quantum secret sharing based on phase encoding of coherent states," *Sci China Phys Mech Astron*, vol. 66, no. 6, p. 260311, 2023.
[20] C. Kollmitzer, S. Petscharnig, M. Suda, and M. Mehic, "Quantum random number generation," in *Quantum Random Number Generation*, Springer, 2020, pp. 11–34.
[21] M. P. A. Fisher, V. Khemani, A. Nahum, and S. Vijay, "Random quantum circuits," *Annu Rev Condens Matter Phys*, vol. 14, no. 1, pp. 335–379, 2023.
[22] V. Mannalatha, S. Mishra, and A. Pathak, "A comprehensive review of quantum random number generators: Concepts, classification and the origin of randomness," *Quantum Inf Process*, vol. 22, no. 12, p. 439, 2023.
[23] S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," *Optik (Stuttg)*, vol. 272, p. 170316, 2023.
[24] A. Pathak, H. Mondal, J. Karmakar, S. Pal, D. Nandi, and M. K. Mandal, "Sparse compression-based image encryption using data encryption standards rc5," *IETE Technical Review*, vol. 41, no. 3, pp. 353–365, 2024.
[25] X. Liu, D. Xiao, and C. Liu, "Quantum image encryption algorithm based on bit-plane permutation and sine logistic map," *Quantum Inf Process*, vol. 19, no. 8, Aug. 2020, doi: 10.1007/s11128-020-02739-w.
[26] H. Liu, B. Zhao, and L. Huang, "Quantum image encryption scheme using Arnold transform and S-box scrambling," *Entropy*, vol. 21, no. 4, Apr. 2019, doi: 10.3390/e21040343.