العدد 21A 2 تموز 2026
المجلة العراقية للبحوث الانسانية والاجتماعية والعلمية
NO.21A2 Jul.2026 Iraqi Journal of Humanitarian, Social and Scientific Research
Print ISSN 2710-0952 Electronic ISSN2790-1254

Hybrid DNA–Chaotic Lightweight Feistel Cipher with Dynamic Round-Key Scheduling for IoT

Zainab Fawzi Abed

Al-Iraqia University, College of Arts

zainab.f.abed@aliraqia.edu.iq

Abstract

it is difficult to secure image transmission in an Internet of Things (IoT) setting, where computation/storage resources and energy used by IoT devices are limited. In this paper, a hybrid lightweight image encryption scheme is proposed which combines the chaos-based key generation, adaptive DNA encoding and Feistel network structure to ensure high security and low computation costs.

The proposed scheme consists of two major phases: the first is the generation of the round-key in a dynamic manner by a DNA–chaotic mechanism, and the second is a Feistel-based encryption process with adaptive DNA transformations and light non-linear operations. Dynamic and round-dependent encoding and key generation techniques help increase randomness and key sensitivity.

The experimental results on the standard benchmark images show that the proposed algorithm generates encrypted images that have good statistical properties, such as uniform histogram distribution, close to zero correlation coefficient, and entropy near the optimal value. Furthermore, the scheme possesses high level of NPCR and UACI values which shows that the scheme has strong resistance against differential attack.

The results support that the suggested technique has a trade-off between security and computational complexity and is appropriate for resource-limited applications in IoT.

keywords : Image Encryption, DNA Cryptography, Chaotic Systems, Feistel Network, Lightweight Cryptography, Internet of Things (IoT), Dynamic Key Generation, Information Security.

خوارزمية فيستل هجينة خفيفة الوزن قائمة على الحمض النووي والفوضى مع توليد مفاتيح ديناميكية لإنترنت الأشياء

زينب فوزي عبد

الجامعة العراقية / كلية الآداب

الملخص:

يُعدّ تأمين نقل الصور في بيئة إنترنت الأشياء (IoT) أمرًا صعبًا، نظرًا لمحدودية موارد الحوسبة والتخزين والطاقة التي تستهلكها أجهزة إنترنت الأشياء. في هذه الورقة، نقترح نظام تشفير صور هجينًا خفيف الوزن يجمع بين توليد المفاتيح القائم على الفوضى، وتشفير الحمض النووي التكيفي، وبنية شبكة فيستل لضمان أمان عالٍ وتكاليف حسابية منخفضة.

يتكون النظام المقترح من مرحلتين رئيسيتين: الأولى هي توليد مفتاح الجولة بشكل ديناميكي باستخدام آلية فوضوية تعتمد على الحمض النووي، والثانية هي عملية تشفير تعتمد على فيستل مع تحويلات الحمض النووي التكيفية وعمليات غير خطية بسيطة. تُسهم تقنيات التشفير وتوليد المفاتيح الديناميكية والمعتمدة على الجولة في زيادة العشوائية وحساسية المفتاح.

تُظهر النتائج التجريبية على صور مرجعية قياسية أن الخوارزمية المقترحة تُولّد صورًا مُشفّرة ذات خصائص إحصائية جيدة، مثل التوزيع المنتظم للرسم البياني، ومعامل ارتباط قريب من الصفر، وإنتروبيا قريبة من القيمة المثلى. علاوة على ذلك، يتميز النظام بمستويات عالية من قيم NPCR وUACI، مما يدل على مقاومته القوية للهجمات التفاضلية.

تدعم النتائج أن التقنية المقترحة لها مفاضلة بين الأمن والتعقيد الحسابي وهي مناسبة للتطبيقات ذات الموارد المحدودة في إنترنت الأشياء.

الكلمات المفتاحية: تشفير الصور، تشفير الحمض النووي، الأنظمة الفوضوية، شبكة فيستل، التشفير الخفيف، إنترنت الأشياء (IoT)، توليد المفاتيح الديناميكية، أمن المعلومات.

1. Introduction

The Internet of Things (IoT) has resulted in a significant growth in data production and sharing among numerous applications like health care, smart cities and industrial systems. These types of environments involve devices constantly sharing and communicating sensitive information, making data security a key requirement. Most IoT devices, however, are constrained in their computing, memory and energy capabilities making the implementation of traditional security mechanisms difficult [1], [2].

Traditional cryptographic methods like "Advanced Encryption Standard (AES)", "RivestShamir Adleman (RSA)", and Elliptic Curve Cryptography (ECC) is robust & secure but are resource-intensive. This renders them less suitable for resource limited IoT environments, where efficiency and importance is a key factor [1],[3]. In order to get a balance between the level of security and computation cost, lightweight cryptographic methods have been introduced [4].

Digital images are often a major part of the data transmitted in many applications of IoT. Images have specific properties which make conventional encryption systems ineffective if applied directly – they are highly redundant and have high correlation between neighbouring pixels [5]. Thus, specialized image encryption techniques are needed to safely send out the image data over an unsaved interaction channel.

The features of chaos such as sensitivity to initial conditions and pseudo-random behavior are very suitable for confusions and diffusions in chaos based cryptographic systems [6] which is an important reason why chaos based cryptography has received a wide range of interest. Concurrently, DNA cryptography has devised a new method of data representation using the sequences of nucleotides (A, T, C, and G) that are found in DNA, which provides more flexibility and greater randomness in data encryption [5] [7].

There have been some recent research efforts and publications on the hybrid systems, which are a combination of chaotic systems and DNA encoding to enhance security performance. These techniques involve the use of chaotic sequences for controlling the encryption

operations, and the use of DNA-based transformation to improve the nonlinearity and statistical and differential attacks resistance [6] [8].

In spite of these advances, existing methods suffer from inefficient lightweight design and do not fully leverage on the dynamic key generation mechanisms, which restricts their use for real use scenarios in IoT [4].

In view of the drawbacks, the author present in this paper a hybrid DNA–chaotic lightweight encryption algorithm that employs a Feistel network structure and dynamic generation of round-key. The proposed approach incorporates chaotic key generation and adaptive DNA encoding into a Feistel system to provide high security and computational efficiency, especially for IoT devices with limited resources.

2. Related Work

The limitations of traditional image encryption methods in IoT environments have drawn the attention of many researchers to combine the methods of DNA computing, chaotic systems and lightweight cryptography in recent years. The goal of these methods is to balance security with low computational demands.

There has been some research on cryptographic methods based on DNA in constrained environments. For example, Ţălu [1] tested the performance of DNA based algorithms for IoT devices and showed how these algorithms enhance its diffusion and resistance to differential attacks. In a similar manner, Qaid and Ebrahim [9] presented a lightweight scheme based on DNA operations which increases the strength of the keys.

The lightweight cryptographic solutions are also extensively studied. Mahlake et al. [2] proposed an energy efficient encryption solution for WSNs, which reduces the amount of power consumed and computation time required. Moreover, Amrita et al. [4] have explored different lightweight cryptographic methods available, highlighting the importance of developing efficient designs for resource limited IoT systems.

There are hybrid methods in which DNA and chaotic systems are used that have been seen to perform well. Dhakal and Shakya presented a DNA-based Feistel encryption scheme [5] and Sekar et al. used chaotic maps with DNA/RNA encoding to increase permutation and diffusion [6]. Likewise, in the work done by Patidar and Kaur [11] a chaotic system-based dynamic DNA encoding system is presented that enhances randomness and sensitivity to keys.

Later models have added on further techniques for performance improvement. In addition, Ahmed et al. [10] connected chaotic systems with deep learning-based compression and DNA coding, while Aqeel et al. [8] used elliptic curve cryptography and DNA coding to ensure the security and efficiency of IoT communications. But other researchers, like Bhaya et al. [12] and Huang et al. [13] were intent on enhancing the key space and differential resistance by the use of advanced chaotic structures. Besides, Nujumudeen et al. [14] suggested a lightweight chaos-based security architecture for IoT, prioritizing computational efficiency, and Selvi and Rajendran [15] proposed a hybrid scheme based on DNA encoding, chaotic maps and hash-

based key generation that improved the security performance and statistical robustness of the system.

Although all these progresses have been made, the current approaches tend to concentrate on security or efficiency and hardly on both together in a lightweight framework. Furthermore, the dynamic generation of round-key in Feistel-based architectures has been scarcely studied.

Therefore, an efficient encryption scheme which is lightweight, generates dynamic keys and hybrid DNA–chaotic operations with a structured framework is required. This inspires in this paper the proposed approach.

3. Proposed Methodology

3.1 Overview of the Proposed System

This section introduces to the Proposed System.

The proposed method presents a hybrid lightweight image encryption system, which is suitable for resource-constrained environments in the IoT. Combines chaotic key generation, DNA based transformations and a Feistel network structure to balance security strength and computation efficiency.

The whole process consists of two steps. Based on the 64-bit master key, a chaos-driven mechanism together with adaptive DNA encoding is used to create the dynamic round keys in the first stage. The second stage is an encryption of image data with Feistel structure with XOR operations, dynamic DNA transformations, circular shifts, and lightweight permutation functions in every round of encryption.

It creates low-computational complexity architecture with high randomness, nonlinearity and diffusion effect, which is suitable to the system with limited resources in IoT.

3.2 Dynamic DNA-Chaotic Round-Key Generation

At this point, a dynamic round-key generation mechanism is added to enhance the unpredictability and key sensitivity during encryption. The proposed method is a combination of chaotic mapping and adaptive DNA encoding, which produce different round key for every round of encryption.

The 64-bit master key MK is divided into four 16-bit segments ($\boldsymbol{S_1}$, $\boldsymbol{S_2}$, $\boldsymbol{S_3}$, $\boldsymbol{S_4}$). The first two segments are used to produce a value that is chaotic in the beginning, and a logistic map is used to create the sequence of chaotic values.

The chaotic values are encoded as a 32-bit binary sequence, and then encoded into a DNA sequence, with a dynamically chosen encoding rule. The encoding rule depends on the key segments and the round number, and therefore, it is very diversified in rounds.

Other operations on the DNA are used to further increase the degree of non-linear, such as complementary mapping (A ↔ T, C ↔ G) and permutation controlled by key segments. The DNA sequence is then inverted back to binary and then performs a circular shift.

Lastly, a 32-bit round key is produced for each round. Improved resistance to cryptographic attack through this dynamic process, key by key, producing highly sensitive and pseudo random keys.

In contrast with traditional key generation techniques, the proposed method changes the DNA encoding rules and chaotic sequences at every round which leads to enhanced key diversity and resistance to known-plaintext and differential attacks.

Algorithm 1: Dynamic DNA–Chaotic Round-Key Generation

Input:

Master Key MK (64-bit), no. of rounds N, Control parameter r

Output:
Round keys $RK_1, RK_2, \ldots, RK_N$, (each 32-bit)

Begin

1. Divide the master key MK into four 16-bit segments:
$MK = (S_1, S_2, S_3, S_4)$

2. Initialize the chaotic value:

$$x_0 = \frac{S_1 \oplus S_2}{2^{16}}$$

3. For each round $i = 1$ to N do:

3.1 Generate chaotic value using logistic map:

$$x_i = r.x_{i-1}(1 - x_{i-1})$$

3.2 Convert x_i into a 32-bit binary sequence B_i

3.3 Apply dynamic DNA encoding based on S_3 and round index i

3.4 Apply DNA transformations:

- Complementary mapping (A ↔ T, C ↔ G)

- DNA permutation controlled by S_4

3.5 Convert the DNA sequence back to binary form B'_i

3.6 Apply circular shift to B'_i

3.7 Generate round key:

$$RK_i = Shift(B'_i) \oplus (S_1 \parallel S_2)$$

4. Store all round key $\{RK_1, RK_2, \ldots, RK_N\}$

End

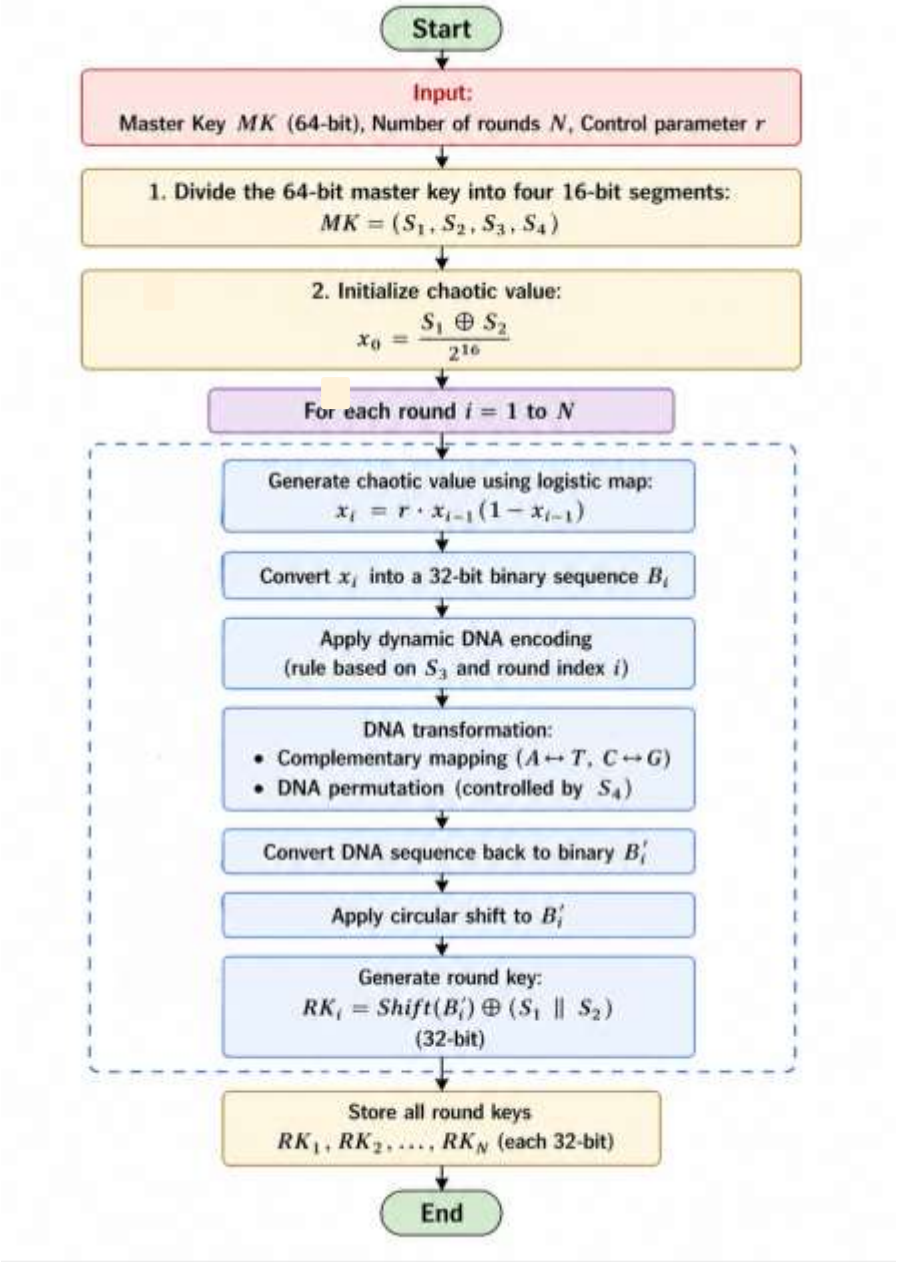

Fig. 1. Flowchart of the proposed dynamic DNA-chaotic round-key generation algorithm.

3.3 Feistel-Based Encryption Structure

In the second stage, the encryption process is implemented using a Feistel network structure, selected for its computational efficiency and inherent reversibility. The input image is first converted into a binary representation and partitioned into fixed-size blocks.

Each block undergoes an initial permutation and is then divided into two equal halves, denoted as L and R, The encryption process proceeds through multiple iterative rounds, where the dynamically generated round keys from the previous stage are utilized.

At each round, the right half is combined with the corresponding round key using an XOR operation to produce an intermediate value. Unlike conventional Feistel designs, this intermediate output is further processed using a dynamic DNA encoding mechanism, where the encoding rule is adaptively selected based on both the round index and key-dependent parameters.

DNA-based transformations are then used after the encoding stage to further enhance the nonlinearity, such as complementary mapping and permutation operation. This sequence is then converted to binary form again and passed through several simplistic operations like circular shift and permutation to introduce further diffusion.

The function processed by the output of the round is defined as this function, which is again XORed with the left half to produce the right half, and the previous right half is assigned to the left half of the next round, as in the Feistel structure.

Once all rounds are completed, the halves are joined together to give an encrypted image by passing through a final permutation.

Unlike traditional Feistel-type encryption methods, this design introduces adaptive DNA transformations and dynamic operations dependent on the keys in each round, which enhances the confusion, diffusion, and statistical and differential attack resistance with minimal computational costs ideal for IoT applications.

Algorithm 2: Hybrid DNA–Chaotic Feistel Encryption

Input:

Plaintext block P (64-bit), Round keys $RK_1, RK_2, \ldots, RK_N$

Output:

Ciphertext block C (64-bit)

Begin

1. Apply initial permutation:

$P' = IP\ (P)$

2. Split P' into two 32-bit halves:

(L_0 , R_0)

3. For each round $i = 1$ to N do:

3.1 Compute:

$$T_i = R_{i-1} \oplus RK_i$$

3.2 Apply dynamic DNA encoding based on RK_i

3.3 Apply DNA transformations:

- **Complementary mapping (A ↔ T, C ↔ G)**
- **DNA permutation**

3.4 Convert the DNA sequence back to binary form

3.5 Apply nonlinear operations:

- **Circular shift**
- **Lightweight permutation**

3.6 Compute round function:

$$F_i = P(Shift(DNA\_Trans(T_i)))$$

3.7 Update Feistel structure:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F_i$$

4. Combine the final halves:

$$C' = (L_N \parallel R_N)$$

5. Apply final permutation:

$$C = FP(C')$$

End

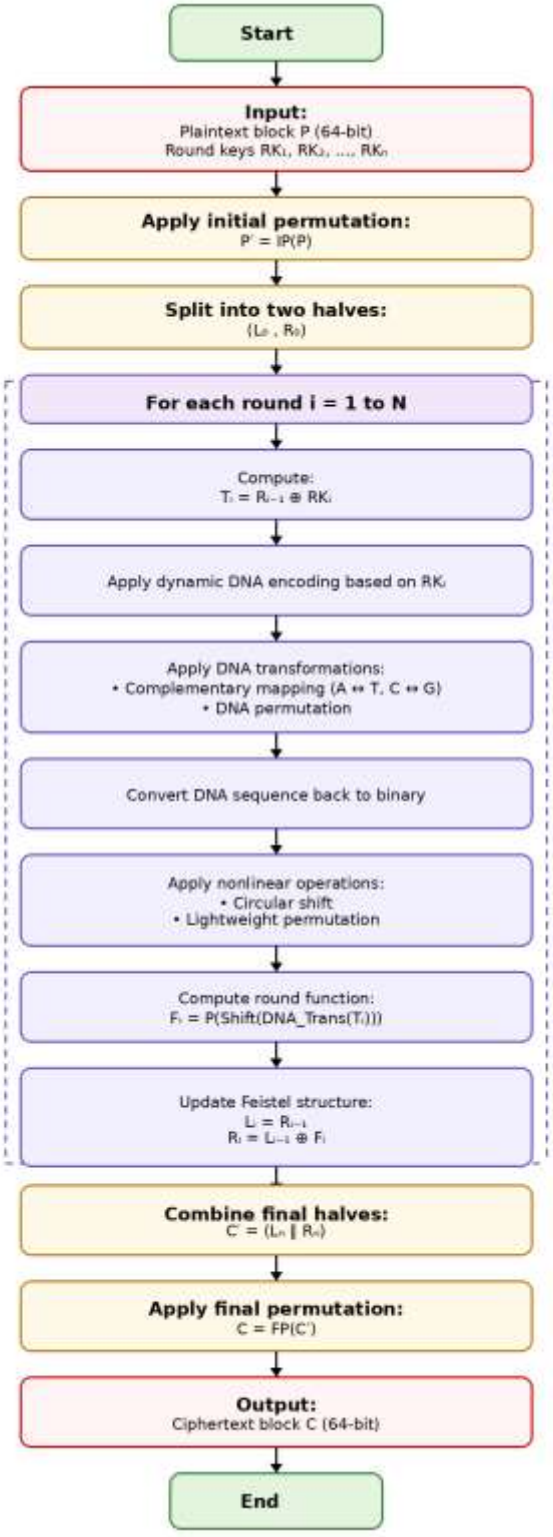

Fig. 2. Flowchart of proposed hybrid DNA-chaotic Feistel encryption process.

3.4 Key Features of the Proposed Method

The proposed encryption scheme provides several key advantages:

- Dynamic round-key generation, which enhances unpredictability and key sensitivity
- Integration of chaotic systems with DNA encoding, improving nonlinearity and randomness
- Feistel-based structure, enabling efficient and reversible encryption and decryption
- Lightweight operations, ensuring low computational complexity suitable for IoT devices
- Adaptive transformation mechanisms, which increase resistance against statistical and differential attacks

4. Experimental Results

4.1 Experimental Setup

The implemented hybrid DNA–chaotic Feistel encryption algorithm is coded in Python 3.10 and tested on typical test images: Lena and Baboon, 256×256 pixels, gray level images.

A combination of commonly used evaluation metrics was used to holistically determine the performance of the proposed scheme. They are histogram analysis, correlation coefficients, information entropy, Number of Pixel Change Rate (NPCR), and Unified Average Changing Intensity (UACI). These are the metrics used to assess the statistics, randomness and resistance of encryption algorithms to different attacks.

4.2 Visual Results

Fig. 3 shows the visual performance of the proposed encryption scheme. The encrypted images show the characteristics of noise without any structural information of the original images. This means that the proposed method is suitable to cover the picture information and does not produce any perception leakage of information.

This randomness in the visual domain is highly indicative of the high level of confusion that is crucial for safe image encryption in IoT applications.

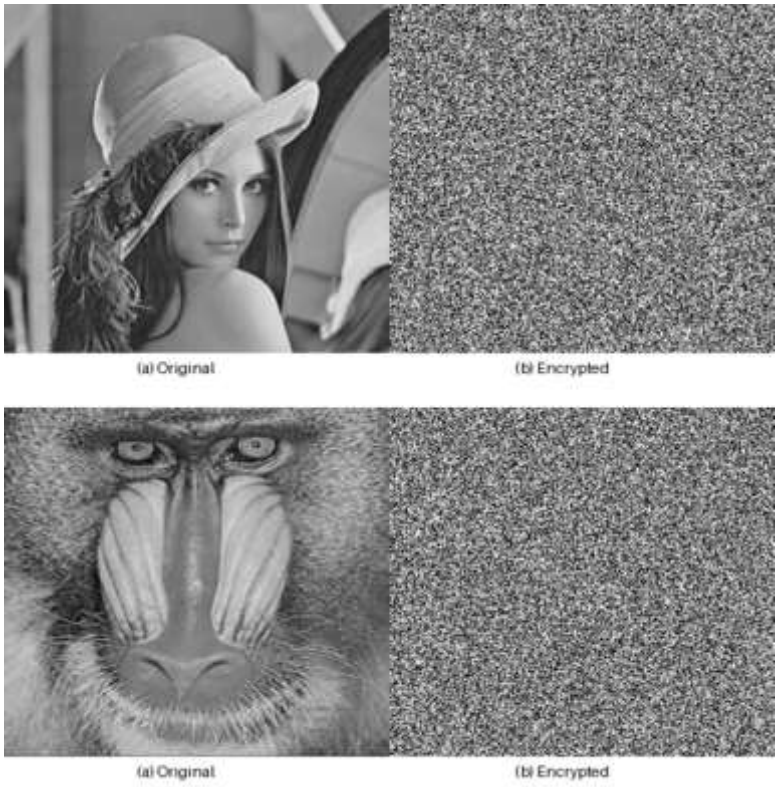

Fig. 3. Visual comparison between original & encrypted images for Lena & Baboon datasets: (a) original Lena, (b) encrypted Lena, (c) original Baboon, (d) encrypted Baboon.

4.3 Histogram Analysis

The histogram distribution of the encrypted images is shown in Fig. 4. The original images show non-uniform distributions, which are characteristic of the image, while the encrypted images show almost uniform distribution of the pixel intensity.

This uniformity shows that the proposed encryption algorithm is able to remove the statistical patterns in the original image and hence, less opportunity for statistical attack. As there are no clear peaks or patterns, the proposed scheme has a good capability of confusion.

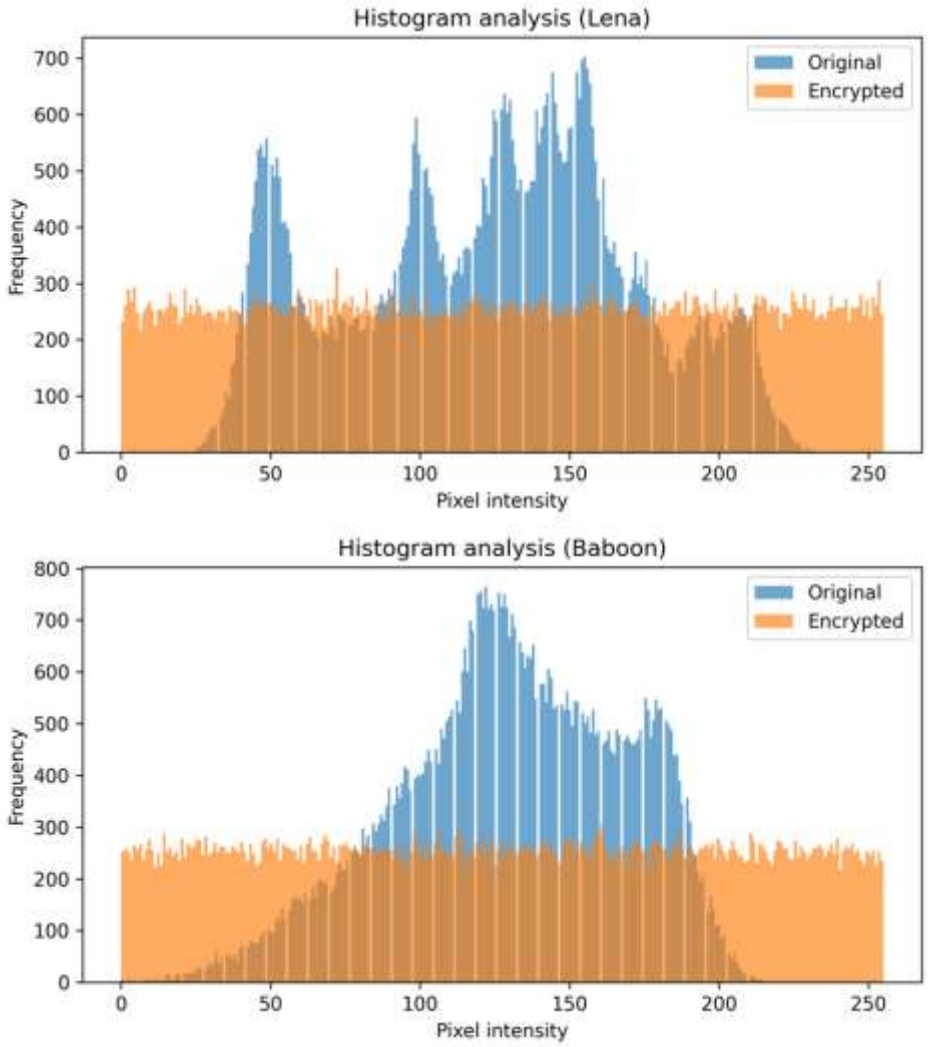

Fig. 4. Histogram analysis of the original and encrypted images for Lena and Baboon datasets.

4.4 Correlation Analysis

The correlation coefficient between the neighbouring pixels was computed in the horizontal, vertical and diagonal directions. As can be seen in the original images (Fig. 5 and Fig. 6), high correlation exists because the neighboring pixels are highly dependent on each other.

The results for the correlation coefficient of the encrypted images, on the other hand, are close to zero in all directions, which reflects the ability of the method presented to disrupt these dependencies. The correlation is significantly decreased, showing the high diffusion property of the encryption process, which is very important to resist against statistical attacks and differential attacks.

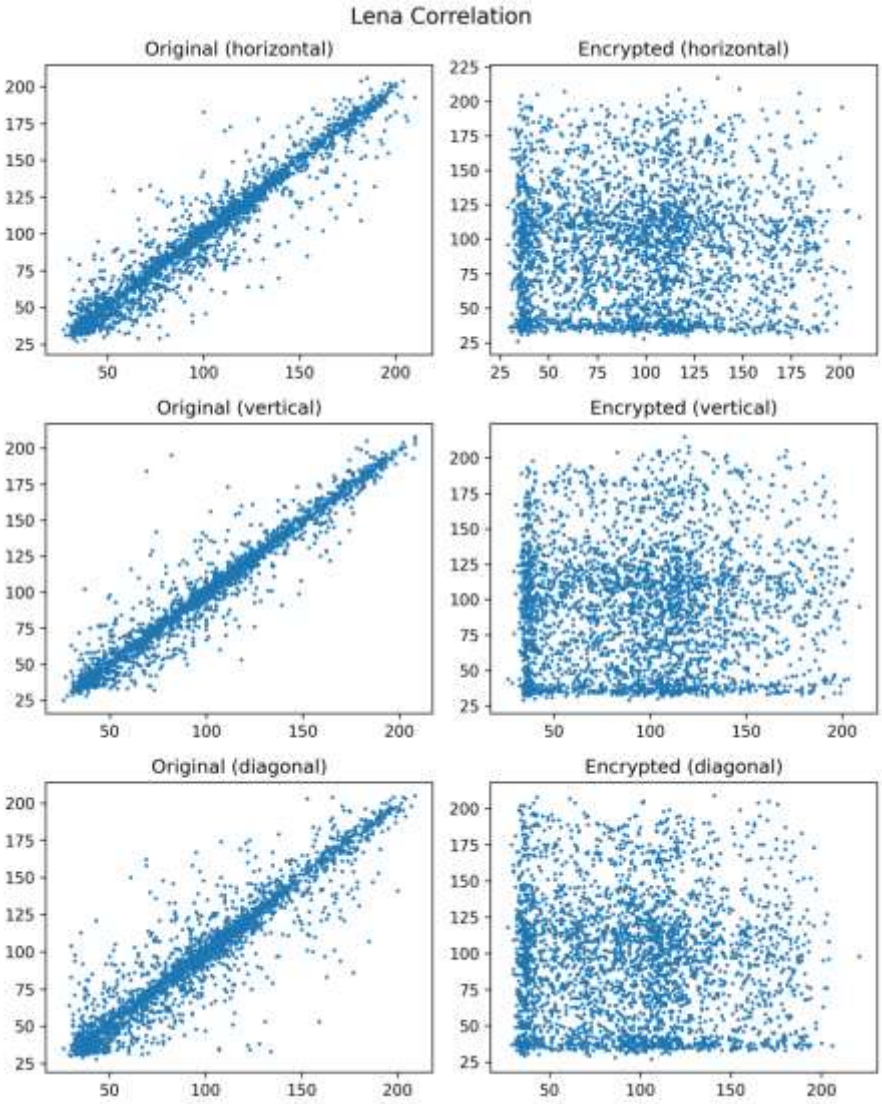

Fig. 5. Correlation distribution for Lena image.

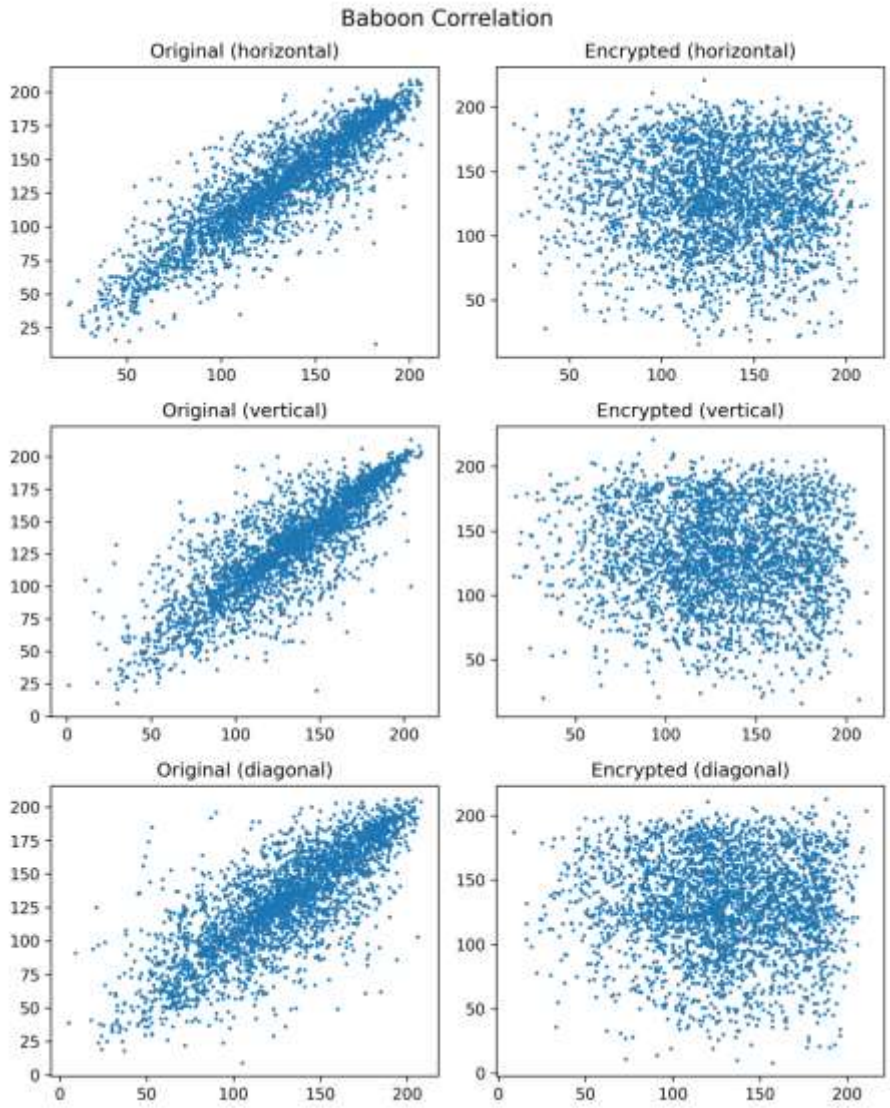

Fig. 6. Correlation distribution for Baboon image.

4.5 Information Entropy

One of the important parameters to assess the randomness of encrypted images is information entropy. An ideal 8-bit image will have an entropy value close to 8 which means that there is maximum unpredictability.

The entropy of the encrypted images is given in Table 1. The results indicate that the value obtained for Lena is 7.9872 and the value obtained for Baboon is 7.9473, which are very close to the ideal value. This reveals that high randomness and low information leakage can be seen in the encrypted images.

The result obtained entropy value is high which establishes that the proposed encryption algorithm is highly resistant to the entropy-based and statistical attacks.

Image	Entropy
Lena	7.9872
Baboon	7.9473

Table 1. Information entropy values of encrypted images for Lena & Baboon datasets.

4.6 Differential Attack Analysis

The evaluation of an encryption algorithm's sensitivity to small changes in the plaintext is done using differential attack analysis. Typically this is done by measuring it with the Number of Pixel Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) that describes the extent to which the algorithm generates different outputs of the same input, but with a small difference in the input.

Table 2 shows the results for the proposed method. For the Lena image, the NPCR and UACI values are 99.6017% and 33.4911%, respectively, while for the Baboon image, the values are 99.5307% and 33.4230%.

The obtained values are close to the theoretical optimal values (NPCR = 99.6% and UACI = 33.3%), which shows that the proposed encryption scheme is highly sensitive to the changes in the input. Such behaviour guarantees that even if the plaintext alters slightly, so will the encrypted image, which will be significantly unpredictable.

The results of the experiment reflect its high diffusion property and prove its robustness against differential attacks, making it more suitable for secure image transmission in IoT applications.

Image	NPCR (%)	UACI (%)
Lena	99.6017	33.4911
Baboon	99.5307	33.4230

Table 2. NPCR and UACI results of the proposed encryption algorithm for Lena and Baboon images.

Compared with existing methods, the proposed algorithm achieves competitive NPCR and UACI values while maintaining lower computational complexity.

4.7 Correlation Coefficients

To assess the dependency between the adjacent pixels in the image, correlation coefficients are used. Neighboring pixels are usually highly correlated in natural images because there is inherent redundancy in the images.

Table 3 displays the correlation coefficients of encrypted images in horizontal, vertical and diagonal directions. For the Lena image, the obtained values are 0.0098, −0.0062, and −0.0111, respectively, while for the Baboon image, the values are −0.0052, −0.0059, and −0.0029.

The values are close to zero, which means that the proposed encryption algorithm provides a good level of independence between neighbouring pixels. Considering the original images, this substantial decrease of the correlation shows that the proposed technique can generate statistically independent pixel distribution.

This behavior highlights the robustness of the diffusion and confusion properties of the encryption procedure, and thus its resistance to statistical attacks.

Image	Horizontal	Vertical	Diagonal
Lena	0.0098	-0.0062	-0.0111
Baboon	-0.0052	-0.0059	-0.0029

Table 3. Correlation coefficients of adjacent pixels in horizontal, vertical, and diagonal directions for the encrypted images.

4.8 Discussion

The experimental results show that the proposed hybrid DNA–chaotic Feistel encryption scheme has a good balance in terms of security performance and computation efficiency. The chaotic key generation, along with the adaptive transformations of the DNA, provides a great deal to the randomness and unpredictability of the encryption process.

The proposed method features nonlinearity, key sensitivity, and introduces dynamic (round-dependent) operations, in contrast to conventional methods using static encoding or key generation. This is demonstrated by the uniform performance over different evaluation parameters.

The statistical analysis shows that the patterns in the original images are indeed removed during the encryption process. The uniformity of the histogram distribution and the decrease in pixels correlation of the near uniformity distribution of the images suggest that the proposed method yields cipher images with low statistical leakage.

Moreover, the high entropy values and optimal values of NPCR and UACI indicate that the algorithm is highly resistant to both statistical and differential attacks. These results suggest that with small variations in the input, there are large and random variations in the encrypted output.

The proposed scheme is lightweight, has competitive security performance with respect to other existing lightweight schemes and is efficient due to its Feistel structure.

In summary, the proposed chaotic system, dynamic DNA encoding, and Feistel processing offer a powerful and efficient encryption solution that is suitable for practical IoT applications.

5. Conclusion

In this paper, a hybrid DNA–chaotic lightweight image encryption algorithm based on a Feistel network structure was proposed for the resource-limited IoT environments. The proposed framework combines the chaos driven key generation and adaptive DNA encoding, which makes it dynamic and round dependent, thus improving the randomness and the security strength.

The experimental results show that the proposed scheme possesses good confusion and diffusion characteristics because of its low correlation coefficient, high entropy and optimal NPCR and UACI. The results showed that the algorithm can effectively withstand the statistical attack, differential attack and maintain the efficiency of the calculation.

The proposed algorithm outperforms the current lightweight encryption techniques in terms of security performance and computational complexity, and hence it can be a potential candidate for real-world IoT applications.

Future research will involve optimizing the proposed scheme for real-time use and its extension to more complex multimedia data, as well as optimizing it for hardware-based implementation to achieve even higher performance.

References

[1] Ţălu, M. (2026). Performance evaluation of DNA-based cryptographic algorithms on constrained IoT devices. Journal of University of Technology and Informatics.

[2] Mahlake, N., et al. (2023). A lightweight encryption algorithm to enhance wireless sensor network security on the Internet of Things. Journal of Communications.

[3] Abdelaal, M. A., et al. (2025). DNA-inspired lightweight cryptographic algorithm for secure image encryption. Sensors.

[4] Amrita, et al. (2024). Lightweight cryptography for Internet of Things: A review. EAI IoT Journal.

[5] Dhakal, M., & Shakya, S. (2025). DNA cryptography and XOR-based Feistel encryption. Journal of Innovative Image Processing.

[6] Sekar, J. G., et al. (2023). Hybrid chaos-based image encryption using Chebyshev map with DNA. International Journal of Electrical and Computer Engineering.

[7] Mondal, M., & Ray, K. S. (2023). Review on DNA cryptography. International Journal of Bio-Inspired Computation.

[8] Aqeel, S., Khan, A. S., Abbasi, I. A., Algarni, F., & Grzonka, D. (2025). Enhancing IoT security with a DNA-based lightweight cryptography system. Scientific Reports, 15(1), 13367. https://doi.org/10.1038/s41598-025-96292-0

[9] Qaid, G. R. S., & Ebrahim, N. S. (2023). A lightweight cryptographic algorithm based on DNA computing for IoT devices.

[10] Ahmed, F., et al. (2022). A DNA-based colour image encryption scheme using a convolutional autoencoder.

[11] Patidar, V., & Kaur, G. (2023). A novel conservative chaos driven dynamic DNA coding for image encryption. Frontiers in Applied Mathematics and Statistics.

[12] Bhaya, C., et al. (2025). A DNA-based color image cryptosystem using chaotic maps, spiral mixing and nonlinear binary operator. Scientific Reports.

[13] Huang, L., et al. (2025). A DNA encoding image encryption algorithm based on chaos. Mathematics.

[14] Nujumudeen, F., et al. (2026). A hybrid chaos-based cryptographic framework for lightweight IoT security.

[15] Selvi, J. H. A., & Rajendran, T. (2025). DNA encoding and chaos based image encryption technique for cloud storage. Indian Journal of Science and Technology.