A NEW APPROACH FOR THE IMAGE ENCRYPTION USING AES CIPHER IN ECB MODE

Auday H. AL-Wattar –

University of Mosul, Ahsa.alwattar@uomosul.edu.iq

Article History: Received: 06 June 2023; Accepted: 30 June 2023; Published Online: 08 July 2023

Abstract: The field of secure digital communication and data security has placed significant emphasis on the issue of image encryption. The present work introduces a unique methodology for improving image encryption by utilizing the Advanced Encryption Standard (AES) cipher in the Electronic Codebook (ECB) mode. The suggested methodology leverages the inherent resilience of AES while integrating a novel DNA-segment-based augmentation to reinforce the encryption process. This technique aims to mitigate the constraints associated with the Electronic Codebook (ECB) mode in picture encryption, with the ultimate goal of attaining an elevated standard of security and confidentiality. The efficacy of the suggested methodology is assessed through extensive experimentation, illuminating its potential to offer a sophisticated kind of image encryption that is well-suited for contemporary data security concerns.

Keywords: Image Encryption, Advanced Encryption Standard (AES), ECB Mode, DNA, Cryptography.

1.Introduction

In the current context of digital communication and data security, the practice of encrypting images plays a crucial role in protecting visual data from illegal access and manipulation. The intersection of cryptography and image processing has led to the development of sophisticated methods designed to guarantee the secrecy and integrity of images[1, 2]. This research investigates the field of image encryption, specifically emphasizing improving the security of the commonly utilized Advanced Encryption Standard (AES) algorithm when employed in the Electronic Codebook (ECB) mode. The present study examines the inherent vulnerabilities associated with the Electronic Codebook (ECB) mode in encryption. Additionally, it proposes a new and innovative method incorporating DNA-based segmentation to enhance the encryption process, increasing its resilience and intricacy level.

The widespread use of digital images in several domains, such as medical imaging and multimedia communication, requires the implementation of rigorous security protocols. Given its sensitive nature, encryption is paramount when contemplating visual data security. The Advanced Encryption Standard (AES), a highly regarded symmetric-key block cipher, possesses robust encryption features. Nevertheless, despite its simplicity and capacity to be processed in parallel, the ECB mode presents specific weaknesses due to its limited dissemination and preservation of patterns[3,4].

The deterministic characteristic of the ECB mode leads to the generation of identical ciphertext blocks when identical plaintext blocks are encrypted. Attackers can use this property to identify patterns within the encrypted data[5]. In order to address this issue, our suggested methodology aims to enhance the ECB mode by including DNA-based segmentation, hence introducing an additional level of intricacy. By associating pixel values with DNA bases, we establish an additional layer of complexity and dispersion, augmenting the overall security level in the picture encryption procedure.

DNA, widely recognized as the fundamental genetic code of living organisms, offers intrinsic characteristics that can be effectively utilized in cryptographic scenarios. The proposed method entails encoding pixel values into their corresponding DNA bases by utilizing predetermined mapping. The DNA sequences are subsequently employed to generate DNA-enhanced bytes integrated with the initial pixel values before undergoing AES encryption. Incorporating DNA-based segmentation brings about a non-linear transition, decreasing the effectiveness of conventional assault vectors[6-8].

Incorporating DNA-based segmentation gives rise to inquiries regarding the computational burden and viability of the suggested methodology. This work aims to comprehensively examine the effects of DNA-based segmentation on the performance of encryption and decryption, considering the inherent resource-intensive nature of AES encryption. The essential consideration lies in striking a balance between the strength of increased encryption and the computational practicality, especially in scenarios that necessitate real-time processing and transmission[9-11].

DNA-based segmentation is added to this study's usual ECB mode of AES encryption. Thus, we hope to overcome the deterministic nature of the ECB mode and improve image encryption security. Our method should strengthen encryption, protecting visual data from new attack vectors. The technology will be tested extensively to prove its efficacy and efficiency, enabling it to contribute substantially to picture encryption and data security.

Combining cryptography, image processing, and DNA-based structure complexity offers a chance to improve image encryption. This study hopes to advance secure picture communication by revealing the unique capabilities of DNA-based segmentation in AES encryption in ECB mode. The following parts will cover the technical specifics, experimentation, and analysis needed to prove the approach's efficacy and practicality [12, 13].

2. Image Encryption and AES Cipher

Image encryption is utilized to safeguard visual data that is considered secure. In order to protect privacy and ensure the integrity of digital environments, it is imperative to enhance the level of encryption employed[1, 14, 15]. The process of converting plain data into ciphered data through the application of cryptographic methods renders it incomprehensible without the utilization of decryption mechanisms.

The Advanced Encryption Standard (AES), a government-approved encryption standard, is the basis for contemporary cryptography. The process of encrypting and decrypting data is accomplished through the use of AES, which is a symmetric-key block cipher. The power of the substitution-permutation network structure lies in its composition of rounds, including intricate transformations such as substitution, permutation, and mixing[16, 17].

2.3 Modes of AES Operation

The Advanced Encryption Standard (AES) offers a range of operation modes that can accommodate diverse encryption settings. One example of a method is the Electronic Codebook (ECB) mode, which involves dividing the plaintext data into blocks and encrypting each block separately using a shared key. Nevertheless, the deterministic structure of ECB mode presents weaknesses since when identical plaintext blocks are encrypted, they produce similar ciphertext blocks[18]. This characteristic renders ECB mode susceptible to pattern-based attacks, which might potentially disclose information about the original image[18-20].

3. Weaknesses of ECB Mode

3.1 Electronic Codebook (ECB) Mode

The Electronic Codebook (ECB) mode is a cryptographic technique block ciphers used to encrypt plaintext into ciphertext. In this mode, each plaintext block is independently encrypted using the same encryption key, resulting in a one-to-one mapping between plaintext. Despite its simplicity and efficiency, the ECB mode does not possess the essential diffusion and confusion properties required to ensure strong encryption. The encryption process operates on each plaintext block individually, generating identical ciphertext blocks when identical plaintext blocks are encountered. As a result, patterns in the plaintext data remain evident in the ciphertext, allowing attackers to exploit these patterns and extract information about the original image[21, 22].

3.2 Limitations of ECB Mode

The deterministic characteristics inherent in the ECB mode give rise to several vulnerabilities. For example, when identical blocks are present in the original image, they are preserved as identical blocks in the encrypted image, potentially enabling attackers to discern recurring patterns. Furthermore, the absence of diffusion in the encryption algorithm results in localized impacts on the output when alterations are made to the input data. Consequently, this vulnerability makes the encryption process open to statistical examination[23, 24].

3.3 Requirements for Improvement

Considering all of these flaws, improving the protection of image encryption in ECB mode becomes essential. One way to improve the security of the encryption process is to introduce new variables that cause disruption and increase confusion and dissemination.

4. Concept and Advantages of DNA-based Segmentation

4.1 Overview of DNA-based Segmentation

Using DNA-based structures in cryptography is an innovative approach that leverages DNA sequences' inherent intricacy and unpredictability. The notion entails converting pixel values into equivalent DNA bases, adding a transformation layer to the encryption process[25, 26].

4.2 Exploiting the Characteristics of DNA

The utilization of DNA in encryption can be enhanced due to its inherent characteristics, including sequence variety, non-linearity, and non-repeatability. The disruption of standard encryption systems can be achieved by mapping pixel values to DNA bases, diminishing the deterministic nature of these methods and reducing the effectiveness of classic attacks[27, 28].

4.3 The Process of Assigning DNA Bases to Pixel Values

Mapping pixel values to DNA bases entails establishing a correlation between pixel intensity levels and certain DNA bases. The novel approach of mapping described here establishes a connection between the digital domain of images and the biological domain of DNA, providing a notable degree of intricacy to the encryption procedure[29, 30].

5.The Proposed Method

Considering the constraints associated with the Electronic Codebook (ECB) mode in picture encryption, we provide a novel methodology incorporating DNA segments into the AES encryption framework. This approach aims to perturb recurring patterns present in images, hence augmenting the level of security in encryption.

Encryption process

1. ***Generating DNA Sequences from Image Data:***

The binary representation of each pixel value in the image will be converted into a corresponding DNA base using a predetermined mapping.

2. ***Converting DNA Sequences into Bytes:***

Converting DNA bases into bytes involves assigning a numerical value to each base. Specifically, the nucleotide A is represented as 00, C as 01, G as 10, and T as 11. This process generates a sequence of bytes that serves as a representation of the DNA sequence.

3. ***Combining DNA-Enhanced Data with Image Data:***

The process involves performing an XOR operation on each original image data byte with the DNA-enhanced data's corresponding byte. This process involves the integration of picture data with DNA-enhanced data.

Combined Data (C(i)) = Image Data (I(i)) XOR DNA-Enhanced Byte (B(i mod len(B)))

4. ***AES Encryption of Combined Data:***

The combined data should be encrypted using the Advanced Encryption Standard (AES) method and a confidential secret key. The AES encryption procedure generates the encrypted data, which is prepared for secure transmission or storage.

Encrypted Data *(E(i)) = AES_Encrypt(C(i), Secret Key (K))*

Decryption Process:

1. **AES Decryption of Encrypted Data***:*

The encrypted data can be decrypted using the identical secret key utilized during the encryption process. The procedure above facilitates the retrieval of aggregated data.

Decrypted Data *(D(i)) = AES_Decrypt(E(i), Secret Key (K))*

2. Recovering DNA-Enhanced Bytes:

The DNA-enhanced bytes can be extracted from the decrypted data using the identical modular arithmetic utilized during the encryption process.

DNA-Enhanced Byte (B(i mod len(B))) = Decrypted Data (D(i)) XOR Image Data (I(i))

3. Converting DNA-Enhanced Bytes to DNA Sequence:

The objective is to reverse the process of turning DNA bases into bytes and recover the original DNA sequence afterward.

4. Reconstructing Original Image Data:

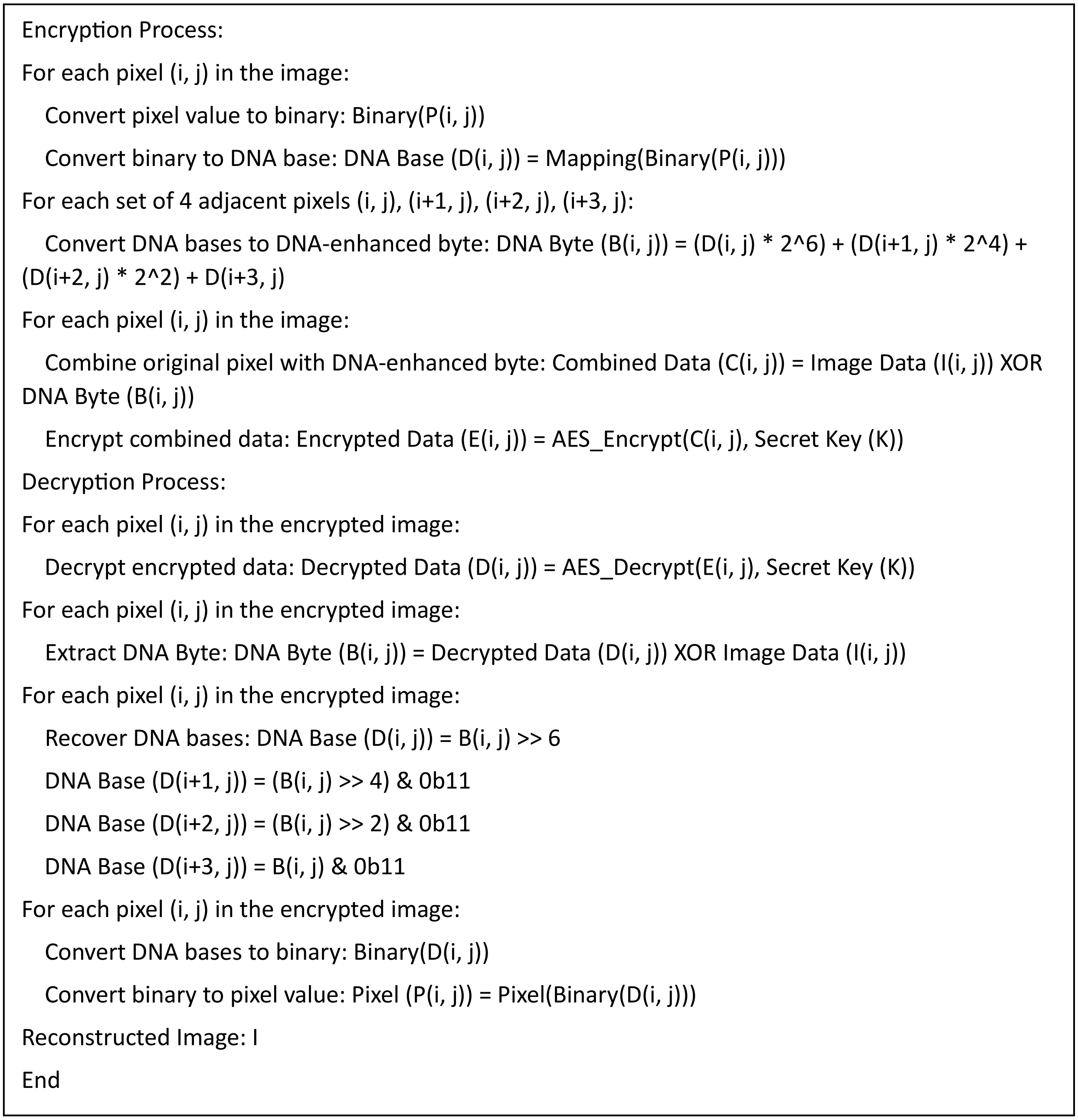
Utilize the inverse mapping technique to convert the DNA sequence into binary data. The original image can be reconstructed by interpreting the binary data as pixel values.

Figure 1 shows the general pseudo-code for the proposed method to encrypt the image using AES in ECB mode using DNA segment, both encryption and decryption processes using DNA segment.

```
Proposed DNA-Enhanced AES-ECB Image Encryption Algorithm:
Start
Input: Original Image Data (I), Secret Key (K)
For each pixel (P(i, j)) in I:
Convert pixel to binary: Binary(P(i, j))
Generate DNA base: D(i, j) = Mapping(Binary(P(i, j)))
For each set of 4 adjacent pixels (P(i, j), P(i+1, j), P(i+2, j), P(i+3, j)):
Convert DNA bases to DNA byte: B(k) = D(i, j) * 2^6 + D(i+1, j) * 2^4 + D(i+2, j) * 2^2 + D(i+3, j)
For each pixel (P(i, j)) in I:
Compute combined data: C(i, j) = Image Data (I(i, j)) XOR DNA-Enhanced Byte (B(k))
For each pixel (P(i, j)) in I:
Encrypt combined data: E(i, j) = AES_Encrypt(C(i, j), K)
Encrypted Image Data: E
Input: Encrypted Image Data (E), Secret Key (K)
For each pixel (P(i, j)) in E:
Decrypt encrypted data: D(i, j) = AES_Decrypt(E(i, j), K)
For each set of 4 adjacent pixels (P(i, j), P(i+1, j), P(i+2, j), P(i+3, j)):
Extract DNA-enhanced byte: B(k) = D(i, j) XOR Image Data (I(i, j))
For each pixel (P(i, j)) in I:
Recover DNA bases: D(i, j) = B(k) >> 6, D(i+1, j) = (B(k) >> 4) & 0b11, D(i+2, j) = (B(k) >> 2) & 0b11, D(i+3, j) =
B(k) & 0b11
For each pixel (P(i, j)) in I:
Convert DNA bases to binary: Binary(D(i, j))
Convert binary to pixel value: P(i, j) = Pixel(Binary(D(i, j)))
Recovered Image Data: I
End
```

Figure 1 :General pseudo-code for the proposed method to encrypt the image using AES in ECB mode using DNA segment

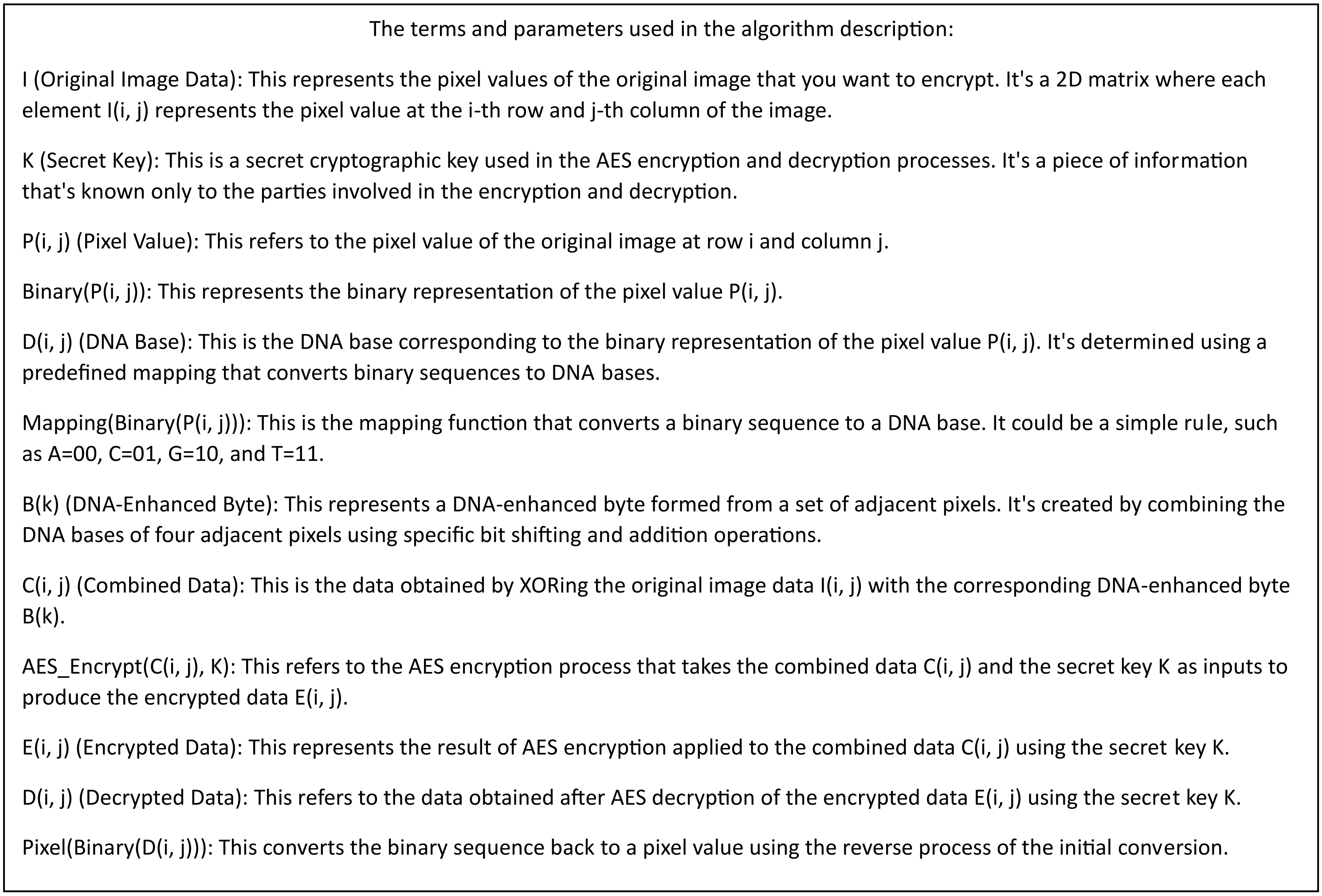
Figure 2 shows the more detailed pseudo-code algorithm.



```
Encryption Process:
For each pixel (i, j) in the image:
    Convert pixel value to binary: Binary(P(i, j))
    Convert binary to DNA base: DNA Base (D(i, j)) = Mapping(Binary(P(i, j)))
For each set of 4 adjacent pixels (i, j), (i+1, j), (i+2, j), (i+3, j):
    Convert DNA bases to DNA-enhanced byte: DNA Byte (B(i, j)) = (D(i, j) * 2^6) + (D(i+1, j) * 2^4) + (D(i+2, j) * 2^2) + D(i+3, j)
For each pixel (i, j) in the image:
    Combine original pixel with DNA-enhanced byte: Combined Data (C(i, j)) = Image Data (I(i, j)) XOR DNA Byte (B(i, j))
    Encrypt combined data: Encrypted Data (E(i, j)) = AES_Encrypt(C(i, j), Secret Key (K))
Decryption Process:
For each pixel (i, j) in the encrypted image:
    Decrypt encrypted data: Decrypted Data (D(i, j)) = AES_Decrypt(E(i, j), Secret Key (K))
For each pixel (i, j) in the encrypted image:
    Extract DNA Byte: DNA Byte (B(i, j)) = Decrypted Data (D(i, j)) XOR Image Data (I(i, j))
For each pixel (i, j) in the encrypted image:
    Recover DNA bases: DNA Base (D(i, j)) = B(i, j) >> 6
    DNA Base (D(i+1, j)) = (B(i, j) >> 4) & 0b11
    DNA Base (D(i+2, j)) = (B(i, j) >> 2) & 0b11
    DNA Base (D(i+3, j)) = B(i, j) & 0b11
For each pixel (i, j) in the encrypted image:
    Convert DNA bases to binary: Binary(D(i, j))
    Convert binary to pixel value: Pixel (P(i, j)) = Pixel(Binary(D(i, j)))
Reconstructed Image: I
End
```

Figure 2: More detailed pseudo-code algorithm to encrypt the image using AES in ECB mode using DNA segment

Figure 3: Shows the terms and the parameters used in the proposed algorithm description.



The terms and parameters used in the algorithm description:

I (Original Image Data): This represents the pixel values of the original image that you want to encrypt. It's a 2D matrix where each element I(i, j) represents the pixel value at the i-th row and j-th column of the image.

K (Secret Key): This is a secret cryptographic key used in the AES encryption and decryption processes. It's a piece of information that's known only to the parties involved in the encryption and decryption.

P(i, j) (Pixel Value): This refers to the pixel value of the original image at row i and column j.

Binary(P(i, j)): This represents the binary representation of the pixel value P(i, j).

D(i, j) (DNA Base): This is the DNA base corresponding to the binary representation of the pixel value P(i, j). It's determined using a predefined mapping that converts binary sequences to DNA bases.

Mapping(Binary(P(i, j))): This is the mapping function that converts a binary sequence to a DNA base. It could be a simple rule, such as A=00, C=01, G=10, and T=11.

B(k) (DNA-Enhanced Byte): This represents a DNA-enhanced byte formed from a set of adjacent pixels. It's created by combining the DNA bases of four adjacent pixels using specific bit shifting and addition operations.

C(i, j) (Combined Data): This is the data obtained by XORing the original image data I(i, j) with the corresponding DNA-enhanced byte B(k).

AES_Encrypt(C(i, j), K): This refers to the AES encryption process that takes the combined data C(i, j) and the secret key K as inputs to produce the encrypted data E(i, j).

E(i, j) (Encrypted Data): This represents the result of AES encryption applied to the combined data C(i, j) using the secret key K.

D(i, j) (Decrypted Data): This refers to the data obtained after AES decryption of the encrypted data E(i, j) using the secret key K.

Pixel(Binary(D(i, j))): This converts the binary sequence back to a pixel value using the reverse process of the initial conversion.

Figure 3 : The terms and the parameters used in the proposed algorithm description

We will take the following example to show the Image Encryption using DNA-enhanced AES-ECB algorithm in practice. The following example shows the proposed algorithm practically with details.

Suppose we have a simple 2x2 grayscale image as follows:

Image Data (I):

100	**150**
200	**50**

Encryption Process:

Generating DNA Sequences from Image Data:

The process involves converting pixel values into binary representation, followed by mapping binary sequences to DNA bases using a specified scheme.

Binary(100) = 01100100

DNA Base = ACGTAC

Similarly, for other pixels.

Converting DNA Sequences into Bytes:

The process involves amalgamating DNA bases to form DNA-enhanced bytes, specifically for every set of four neighboring pixels.

DNA Byte = ACGTACACGT

Combining DNA-Enhanced Data with Image Data:

XOR original pixel values with DNA-enhanced bytes:

For pixel (1, 1):

Combined Data = 100 XOR ACGTACACGT

Similarly, for other pixels.

AES Encryption of Combined Data:

Encrypt the combined data using AES:

For pixel (1, 1):

Encrypted Data = AES_Encrypt(Combined Data, Secret Key)

Decryption Process:

AES Decryption of Encrypted Data:

Decrypt the encrypted data using AES:

For pixel (1, 1):

Decrypted Data = AES_Decrypt(Encrypted Data, Secret Key)

Recovering DNA-Enhanced Bytes:

Extract DNA-enhanced bytes from decrypted data:

For pixel (1, 1):

DNA Byte = Decrypted Data XOR 100

Converting DNA-Enhanced Bytes to DNA Sequence:

Convert DNA-enhanced bytes back to DNA bases:

For DNA Byte:

DNA Base = Reverse_Mapping(DNA Byte)

Reconstructing Original Image Data:

Map DNA bases back to binary and then to pixel values:

For DNA Base:

Binary = Reverse_Mapping(DNA Base)

Pixel = Binary_to_Pixel(Binary)

Reconstructed Image Data:

After completing steps 6 to 8 of the decryption process, we would obtain the reconstructed image data:

Reconstructed Image Data (I'):

100	**150**
200	**50**

6. Experiment Results

This section presents an empirical evaluation of the proposed AES-ECB image encryption method. This evaluation aims to gauge the method's performance, security, and limitations in a controlled experimental setting. Examining Figures 1 and 2 shows the difference between the utilization of encryption via the conventional approach of the standard and adapted encryption algorithms. Based on the observations made in Figure 4, it is evident that the image encryption method exhibits different features of the picture, thus indicating a need for more adequacy in the encryption process. Regarding Figure 5, it is evident that encrypting the picture results in the comprehensive hiding of the image's attributes, thereby nullifying all the qualities initially contained in the image. All the qualities that were originally included in the image.

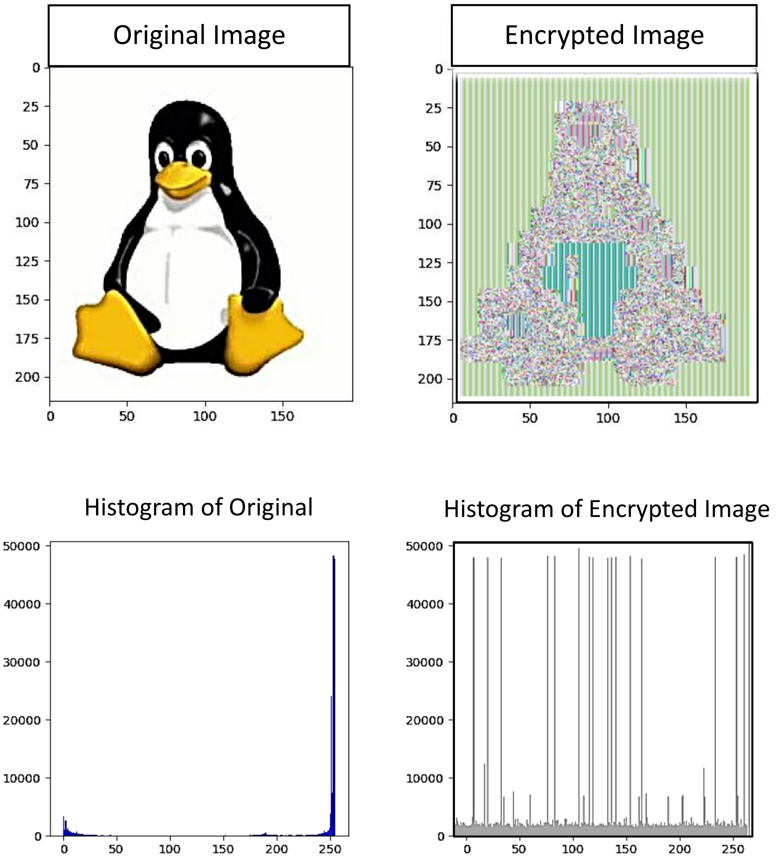


Figure 4: The encryption of the image using standard AES in ECB mode

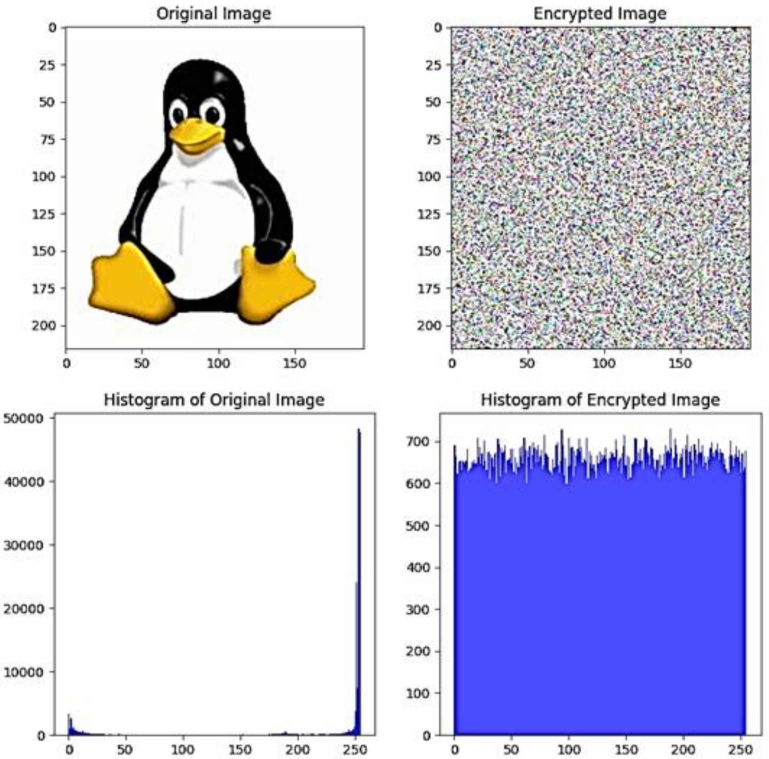


Figure 5: The encryption of the image using the proposed method

Figures 6 and 7 show the result of encrypting an image using the standard AES in ECB mode (figure 3) and the proposed method (figure 7). It is clear from the previous figures that the proposed method's encryption process has solved the problem of the standard encryption algorithm in encrypting images, as the figures and their histograms show the success of the proposed method in achieving its purpose.

6.1 PSNR and MSE

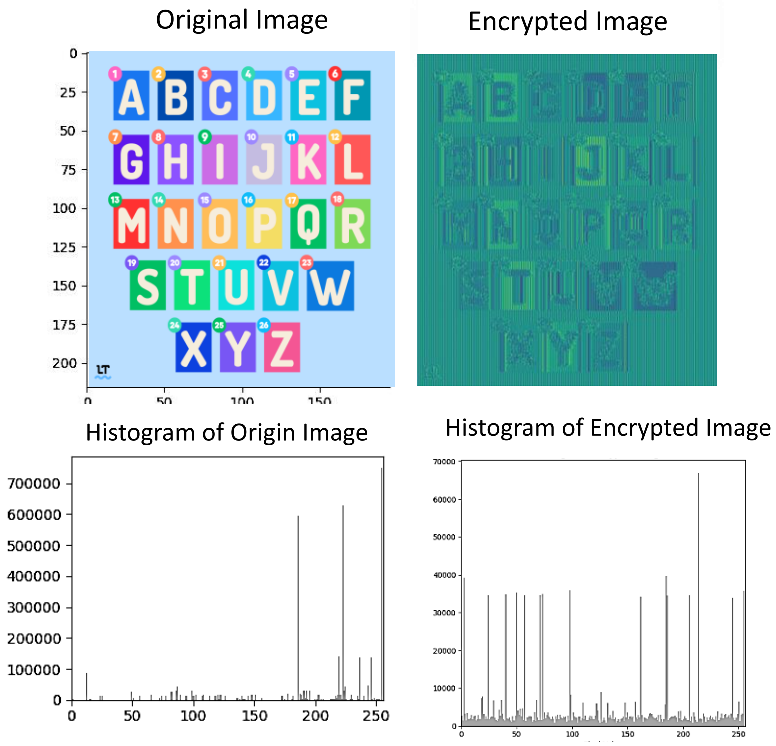


Figure 6 The encryption of the image using standard AES in ECB mode

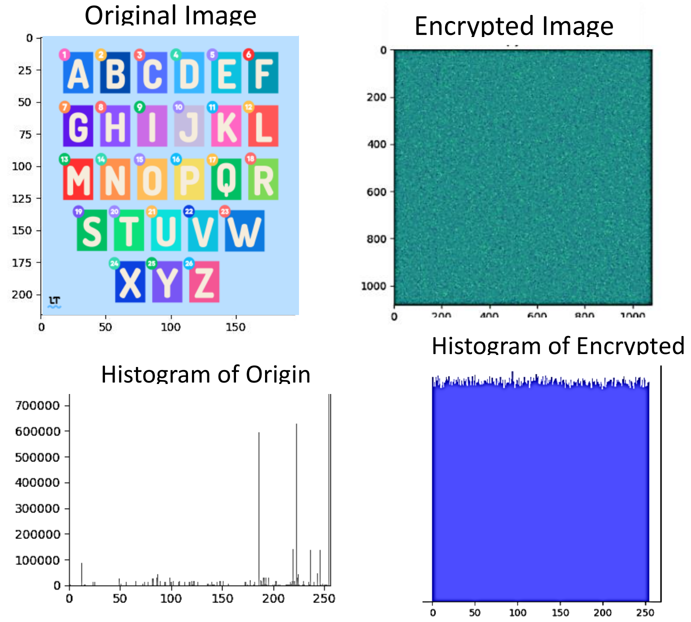


Figure 7: The encryption of the image using standard AES in

In picture encryption, the objective is to achieve greater values of PSNR (Peak Signal-to-Noise Ratio) and lower values of MSE (Mean Squared Error) to enhance image quality and maintain encryption fidelity.

The Peak Signal-to-Noise Ratio (PSNR) is a metric used to evaluate the quality of a signal by measuring the ratio between the maximum possible power of a signal and the power of the noise present in Greater PSNR levels, measured in decibels (dB), are indicative of superior image quality.

PSNR levels over 30 dB in several image processing applications are considered satisfactory.

A higher Peak signal-to-noise ratio (PSNR) indicates more excellent quality and the visual resemblance between the encrypted picture and the original image.

The Mean Squared Error (MSE) is a statistical metric that measures the average squared difference between the predicted and actual values in a dataset.

The desirability of lower Mean Squared Error (MSE) values lies in their indication of reduced disparity between the original and encrypted pictures.

MSE values that approach 0 indicate a low disparity between the original and encrypted pictures.

A lower mean squared error (MSE) value indicates a higher level of fidelity in picture encryption, suggesting that the encryption process effectively preserves image information with greater accuracy.

In brief, when assessing picture encryption algorithms, getting a substantial peak signal-to-noise ratio (PSNR) above 30 dB and a minimal mean squared error (MSE) approaching zero is desirable. These criteria are crucial to ascertain that the encryption procedure adequately maintains image quality while minimizing any potential distortion or loss of information. Nevertheless, the optimal parameters for encryption may differ depending on the particular demands of the application and the characteristics of the photos involved.

For the proposed method, the value of PSNR and MSE for the encrypted images was as follows:

The encrypted penguin image has a PSNR value of 5.06 dB and an MSE value of 20289.99

The encrypted alphabet image has a PSNR value of PSNR 5.06 dB and MSE: 20259.41.

The findings indicate that the suggested approach successfully produced favorable outcomes in picture encryption by effectively implementing the standard encryption technique during the ECP phase.

7. Conclusion

The method presented above illustrates a straightforward encryption technique employing AES-ECB and including other alterations derived from DNA bases. Nevertheless, it is crucial to acknowledge that the ECB mode has vulnerabilities in some contexts, mainly when employed for encrypting pictures, owing to the deterministic characteristics of the method.

References

[1] K. D. Patel and S. Belani, "Image encryption using different techniques: A review," *International Journal of Emerging Technology and Advanced Engineering,* vol. 1, pp. 30-34, 2011.

[2] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," *Archives of Computational Methods in Engineering,* vol. 27, pp. 15-43, 2020.

[3] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A modified AES based algorithm for image encryption," *International Journal of Computer and Information Engineering,* vol. 1, pp. 745-750, 2007.

[4] S. M. Wadi and N. Zainal, "High definition image encryption algorithm based on AES modification," *Wireless personal communications,* vol. 79, pp. 811-829, 2014.

[5] S. De and J. Bhaumik, "An aes-based robust image encryption scheme," *International Journal of Computer Applications,* vol. 109, pp. 29-34, 2015.

[6] J. Watada and R. binti abu Bakar, "DNA computing and its applications," in *2008 Eighth international conference on intelligent systems design and applications*, 2008, pp. 288-294.

[7] V. Kolate and R. Joshi, "An information security using DNA cryptography along with AES algorithm," *Turkish Journal of Computer and Mathematics Education,* vol. 12, pp. 183-192, 2021.

[8] M. Sabry, M. Hashem, T. Nazmy, and M. E. Khalifa, "Design of DNA-based advanced encryption standard (AES)," in *2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS)*, 2015, pp. 390-397.

[9] J. Kh-Madhloom, M. K. A. Ghani, and M. R. Baharon, "ECG Encryption Enhancement Technique with Multiple Layers of AES and DNA Computing," *Intelligent Automation & Soft Computing,* vol. 28, 2021.

[10] K. Sajisha and S. Mathew, "An encryption based on DNA cryptography and steganography," in *2017 international conference of electronics, communication and aerospace technology (ICECA)*, 2017, pp. 162-167.

[11] Q. S. Alsaffar, H. N. Mohaisen, and F. N. Almashhdini, "An encryption based on DNA and AES algorithms for hiding a compressed text in colored Image," in *IOP Conference Series: Materials Science and Engineering*, 2021, p. 012048.

[12] S. Sadeg, M. Gougache, N. Mansouri, and H. Drias, "An encryption algorithm inspired from DNA," in *2010 International Conference on Machine and Web Intelligence*, 2010, pp. 344-349.

[13] A. Kumar, "Data Security and Privacy using DNA Cryptography and AES Method in Cloud Computing," in *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, 2021, pp. 1529-1535.

[14] P. Radhadevi and P. Kalpana, "Secure image encryption using AES," *International Journal of Research in Engineering and Technology,* vol. 1, pp. 115-117, 2012.

[15] I. Ozturk and I. Sogukpinar, "Analysis and comparison of image encryption algorithms," *International Journal of Information Technology,* vol. 1, pp. 108-111, 2004.

[16] S. Heron, "Advanced encryption standard (AES)," *Network Security,* vol. 2009, pp. 8-12, 2009.

[17] A. M. Abdullah, "Advanced encryption standard (AES) algorithm to encrypt and decrypt data," *Cryptography and Network Security,* vol. 16, p. 11, 2017.

[18] D. Blazhevski, A. Bozhinovski, B. Stojchevska, and V. Pachovski, "Modes of operation of the AES algorithm," 2013.

[19] S. Almuhammadi and I. Al-Hejri, "A comparative analysis of AES common modes of operation," in *2017 IEEE 30th Canadian conference on electrical and computer engineering (CCECE)*, 2017, pp. 1-4.

[20] J. A. Artiles, D. P. Chaves, and C. Pimentel, "Image encryption using block cipher and chaotic sequences," *Signal processing: image communication,* vol. 79, pp. 24-31, 2019.

[21] B. Schneier, "Algorithm Types and Modes," *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C,* pp. 189-211, 2015.

[22] H. S. Mohan and A. R. Reddy, "Revised aes and its modes of operation," *International Journal of Information Technology,* vol. 5, pp. 31-36, 2012.

[23] C.-W. Huang, Y.-H. Tu, H.-C. Yeh, S.-H. Liu, and C.-J. Chang, "Image observation on the modified ECB operations in Advanced Encryption Standard," in *International Conference on Information Society (i-Society 2011)*, 2011, pp. 264-269.

[24] M. Hassan and M. Hussein, "NETWORK SECURITY BY BLOCK CIPHERS," *Journal of Al-Azhar University Engineering Sector,* vol. 15, pp. 981-991, 2020.

[25] B. T. Hammad, A. M. Sagheer, I. T. Ahmed, and N. Jamil, "A comparative review on symmetric and asymmetric DNA-based cryptography," *Bulletin of Electrical Engineering and Informatics,* vol. 9, pp. 2484-2491, 2020.

[26] A. Gehani, T. LaBean, and J. Reif, "DNA-based cryptography," *Aspects of molecular computing: essays dedicated to tom head, on the occasion of his 70th birthday,* pp. 167-188, 2004.

[27] S. Cresci, R. Di Pietro, M. Petrocchi, A. Spognardi, and M. Tesconi, "Exploiting digital DNA for the analysis of similarities in Twitter behaviours," in *2017 IEEE International Conference on Data Science and Advanced Analytics (DSAA)*, 2017, pp. 686-695.

[28] A. JarJar, "Two advanced classics exploiting DNA and RNA characteristics to encrypt a color image," *Multimedia Tools and Applications,* vol. 80, pp. 24603-24629, 2021.

[29] H. Liu and X. Wang, "Image encryption using DNA complementary rule and chaotic maps," *Applied Soft Computing,* vol. 12, pp. 1457-1466, 2012.

[30] X.-Y. Wang, P. Li, Y.-Q. Zhang, L.-Y. Liu, H. Zhang, and X. Wang, "A novel color image encryption scheme using DNA permutation based on the Lorenz system," *Multimedia Tools and Applications,* vol. 77, pp. 6243-6265, 2018.