2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT) | 979-8-3503-6908-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICEEICT61591.2024.10718453

QCrypt: Advanced Quantum-based Image Encryption for Secure Satellite Data Transmission

Mohamed Ihsan P.M, Arun Amaithi Rajan*, Vetriselvi V, Gautham Kumar G and Praveen Kumar R

Security Research Laboratory, Department of Computer Science and Engineering
College of Engineering Guindy, Anna University, Chennai, Tamil Nadu, India ihsanpmh@gmail.com,
**arunamaithirajan@gmail.com, kalvivetri@gmail.com, gauthamkumar.ganesan@gmail.com, praveenkr1452@gmail.com*

***Abstract*—With the advancements in satellite communication, there arises a demand for the secure transmission of satellite and remote sensing images to the ground monitoring stations which has significant challenges due to the increased threat of cyber-attacks and the sensitive nature of those images. Existing classical cryptography methods fail to meet the advanced security demands. Thus, there arises a need for advanced cryptography techniques which ensure secure transmission of data in satellite communication. Recent advancements in quantum computing and research have shown that leveraging quantum mechanics and principles enhances security. We propose a novel quantum-based image encryption technique for securing satellite and remote sensing images during transmission named QCrypt. QCrypt utilizes the power of quantum chaotic maps, classic chaotic maps, and DNA encoding techniques to ensure the security of the images. QCrypt has been tested using a remote sensing image dataset and achieved increased performance in terms of resistance to histogram analysis, differential attacks, and chosen- plaintext attacks compared to traditional encryption methods. Our approach addresses the critical need for secure satellite data transmission and the use of quantum-based encryption to meet security demands.**

***Index Terms*—Satellite Communication, Image Security, Quantum Computing, Chaotic Maps, DNA Computing**

I. Introduction

Recent advancements in space science, space technologies, and network communication have attracted many researchers and industry experts because of the wide range of applications that can be drawn out from remotely sensed data [1]. Remote sensing refers to the way of acquiring information about objects, planetary bodies (like Earth), or phenomena from a distance without making physical contact. This can be achieved via remote sensors aboard satellites, aircraft, or even drones. Satellite images being one of the common products of remote sensing are used in a wide range of areas from weather monitoring, urban planning, and disaster management to charting armed force emplacements, assessing geopolitical developments, and intelligence gathering [2]. In some cases, a space-borne system like a satellite collects or senses data and transmits it to the ground station. In the ground segments, several image products might be created for storage or transmission for further analysis and commercial purposes. In some other cases, the Earth Observing Satellites might transmit images to the station or to other satellites. Over the past, the commercial space growth of this remote sensing industry has been so high that it even complements government-based systems for national security missions.

Several national security organizations have realized the need for security in this classified real-time intelligence information available in the form of satellite imagery. Unclassified commercial satellites promote the need for greater security and accountability. With these images acting as powerful tools for a nation’s critical infrastructure protection [3], securing its communication is essential. Therefore, several methods for secure satellite imagery have been proposed like Elliptic Curve Cryptography for encryption with the ECDH used for key exchange [4]. There are also methods for improved efficiency using MapReduce jobs for concurrent encryption as proposed in [5] for transit as well as storage. But all these strategies are within the classical encryption scheme where the hardness of cracking the algorithm lies in solving an underlying mathematical problem though it’s highly difficult. Introducing quantum image encryption will take advantage of fundamental principles of quantum mechanics to achieve unparalleled security. Figure 1 shows the general flow of secure satellite data communication.

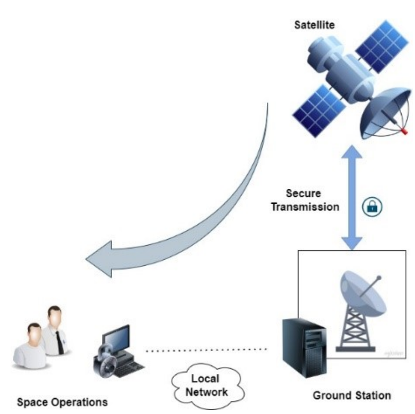


Fig. 1: Secure Satellite Communication Flow

Recently DNA encoding and chaos have attracted much attention in encryption methods. Minimum power consumption, good storage capacity, and massive parallelism for high speed in encryption are a few advantages of DNA computing using several DNA operation rules, whereas chaotic maps are known for their pseudo randomness and long-term unpredictability of orbits. Further high dimensional chaotic maps produce highly complex random sequences [6]. Attention gradually shifted to the use of quantum chaos which has high sensitivity to initial parameters resulting in larger key space and high complexity. Using such maps in combination with classical chaotic maps to dynamically select DNA rules has achieved a significant effect in encryption [7]. However, after proper cryptanalysis, it's clear that further improvements can be made due to the existence of equivalent keys.

Hence, in this work, we introduced a new encryption technique for satellite images, QCrypt, integrating pixel permutation, quantum, and classical chaotic maps, with DNA encoding techniques. The major contributions to the article are outlined below.

1) An image encryption scheme, QCrypt is proposed for secure satellite image sharing using pixel permutations, hybrid chaos, and DNA encoding.
2) Utilized the pixel permutation to achieve a good diffusion rate and used different DNA encoding techniques and operations to obtain better pixel substitutions in the confusion region.
3) For the secret both quantum chaotic maps and Lorenz maps are leveraged to introduce more randomness.
4) QCrypt has validated using the MRLSNet Remote Sensing Image dataset and shown that the scheme is secure and attack-resistant with multiple statistical analyses.

The remaining paper is structured as follows: section 2 briefing the existing and related works in this area. The building blocks of this encryption scheme are explained in section 3 followed by a detailed working of the proposed method in section 4. Section 5 shows the results, analysis, and comparison of the discussed encryption scheme and the paper ends with Section 6 drawing a conclusion.

II. Related Work

The existing image encryption algorithms and their evolution are discussed in this section. Classical image encryption has two primary categories: spatial and transform [8]. There are increasingly interesting algorithms utilizing DNA encoding, cellular automata, metaheuristics, chaotic maps, fuzzy logic, and more in the spatial domain. More algorithms exist in the medical domain. Satellite Image transmission is also one of the most important services, that requires this kind of secure and confidential image-sharing technique. Very recently, SaberiKamarposhti et al. [9] offers a detailed exploration of the encryption techniques applicable, along with suggestions for future research directions.

Encryption techniques like ChannelEnc, SequenceEnc, and PositionEnc are used to protect both the color and texture information of images. The confidentiality and integrity of sensitive remote sensing images are ensured by using quantum encryption methods. This approach safeguards the images during storage and transmission, making it particularly relevant where data privacy and security are important [10]. Other quantum image encryption can be based on a chaotic-based parallel keyed hash function that utilizes chaotic maps to create hash values and utilizes 'TCM' which refers to a combination of two chaotic maps, namely the Tent and Chebyshev chaotic maps [11]. Chaotic maps are nonlinear mathematical functions used in encryption to generate pseudo-random sequences. Combining different chaotic maps can enhance the complexity and unpredictability of the generated sequences, thereby im- proving the security of the encryption process [12]. Another approach can utilize adaptive DNA code bases, which may in- volve encoding data based on DNA sequences. This approach also introduces a new multi-chaotic map architecture, which combines Henon, Gaussian, and Logistic maps which are employed to generate more chaotic pseudo-random sequences for encryption [13].

However, all these techniques are classical cryptography-based, and these are quickly compromised by quantum computing. So, we require a quantum-based image encryption algorithm. Recently, Amaithi Rajan et al. [14] proposed a new technique QMedShield, based on quantum operations and chaotic maps to secure medical images in the cloud. Based on the insights from the literature analysis, integrating quantum chaotic maps, pixel scrambling, and DNA encoding could increase image encryption security and privacy. In line with these findings, we designed a novel image encryption model for satellite image transmission. Table 1 shows how our model differs from existing models. PP refers to the Pixel Permutation.

TABLE I: Methods: Comparative Analysis

Year	**Ref**	**Chaotic Map**		**DNA Enc**	**PP**	**Sat. Images**
		Classic	**Quantum**			
2022	[15]	✓				✓
2023	[6]	✓		✓		
2024	[14]	✓	✓	✓		
2024	QCrypt	✓	✓	✓	✓	✓

III. Technical Background

This section details the basic concepts used in the proposed encryption scheme. It covers topics such as pixel scrambling, different chaotic maps, and DNA encoding.

A. Pixel Permutation

Pixel permutation refers to the process of rearranging the pixels of an image such that the spatial relationship among the pixels is altered. This transformation is typically defined by a permutation function or a permutation key, which dictates the new positions of the pixels. This operation helps to improve the diffusion rate of the pixels.

B. Chaotic Maps

Chaotic maps explore the behaviors of dynamic systems that often express non-linear randomness. They are categorized into two types: classical and quantum maps. They are too sensitive to initial conditions. We use a 1D Tent map, a 3D Lorenz chaotic map, and a 3D quantum logistic map in the proposed encryption model.

1) *Tent Map:* This map is a piecewise linear, 1D map with chaotic dynamics on the range [0,1] [16]. It is mathematically written as

$$\tau_{k+1} = \begin{cases} r\tau_k, & if\ \tau_k < 0.5 \\ r(1-\tau_k), & if\ \tau_k \geq 0.5 \end{cases} \quad (1)$$

Where τ_0 is the initial parameter $\tau_0 \in [0,1]$ and the control parameter r, $r \in [0,2]$. The bifurcation diagram of the tent map is shown in Figure 2.

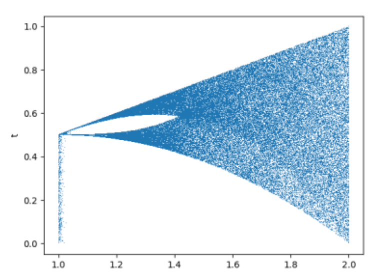


Fig. 2. Tent Map - Bifurcation diagram

2) *Lorenz Chaotic Map:* The Lorenz is a three-dimension chaotic dynamic map [17]. Equations 2-4 below can be used to characterize the system.

$$\dot{x} = \vartheta(y - x) \quad (2)$$
$$\dot{y} = x(\kappa - z) - y \quad (3)$$
$$\dot{z} = xy - \xi z \quad (4)$$

x_0, y_0, z_0 are the initial values and ϑ, κ, ξ are the control parameters. When the precise value of chaos is fixed, the system generates chaotic sequences. The proposed image encryption algorithm used a system of equations that displayed chaotic behavior for the $\vartheta = 10$, $\kappa = 28$, and $\xi = 8/3$. Figure 3 illustrates the attractor produced using an employed 3D Lorenz chaotic map. Because of its higher rate of pseudo-randomness and unpredictability, secret keys are generated from this map.

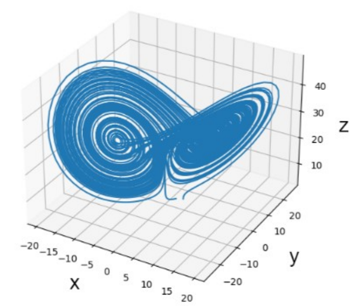


Fig. 3. 3D Lorenz map - Bifurcation diagram

C. Quantum Logistic Chaotic Map:

The quantum variant of the map shows unique quantum characteristics, having interference, and entanglement, stemming from its quantum nature [14]. More research involves leveraging the system for quantum-based cryptography, utilizing its chaotic dynamics to generate secure keys. The 3D quantum logistic chaotic system is represented by equations 5-7.

$$x_{n+1} = \Psi(x_n - |x_n|^2) - \Psi y_n \quad (5)$$

$$y_{n+1} = -y_n e^{-2\beta} + e^{-\beta}\Psi[(2 - x_n - x_n^*)y_n - x_n z_n^* - x_n^* z_n] \quad (6)$$

$$z_{n+1} = -z_n e^{-2\beta} + e^{-\beta}\Psi[2(1 - x_n^*)z_n - 2x_n y_n - x_n] \quad (7)$$

In this equation, β is the dissipation parameter, Ψ is the control parameter, and x_n^*, y_n^* represent the complex conjugates of x_n, y_n. The state of equations is chaotic when $\Psi = 4$, $x_n \in (0,1]$, $y_n \in (0,0.1]$, $z_n \in (0,0.2]$, $\beta \in [6, +\infty]$. Figure 4 shows the bifurcation diagram of the quantum logistic map.

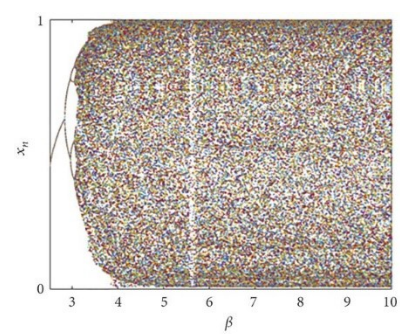


Fig. 4: Quantum Logistic Map - Bifurcation diagram

D. DNA encoding

TABLE II. DNA Encoding Rules

Rule	i	ii	iii	iv	iv	vi	vii	viii
A	00	00	01	01	10	10	11	11
C	01	10	00	11	00	11	01	10
G	11	11	10	10	01	01	00	00
T	10	01	11	00	11	00	10	01

This technique utilizes the unique properties of DNA molecules, such as their high storage capacity and stability, for data storage and computation [18]. A DNA sequence can be generated from binary data, and Table 2 lists 8 DNA encoding techniques. Arithmetic operations can also be executed on DNA-encoded data, with the truth table of the DNA Addition operation shown in Table 3.

TABLE III. DNA Addition truth_table

+	**A**	**G**	**T**	**C**
T	T	A	C	G
G	G	C	A	T
A	A	G	T	C
C	C	T	G	A

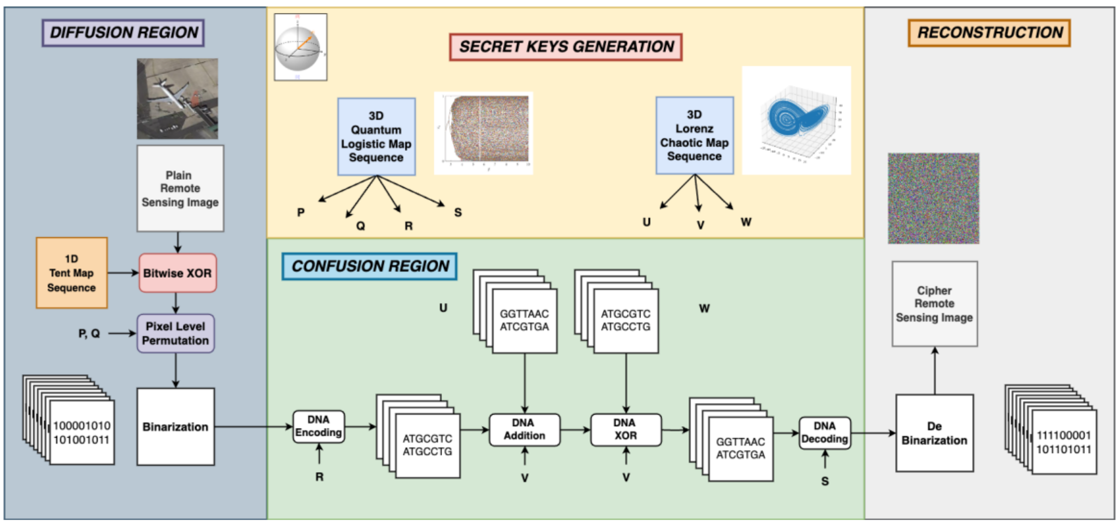


Fig. 5. Flow Diagram of the Image Encryption

IV. Proposed Encryption Scheme

The proposed QCrypt: a Quantum-based image encryption model for secure satellite communication, is explained in this module. The detailed encryption flow is shown in Figure 5. Key Management Centre (KMC) generates the keys to share with users.

Shannon's permutation-diffusion model is the base for this encryption model. QCrypt has 4 regions to be processed. Secret key generation region which utilizes both classical and quantum-based chaotic maps to generate pseudo-random sequences P, Q, R, S, U, V, W. In the diffusion region, the original image $RS(I_1)$ is bitwise XOR with a 1D tent map sequence to resist the CP attack and produces I_2. Both column and row-wise pixels of I_2 are permuted using the P, Q sequences. This permuted sequence is converted to binary matrix I_3. As shown in DNA encoding rules in Table 2, I_3 is converted into DNA encoded data with key sequence R and produces I_4. By applying the same random sequence R, both U and W matrices are DNA encoded. They are named I_5, I_7 accordingly. I_4 is added with I_5 and obtained I_6. Then the I_6 is DNA XOR with I_7 to obtain I_8. So, the entire pixel substitution in the confusion region is done in the domain of DNA-encoded data. Using S, I_8 is decoded into binary matrix I_9. Finally, in the reconstruction region I_9 is converted into cipher image $I_{10} = CRS$.

Algorithm 1 shows all the steps in detail. The secureness of the algorithm lies in the generated pseudo-random sequences based on chaotic maps. It is because of the non-linear nature of the chaotic maps. The DNA substitution also brings more confusion in the encryption model. The XOR with Tent map sequence is done to prevent CP attacks in the image encryption models. Pixel permutation beings excess diffusion in the model.

Algorithm 1: QCrypt Image Encryption

1: Convert Remote Sensing Image RS into $\mathcal{W} \times \mathcal{H}$ matrix I_1

Lorenz Chaotic Sequence Generation:

2: Generate pseudo-random sequences U, V, W using Equations 2-4

Quantum Chaotic Sequence Generation:

3: Generate pseudo-random sequences P, Q, R, S using Equations 5-7

Scrambling and Binary Conversion:

4: Bitwise XOR image pixels with Tent map sequence and obtain matrix I_2

5: Permute the pixels of I_2 and convert into binary matrix I_3

DNA Encoding:

6: Select encoding rules based on R, encode I_3 to get DNA matrix I_4

7: Use R to choose DNA encoding rules, encode U and get DNA matrix I_5

8: Use R to choose DNA encoding rules, encode W and get DNA matrix I_7

DNA Operations:

9: Select addition rules based on V, add I_4, I_5 to obtain DNA matrix I_6

10: Select XOR rules based on V, XOR I_6 and I_7 to obtain DNA matrix I_8

DNA Decoding:

11: Use S to choose DNA decoding rules, decode I_8 to get binary matrix I_9

12: Convert I_9 into decimal matrix $I_{10} = CRS$

13: return encrypted remote sensing image CRS

V. Experimental Results and Analysis

This section is for analyzing the proposed encryption algorithm QCrypt. We have detailed the experimental setup, including the dataset used for analysis, and demonstrated different experimental results accordingly. This adds analyses such as key security analysis, analyses of resistance to statistical attack, chosen plaintext, and differential attacks.

A. Experimental Setup and Dataset

The designed scheme has been implemented on a system with an Intel Xeon processor, 64 GB RAM, 16 GB of memory with an NVIDIA Quadro P5000 GPU, and a 64- bit Windows operating system. Python OpenCV libraries and Qiskit have been used in the development of the entire scheme. To experiment and evaluate the proposed algorithm, three different remote sensing images are chosen from the MLRSNet dataset. This is a multi-label high spatial resolution remote sensing dataset for semantic scene understanding. It contains 109,161 remote sensing images that are annotated into 46 scene categories and 60 predefined class labels. Throughout the section, 3 sample remote sensing images, airport RS_1, airplane RS_2, and stadium RS_3 are taken to show the performance comparison. Figure 6 shows the selected sample remote sensing images and their corresponding encrypted images.

B. Key Sensitivity Analysis

The encryption algorithm has to be sensitive to the key. Even slight changes to the key should result in an entirely different cipher image. The proposed QCrypt demonstrates a high level of sensitivity to the key. The original remote sensing image RS_2 is encrypted with initialization values for quantum logistic chaotic map $x_0 = 0.4$, $y_0 = 0.03$, and $z_0 = 0.01$. If we utilize the same initial values while decrypting, we will get the exact original remote sensing image RS_2. If y_0 is given as 0.003, we get entirely different cipher image. It shows that even a minor modification can have a significant impact.

C. Chosen Plaintext Attack Analysis

To diffuse pixel values effectively, QCrypt employs an XOR operation, while Equation 11 is used to assess its resistance against chosen-plaintext attack. If equation 8 is fulfilled, then the CP attack is possible. The proposed method offers protection against such attacks, as demonstrated in Figure 7, where equation 8 is unjustified.

$$RS_m(i,j) \oplus RS_n(i,j) = CRS_m(i,j) \oplus CRS_n(i,j) \qquad (8)$$

D. Histogram Analysis

The statistical properties of the image are observed via the histogram. A uniform distribution results in a flat histogram, indicating that pixel values are nearly equal throughout the image. The histograms of sample plain images are shown in Figure 8 (a-c). The corresponding image's encrypted image histograms are shown in Figure 8 (d-f). This test reveals how pixel value distribution in the original image can be effectively hidden by the cipher image which secures the image from statistical attacks.

E. Chi-Square Test

The chi-square (χ^2) test is used to evaluate the evenness of the histogram by utilizing Equation 9.

$$\chi^2 = \Sigma_{n=0}^{255} \frac{(O_n - E_n)^2}{E_n} \qquad (9)$$

A critical value denoted as $\chi^2(255{,}0.05) = 293$. If the χ^2 value is lower than 293, it is concluded that the null hypothesis (Pixels are evenly distributed) is valid. Table 4 shows the χ^2 values of the sample images.

TABLE IV. χ^2 Test

Image	χ^2 **Value**	**Critical Value**	**Decision (H=0)**
RS_1	255.33	293	Pass
RS_2	268.64	293	Pass
RS_3	284.97	293	Pass

F. Entropy Analysis

The unpredictability of image information is characterized by entropy $\mathcal{E}$ which is computed using Equation 10.

$$\mathcal{E} = -\Sigma_{n=1}^{255} p_n log(p_n) \quad (10)$$

The probability of occurrence of pixel value n is denoted by p_n. The value of $\mathcal{E} \in [0,8]$. For an 8-bit image, the $\mathcal{E}$ value should be close to 8. Table 5 shows the $\mathcal{E}$ values of the sample images.

TABLE V. ENTROPY ANALYSIS

	$\mathcal{E}$ **Value**	
Image	Original	Encrypted
RS_1	6.3374	7.6471
RS_2	6.0556	7.6466
RS_3	6.4199	7.6420

G. Differential Attack Analysis

The sensitivity of the encryption technique to even minor changes in the plain image is evaluated using the differential attack. The Number of Pixel Change Rate (NPCR) and Unified Average Change in Intensity (UACI) are the two performance measures to assess the proposed technique's resistance to differential attacks. NPCR is employed to evaluate the resistance to differential attack and it should be close to 100. NPCR is evaluated using the following Equations 11 and 12.

$$NPCR = \frac{\Sigma_{i,j} Pix\_Diff(i,j)}{\mathcal{WT} \times \mathcal{HT}} \times 100\% \quad (11)$$

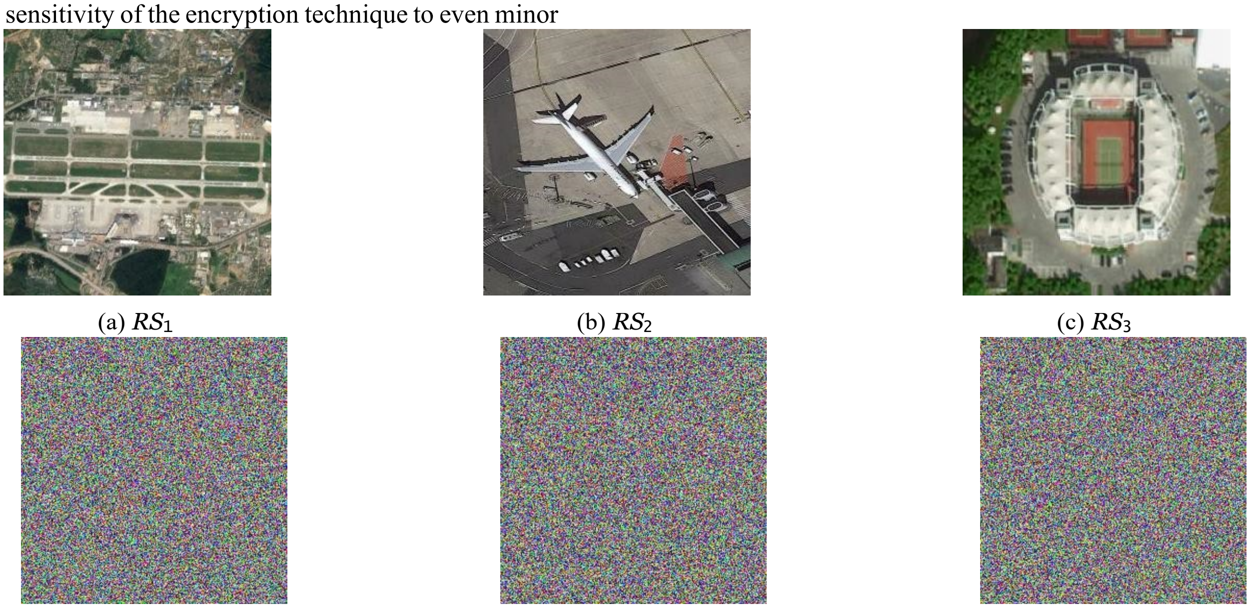
Here,

$$Pix\_Diff(i,j) = \begin{cases} 1, & \text{if } RS(i,j) \text{ equals } CRS(i,j) \\ 0, & \text{if } RS(i,j) \text{ not equals } CRS(i,j) \end{cases} \quad (12)$$

The Unified Average Changing Intensity (UACI), measures the average disparity in pixel intensity between the original and encrypted images. This metric is frequently leveraged to show resilience against a differential attack. An ideal UACI value is around 33%, evaluated using Equation 13.

$$UACI = \frac{\Sigma_{i,j} RS(i,j) - CRS(i,j)}{255 \times \mathcal{WT} \times \mathcal{HT}} \times 100\% \quad (13)$$

Table 6 shows the NPCR and UACI of the sample remote sensing images and proves the withstanding power of the proposed encryption model.



(a) RS_1 (b) RS_2 (c) RS_3

(d) Encrypted RS_1 (e) Encrypted RS_2 (f) Encrypted RS_3

Fig. 6: Selected sample plain remote sensing images and the corresponding encrypted cipher images

(a) $RS_m(i,j) \oplus RS_n(i,j)$ (b) $CRS_m(i,j) \oplus CRS_n(i,j)$

Fig. 7: Chosen Plaintext Attack Analysis

H. Error Metrics

RMSE and PSNR are the standard error metrics to assess whether the encryption scheme produces fewer errors. MSE is useful for comparing exact pixel values between an original image and an encrypted image. In order to provide more precise and reliable data, RMSE evaluates the MSE root. Equations 14 and 15 can be used to calculate these measures. The range of RMSE $\in [0,\infty]$.

$$MSE = \frac{1}{\mathcal{WT}\times\mathcal{HT}} \Sigma_{i,j}\big(CRS(i,j) - RS(i,j)\big)^2 \qquad (14)$$

$$RMSE = \sqrt{MSE} \qquad (15)$$

PSNR is used as a quality measurement between the original and decrypted images and is measured in decibels (dB). PSNR is calculated as follows in Equation 16.

$$PSNR = 10log_{10}\frac{(2^k-1)^2}{MSE} \qquad (16)$$

where k represents the number of bits per pixel. Table 6 shows the error metrics of the sample remote sensing images.

I. Pixel Correlation Analysis

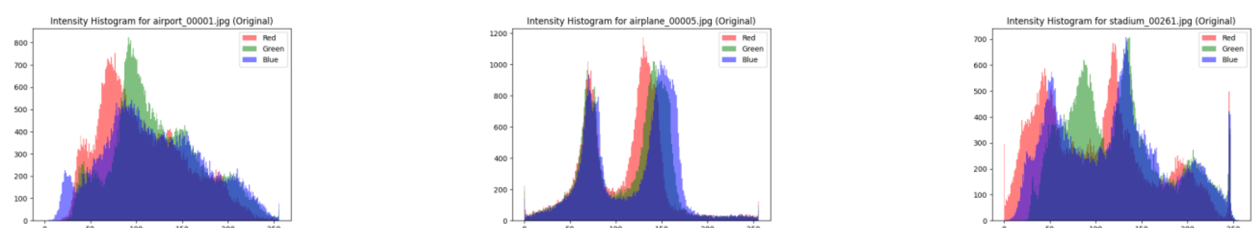
In image encryption, horizontal, vertical, and diagonal correlation analyses the statistical relationships between pixels along different directions within the encrypted image. By analyzing correlation patterns in 3 directions, encryption researchers could identify vulnerabilities and optimize algorithms to enhance security and preserve image quality. Equation 17 can be used to get the correlation coefficient of an image in any of direction.

$$\rho_{xy} = \frac{Cov(x,y)}{D(x)D(y)} \qquad (17)$$

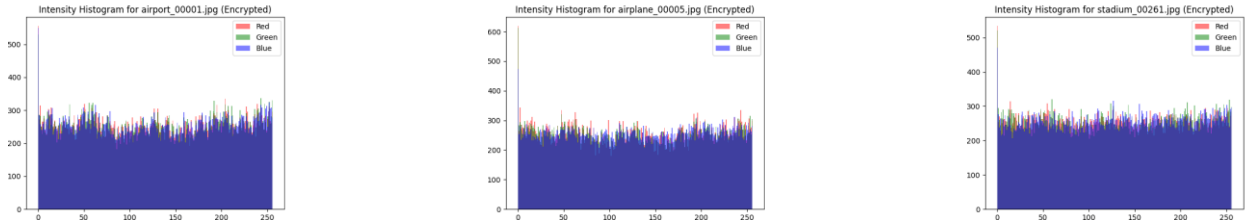
The sub-figures 9 (a-f) show the correlation in Horizontal, Vertical, and Diagonal directions of the plain and encrypted images of selected remote sensing image samples. The correlation coefficients for all 3 directions are presented in Table 7, showing the statistical attack resistance of the proposed encryption scheme.

TABLE VI. ERROR METRICS AND DIFFERENTIAL ATTACK ANALYSIS

Image	**RMSE**	**PSNR(dB)**	**NPCR**	**UACI**
RS_1	90.85	8.96	99.61	33.18
RS_2	88.59	9.18	99.62	33.21
RS_3	95.79	8.50	99.62	33.34

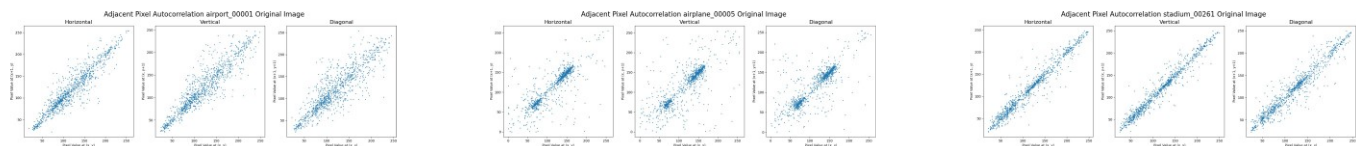


(a) Original (RS_1) (b) Original (RS_2) (c) Original (RS_3)

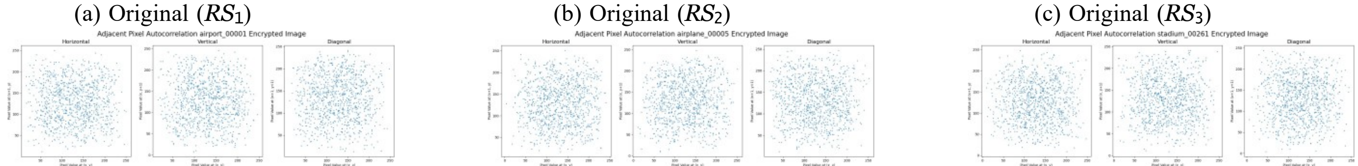


(d) Encrypted (RS_1) (e) Encrypted (RS_2) (f) Encrypted (RS_3)

Fig. 8: Histogram Analysis of sample remote sensing images



(a) Original (RS_1) (b) Original (RS_2) (c) Original (RS_3)



(d) Encrypted (RS_1) (e) Encrypted (RS_2) (f) Encrypted (RS_3)

Fig. 9: Correlation Analysis of sample remote sensing images

TABLE VII: Correlation Analysis

	Horizontal Correlation		**Vertical Correlation**		**Diagonal Correlation**	
Image	Original	Encrypted	Original	Encrypted	Original	Encrypted
RS_1	0.8649	-0.0038	0.9301	-0.0012	0.9124	0.0158
RS_2	0.6635	0.0048	0.7977	0.0058	0.8401	-0.0295
RS_3	0.9723	0.0062	0.9557	-0.0006	0.9715	0.0309

J. Comparative Security Analysis

The proposed QCrypt is compared with other existing remote sensing image encryption models. We have taken correlation coefficients, NPCR, and UACI to compare our proposed method with existing encryption models. Table 8 shows the better correlations and UACI of the proposed model. Thus, the proposed QCrypt yields an improved UACI value, and reduces the correlation coefficient among the pixels in the encrypted image. An improved UACI value indicates that the QCrypt is enhancing image security. A reduction in correlation coefficients is making it more complex for adversaries to attack and get the original image. Figure 10 illustrates the comparative analysis.

TABLE VIII: ENCRYPTION MODEL PERFORMANCE: COMPARATIVE ANALYSIS

Reference	**HCorr**	**VCorr**	**Dcorr**	**NPCR**	**UACI**
Zhang et al. [19]	-0.0047	0.0025	0.0014	99.62	33.38
Liu et al. [20]	0.0180	0.0159	0.0066	99.61	33.45
Nan et al. [15]	-0.0009	-0.0005	0.0029	99.61	33.46
QCrypt (Ours)	**0.0023**	**-0.0004**	**-0.0090**	**99.60**	**33.63**

VI. CONCLUSION AND FUTURE WORKS

In this article, we proposed a novel image encryption model for satellite images in the transmission to the ground station. The model utilizes quantum chaotic maps, and classic 1D, 3D chaotic

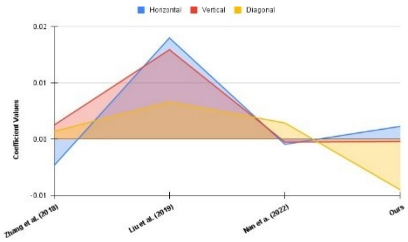


Fig. 10: Performance: Comparative Analysis

maps for secret sequence generation. DNA encoding has been used for pixel substitution and pixel scrambling has also been done in the diffusion phase. The model has been experimented with and compared with existing models, proving its strength against attacks. In the future, more quantum-based random numbers can be used for image encryption schemes.

References

[1] Y. Chen, F. Wang, L. Lu, and S. Xiong, "Unsupervised Transformer Balanced Hashing for Multispectral Remote Sensing Image Retrieval," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 16, pp. 7089–7099, 2023.

[2] K. Ding, Z. Yang, Y. Wang, and Y. Liu, "An improved perceptual hash algorithm based on U-net for the authentication of high-resolution remote sensing image," *Applied Sciences (Switzerland)*, vol. 9, no. 15, 2019.

[3] A. M, D. M, A. Amaithi Rajan, V. V, and H. D, "EdgeShield: Attack resistant secure and privacy-aware remote sensing image retrieval system for military and geological applications using edge computing," *Earth Science Informatics*, 2024.

[4] A. A. Ghaleb, S. Sasi, and A. R. Aswatha, "Design and implementation of satellite image encryption by using ecc," in *2018 3rd IEEE Inter-national Conference on Recent Trends in Electronics, Information and Communication Technology (RTEICT)*, 2018, pp. 1438–1443.

[5] M. A. S. Al-Khasawneh, M. Faheem, E. A. Aldhahri, A. Alzahrani, and A. A. Alarood, "A mapreduce based approach for secure batch satellite image encryption," *IEEE Access*, vol. 11, pp. 62 865–62 878, 2023.

[6] A. Amaithi Rajan, V. Vetrian, and A. Gladys, "Secure Image Encryption Model for Cloud-Based Healthcare Storage Using Hyperchaos and DNA Encoding," 2023, pp. 89–103. [Online]. Available: https://link.springer.com/10.1007/978-3-031-38296-3 8_

[7] J. Zhang and D. Huo, "Image encryption algorithm based on quantum chaotic map and dna coding," *Multimedia Tools and Applications*, vol. 78, no. 11, pp. 15 605–15 621, Jun 2019. [Online]. Available: https://doi.org/10.1007/s11042-018-6973-6

[8] M. Kaur and V. Kumar, "A Comprehensive Review on Image Encryption Techniques," *Archives of Computational Methods in Engineering*, vol. 27, no. 1, pp. 15–43, 2020. [Online]. Available: https://doi.org/10.1007/s11831-018-9298-8

[9] M. SaberiKamarposhti, A. Ghorbani, and M. Yadollahi, "A comprehensive survey on image encryption: Taxonomy, challenges, and future directions," *Chaos, Solitons and Fractals*, vol. 178, p. 114361, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0960077923012638

[10] B. Abd-El-Atty, M. A. El-Affendi, S. A. Chelloug, and A. A. Abd El- Latif, "Double medical image cryptosystem based on quantum walk," *IEEE Access*, vol. 11, pp. 69 164–69 176, 2023.

[11] R. Ismail Abdelfatah, "Quantum image encryption using a self-adaptive hash function-controlled chaotic map (sahf-ccm)," *IEEE Access*, vol. 10, pp. 107 152–107 169, 2022.

[12] W. Bao and C. Zhu, "A secure and robust image encryption algorithm based on compressive sensing and DNA coding," 2022.

[13] R. I. Abdelfatah, H. M. Saqr, and M. E. Nasr, "An efficient medical image encryption scheme for (wban) based on adaptive dna and modern multi chaotic map," *Multimedia Tools and Applications*, vol. 82, no. 14, pp. 22 213–22 227, Jun 2023. [Online]. Available: https://doi.org/10.1007/s11042-022-13343-8

[14] A. A. Rajan and V. V, "Qmedshield: A novel quantum chaos-based image encryption scheme for secure medical image storage in the cloud," 2024.

[15] S. x. Nan, X. f. Feng, Y. f. Wu, and H. Zhang, "Remote sensing image compression and encryption based on block compressive sensing and 2D-LCCCM," *Nonlinear Dynamics*, vol. 108, no. 3, pp. 2705–2729, 5 2022.

[16] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 1 2017.

[17] Y. Zhang, Y. He, J. Zhang, and X. Liu, "Multiple Digital Image Encryption Algorithm Based on Chaos Algorithm," *Mobile Networks and Applications*, 2022.

[18] J. Du, Z. Zhao, S. Li, B. Lu, and J. Zhang, "A novel image encryption algorithm based on hyperchaotic system with cross-feedback structure and diffusive DNA coding operations," *Nonlinear Dynamics*, 2024.

[19] X. Zhang and X. Wang, "Remote-sensing image encryption algorithm using the advanced encryption standard," *Applied Sciences (Switzer-land)*, vol. 8, no. 9, 9 2018.

[20] H. Liu, B. Zhao, and L. Huang, "A Remote-Sensing Image Encryption Scheme Using DNA Bases Probability and Two-Dimensional Logistic Map," *IEEE Access*, vol. 7, pp. 65 450–65 459, 2019.