Journal of Engineering Issues and Solutions

Secure Grayscale Image Encryption Using DNA-Based Randomized Sequencing Technique and Pseudorandom Number Generation

Madhav Dhakal[1*], Hari Narayan Ray Yadav[2]

[1]Graduate School of Science and Technology, Mid-West University, Surkhet, Nepal
[2]Graduate School of Engineering, Mid-West University, Surkhet, Nepal
email address:[1] madhav.dhakal@mu.edu.np, [2]harinarayan.yadav@mu.edu.np
**Corresponding email: madhav.dhakal@mu.edu.np*
Received: November 25, 2025; Revised: 27 January, 2026; Accepted: March 21, 2026

Abstract

In this research, a random selection technique for sequencing DNA bases with a secret key encryption technique is proposed. Two layers of encryption techniques are proposed in this research. Here, the first layer is inspired by the Feistel structure which includes the mathematical logical operation, including the XOR operation. In this layer, the security of image date is maintained by the Pseudo Random Number Generation (PRNG) and the second layer is followed by the concept of the biological information transform process.

In this proposed technique, the generation of the permutation box depends upon the inputted image, which creates more randomness and makes it difficult to guess the secret key and maintain confidentiality from the intruder. Here, the seed value works as the private key. In this encryption technique, first, the original image is divided into various blocks of 256 bit size and padding is necessary if the last block does not contain the bits of 256 size and then data obtained from the blocks are XOR with the key value. After that, results obtained from this operation are transformed into the cipher image using the concept of DNA cryptography translation.

Keyword: *DNA computing, , Pseudo random number, Image security, Cryptography*

Introduction

Transmission of confidential information through the communication media is greatly increasing day by day. With the transmission of those data, the risk associated data are also increasing in the same ratio. To overcome these situations, the researchers are focused on the implementation of a new concept to secure the transmission media and data transmitted through them.

Several mathematical cryptographic approaches, like symmetric, anti-symmetric, and other techniques are a few concepts to maintain the confidentiality and integrity during the transmission of data through IoT- enable devices. Cryptography is the process of encrypting and decrypting data. Here, the encryption technique is carried out at the sender's side before transmission of data and decryption takes place at the

receiver's side after receiving the ciphertext data from the sender.

The main goal of cryptography is to protect the original message and its key value from the unauthorized parties until they reach the receiver. Commonly, the symmetric key technique and the asymmetric key technique are the techniques behind the cryptography process.

In asymmetric key encryption, data are encrypted and decrypted using distinct keys. Here, a set of two keys, including the private key and the public key, is given to each side. While the public key is available for public use, the private key is always kept confidential.

In the case of the transmission of image data, adjacent pixels have high correlation and redundancy, and thus the traditional mathematically based encryption techniques are not suitable for image data encryption. The primary concern of image data security is to maintain encryption that is resistant to various forms of attacks, including statistical attacks, exhaustive attacks, differential attacks, noise attacks, and others.

Nowadays, for the protection of data despite the other security techniques, DNA computing is extensively used in the encryption/ decryption process that Implements a reliable protection system that blocks unauthorized, attackers, and malicious users from accessing the original data content. Instead of representation of data in binary form as in the traditional-based encryption technique, in DNA-based encryption technique four nucleotides namely Adenine, Cytosine, Guanine, and Thymine are utilized for the data security purpose.

Related Work

Several researchers made contributions to the study of DNA based data security. The authors in (Zan et al., 2023) suggest a two-step picture encryption approach for DNA storage. The first layer implements the traditional based encryption technique, and the second layer is DNA storage channel encryption, which increases the complexity of DNA storage. The finding demonstrates that it is viable and capable of secure image encryption and decryption despite a DNA channel error rate greater than 20%.

It emphasizes the significance of unexpected transmission signals in an unreliable DNA storage medium. The fundamental idea behind the study applies unpredictable modulation signals to secure images in extremely error-prone DNA storage pathways. For securing data during transmission, the authors in ref. (Basu et al., 2019) proposed the concept of machine learning and DNA cryptography. This concept is derived from the principle of genetic information flow. Here, text data are secured on the basis of principles of genetic algorithms, which include conversion, transcription, and translation to encrypt and the reverse process to decrypt. Here, by using the variable length in Huffman encoding, the input text is first encoded in a 16-bit block, then performs the XOR operation with key values, and then the entire result is genetically encoded. In the same way, (Şatir&Kendirli, 2022) studied the use of biotechnological hardware in a symmetric DNA encryption technique. The amount of data being created worldwide is continuously increasing as network technologies continue to advance. Cryptography and steganography techniques have been employed to protect data from the past to the present. The use of DNA as the carrier medium is intended to increase the number of hidden bits and use biological tools as implementation tools. As a result, the concept shows its effectiveness with its capacity, measurement of exhaustive attack resistance capacity, as well as its randomness with the entropy value analysis.

In the study by (Akkasaligar & Biradar, 2016), the authors proposed a novel encryption technique combining chaotic maps and DNA encoding to protect digital medical images. Experimental results indicate that this algorithm offers high security, integrity, and robustness, making it well-suited for medical image encryption. However, while effective, the reliance on separate chaotic maps for odd and even pixels may introduce

computational complexity, and scalability for larger image datasets could be an area for further optimization.

For the purpose of data security during the transmission between sender and receiver, several traditional encryption methods, including Blowfish, Rivest-Shamir-Adleman (RSA), Data Encryption Standard (DES), and Advanced Encryption Standard (AES) for textual data are available. Those techniques, however, are not appropriate for image encryption to produce satisfactory results in terms of security and speed of encryption because of certain intrinsic characteristics of images, including large computational times, high correlation among neighboring pixels, bulky data capacities, and high redundancy (Yaghouti et al.,2017) .

In ref. (Chen et al., 2018) for secure transmission of the encrypted image data self adaptive permutation and Random DNA encoding concept is proposed. This research identifies the random DNA coding technique with fixed coding rules, self adaptive permutation and self synchronization of plain text as the three major contributions for achieving the secure encrypted image.

Methodology

Encryption/Decryption Rules

First of all the binary equivalent of the pixel values of images is transformed into four different DNA nucleotides. Here, the concept of Watson-Crick complementary rules, as Table 1, is implemented for encoding binary values into DNA (Dhakal & Shakya, 2025).

Table1: Binary to DNA encoding rule

Binary Digit	DNA Base Rule							
00	A	A	C	C	G	G	T	T
01	C	G	A	T	A	T	C	G
10	G	C	T	A	T	A	G	C
11	T	T	G	G	C	C	A	A

Encryption/Decryption Rule

In this study, the DNA-based encoding matrix is implemented with the different DNA encoding rules. This concept is based on the pixels of the image. The randomized selection of encoding technique is carried out as: (Index Io (i, j) mod 8), where i and j are the locations associated with pixel value.

Technique for Permutation box Generator

In our study, we used a seed value and the number of bits that define the size of the permutation box to create a pseudo-random number to keep the data safe. First, an empty list is defined that stores the random numbers that will be generated. A pseudo-random number rand_num is then generated with formula: *rand_num* =((seed*⌊48271⌋+⌊12345⌋)//65536)mod bits. If the number is not already in the list, then it is appended to the list to ensure uniqueness. This step is continued until the lists have the required number of unique elements equal to the specified number of bits. Finally, the list nums, representing the generated permutation box, are returned.

Working Model

In this technique, first of all plaintext image is converted into binary data and those data are split into a number of blocks including B1,B2,…Bn. Those blocks are shuffling via the permutation method and

splitting the result into two halves. Using the concept of a secret key scramble each half into two parts via XOR operations. The scrambled data is recombined and converted into DNA-bases (AT,C,G). It is processed through the biological steps like cellular translation (DNA →mRNA→tRNA→ reverse tRNA). Finally, turn back into binary to create the ciphertext image.

Decryption reverses the encryption flow: start with the cipher Image to retrieve binary data, then invert the tRNA, mRNA, and DNA transformations to recover the data block. Next, split into data blocks, apply XOR with the respective keys to obtain permuted data, and reverse the permutation and block operations to reconstruct the original plain image.

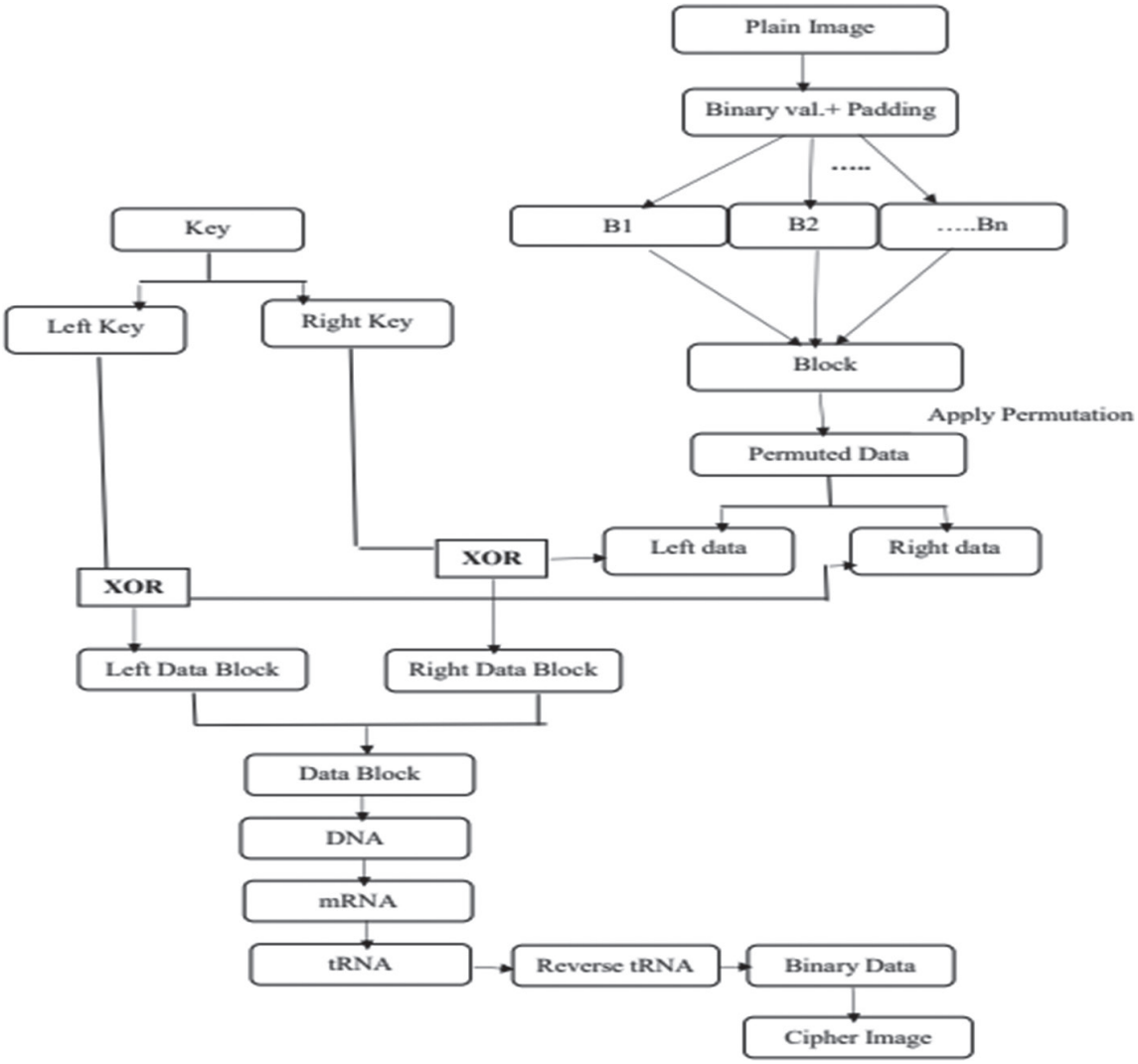

Figure 1: Steps in Proposed Method

Experimental Result and Security Analysis

Here, simulation results obtained through the encryption and decryption process are presented. Which clarify the proficiency and randomness of algorithm. The benchmark images Lena and Moon of size 256 x256 are taken from SIPI image database with TIFF format.

Figure 2: Encrypted and decrypted image of plain image

Statistical Attack Analysis

a. Histogram Analysis of Image

This diagram shows the distribution of pixel values of the image. During the experiment, it is clear that the pixel values in the histogram of the original plaintext image are not uniform. While the pixel intensity in histogram of the ciphertext image is evenly distributed. Which hides statistical detail of the image, and then we can say that it able to resist the image from a statistical attack.

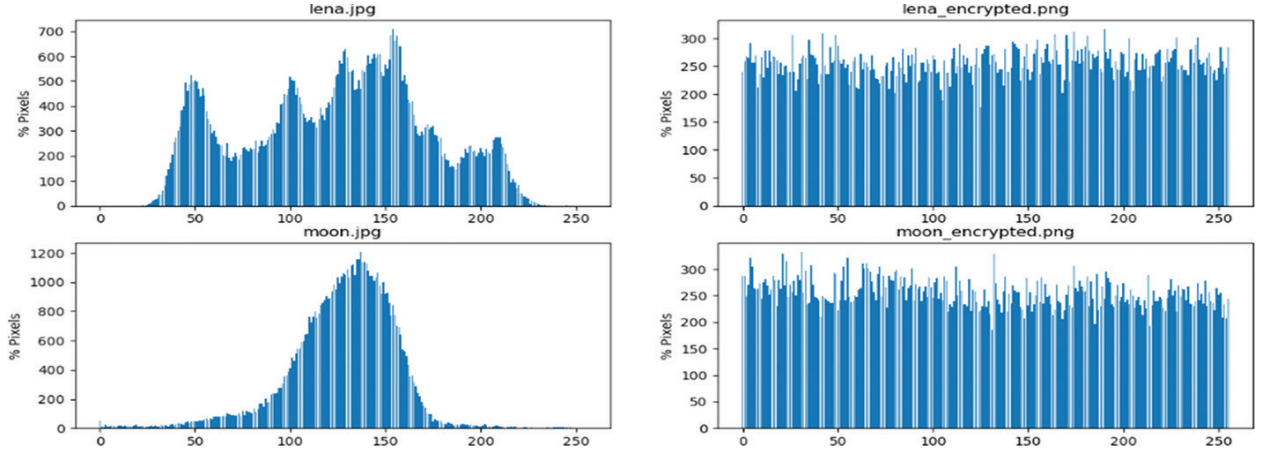

Figure 3: Histogram of images

This analysis gives the qualitative measurement of the pixel values. The chi-square test is performed to quantitatively analyze the pixel values. Here, the values of tested images are below the threshold value, i.e., 293.2. This result also ensures the random distribution of image pixels.

b. Correlation Analysis of Image

This analysis is performed to investigate the status of the associations among the pixels. Here, adjacent pixels are calculated in all three horizontal, vertical, and diagonal directions when analyzing image data correlations. It is assumed that when the pixel values are highly correlated, it is easier to retrieve the image information. Therefore, in a statistically secured image, correlation in pixels should be low (near to 0). Thus,

the algorithm should be structured to ensure that designed in such a way that the correlation in pixels has to be removed. In this study, correlation analysis between the original and encrypted images generated with the proposed concept is included in Table 2. Following formula is used to compute the correlation of image:

$$r_{x,y}=\frac{cov(x,y)}{\sqrt{D(x)}\ \sqrt{D(y)}}$$

Table 2: Correlation test result of Image

Image	Correlation			
	Plain Image		Cipher Image	
Lena	H	0.99712	H	-0.02161
	V	0.99225	V	-0.1041
	D	-0.35826	D	0.11221
Moon	H	0.98632	H	0.7108
	V	0.49097	V	0.11235
	D	0.23566	D	0.00667

c. Entropy Analysis of Image

Entropy measures the level of unpredictability of pixels of an image. In the highly encrypted image, the entropy value is high. The basic value of the randomness of image is 8. It means that if the randomness of the encrypted image is near the threshold value, then it is clear that the randomness in the pixels of image is high. The entropy of the images with the proposed concept is close to 8; thus, the proposed technique sustains the randomness in the image. Here, randomness of tested images are tabulated in Table 3. The formula for entropy value calculation of the grayscale image is as follows:

$H(x) = -\sum_{i=0}^{255} p(x_i) log p(x_i)$, Where, $x_i \in p(x)_i$ is the probability of occurrence of x_i,

Table 3: Image entropy measurements

Image	Entropy	
	Plaintext Image	Ciphertext Image
Lena	7.45109	7.9937
Moon	6.7189	7.9923

Differential Attack Analysis of Image

In this study, the differential attack over the encrypted image is calculated with two metrics: Number of pixels change rate (NPCR) and Unified average changing intensity (UACI).these concept is carried out to determine the how much the image is affected while tiny pixel value is change over the ciphertext image. Referring to (Wu & Agaian, 2011), NPCR & UACI values depend upon the image size and format of that image; the threshold values of NCPR and UACI of 256 image size is 99.6094% and 33.4635% respectively. In this study, these values for tested images are greater or nearly equal to these threshold values (as listed in Table 4). The obtained result shows that when we change the small pixel value of the image, then the proposed concept is highly sensitive, and the proposed concept exhibits resilience against differential attacks.

NPCR value is computed as: $NPCR = \frac{\sum_{i,j} D(i,j)}{M \; x \; N} x100\ \%$

$$D(i,j) = \begin{cases} 0 & C_1(i,j) = C_2(i,j) \\ 1 & Otherwise \end{cases}$$

UACI value is computed as: $UACI = \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255 * M * N} * 100\%$

Where, O_1 is the original plaintext image and O_2 image is caused by the alteration of one pixel in O_2. C_1 and C_2 are the ciphertext images of O_1 and O_2 respectively.

Table 4: Summary Report of Differential Attack

Image	NPCR	UACI
Lena	99.6353	33.6486
Moon	99.6002	33.4599

Conclusion

In this study, the grayscale image encryption concept uses the technique of random selection of DNA rules and pseudorandom number keys. Here, the pseudo key is generated with the permutation table. Here, the permuted pixels of the original image are decoded into a binary form. Then, XOR operation between the binary form of data and the secret key value is occurs. Finally, using the concept of DNA translation rules, each data block is represented in the form of the ciphertext image. Finally, the plaintext image is getting through the ciphertext image with the reverse concept of DNA translation. The results from the experiments demonstrate that the proposed encryption technique substantially improves and maintains the preservation of image confidentiality under various attacks, in contrast to the ideal values observed during transmission.

References

Akkasaligar, P. T., &Biradar, S. (2016). Secure medical image encryption based on intensity level using Chao's theory and DNA cryptography. *2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, 1–6. https://doi.org/10.1109/ICCIC.2016.7919681

Basu, S., Karuppiah, M., Nasipuri, M., Halder, A. K., &Radhakrishnan, N. (2019). Bio-inspired cryptosystem with DNA cryptography and neural networks. *Journal of Systems Architecture*, *94*, 24– 31. https://doi.org/10.1016/j.sysarc.2019.02.005

Chen, J., Zhu, Z., Zhang, L., Zhang, Y., & Yang, B. (2018). Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption. *Signal Processing*, *142*, 340–353. https://doi.org/10.1016/j.sigpro.2017.07.034

Dhakal, M., & Shakya, S. (2025). Enhancing Image Data Security: DNA Cryptography and XOR- Based Feistel Encryption. *Journal of Innovative Image Processing*, *7*(1), 1–27. https://doi.org/10.36548/jiip.2025.1.001

Zan, X., Chu, L., Xie, R., Su, Y., Yao, X., Xu, P., & Liu, W. (2023). An image cryptography method by highly error-prone DNA storage channel. *Frontiers in Bioengineering and Biotechnology*, *11*, 1173763. https://doi.org/10.3389/fbioe.2023.1173763

Şatir, E., &Kendirli, O. (2022). A symmetric DNA encryption process with a biotechnical hardware. *Journal of King Saud University - Science*, *34*(3), 101838. https://doi.org/10.1016/j.jksus.2022.101838

Wu, Y., & Agaian, S. (2011). *NPCR and UACI Randomness Tests for Image Encryption.*

Yaghouti Niyat, A., Moattar, M. H., & Niazi Torshiz, M. (2017). Color image encryption based on hybrid hyper-chaotic system and cellular automata. Optics and Lasers in Engineering, 90, 225–237. https://doi.org/10.1016/j.optlaseng.2016.10.019