# An Image Encryption Technique based on DNA Encoding and Round-reduced AES Block Cipher

Eman Shehab
Faculty of Computers and Information, Menofia University, Shebin El-kom, Menofia, Egypt

AbdelAlim K. Farag
Faculty of Computers and Information, Menofia University, Shebin El-kom, Menofia, Egypt

Arabi Keshk
Faculty of Computers and Information, Menofia University, Shebin El-kom, Menofia, Egypt

## ABSTRACT

Despite the difficulties of applying DNA computational tool on cryptography, a new direction in DNA cryptography research is performed to provide data and information security. DNA can be used to store and transmit the information and also to perform computation. Using block ciphers, images have poor encryption effect due to their intrinsic features such as bulky data capacity and high data redundancy. In this paper, a combination of DNA computing and round-reduced AES block cipher is proposed. The proposed technique can be used not only to achieve a high level of security but also to obtain fast implementation.

## General Terms:

Information Security, Cryptography

## Keywords:

AES, DNA, Image Encryption

## 1. INTRODUCTION

Information security is the science of protecting information from unauthorized access or use. Confidentiality, integrity and availability are the key principals of information security, which should be guaranteed the security of the system. Cryptography is the technique which provides these information security principals. It has become a very critical aspect of modern computing systems to secure the data transmission and storage [1]. The main processes in cryptography are encryption and decryption; encryption is the process of encoding information (plaintext) such that the only authorized persons can access it. A cryptographic algorithm is used to encode the information and turning it to (ciphertext). On the other hand, decryption is the decoding process in which the ciphertext can be converted back to the plaintext based on the decryption algorithm. The Advanced Encryption Standard (AES) has become the default choice for various applications since its adoption as a new encryption standard by NIST in 2001 [7]. It is a symmetric block cipher that processes data blocks of 128-bits using a cipher key of length 128, 192 or 256 with number of rounds $Nr$=10, 12, or 14 respectively. Fig. 1 shows the AES encryption algorithm.

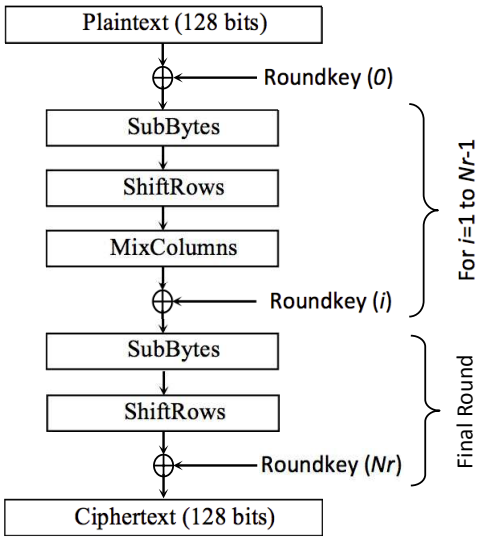



Fig. 1: 128-bits AES encryption algorithm.

In this figure, the data block consists of an array of 4x4 bytes called a state. Four different transformations are applied on the state: SubBytes, ShiftRows, MixColumns and add RoundKey. The four transformation are described briefly as follows:

(1) Add round key transformation: The XOR operation is applied between the state and the round key. In decryption process, this transformation is its own inverse.

(2) SubByte transformation: Is a non-linear byte substitution function. This function can be described in a substation table called s-box, which is constructed by multiplicative inverse and Affine transformation. Fig. 2 shows the SubByte transformation. In decryption process, the inverse SubByte transformation can be used.

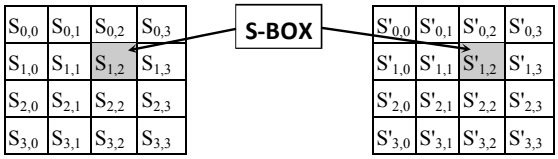



Fig. 2: SubByte in each byte in the state matrix.

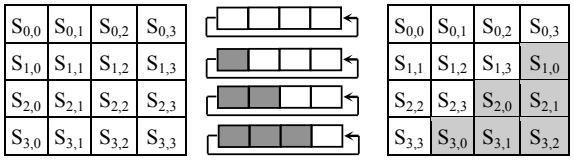


Fig. 3: ShiftRows transformation.

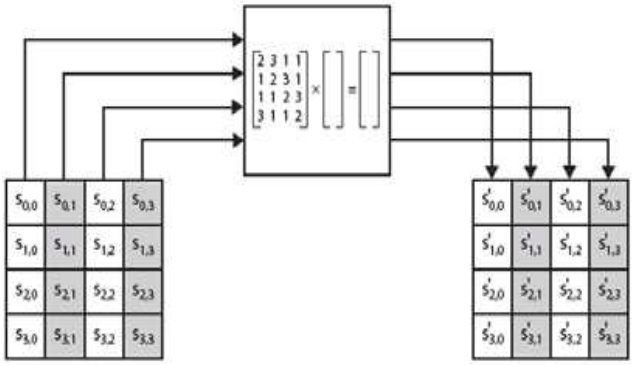


Fig. 4: MixColumns transformation.

(3) ShiftRows transformation: The bytes in the last three rows of the state are cyclically shifted to left; the left shift varies from one to three bytes. Fig. 3 shows the ShiftRows transformation. The cyclical right shift can be used in the decryption process.

(4) MixColumns transformation: In this transformation each column of the state multiplied by a fixed matrix. In this multiplication, the bytes are treated as polynomials rather than numbers. Fig. 4 shows the MixColumns transformation. In the decryption process, the inverse MixColumns can be used in which the fixed matrix is different.

Deoxyribo nucleic acid (DNA) is a nucleic acid that represents the genetic blueprint of living creatures. The main advantage of DNA molecules is that it can store huge amount of information. DNA is made up of two twisted strands of nucleotides. Each nucleotide composed of a phosphate group, a deoxyribose sugar, and four bases: A-Adenine, C-Cytosine, T-Thymine and G-Guanine. Theses four bases represent the genetic code where 'A' and 'T' are complementary, and 'G' and 'C' are complementary [3]. Fig. 5 shows the structure of double stranded DNA sequence [9]. This paper is organized as follows: The related work is introduced in section 2. The proposed image encryption scheme is described in section 3. In section 4, the results and the security analysis of the proposed scheme are presented. Finally, The conclusion of the paper is presented.

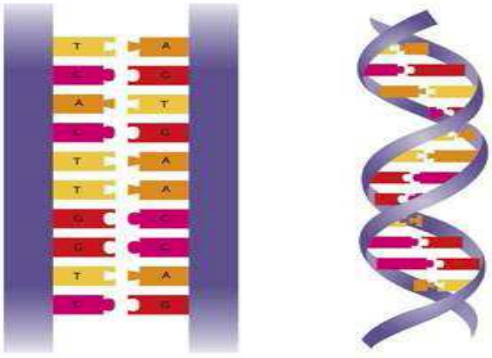


Fig. 5: Structure of double stranded DNA.

## 2. RELATED WORK

In this section related methodologies and techniques to design a secure symmetric image encryption are presented. In [13], Zeghid *et al.* presented a modified AES based algorithm in which a key stream generator (A5/1, W7) is added to AES to ensure improving the encryption performance. In [10], Wadi and Zainal modified the AES algorithm to be used for images ciphering especially the HD images. Their modifications are applied by decreasing the number of rounds to one and by replacing the S-box with a new S-box to decrease the hardware requirements. Their experimental results ensure that the proposed work make AES algorithm faster while fulfill the security requirements.
In [5], an RGB image encryption algorithm based on DNA encoding and chaos map is proposed. The proposed algorithm effectively eliminates the pixels correlation of the RGB image in the spatial domain by using DNA addition operation. Also, in order to increase security, a combined chaotic system is used to disturb the value of the pixels. In [6], Mandal *et al.* presented an image encryption process based on chaotic logistic map. The XOR operations and pixel shuffling of the image are used to confuse and defuse the pixel value and pixel position. In [11] a novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system is proposed. The positions of pixels are scrambled by Chens hyper-chaotic system and the pixel grey values of the original image are scrambled by DNA sequence addition operation.

## 3. PROPOSED WORK

Using AES algorithm, images have poor encryption effect due to their intrinsic features such as bulky data capacity and high data redundancy. To overcome this problem, in this paper, a new method of encryption/decryption and its application for images ciphering is presented. In this method, a combination of AES cryptographic algorithm and DNA computing is applied. This combination achieves high level of security rather than using AES algorithm only.
Algorithm 1 describes the proposed method. In this algorithm, the original image of size $n \times m$ pixels can be separated into $4 \times 4$ pixels size matrices so that each matrix can be encrypted using AES encryption/decryption algorithm. In this case, the cipher-block chaining (CBC) mode of operations is used. The proposed AES consists of two blocks: Firstly, a round-reduced of the AES-128 block cipher is used. Secondly, a DNA sequence can be chosen from the gene-bank database [12] to create a secret key and also to easily distribute it. The DNA sequence is XORed with the output of the first block.

The DNA-sequence can be exchanged between different parities using key exchange scheme. In this scheme the parities can agree on the type of entirely sequenced genomes databases from different organisms and on the starting index and the size of this sequence. The main advantage of using this method is that it achieves high level of security and also it fulfills fast implementation.

**Algorithm 1** The pseudo code for the proposed encryption algorithm

**Require:** Plain-image[$n \times m$], key[$Nr$][$4 \times 4$], and DNA-key[$4 \times m$] bytes.
**Ensure:** Cipher-image[$nxm$] bytes.
1: Suppose that the plain-image size is $n \times m$ pixels and the state size is [$4 \times 4$] bytes.
2: **for** $i = 1$ step 1 to $n/4$ **do**
3:  **for** $j = 1$ step 1 to $m/4$ **do**
4:  AddRoundKey(state[$i, j$], key[0][$4 \times 4$]);
5:  **for** $r = 1$ step 1 to $Nr - 1$ **do**
6:  SubBytes(state[$i, j$]);
7:  ShiftRows(state[$i, j$]);
8:  MixColumns(state[$i, j$]);
9:  AddRoundKey(state[$i, j$], key[$r$][$4 \times 4$]);
10:  **end for**
11:  SubBytes(state[$i, j$]);
12:  ShiftRows(state[$i, j$]);
13:  AddRoundKey(state[$i, j$], key[$Nr$][$4 \times 4$]);
14:  **end for**
15: **end for**
16: //Note that: The DNA-key size is $4 \times m$ bytes, consequently, the state size will be changed to $4 \times m$ bytes.
17: **for** $i = 1$ step 1 to $n/4$ **do**
18:  xor(state[i], DNA-key);
19: **end for**

## 4. EXPERIMENTAL RESULTS

### 4.1 Experimental Results

This section describes the simulations carried out to evaluate the proposed encryption scheme and discusses their results. The experiments run on Matlab® software tool to implement the proposed encryption technique. Fig. 6 shows original and encrypted gray scale images used in the simulations. In these simulations, all images have dimensions $n \times m = 256 \times 256$ pixels.
Our experiments show that two rounds of AES block cipher is enough to achieve high level of security with low encryption time in comparison with the all rounds AES algorithm.

## 5. SECURITY ANALYSIS

The performance of our method is evaluated using different quantitative measures such as key space, statistical, and differential analysis.

### 5.1 Key Space Analysis

The key space is the total number of different keys that can be used for encryption. The key space must be large enough to repel the brute force attack. Nowadays, the scale of DNA gene-bank becomes larger and larger with the fast development in this branch of science. In our approach, DNA sequences are used as secret keys with sequence size $4 \times 256$. In addition to 128-bits for the round-reduced AES block cipher. So the key space of our approach is large enough to resist brute-force attacks.

### 5.2 Statistical Analysis

*5.2.1 Histogram Analysis.* Considering the statistical analysis of the original image and the encrypted image, Fig. 7 shows the histograms of original and encrypted image, respectively. In this figure, pixel values of original image are tortuous, but the corresponding histograms of encrypted image are very uniform which makes the statistical attacks difficult to recover the original images.

*5.2.2 Correlation Analysis of the Adjacent Pixels.* It is known that the original image have high correlation between its adjacent pixels so we must reduce that in encrypted image to resist statistical attack. In this section, correlation coefficient of two adjacent pixels in original image and encrypted image is studied. In order to test the correlation between two adjacent pixels, we randomly select 5000 pairs (horizontal, vertical and diagonal) of adjacent pixels from the original image and the encrypted image, using the following equations to calculate the correlation coefficient:

$$\rho = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \text{where}$$

$$D(x) = \frac{1}{n}\sum_{i=1}^{n}(x_i - E(x))^2$$

$$E(x) = \frac{1}{n}\sum_{i=1}^{n}(x_i)$$

$$cov(x,y) = \frac{1}{n}\sum_{i=1}^{n}(x_i - E(x))(y_i - E(y))$$

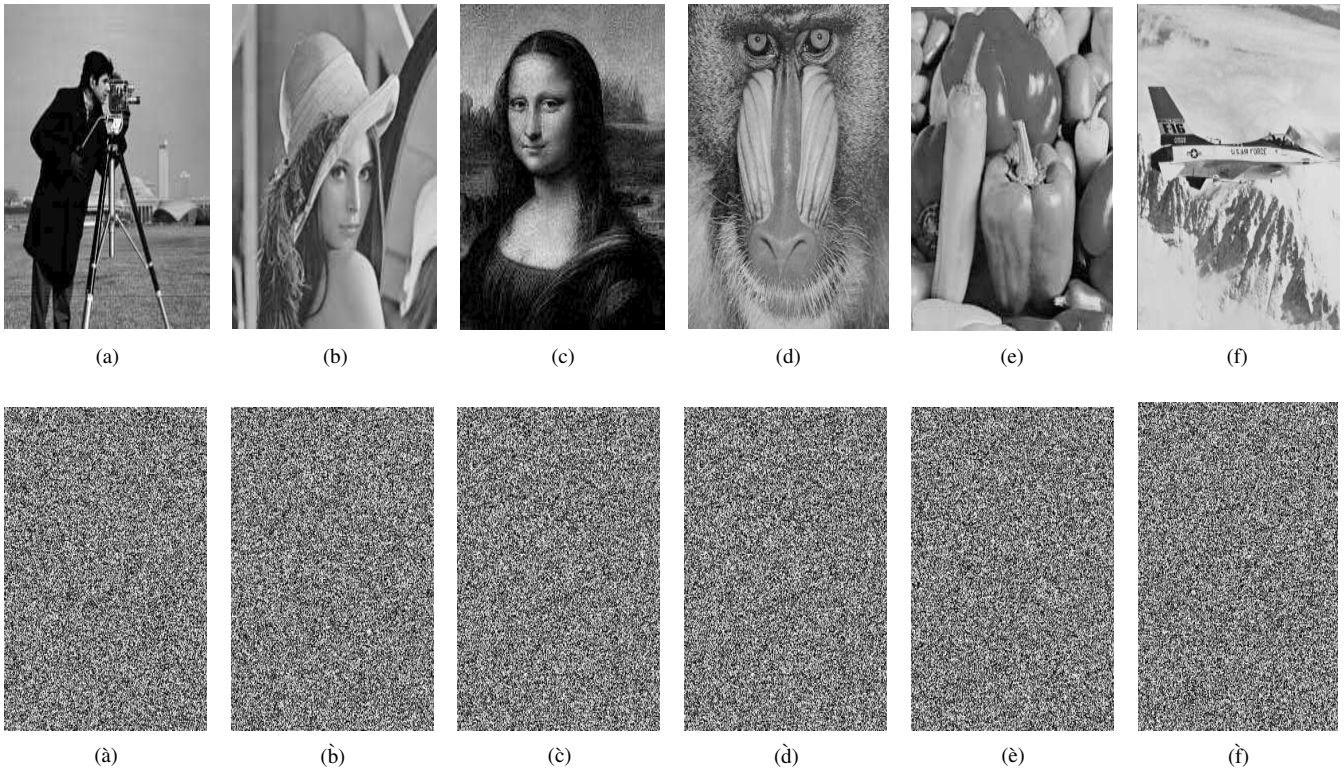
Where $x$ and $y$ are the values of two adjacent pixels of the plain images or the encrypted images, $n$ is the number of pixel pairs. Fig. 8 shows the horizontal correlation of original and encrypted gray scale images used in the simulations. It provides that correlation in original image has high value but it is close to zero in the encrypted image. In other words, the proposed image encryption algorithm has strong ability against the statistical attack.

*5.2.3 Correlation Analysis of Original and Encrypted Image.* The correlation coefficient between the original and the encrypted images can be defined as

$$\rho = \frac{\sum_{i=1}^{n}\sum_{i=1}^{m}(X(i,j) - E(X))(Y(i,j) - E(Y))}{\sqrt{\sum_{i=1}^{n}\sum_{i=1}^{m}(X(i,j) - E(X))^2 \sum_{i=1}^{n}\sum_{i=1}^{m}(Y(i,j) - E(Y))^2}}$$

Where, $X(i,j)$, $Y(i,j)$ are the $i^{\text{th}}$ row and $j^{\text{th}}$ column pixel values of plain image and cipher image respectively. $E(X)$, $E(Y)$ represent the average of plain image and cipher image respectively. $(n, m)$ is the image dimension. The result in Table 1 shows that there is a negligible correlation between the plaintext and the cipher image. So, the proposed scheme possesses high security against statistical attacks.

*5.2.4 Information Entropy Analysis.* Entropy is a statistical measure of randomness that can be used to test the robustness of the im-



(a) (b) (c) (d) (e) (f)

(à) (b̀) (c̀) (d̀) (è) (f̀)

Fig. 6: Original and encrypted gray scale images used in the simulations. (a), (à) cameraman; (b), (b̀) lena; (c), (c̀) monalisa; (d), (d̀) mandril; (e), (è) peppers; (f), (f̀) plane. All images have dimensions $256 \times 256$ pixels. 2-rounds of AES followed by XOR-ing the results with a DNA sequence are used for encryption

Table 1. : The correlation of plain-image and cipher-image. The images are encrypted using: 2-rounds of AES only and using 2-rounds of AES followed by XOR-ing the results with a DNA sequence

| | 2-rounds AES only | 2-rounds AES&DNA |
|---|---|---|
| Cameraman | 0.0088 | -0.0076 |
| Lena | -0.0036 | -0.0014 |
| Monalisa | -0.0128 | 0.0046 |
| mandrill | -0.0060 | -0.0019 |
| peppers | 0.00072 | 0.00039 |
| plane | -0.00042 | -0.00010 |

age encryption algorithm [8]. The measure of entropy of a source $m$ is defined as,

$$H(m) = \sum_i p(m_i) log_2 \frac{1}{p(m_i)}$$

Where $p(m_i)$ represents the probability of the symbol (pixel value) $m_i$. Therefore, according to the above equation the entropy of the system will be $H(m) = 8$. Therefore, the higher the entropy value of an encrypted image, the better the security. Table 2 shows the entropy of the plain images and the encrypted images. From these data it is clear that the entropy of the encrypted images is slightly less than 8, which proves the ability against the entropy attack.

Table 2. : Entropy of original and encrypted images

| | plain-image | cipher-image |
|---|---|---|
| Cameraman | 7.0097 | 7.9977 |
| Lena | 7.5683 | 7.9973 |
| Monalisa | 7.3293 | 7.9970 |
| mandrill | 4.2484 | 7.9971 |
| peppers | 7.5251 | 7.9975 |
| plane | 6.6744 | 7.9975 |

### 5.3 Differential Analysis

To find some relationships between the original image and the encrypted image, the attacker uses the differential attacks in which he makes a slight change to the original image and encrypt it before and after changing. Based on the differential attacks, the attacker can recover the secret key. Different measures are used to examine the performance of the encryption algorithm against this kind of attack. Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are two indicators that can be used to examine the sensitivity to this kind of attack [4, 2]. NPCR and UACI can be calculated using the following formula:

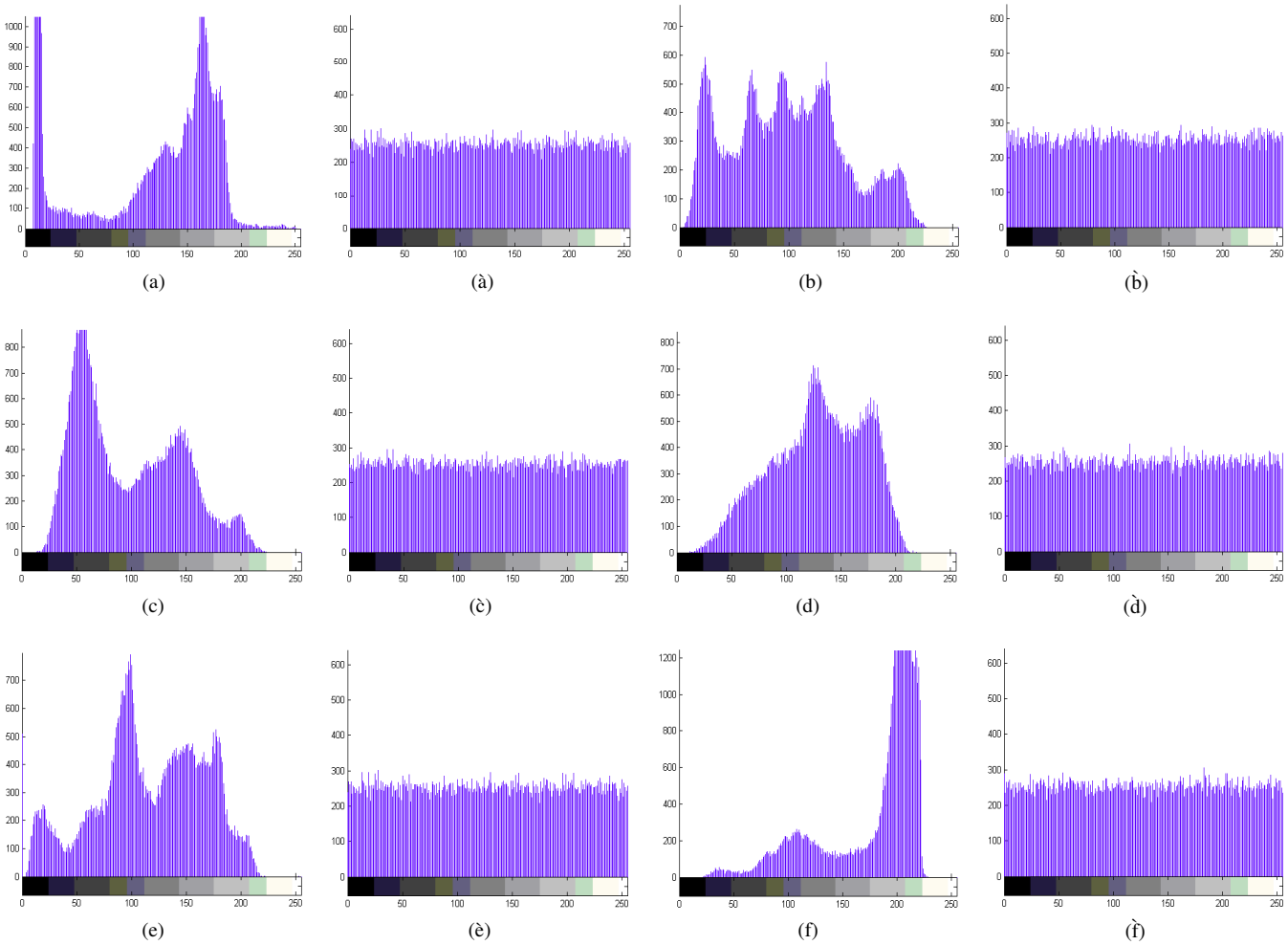



Fig. 7: Histograms of original and encrypted gray scale images used in the simulations. (a), (à) cameraman; (b), (b̀) lena; (c), (c̀) monalisa; (d), (d̀) mandril; (e), (è) peppers; (f), (f̀) plane.

$$\texttt{NPCR} = \frac{\sum_{i=1}^{n}\sum_{i=1}^{m} D(i,j)}{n \times m} \times 100$$

$$\texttt{UACI} = \frac{1}{n \times m} \times \frac{\sum_{i=1}^{n}\sum_{i=1}^{m} |C_1(i,j) - C_2(i,j)|}{255} \times 100$$

where $C_1, C_2$ are two images with the same size $n \times m$ and if $C_1(i,j) \neq C_2(i,j)$ then $D(i,j) = 1$ otherwise $D(i,j) = 0$.
Table 3 shows the NPCR and UACI values for the different images. This table indicates that our method possesses high level of security against differential attacks.

Table 3. : NPCR and UACI performance of the corresponding images that are scrambled using 2-rounds of AES followed by XOR-ing the results with a DNA sequence

| | NPCR | UACI |
|---|---|---|
| Cameraman | 99.62% | 31.16% |
| Lena | 99.62% | 30.48% |
| Monalisa | 99.60% | 29.64% |
| mandrill | 99.59% | 27.36% |
| peppers | 99.62% | 29.19% |
| plane | 99.62% | 32.40% |

## 6. CONCLUSION

In this paper, a new encryption/decryption of image ciphering method is proposed. The new method is based on DNA sequence operations and a round-reduced AES block cipher. The image pixels are scrambled using two rounds of AES cipher followed by XOR-ing the results with a DNA sequence. The sender/receiver can choose the DNA sequence from the gene-bank database by agreeing on the genomes database, the starting index, and the size of the sequence. Our experimental results and security analysis show that

our algorithm has good encryption effect. Furthermore, it has high resistance to most of the known attacks such as exhaustive search, statistical analysis, and differential analysis. We conclude that our method achieves high level of security and fast implementation.

## 7. REFERENCES

[1] Manoj B and Manjula N Harihar. Image encryption and decryption using AES. *International Journal of Engineering and Advanced Technology (IJEAT)*, 1(5):290–294, 2012.

[2] Shahram Etemadi Borujeni and Mohammad Eshghi. Chaotic image encryption design using tompkins-paige algorithm. *Hindawi Publishing Corporation Mathematical Problem in Engineering*, 2009:1–22, 2009.

[3] Kritika Gupta and Shailendra Singh. DNA based cryptographic techniques: A review. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(3):607–610, 2013.

[4] H.S. Kwok and Wallace K.S. Tang. A fast image encryption system based on chaotic maps with finite precision representation. *Chaos Solitons Fractals*, 32(4):1518–1529, 2007.

[5] Lili Liu, Qiang Zhang, and Xiaopeng Wei. A RGB image encryption algorithm based on DNA encoding and chaos map. *International Journal of Computers & Electrical Engineering*, 38(5):1240–1248, 2012.

[6] Mrinal K. Mandal, Gourab D. Banik, Debasish Chattopadhyay, and Debashis Nandi. An image encryption process based on chaotic logistic map. *IETE Technical Review*, 29(5):395–404, 2012.

[7] National Institute of Standards and Technology. FIPS 197. *National Institute of Standards and Technology, November*, pages 1–51, 2001.

[8] Claude E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[9] Siddaramappa V. Data security in DNA sequence using random function and binary arithmetic operations. *International Journal of Scientific and Research Publications*, 2(7):1–3, 2012.

[10] Salim M. Wadi and Nasharuddin Zainal. Rapid encryption method based on AES algorithm for grey scale HD image encryption. *Procedia Technology*, 11:51–65, 2013.

[11] Xiaopeng Wei, Ling Guo, Qiang Zhang, Jianxin Zhang, and Shiguo Lian. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. *Journal of Systems and Software*, 85(2):290–299, 2011.

[12] Rasmus Wernersson and Henrik Nielsen. Exercise: Searching the genbank database, April 2008.

[13] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki. A modified AES based algorithm for image encryption. In *Proceeding of the World Academy of Science, Engineering and Technololgy, May, WASET Organization, USA*, pages 206–211, 2007.

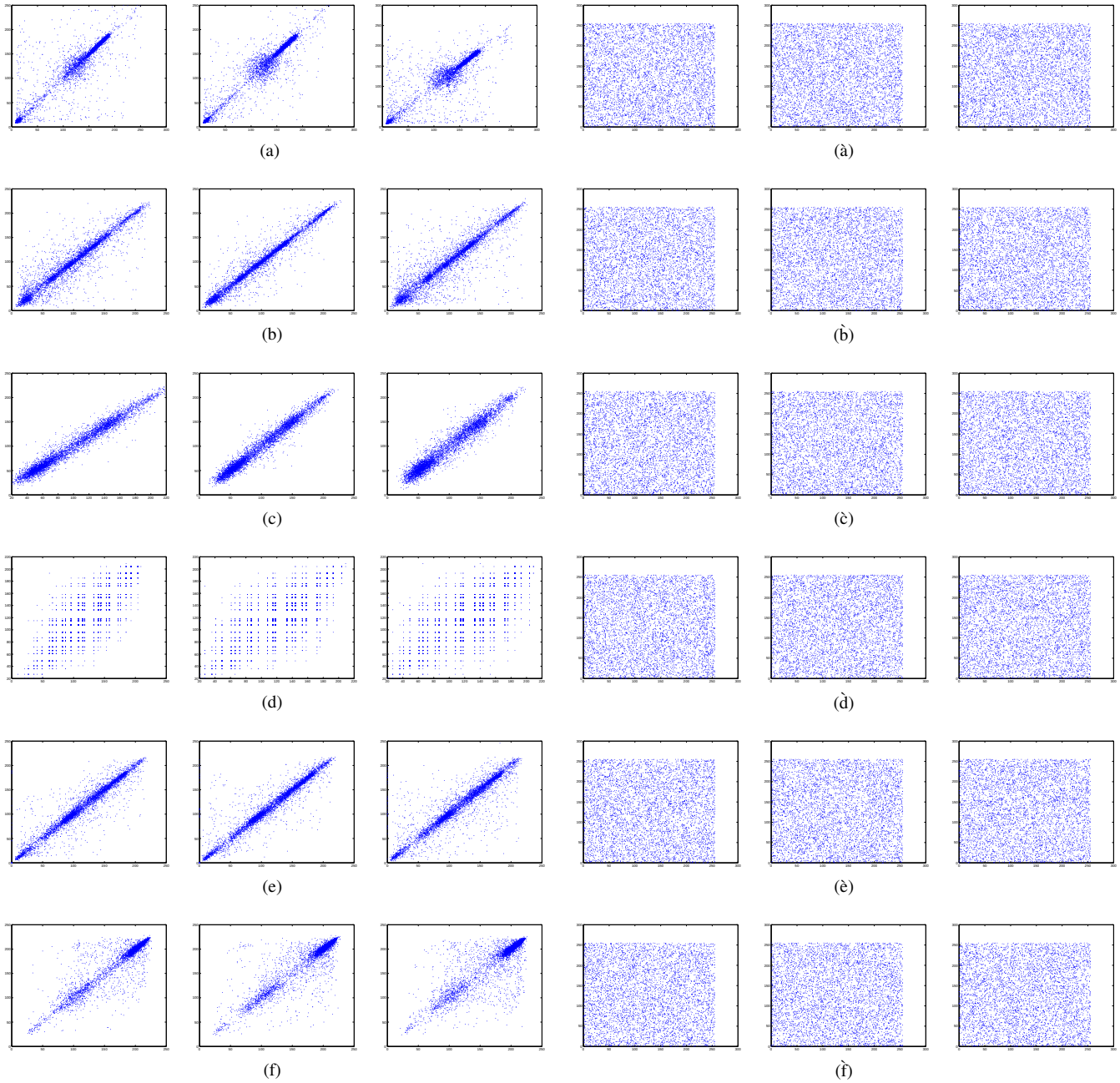



Fig. 8: Horizontal, vertical, and diagonal correlation of original and encrypted gray scale images respectively. (a), (à) cameraman; (b), (b̀) lena; (c), (c̀) monalisa; (d), (d̀) mandril; (e), (è) peppers; (f), (f̀) plane.