A Secure Chaotic DNA-Based Framework for Satellite Image Encryption

Asim Seedahmed Ali Osman[1]*, Ibrahim Rizqallah Alzahrani[2],
Aeshah Khalil I Alotaibi[3], Adil Mahmoud Mohamed Mahmoud[4], Daifallah Zaid Alotaibe[5]
Department of Software Engineering-College of Computer Science & Engineering,
University of Hafr Al Batin, Kingdom of Saudi Arabia[1]
Department of Computer Science and Engineering-College of Computer Science and Engineering,
University of Hafr Al Batin Kingdom of Saudi Arabia[2]
Department of Computer Science-College of Computer and Information Sciences, Jouf University, Kingdom of Saudi Arabia[3]
Faculty of Computer Science and Information Technology, White Nile University, Kosti, White Nile, Sudan[4]
Department of Software Engineering-College of Computer Science & Engineering,
University of Hafr Al Batin, Kingdom of Saudi Arabia[5]

***Abstract*—With the growing use of satellite imaging in environmental monitoring, defense, and remote sensing applications, protecting satellite images during storage and transmission has become increasingly important. Unlike textual data, satellite images contain high spatial redundancy and strong correlations among neighboring pixels, which can limit the effectiveness of conventional encryption methods when applied directly. To address this issue, this study presents a chaotic DNA-based framework for satellite image encryption. The proposed approach combines logistic-map-based chaotic key generation with DNA-inspired encoding and XOR operations to enhance pixel-level confusion and diffusion. The method was evaluated on a grayscale satellite image using common statistical security measures, including information entropy, adjacent-pixel correlation, NPCR, and UACI. The reported results indicate that the encrypted image achieved high entropy, low correlation between adjacent pixels, and strong sensitivity to small changes in the input image. These findings suggest that the proposed framework provides a reasonable basis for secure satellite image encryption. Although the current evaluation is limited in scope, the method shows encouraging performance and offers a useful direction for further investigation on larger and more diverse satellite image datasets.**

Keywords*—Chaotic cryptography; DNA computing; satellite image security; image encryption; information security; secure image transmission

I. Introduction

Satellite images have become an essential resource in many fields, including environmental monitoring, disaster response, military reconnaissance, and urban planning [15]. As satellite sensing technologies continue to advance, both the volume and resolution of captured images have increased significantly. This rapid growth has created a corresponding need for secure storage and transmission mechanisms to protect sensitive image data [17] from unauthorized *access* and misuse [1],[19]. Although conventional encryption algorithms such as AES and RSA provide strong security for general digital data [22], they are not always well suited to the structural characteristics of image data, particularly the high spatial redundancy and strong correlation among adjacent pixels. For this reason, their direct application to large image datasets may lead to practical limitations in efficiency and performance in some image-encryption settings [2, 12].

To address these limitations, chaos-based encryption methods have received considerable attention because of their sensitivity to initial conditions, nonlinear dynamic behavior, and ability to generate pseudo-random sequences. These characteristics make chaotic systems attractive for designing image-encryption schemes that require high unpredictability and strong key sensitivity [3],[24],[25]. In parallel, DNA-based cryptographic techniques have emerged as a promising approach for image protection by representing binary data using nucleotide symbols such as A, C, G, and T and performing logical operations in this encoded form. This representation can improve the confusion and diffusion properties of the encryption process, thereby enhancing the overall complexity of the protected image data [1],[4],[5].

Recent studies have explored the integration of chaotic systems with DNA-inspired operations for image encryption. Such approaches have shown encouraging results in terms of statistical security indicators, including improved entropy and reduced correlation among neighboring pixels in encrypted images [4],[5],[23]. However, the effectiveness of these methods still depends on several important factors, including the clarity of the encryption procedure, the reliability of the key-generation mechanism, and the scope of the experimental validation used to support the reported security claims.

Motivated by these considerations, this study presents a chaotic DNA-based framework for satellite image encryption. The proposed approach combines logistic-map-based chaotic key generation with DNA-inspired encoding and XOR operations to strengthen pixel-level transformation during the encryption process. In the current study, the framework is examined as a proof-of-concept for grayscale satellite image encryption. The main contributions of this work can be summarized as follows:

- A chaotic DNA-based framework for satellite image encryption.

- A logistic-map-driven key-generation process for generating encryption sequences.
- The use of DNA-inspired encoding and XOR-based operations to enhance confusion and diffusion at the pixel level.
- A preliminary statistical evaluation based on entropy, correlation, NPCR, and UACI.

The remainder of this study is organized as follows. Section II reviews the related literature. Section III presents the proposed methodology. Section IV describes the experimental setup and reports the results. Section V discusses the findings and limitations of the study. Finally, Section VI concludes the study and outlines directions for future work.

II. Related Work

A. Image Encryption: Challenges Beyond Traditional Methods

Securing the transmission of digital images is increasingly vital, particularly in satellite imaging, where both the sensitivity and sheer size of data are significant concerns. While established encryption methods such as AES and RSA offer strong protection for conventional data, they may not always be well suited for image encryption. Their intensive computational demands and inability to handle image-specific properties—like high redundancy and strong pixel correlation—make them less effective in this context [2],[12]. Furthermore, these techniques often fail to manage the large file sizes typical of satellite imagery, especially when real-time processing is required.

B. Chaos Theory in Image Encryption

Chaos-based encryption methods have received considerable attention in the field of image security because of their sensitivity to initial conditions, nonlinear dynamic behavior, and ability to generate pseudo-random sequences. These properties make chaotic systems well-suited for image-encryption tasks, where unpredictability and key sensitivity play an important role. Various chaotic models, including logistic maps, tent maps, the Henon system, and piecewise linear chaotic maps (PWLCM), have been used in previous studies to generate key streams and support permutation and diffusion processes in encrypted images [3], [6],[24].

In addition, chaos-based approaches are often considered attractive because they can increase the complexity of the encryption process while maintaining relatively low computational cost [18]. This makes them suitable for applications that require efficient image protection, particularly in settings where processing speed and limited computational resources are important [6]. Previous studies have reported that combining chaotic mechanisms can further improve the complexity of image-encryption schemes and enhance their resistance to unauthorized recovery attempts [24, 25]. Overall, chaos-based encryption remains a widely studied approach in image security due to its flexibility, efficiency, and strong dependence on initial parameter values.

C. DNA Cryptography in Multimedia Protection

DNA-based cryptographic techniques have attracted growing attention in multimedia security because they provide an alternative way to represent and process digital data. In this approach, binary information is encoded using nucleotide symbols such as A, T, C, and G, and a set of logical operations can then be performed within this encoded domain. Early DNA-based encryption models often relied on fixed encoding rules, whereas more recent studies have introduced dynamic DNA coding strategies and logical operations such as XOR, addition, and subtraction, often controlled by chaotic sequences [4], [5], [14].

Previous studies have shown that combining DNA-based data representation with chaotic control can improve image-encryption performance and strengthen statistical security properties [5], [7]. Previous studies reported that DNA-based operations can contribute to both confusion and diffusion during the encryption process [5], [23], making the encrypted image less predictable and more resistant to statistical analysis. These methods have also been associated with reduced correlation among adjacent pixels and improved entropy values in encrypted images, which are widely used indicators in image-security evaluation.

D. Hybrid Chaos-DNA Image Encryption

The combination of chaos and DNA encryption has been proposed as a way to address the limitations of each approach individually. Previous studies introduced a chaos-driven dynamic DNA coding method that adapts encoding rules based on chaotic sequences, ensuring per-pixel variability and greater unpredictability [8], [23].

Hybrid systems apply chaotic maps for key stream generation and pixel permutation, while DNA encoding and logical operations provide data transformation at the nucleotide level [3], [9]. This dual-layer approach disrupts statistical patterns within the image, achieving superior encryption quality compared to single-domain techniques [10, 24].

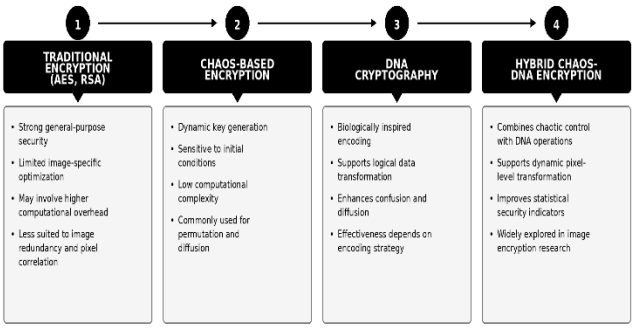

Fig. 1. Overview of conventional, chaos-based, DNA-based, and hybrid image encryption approaches.

E. Gaps in Existing Literature

Although chaos-DNA image-encryption methods have shown promising results in previous studies, several limitations remain in the existing literature. First, many reported works focus on general image datasets rather than satellite imagery as a specific application context [2, 8]. Second, several studies emphasize statistical security indicators without providing sufficiently clear methodological descriptions or broad experimental validation. In addition, the reported performance of many existing methods depends strongly on the design of the

key-generation process and the way DNA-based operations are integrated into the encryption framework [4], [13]. These observations indicate the need for further studies that provide clearer encryption procedures and a more focused evaluation for satellite image encryption.

F. Motivation for the Proposed Framework

Motivated by the above observations (Fig. 1), this study proposes a chaotic DNA-based framework for satellite image encryption. The framework is intended to combine logistic-map-based chaotic key generation with DNA-inspired encoding and XOR operations in order to strengthen pixel-level transformation during encryption. The main motivation behind this design is to explore a simple and structured encryption approach that can benefit from the sensitivity of chaotic sequences and the representational flexibility of DNA-based operations.

In this study, the proposed framework is examined as a proof-of-concept for grayscale satellite image encryption. The work is intended to provide a clearer methodological basis for integrating chaotic key generation with DNA-based processing, while offering a preliminary statistical evaluation using common image-security indicators.

III. Proposed Methodology

This section presents the design and operational workflow of the proposed encryption framework for satellite image protection. The framework is intended to combine chaotic key generation with DNA-inspired data transformation in a structured and lightweight encryption process. The main objective is to enhance pixel-level confusion and diffusion while maintaining a clear methodological design that can be applied to grayscale satellite image encryption. In this study, the framework is examined as a proof-of-concept setting for secure image encryption using common statistical security indicators.

A. Overall Architecture

The proposed encryption framework is organized around three main components:

1) Preprocessing module: This stage prepares the input satellite image in a suitable format for the encryption process. In the current implementation, the framework is applied to grayscale image data to ensure a consistent input structure for subsequent processing steps.

2) Chaotic key-generation module: This component uses the logistic map to generate pseudo-random sequences that serve as the basis for the encryption process. Because chaotic systems are highly sensitive to initial conditions [3], [24], the generated sequences introduce unpredictability and strengthen the key-dependent behavior of the framework [3], [25].

3) DNA-based encryption module: In this stage, image data are transformed using DNA-inspired encoding and XOR operations. These operations are applied to increase confusion and diffusion at the pixel level [4], [5], [10] and to support the overall complexity of the encryption process.

Fig. 2 illustrates the overall workflow of the proposed framework for satellite image encryption. The framework consists of sequential stages that begin with image preprocessing, followed by logistic-map-based key generation, DNA encoding, and XOR-based transformation, and then proceed to the corresponding decryption steps for image recovery.

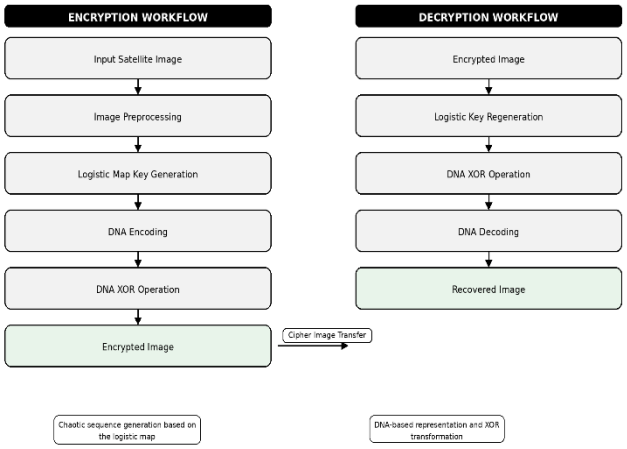

Fig. 2. Overall workflow of the proposed chaotic DNA-based satellite image encryption framework.

As shown in Fig. 2, the encryption process starts with preparing the input satellite image in a suitable format for further processing. A pseudo-random key sequence is then generated using the logistic map and used to support the encryption procedure. After that, the image data are transformed through DNA-based encoding and XOR operations to produce the encrypted image. For decryption, the same key-generation mechanism is used to regenerate the required sequence, after which inverse XOR and DNA decoding steps are applied to recover the original image. This workflow provides a clear representation of the main operational stages of the proposed framework.

B. Chaotic Key Generation

Chaotic key generation is a central component of the proposed framework because it introduces sensitivity to the initial parameters and supports the production of pseudo-random sequences for encryption. In this study, the logistic map is used as the chaotic generator because of its simple formulation and well-known nonlinear behavior. The logistic map is defined as Eq. (1).

$$x_{(n+1)} = \mu x_n(1 - x_n) \quad (1)$$

where, x_n in (0,1) denotes the chaotic state at iteration n, and \mu is the control parameter. When \mu is chosen in the chaotic region, the generated sequence becomes highly sensitive to small changes in the initial value x_0, which makes it suitable for encryption-oriented key generation.

For an input image of size M x N, the logistic map is iterated to generate a sequence of length M x N. The resulting real-valued chaotic sequence is then transformed into an integer-valued key stream that can be used in the subsequent encryption stages. A practical form of this transformation is given in Eq. (2).

$$k_i = \lfloor 256x_i \rfloor,\ i = 1,2,\ldots,MN \quad (2)$$

where, k_i represents the generated key value corresponding to the chaotic state x_i. This step maps the continuous chaotic output to discrete values that are compatible with digital image processing.

The generated key stream is then used to support the DNA-based encryption stage. Because the logistic map is highly sensitive to the initial condition x_0 and the control parameter \mu, even a small change in these values leads to a different chaotic sequence and, consequently, a different encryption result. This sensitivity strengthens the key-dependent behavior of the proposed framework and contributes to the unpredictability of the encryption process.

C. DNA Encoding and Logical Operations

After generating the chaotic key sequence, the framework applies DNA-inspired encoding to the image data. In DNA-based image encryption, binary values are represented using nucleotide symbols, namely A, T, C, and G. This representation provides an additional transformation layer and allows logical operations to be performed in the encoded domain.

In the proposed framework, each image pixel is first converted into its 8-bit binary form and then mapped into a DNA sequence according to a predefined encoding rule. This process can be expressed as Eq. (3).

$$D_i = E(p_i) \tag{3}$$

where, (p_i) denotes the original pixel value, (E(\cdot)) represents the DNA encoding function, and (D_i) is the DNA-encoded representation of that pixel.

After DNA encoding, the generated chaotic key sequence is transformed into a compatible form and combined with the encoded image data through a DNA-based XOR operation. This step increases the complexity of the encryption process and enhances pixel-level confusion. The operation can be written as Eq. (4).

$$C_i = D_i \oplus K_i \tag{4}$$

where, (K_i) is the encoded key element generated from the chaotic sequence, and (C_i) is the resulting DNA-coded encrypted value after the XOR operation.

Once this step is completed, the resulting DNA sequence is converted back into binary form and then reconstructed into pixel values to produce the encrypted image. During decryption, the same chaotic key sequence is regenerated, and the inverse procedure is applied to recover the original image. In this way, the DNA-based stage contributes to both confusion and diffusion within the proposed encryption framework.

D. Encryption Process Flow

The encryption process of the proposed framework is carried out through a sequence of structured stages that combine chaotic key generation with DNA-based data transformation. The purpose of this process is to convert the original satellite image into an encrypted form with reduced statistical predictability and stronger pixel-level confusion.

First, the input satellite image is prepared in a suitable format for encryption. In the current implementation, the image is processed as a grayscale image to ensure consistency in the subsequent stages. After preprocessing, the logistic map is iterated using the selected initial condition and control parameter to generate a chaotic sequence. This sequence is then transformed into a key stream that can be used in the encryption stage.

Next, the image pixel values are converted into binary form and encoded according to the selected DNA representation rule. The generated chaotic key stream is also transformed into a compatible encoded form. A DNA-based XOR operation is then applied between the encoded image data and the corresponding key sequence. This step introduces additional transformation at the pixel level and contributes to the complexity of the encrypted output.

After the XOR operation, the resulting DNA sequence is converted back into binary form and reconstructed into pixel values. These values form the encrypted image. Through this sequence of operations, the framework combines the sensitivity of chaotic key generation with the symbolic transformation provided by DNA-based encoding.

For clarity, the encryption procedure can be summarized as follows:

- Read the input satellite image.
- Preprocess the image and represent it in grayscale form.
- Generate a chaotic sequence using the logistic map.
- Convert the chaotic sequence into a key stream suitable for encryption.
- Encode the image pixels using the selected DNA rule.
- Apply the DNA-based XOR operation between the encoded image data and the encoded key sequence.
- Decode the resulting sequence and reconstruct the encrypted image.

E. Decryption Process Flow

The decryption process is carried out by reversing the main stages of the encryption procedure. To recover the original image correctly, the same initial condition and control parameter used in the logistic map during encryption must be applied again in the decryption stage. This allows the chaotic key sequence to be regenerated in an identical form.

First, the received encrypted image is converted into a suitable format for decryption. The logistic map is then re-initialized using the same secret parameters in order to regenerate the corresponding chaotic key sequence. After that, the encrypted image data is represented in DNA form using the same encoding rule adopted during the encryption process.

Next, the regenerated key sequence is transformed into a compatible encoded form and used in the DNA-based XOR operation. Because the same key sequence is reproduced, this step reverses the transformation applied during encryption. The resulting DNA sequence is then decoded back into binary form and reconstructed into pixel values to recover the original image.

For clarity, the decryption procedure can be summarized as follows:

- Read the received encrypted image.
- Regenerate the chaotic key sequence using the logistic map and the original secret parameters.
- Encode the encrypted image data using the same DNA rule used in encryption.
- Apply the DNA-based XOR operation using the regenerated key sequence.
- Decode the resulting DNA sequence and reconstruct the original pixel values.
- Recover the original satellite image.

Accurate synchronization of the logistic-map parameters and the DNA encoding rule between the sender and the receiver is essential for successful decryption and correct recovery of the original image data.

F. Key Features of the Framework

The proposed framework includes several characteristics that distinguish it from conventional image-encryption approaches. First, it combines chaotic key generation with DNA-inspired data transformation within a single encryption workflow. This integration provides a structured mechanism for introducing key sensitivity and pixel-level transformation during encryption.

Second, the framework is designed in a relatively simple and interpretable manner. The use of the logistic map enables pseudo-random sequence generation through a compact mathematical model, while DNA-based encoding and XOR operations provide an additional transformation layer for image data. This combination supports the overall complexity of the encryption process without relying on an overly complicated design.

Third, the framework is developed as a proof-of-concept for grayscale satellite image encryption. In this context, it is intended to demonstrate how chaotic sequence generation and DNA-based representation can be integrated within a clear methodological structure and evaluated using common statistical image-security indicators.

Overall, the proposed framework provides a lightweight and structured approach for exploring satellite image encryption using chaotic and DNA-based operations [2, 8].

IV. Experimental Setup and Results

This section describes the experimental setting used to evaluate the proposed chaotic DNA-based encryption framework. It presents the image preparation procedure, the implementation setting, and the statistical measures used to assess the encryption results. The evaluation is intended as a proof-of-concept analysis of the proposed method on grayscale satellite image data. The obtained results are reported and discussed in terms of commonly used image-security indicators, including entropy, adjacent-pixel correlation, NPCR, and UACI.

A. Experimental Environment

The experimental evaluation was conducted on a Windows 11 Pro (64-bit) platform equipped with an Intel Core i7-11800H processor and 16 GB of RAM. The proposed encryption framework was implemented in Python 3.11 using the Anaconda environment.

The main Python libraries used in the implementation were as follows:

- NumPy: used for numerical computations and the generation of pseudo-random sequences required in the chaotic processing stage.
- OpenCV: used for image reading, writing, and pixel-level image manipulation.
- Matplotlib: used for visualizing histograms and correlation plots.
- SciPy: used for entropy calculation and related statistical analysis.

B. Dataset Preparation and Preprocessing

A publicly available grayscale satellite image of size 256 × 256 pixels was used in the experimental evaluation. This image was selected to provide a proof-of-concept setting for examining the behavior of the proposed encryption framework on satellite image data. Fig. 3 shows the original input image used in the experiments.

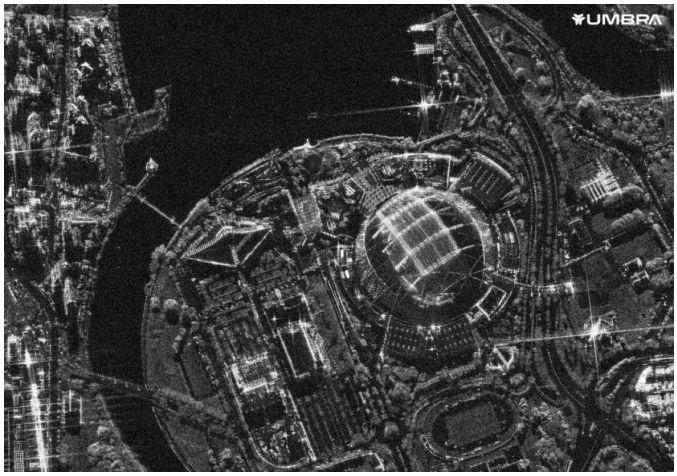

Fig. 3. Original grayscale satellite image used for encryption experiments.

Before encryption, the image was preprocessed using OpenCV to ensure a consistent input format for the subsequent stages of the proposed framework.

The preprocessing stage involved reading the input image in grayscale mode and resizing it to 256 × 256 pixels. This step ensured consistency in the input representation before applying the encryption procedure.

C. Chaotic Key Generation

A logistic map was used to generate the chaotic sequence employed in the key-generation stage. The mathematical formulation of the logistic map and its transformation into a discrete key stream were presented earlier in Section III-B. In the experimental implementation, the generated chaotic sequence was used to construct the key stream required for the encryption process.

D. DNA Encoding and Logical Operations

In this stage, binary pixel values were mapped to DNA sequences, and DNA-based XOR operations were applied to support pixel-level transformation during encryption. The mathematical formulation of the DNA encoding and XOR operations was introduced earlier in Section III-C. In the implementation, each pixel value was converted into its 8-bit binary form, divided into four pairs of bits, and mapped using the adopted DNA rule: 00 → A, 01 → C, 10 → G, and 11 → T. After that, the encoded image data were combined with the encoded chaotic key sequence through a DNA-based XOR operation. The resulting DNA sequence was then converted back into binary form and reconstructed into pixel values to produce the encrypted image.

E. Encryption Process

In the implementation, the encryption procedure was applied to each pixel of the input image using the generated chaotic key stream. For every pixel, the binary value of the image data was converted into DNA form, and the corresponding key element was transformed into a compatible DNA representation. A DNA-based XOR operation was then applied between the encoded pixel value and the encoded key value. The resulting DNA sequence was subsequently converted back into binary form and reconstructed into the encrypted pixel value. This process was repeated over the entire image to produce the final encrypted image.

Fig. 4 shows the encrypted output generated by the proposed framework after applying chaotic key generation, DNA encoding, and DNA-based XOR transformation to the input satellite image.

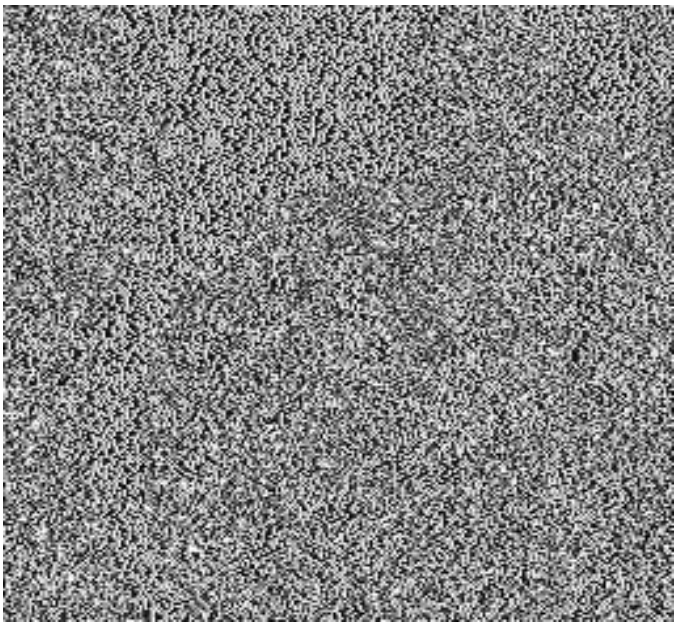

Fig. 4. Encrypted image produced by the proposed framework.

As shown in Fig. 4, the encrypted image exhibits a noise-like appearance with no visually recognizable structures from the original image. This visual behavior indicates that the proposed framework was able to significantly alter the spatial distribution of pixel intensities in the encrypted output.

F. Evaluation Metrics

The encryption performance was evaluated using standard statistical security metrics commonly employed in image-encryption studies.

The evaluation focused on four widely used indicators: information entropy, adjacent-pixel correlation, NPCR, and UACI. Information entropy was used to assess the randomness of the encrypted image distribution. Adjacent-pixel correlation was used to measure the relationship between neighboring pixels in the horizontal, vertical, and diagonal directions. NPCR was used to quantify the percentage of differing pixels between two images, while UACI was used to measure the average intensity difference between them. Together, these metrics provide a statistical view of the encryption behavior of the proposed framework.

Although these metrics are widely used in image-encryption analysis, they do not by themselves provide a complete proof of security against all possible attack models. In this study, they are used as standard indicators for a preliminary statistical evaluation of the proposed framework.

G. Results and Analysis

The experimental results indicate that the proposed framework produced statistically encouraging encryption behavior for the tested satellite image. The entropy of the encrypted image reached 7.99, which is close to the ideal value of 8 and suggests a high level of randomness in the encrypted output [1],[5],[23]. In addition, the NPCR value reached 99.61%, indicating a high percentage of pixel changes between the compared images. The UACI value was 33.32%, which is consistent with the expected behavior of a strongly transformed encrypted image. Furthermore, the correlation values in the horizontal, vertical, and diagonal directions were close to zero, indicating a substantial reduction in the linear dependency among adjacent pixels after encryption [5],[7],[23].

Overall, these results suggest that the proposed framework was effective in altering the statistical structure of the original image and producing an encrypted output with noise-like characteristics. Table I summarizes the main performance metrics obtained in the experimental evaluation.

TABLE I. PERFORMANCE METRICS OF THE PROPOSED ENCRYPTION FRAMEWORK

Metric	Result
Entropy (Encrypted)	7.99
NPCR (%)	99.61
UACI (%)	33.32
Correlation (H, V, D)	-0.003, 0.005, -0.002

V. SIMULATION RESULTS AND SECURITY EVALUATION

This section presents a statistical evaluation of the proposed chaotic DNA-based encryption framework, with emphasis on the encryption performance of the tested satellite image. The analysis was carried out using standard image-security indicators and implementation-based observations. A publicly available grayscale satellite image of size 256 × 256 pixels was used in the experiments. The implementation was performed on

a Windows 11 system equipped with an 11th Gen Intel Core i7 processor and 16 GB of RAM, using Python 3.11 within the Anaconda environment.

A. Ability to Resist Statistical Attacks

1) Histogram analysis: A common objective of image encryption is to reduce visible redundancy in pixel-intensity distributions and make the encrypted image less predictable than the original image. As shown in Fig. 5, the histogram of the original satellite image exhibits noticeable variations in intensity distribution, reflecting the structural patterns present in the plain image. By contrast, the histogram of the encrypted image appears more dispersed across the grayscale range, with no obvious dominant peaks comparable to those observed in the original image. This visual change suggests that the proposed framework altered the statistical distribution of pixel intensities in the encrypted output. However, histogram analysis alone is not sufficient to establish complete statistical security, and it should be interpreted together with quantitative indicators such as entropy and adjacent-pixel correlation.

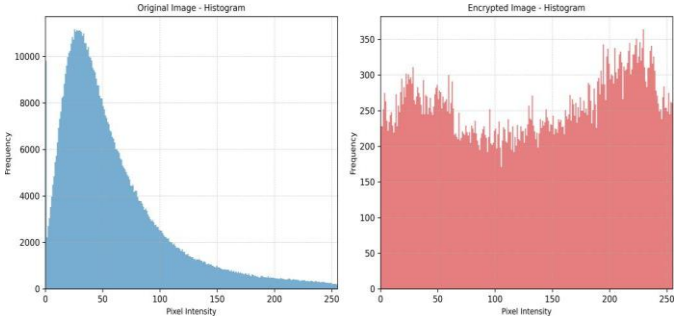

Fig. 5. Histogram comparison between the original and encrypted satellite images: (a) Histogram of the original image, (b) Histogram of the encrypted image.

2) Correlation analysis: To evaluate the statistical relationship between neighboring pixels, correlation coefficients were calculated in the horizontal, vertical, and diagonal directions. In the original satellite image, relatively high correlation values were observed, reflecting the spatial redundancy that is typically present in plain image data. After encryption, these values were reduced substantially and became close to zero, indicating a strong reduction in linear dependency among adjacent pixels.

Fig. 6-8 presents scatter plots for the original and encrypted images and illustrates the visual change in pixel correlation before and after encryption. In the original image, the points appear more strongly clustered, reflecting the spatial dependency among neighboring pixels. In contrast, the encrypted image shows a substantially more dispersed distribution, indicating a marked reduction in linear dependency after encryption. Although some local clustering can still be observed in the encrypted scatter plots, they remain considerably less structured than those of the original image. This behavior is consistent with the numerical correlation results reported in Table II and suggests that the proposed framework significantly reduced pixel-level statistical dependency in the encrypted output.

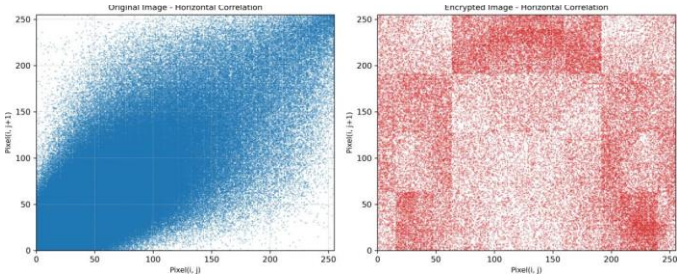

Fig. 6. Scatter plot comparison of horizontally adjacent pixels in the original and encrypted satellite images, showing the reduction in pixel correlation after encryption.

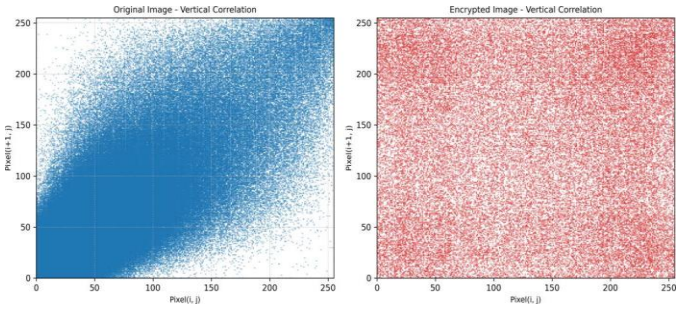

Fig. 7. Scatter plot comparison of vertically adjacent pixels in the original and encrypted satellite images, showing the reduction in pixel correlation after encryption.

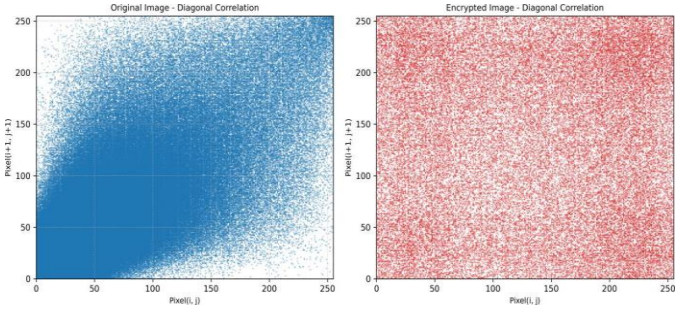

Fig. 8. Scatter plot comparison of diagonally adjacent pixels in the original and encrypted satellite images.

TABLE II. CORRELATION COEFFICIENTS OF ADJACENT PIXELS BEFORE AND AFTER ENCRYPTION

Image	Plain Image			Encrypted Image		
	Horizontal	*Vertical*	*Diagonal*	*Horizontal*	*Vertical*	*Diagonal*
Satellite Image	0.96	0.95	0.94	-0.003	0.005	-0.002

Table II reports the correlation coefficients of adjacent pixels in the horizontal, vertical, and diagonal directions before and after encryption. The original image shows high correlation values, which reflect the strong spatial dependency typically present in plain image data. After encryption, the corresponding values become very close to zero, indicating a substantial reduction in linear dependency among neighboring pixels.

3) Information entropy: Information entropy is commonly used to measure the degree of randomness or unpredictability in an encrypted image. For an 8-bit grayscale image, the ideal entropy value is 8. In this study, the encrypted image achieved

an entropy value of 7.99, which is very close to the ideal value. By comparison, the entropy of the plain satellite image was 7.55. This result suggests that the proposed framework increased the randomness of the image data after encryption and supports the statistical effectiveness of the encryption process. The corresponding entropy values are reported in Table III.

TABLE III. INFORMATION ENTROPY OF THE PLAIN AND ENCRYPTED SATELLITE IMAGES

Image	Plain Image Entropy	Encrypted Image Entropy
Satellite Image	7.55	7.99

B. Resistance to Differential Attacks

Differential attack analysis is commonly used to evaluate the sensitivity of an encryption method to small changes in the input image. In this study, the Number of Pixel Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) were used to assess the effect of pixel-level changes on the encrypted output. The experimental results showed an NPCR value of 99.61% and a UACI value of 33.35%, indicating that the proposed framework produced substantial changes in the encrypted image in response to small variations in the input. These results suggest a high degree of sensitivity to differential changes [1] and support the statistical effectiveness of the encryption process. A summary of the obtained results is presented in Table IV.

TABLE IV. NPCR AND UACI RESULTS FOR DIFFERENTIAL ATTACK ANALYSIS

Image	NPCR (%)	UACI (%)
Satellite Image	99.61	33.35

C. Key Sensitivity Analysis

An important property of the proposed framework is its sensitivity to the secret parameters used in the chaotic key-generation stage. Because the logistic map is highly dependent on its initial condition and control parameter, even a very small change in these values leads to a different chaotic sequence and, consequently, a different encrypted output.

In the present framework, the parameters (x_0) and (\mu) must be reproduced accurately during decryption to regenerate the same key sequence used in the encryption stage. Any mismatch in these parameters prevents the correct recovery of the original image. This behavior indicates that the proposed method is strongly dependent on parameter synchronization and exhibits a high degree of key sensitivity [25].

From a security perspective, this sensitivity is important because it reduces the likelihood of recovering the correct image without the exact parameter settings. Therefore, the strength of the proposed framework is supported by the strong dependence of the encryption and decryption processes on the correct chaotic parameters.

D. Computational Complexity Analysis

The computational complexity of the proposed encryption framework can be expressed as $O(M \times N)$, where M and N denote the height and width of the input image, respectively. This complexity arises because the main encryption operations are applied at the pixel level across the entire image. In the current implementation, the framework combines logistic-map-based key generation with DNA encoding and XOR operations in a relatively simple processing structure.

From an implementation perspective, the framework does not rely on deeply nested transformations or computationally expensive optimization procedures. This makes the overall processing workflow relatively lightweight for the tested image size. However, the present evaluation is limited to a proof-of-concept setting on grayscale satellite imagery, and broader analysis on larger datasets and different computational settings remains an important direction for future work.

E. Summary of Security and Performance Metrics

A summary of the main security and performance metrics obtained for the proposed framework is presented in Table V.

TABLE V. SUMMARY OF THE PROPOSED FRAMEWORK'S SECURITY AND PERFORMANCE METRICS

Metric	Proposed Framework	Reference / Expected Behavior
Entropy (bits)	7.99	Close to 8.0
NPCR (%)	99.61	Greater than 99.5
UACI (%)	33.35	Around 33%
Correlation (H, V, D)	-0.003, 0.005, -0.002	Close to 0

VI. DISCUSSION

The experimental results indicate that the proposed chaotic DNA-based framework was able to alter the statistical characteristics of the tested satellite image and produce an encrypted output with increased randomness and reduced pixel-level dependency. The obtained values of entropy, correlation, NPCR, and UACI suggest that the framework achieved statistically encouraging encryption behavior under the experimental setting considered in this study. At the same time, these results should be interpreted within the scope of a proof-of-concept evaluation based on grayscale satellite image data and standard statistical image-security indicators.

A. Theoretical Contributions

From a methodological perspective, the proposed framework contributes to the integration of chaotic key generation with DNA-inspired image transformation within a relatively simple encryption structure. The logistic map provides a compact nonlinear mechanism for generating key-dependent pseudo-random sequences, while DNA-based encoding and XOR operations introduce an additional symbolic transformation layer during encryption. The combination of these two components supports pixel-level confusion and contributes to the overall complexity of the encrypted image representation.

The reported entropy, correlation, NPCR, and UACI results suggest that the proposed framework was effective in changing the statistical structure of the tested image after encryption. In this sense, the theoretical contribution of the study lies not in introducing an entirely new cryptographic primitive, but in

presenting a structured proof-of-concept framework that combines chaotic and DNA-based operations in a clear and interpretable way for satellite image encryption.

B. Practical Implications for Satellite Image Security

From an application perspective, the proposed framework illustrates how chaotic key generation and DNA-based transformation can be combined to protect satellite image data within a lightweight implementation structure. The present results suggest that the method can alter the visual and statistical characteristics of the input image in a way that makes the encrypted output less predictable than the original image.

However, the current implementation should be viewed as an initial proof-of-concept rather than a complete deployment-ready solution for operational satellite systems. Broader practical use would require additional validation on larger and more diverse image datasets, as well as further analysis under different computational and communication settings.

C. Comparison with Related Work

Relative to prior chaos-based and DNA-based image-encryption studies, the proposed framework follows a similar general direction by combining nonlinear key generation with symbolic image transformation. The statistical results obtained in this study, particularly in terms of entropy, adjacent-pixel correlation, NPCR, and UACI, are consistent with the types of indicators commonly reported in the related literature.

At the same time, the present work should be interpreted within its actual experimental scope. The proposed framework was evaluated as a proof-of-concept on grayscale satellite image data, and therefore the comparison with related work is best understood as a contextual rather than an exhaustive benchmark comparison. A broader and more rigorous comparative analysis against additional recent methods remains an important direction for future research.

D. Limitations and Future Work

Several limitations of the current study should be acknowledged. First, the evaluation was conducted on grayscale satellite imagery within a proof-of-concept setting, which limits the generalizability of the reported results. Second, the current analysis relied mainly on standard statistical security indicators such as entropy, correlation, NPCR, and UACI. Although these metrics are widely used in image-encryption studies [11], they do not by themselves provide a complete assessment against all possible attack models.

In addition, the present implementation did not include a broader evaluation on multispectral or high-dynamic-range satellite imagery, nor did it include extensive benchmarking against a large set of recent encryption baselines. Future work may therefore extend the framework to more diverse image types, incorporate additional robustness and comparative experiments, and explore alternative chaotic designs or more advanced DNA-based transformation strategies.

E. Broader Implications in Cryptography

The study also highlights the potential value of combining ideas from nonlinear dynamics and biologically inspired data representation in multimedia security research. Even within the limited scope of the present implementation, the integration of chaotic processing and DNA-based transformation demonstrates how cross-disciplinary concepts can be used to develop structured image-encryption frameworks [4],[8],[23].

More broadly, this line of research may support future work on lightweight and application-oriented cryptographic methods for image and multimedia protection [20], [21]. In this respect, the proposed framework serves as a useful exploratory step toward more comprehensive studies on secure image encryption using chaos-based and DNA-inspired techniques.

VII. Conclusion

This study presented a chaotic DNA-based framework for satellite image encryption that combines logistic-map-based key generation with DNA-inspired encoding and XOR operations. The proposed framework was developed as a proof-of-concept approach for grayscale satellite image encryption and was evaluated using common statistical security indicators.

The experimental results showed that the encrypted image achieved high entropy, low adjacent-pixel correlation, and encouraging NPCR and UACI values under the adopted evaluation setting. These findings suggest that the proposed framework was effective in altering the statistical characteristics of the tested image and producing an encrypted output with reduced predictability.

At the same time, the current study is limited to a proof-of-concept evaluation on grayscale satellite imagery and standard statistical image-security metrics. Therefore, the reported results should be interpreted within this scope. Future work may extend the framework to more diverse satellite image types, incorporate broader comparative and robustness analyses, and investigate alternative chaotic designs or more advanced DNA-based transformation strategies.

References

[1] Belazi, A., Talha, M., Kharbech, S., & Xiang, W. (2019). Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding. IEEE Access, 7, 36667–36681.

[2] Zhang, B., & Liu, L. (2023). Chaos-Based Image Encryption: Review, Application, and Challenges. Mathematics, 11(11), 2585.

[3] Chai, X., Fu, X., Gan, Z., Lu, Y., & Chen, Y. (2019). A color image cryptosystem based on dynamic DNA encryption and chaos. Signal Processing, 155, 44–62.

[4] Liu, L., Wang, D., & Lei, Y. (2020). An Image Encryption Scheme Based on Hyper Chaotic System and DNA With Fixed Secret Keys. IEEE Access, 8, 46400–46416.

[5] Zhang, Y. (2018). The Image Encryption Algorithm Based on Chaos and DNA Computing. Multimedia Tools and Applications, 77(16), 21589–21615.

[6] Yan, M., Liu, M., & Li, C. (2025). DNA Color Image Encryption Based on Conservative Chaotic System. Scientific Reports, 15(1), 9278.

[7] Liu, Y., Tang, J., & Xie, T. (2014). Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map. Optics & Laser Technology, 60, 111–115.

[8] Patidar, V., & Kaur, G. (2023). A Novel Conservative Chaos Driven Dynamic DNA Coding for Image Encryption. Frontiers in Applied Mathematics and Statistics, 8, 1100839.

[9] Enayatifar, R., Guimaraes, F. G., & Siarry, P. (2019). Index-based permutation-diffusion in multiple-image encryption using DNA sequence. Optics and Lasers in Engineering, 115, 131–140.

[10] Ur Rehman, A., Liao, X., Ashraf, R., Ullah, S., & Wang, H. (2018). A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2. Optik, 159, 348–367.

[11] Sokouti, M., & Sokouti, B. (2018). A systematic review on color image encryption using DNA properties. Computer Science Review, 29, 14–20.

[12] Panda, M. (2016). Performance analysis of encryption algorithms for security. Proceedings of SCOPES 2016, IEEE, 278–284.

[13] Li, C., Li, S., Asim, M., Nunez, J., Alvarez, G., & Chen, G. (2016). On the Security Defects of an Image Encryption Scheme. arXiv.

[14] Chattopadhyay, C., Sarkar, B., & Mukherjee, D. (2015). Encoding by DNA Relations and Randomization Through Chaotic Sequences for Image Encryption. arXiv.

[15] Galdran, A. (2018). Image Dehazing by Artificial Multiple-Exposure Image Fusion. Signal Processing, 149, 135–147.

[16] Vanishreeprasad, S., & Pushpalatha, K. N. (2015). Design and implementation of hybrid cryptosystem using AES and Hash Function. IOSR Journal of Electronics and Communication Engineering, 10(3), 18–24.

[17] Meenakumari, M., & Athisha, G. (2014). Improving message authentication by integrating encryption with hash function and its VLSI implementation.

[18] Thabit, F., Alhomdy, S., & Jagtap, S. (2021). Security analysis and performance evaluation of a new lightweight cryptographic algorithm for cloud computing.

[19] Gastermann, B., Stopper, M., Kossik, A., & Katalinic, B. (2015). Secure implementation of an on-premises cloud storage service for SMEs.

[20] Khan, S. S., & Tuteja, R. R. (2015). Security in cloud computing using cryptographic algorithms.

[21] Gong, Z., Nikova, S., Law, Y. W., Juels, A., & Paar, C. (2012). RFID Security and Privacy.

[22] Princy, P. (2015). A comparison of symmetric key algorithms DES, AES, Blowfish, RC4, RC6.

[23] Wu, X., Kan, H., & Kurths, J. (2015). A New Color Image Encryption Scheme Based on DNA Sequences and Multiple Improved 1D Chaotic Maps. Applied Soft Computing, 37, 24–39.

[24] Mondal, B., Singh, S., & Kumar, P. (2019). A secure image encryption scheme based on cellular automata and chaotic skew tent map. Journal of Information Security and Applications, 45, 117–130.

[25] Leo, M., & Kumar, R. (2021). Chaos-based secure image encryption techniques and applications. Journal of Information Security Applications.