Indonesian Journal of Electrical Engineering and Computer Science
Vol. 21, No. 3, March 2021, pp. 1455~1464
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v21.i3.pp1455-1464

A novel image encryption scheme based on DCT transform and DNA sequence

Ali A.Yassin[1], Abdullah Mohammed Rashid[2], Abdulla J. Yassin[3], Hamid Alasadi[4]
[1,3,4]Computer Science Department, Education College for Pure Science, University of Basrah, Basrah, Iraq
[2]Education College for Human Science, University of Basrah, Basrah, Iraq

Article Info

Article history:

Received Oct 10, 2020
Revised Dec 7, 2020
Accepted Dec 23, 2020

Keywords:

Cryptanalysis
DCT transform
DNA sequence
Image encryption

ABSTRACT

Recently, the concept of DNA has been invested in computing technology in different ways which linking information technology and biological sciences. However, the DNA encryption scheme has drawbacks such as expensive experimental equipment and hard to hold its biotechnology. Additionally, during careful cryptanalysis that applied to most of these image encryption schemes, we notice that DNA can only influence one DNA base, which causes poor diffusion. Our proposed scheme is not applied complex biological operation but just is given to improve the diffusion ability of image encryption scheme by using DNA sequence and DCT transform. Furthermore, empirical results on real images and security analysis demonstrate that our scheme not only has flexibility and efficiency encryption scheme but also has the ability to resist well-known attacks such as entropy attack and statistical attack. Additionally, our work enjoys several strong characteristics as follows: (1) the decryption error is very low to recover the original image; (2) Once key for each encryption process and if the user wants to use the same key in many times, our scheme supports secret key sensitivity; (3) the value of correlation of the encrypted image is null.

Corresponding Author:

Abdulla J. Yassin
Computer Science Department
Education College for Pure Science
University of Basrah. Iraq 42001
Email: abdullajas@uobasrah.edu.iq

1. INTRODUCTION

In the last years, the communication and network systems have been changed due the information technology and Internet. At the present time, ten-thousands of kilobytes of trusted information are transferred in Internet over insecure communication channels, the information may be exposed to interrupting by an adversary that tries to obtain or change information. The protected communication method is that an user (sender) encrypts the original image in to encrypted image based on certain encryption method and only the legal receiver has ability to decrypt the encrypted image with the secret key(s) to retrieve the sender's image. There are many mainly schemes for image encryption such as diffusion (by using pixel replacement), permutation (by using pixel scrambling), or both diffusion and permutation. Furthermore, we find several applications of image encryption in many fields such as video conference, military, biometric systems, personal image. These applications require strong encryption scheme that has a good balanced between security and performance. There are several studies appear recently used DNA in cryptography [1-3].

Conversely, several image encryption schemes have been presented for both gray image and real image, for instance, partial encryption, DNA cryptography, transform domain, and modern cipher text but

most of these schemes have vulnerabilities [4]. Continuously, the modern cryptography methods such as advanced encryption standard (AES), data encryption standard (DES), international data encryption algorithm (IDEA), etc., are strong algorithms for plain text encryption, but they have many drawbacks when applied in image encryption [5, 6], because they cannot resist the attaches. Shah & Farooq [7], using an algorithm called SERPENT chain ring-based to encrypt the image by utilizing the set of boxes each one 128 bites, which meet the high level of performance but low efficiency. From other Chen et al, [8] Chen et al, proposed an encryption approach that classified an excellent due the features of chaos such as periodicity.

Our proposed scheme is forceful against chosen/known plain image attack and can use one permutation-diffusion round for encryption function. Moreover, a security analysis is critical to prove the strength and efficiency of the encryption function against the most common attacks. Additionally, the presented encryption scheme has several advantages such as high encryption rate, involves less computation, and suitable to small modifications in the secret key of image encryption. Continuously, the key is generation once time for each encryption function so even with the knowledge of the estimated key values, the adversary does not has possibility to attack the cipher text. Finally, Table 1 explains the main differences among our proposed scheme and related works. The rest of paper is classified as follows. Section 2 views primitive tools used in the present schemewhile Section 3 focuses on the proposed scheme. The experimental results are viewed in the Section 4. The security analysis presents in the Section 5. Finally, the Section 6 indicates of the conclusion.

Table 1. Comparison of image encryption schemes

Scheme	C1	C2	C3	C4	C5	C6	C7	C8	C9
Patidar et al. [9]	Md	No	Md	No	No	No	Variable	Md	Md
Wang et al. [10]	Md	No	Variable	No	No	Yes	Variable	Md	Md
Li et al .'s al. [11]	Md	No	Variable	No	No	Yes	Variable	Md	Md
Tong et al. [12]	Variable	No	Md	No	No	No	Md	Md	Md
Zhang et al.(2009) [13]	Md	No	High	Yes	Yes	No	Variable	Md	Md
Xue et al. [14]	Md	No	High	Yes	Yes	Yes	High	High	Md
Murillo-Escobar et al. (2014) [15]	Md	No	Variable	Yes	Yes	Yes	High	High	Md
Zhou et al. (2014) [16]	Variable	No	High	No	No	No	Variable	Md	Md
Our Proposed scheme	Md	Yes	High	Yes	Yes	Yes	High	High	High

C1:Key Space; C2:One Time Key; C3:Time Encryption; C4: Entropy; C5:DNA; C6: Chosen plain image attack; C7: Imperceptibility; C8: Visual Degradation; C9: Cryptographic Security.

2. PRIMITIVE TOOLS

2.1. DNA and digital image

A DNA sequence composed of the main four nucleic acid cores as follows. A (adenine), C (cytosine), G (guanine), T (thymine), where A and T are corresponding, G and C are corresponding [17]. Based on four cores A, C, G and T for applying encoded function on 00, 01, 10 and 11, there are 24 types of coding manners. But there are only 8 type of coding manners fulfill the Watson-Crick complement law, which are viewed in Table 2. Our proposed scheme focuses to use the DNA code for encoding the input images. For the 24 bits color image, we divide into three layers (Red, Green, Blue), for the 8 bits for each layer, each layer's pixel can be related with the DNA sequence whose length connects with 4 (normally, the length of binary sequence is 8).

Table 2. Eight types of methods encoding and decoding map rule of DNA sequence

+	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

2.2. The algebraic operations in DNA sequences

With the fast progresses of DNA development technology, the authors [18-19] presented mixed operation based on some biology operations, algebraic operations, and DNA sequence. Furthermore, addition and subtraction operations for DNA sequences are implemented according to conventional addition and subtraction in the binary system. Corresponding to 8 types of DNA encoding methods, there also exist 8 types of DNA addition rules and 8 types of DNA subtraction rules that are viewed in Tables 2 and 3, respectively. From Tables 2, 3 and 4, we notice that any one rule base in each row or column is single, consequently, the result of addition and subtraction operations consider uniquely result.

Table 1. One type of addition operation for DNA sequences

+	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G
T	T	A	G	C

Table 2. One type of subtraction operation for DNA sequences

-	A	G	C	T
A	A	T	C	G
G	G	A	T	C
C	C	G	A	T
T	T	C	G	A

2.3. XOR operation for DNA sequences

In practice, XOR operation for DNA sequences is implemented accommodating to conventional XOR in the binary. There are eight types of DNA encoding methods that lead to exist eight types of DNA XOR rules. In our proposed scheme, the XOR operation plays main role to fusion the input image and the key image. For instance, assume we have two DNA sequences such as [GATC] and [TGCT], we use one type of XOR operation which is viewed in Table 5 to XOR them and we can obtain the sequence [CGGG] as a result. In this paper, the main aim of using XOR operation is to scramble the pixel values of the input image [20].

Table 5. XOR operation with DNA sequences

XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

2.4. DCT transform

Generally, the discrete cosine transform considers one of the most widespread transforms that has been used in many fields such as image compression. It has several advantages like clearly of computation where inverse of DCT can be easily computed. To get high correlation of image data, the DCT supports an effectual compaction and has the property of reparability [21]. Based on (1) in two-dimensional state, the DCT runs on N by N block of image's pixels like X, and its result represents by blocks with N by N block of image's pixels like Y.

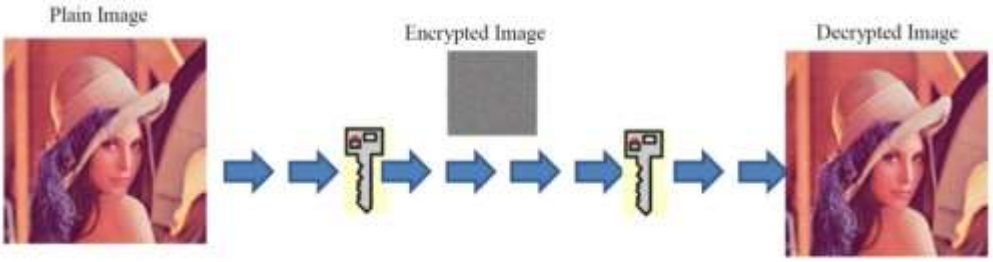
$$Y_{xy} = \frac{2}{N} C_x C_y \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} x_{i,j} \cos\frac{(2i+1)x\pi}{2N} \cos\frac{(2j+1)x\pi}{2N}$$

$$C_\partial = \begin{cases} \sqrt{\frac{1}{2}} & \partial = 0 \\ 1 & otherwise \end{cases} \quad (1)$$

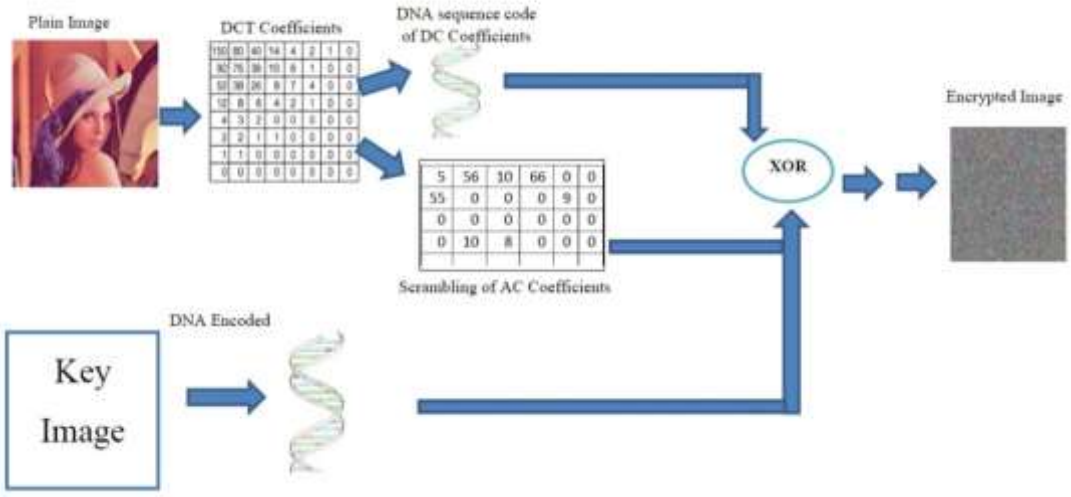
where Y is an element in set of N by N coefficients demonstrating of the data in the transformed domain. The set of data in waveforms is referred for each probable value of N (typically N=8, thus there is 64 waveforms).

3. OUR PROPOSED SCHEME

In this section, we propose a new image encryption scheme based on DNA encoding sequence and DCT transformation. The following notations in Table 6 will be used throughout our scheme. The proposed encryption scheme includes three components: original image, key image, and encryption image. Figure 1 explains the essential differences between the proposed scheme and the traditional image encryption scheme. Our work consists of four phases-setup of secret key, DCT, encryption process, and decryption process.



(a) Block diagram of the traditional image encryption



(b) Basic architecture of our proposed image encryption scheme

Figure 1. The proposed scheme feature (a) traditional method, (b) proposed method

Table 6. Notations of symbols used in proposed scheme

Symbol	Description
DCT	Discrete Cosine transformation.
$idct$	inverse discrete cosine transformation.
N	The number of rows in original image im_I .
M	The number of columns in original image im_I .
im_h	hash matrix.
h	crypto-hash function (SHA-512).
im_k	image key.
im_{Ascii}	Ascii Code matrix that is used to get binary code for each symbol and then the result of this step is im_B .
im_B	Binary matrix for each element in im_{Ascii} .
im_r	Random matrix is used for getting image key im_k based on DNA sequence.
im_I	Input color image.
DCT	Discrete cosine function
$idct$	Inverse Discrete cosine function
DC_R,DC_G , DC_B	The DC coefficients of color image; where, R is read layer of image, G is green layer of image, and B is blue layer of image.
DC'_R, DC'_G, DC'_B	The DC coefficients of color image after applied DNA sequence.
AC_R , AC_G , AC_B	The AC coefficients of color image.
S	Integer random number that is used to encrypt AC coefficients to obtain (AC'_R, AC'_G, AC'_B).
$Accum$	Accumulate function to get color image from main layer (Red, Green, Blue).
Md	Moderate

3.1. Setup of secret key

This phase focuses on key image that is generated by using a random image im_r based on the randomly generator. Then use the random function to create N×M integer matrix. So, the N and M represented the size of original image (im_I) which submits to our proposed scheme for encrypted it. This

case of image's key considers more appropriate compared with the average of template image. To build secure key, our proposed schemes performs the following steps:

a) Apply crypto-hash function (SHA-512) on each 512 pixel of image key(im_k) $\in Z^*_{N\times M}$. The output of this step is hash matrix $im_h = h(im_{(0..512)}, im_{(512..1024)} \ldots., im_{(N0..N\times M)})$ that consists of alphabetic and numeric symbols (alphabetical and numerical).
b) Convert hash matrix into Ascii Code matrix im_{Ascii} based on table of Ascii Code. After that, each elements of im_{Ascii} convert in binary sequence to generate a new matrix im_B.
c) Use the eight kinds of DNA encoding schemes in Table 2 to obtain key image im_r that depends on convert each twice binary bits from binary mode to DNA mode selecting one rule for each encryption phase. So, when user wishes to encrypt the same or other image again, he should be generated a new image key and uses another DNA's rule. This process prevents many attacks such as plain image attack, MITM attack, and generate once key for each encryption process. Finally, we obtain the secret image key based on DNA sequence (im_k).

3.2. DCT transform

The main steps of the DCT are explained as follows (as demonstrated in Figure 2):

a) Input the color original image (im_I) and divided it into three layers (Red (im_R), Green (im_G), Blue (im_B)).
b) Apply DCT to gain coefficient matrices on each layers (im_R, im_G, im_B). In coding by using DCT transform, each layer of original image im_I) is separated into 8*8 blocks and DCT transform is applied on each block. After that, these coefficients should be quantized based on JPEG compression standard matrix. Each pixel value of input image is split by the matching value of quantization matrix. We notice the first coefficient knowingly DC coefficient has the most energy and the other coefficients knowingly AC have the important details of input image. The DCT splits the image into several frequencies that is low frequencies locates on left top corner of original image. In the encryption process, the AC coefficients can be only reduced quality of the original image in the encrypted state and is actionable for reducing image resolution in marketable applications. Additionally, the coefficient with low frequency (non-zero) in both dimensions is related with DC coefficient and the remaining 66 coefficients are connected with the AC coefficients with high frequencies. This way recuperates the original images by statistical models and the cipher text-only attack [22]. Furthermore, taking in account the point stream encryption function is used, image key sequence with the original image is sound Xor, as a result any coefficient has ability to encrypt by a specific number of bits from key sequence. Figure 3 explains the drawbacks of AC coefficients as well as we focus on using DC and AC in clever manner. The output of this phase is ($AC_R, AC_G, AC_B, DC_R, DC_G, DC_B$) represent useful parameters in the next phases.

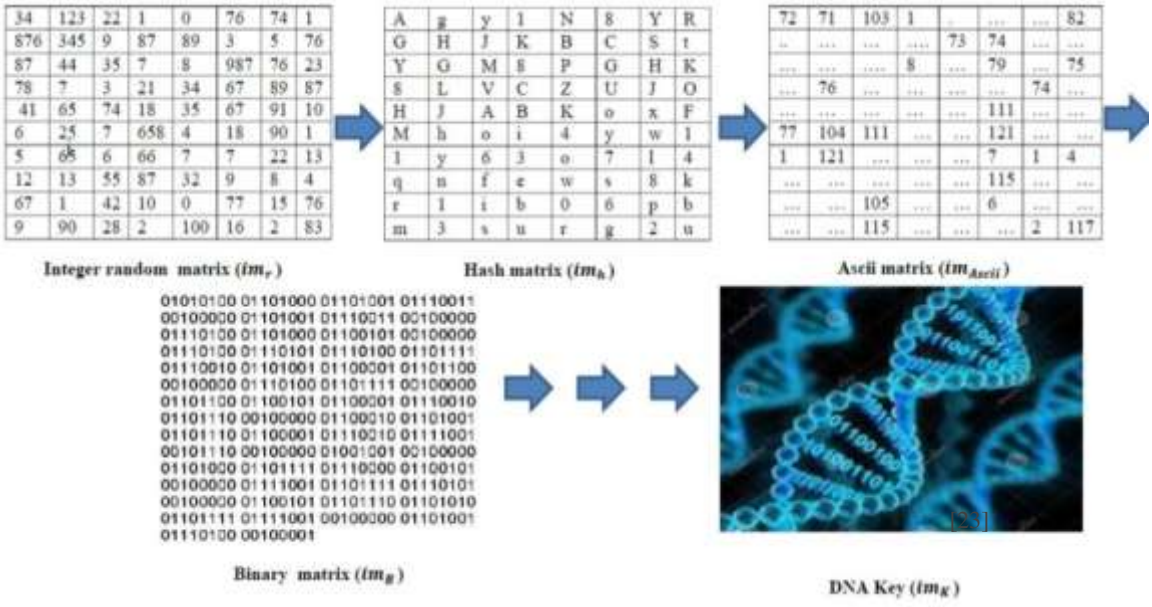


Figure 2. The main steps to generate key image

(a) (b) (c) (d)

Figure 3. Encrypted and recovered image based on AC coefficients (a) Gray image, (b) Encrypted image, and (c) Decrypted image (d) Restored image

3.3. Encryption process

In this phase, the proposed encryption scheme includes three steps as follows:

a) The DC coefficients are encoded into DNA sequences matrices (DC_R, DC_G, DC_B). The result of this step is (DC'_R, DC'_G, DC'_B).

b) The AC coefficients of original image is permutated under the scramble method. In this phase, image scrambling applied on AC matrices (AC_R, AC_G, AC_B) proceeds coding to the pixel values of the AC matrices changing the values of the matrices' elements. So, we notice the histograms of the scrambling matrices (AC'_R, AC'_G, AC'_B) and the original matrices (AC_R, AC_G, AC_B) are then different. An introduction of AC matrix scrambling method based on element value switching using X-OR operation is given below:
   - Assuming that the size of the matrix is N×M, a random integer numbers sequence $S = \{S_1, S_2, S_3, \ldots, S_{\mathrm{N\times M}}\}$ is created to use with AC matrices in the next step.
   - The scrambling operation is applied on each layer of AC matrices (AC_R, AC_G, AC_B) with sequence S as follows:

c) In this step, using XOR operation to encrypt each image key (im_k) with DNA coding (DC'_R, DC'_G, DC'_B) and scrambling matrices (AC'_R, AC'_G, AC'_B).
   - Apply inverse discrete cosine transform to restore image into spatial domain for each layers $im'_R = idct(AC'_R, DC'_R)$, $im'_G = idct(AC'_G, DC'_G)$, $im'_B = idct(AC'_B, DC'_B)$.
   - $im_{RE} = im'_R \oplus im_k$, $im_{GE} = im'_G \oplus im_k$, $im_{BE} = im'_B \oplus im_k$.
   - Then, the output of this step is ($im_E = Accum(im_{RE}, im_{GE}, im_{BE})$) where $Accum$ is function that used to accumulate all layers of image encryption.

3.4. Decryption process

The main steps of this phase as follows.

a) Split encryption image (im_E) into three layers based on major color red, green, and blue. $im_E \xrightarrow{Split} im_{RE}, im_{GE}, im_{BE}$.

b) Apply shared key im_k to retrieve (im'_R, im'_G, im'_B) where each layer decrypts as follows. $im'_R = im_{RE} \oplus im_k$, $im'_G = im_{GE} \oplus im_k$, $im'_B = im_{BE} \oplus im_k$.

c) Using discrete cosine transform (DCT) for each layer to retrieve the useful factors ($im_{RE} \xrightarrow{DCT} AC'_R, DC'_R$, $im_{GE} \xrightarrow{DCT} AC'_G, DC'_G, im_{BE} \xrightarrow{DCT} AC'_B, DC'_B$).

d) Recover DC coefficients (DC_R, DC_G, DC_B) based on DNA rule in Table 2.

e) Retrieve AC coefficients (AC_R, AC_G, AC_B) by using sequence $S = \{S_1, S_2, S_3, \ldots, S_{\mathrm{n\times m}}\}$. Where $AC_R = S \oplus AC'_R$, $AC_G = S \oplus AC'_G$, $AC_B = S \oplus AC'_B$.

f) Apply inverse discreet cosine transform to return the image from sequential domain to spatial domain. $im_R = idct(AC_R, DC_R)$, $im_G = idct(AC_G, DC_G)$, $im_B = idct(AC_B, DC_B)$. Then, use $Accum$ function to obtain color image where $im'_I = Accum(im_R, im_G, im_B)$

In this section, we address the scenario of our proposed scheme between two parties (Alice and Bob) in a privacy-preserving method without losing any useful information of encryption image. Figure 4 demonstrates image encryption and decryption of our proposed scheme.

Alice Side (*Alice* → *Bob*: $\mathrm{im_E}$):

Given image im_I, Alice would like to encrypt im_I and then applies our proposed scheme to obtain encrypted image im_E. Then, he submits im_E to Bob.

Bob Side ($Bob \rightarrow Bob$: im_I):

Upon receiving the encrypted image in encryption process from Alice, Bob decrypts im_E based on decryption process in our proposed scheme to get color image based on important information ($im_K, S, DNA\ rule$) which both parties (Bob and Alice) are agreement it in setup phase.

3.5. Security analysis and experimental evaluation of our proposed scheme

We focus on security analysis and experimental results in this section.

Proposition 1. Our proposed scheme has ability to prevent of forgery and parallel-session attacks.

Proof. If an attacker attempts to impersonate the Alice/Bob, access to a valid session image encryption (im_E) through secret parameters ($DNA\ rules, im_r, im_h, im_{Ascii}$) will be required. Since the attacker will not possess any knowledge of (im_k, S) required to calculate DC'_R, DC'_G, DC'_B, AC'_R, AC'_G, AC'_B and then apply encryption function as follows:

1. $im_{RE} = im'_R \oplus im_k$, $im_{GE} = im'_G \oplus im_k$, $im_{BE} = im'_B \oplus im_k$
2. $im_E = Accum(im_{RE}, im_{GE}, im_{BE})$

So, this type of attacks will be averted and an attacker cannot apply these type of attacks.

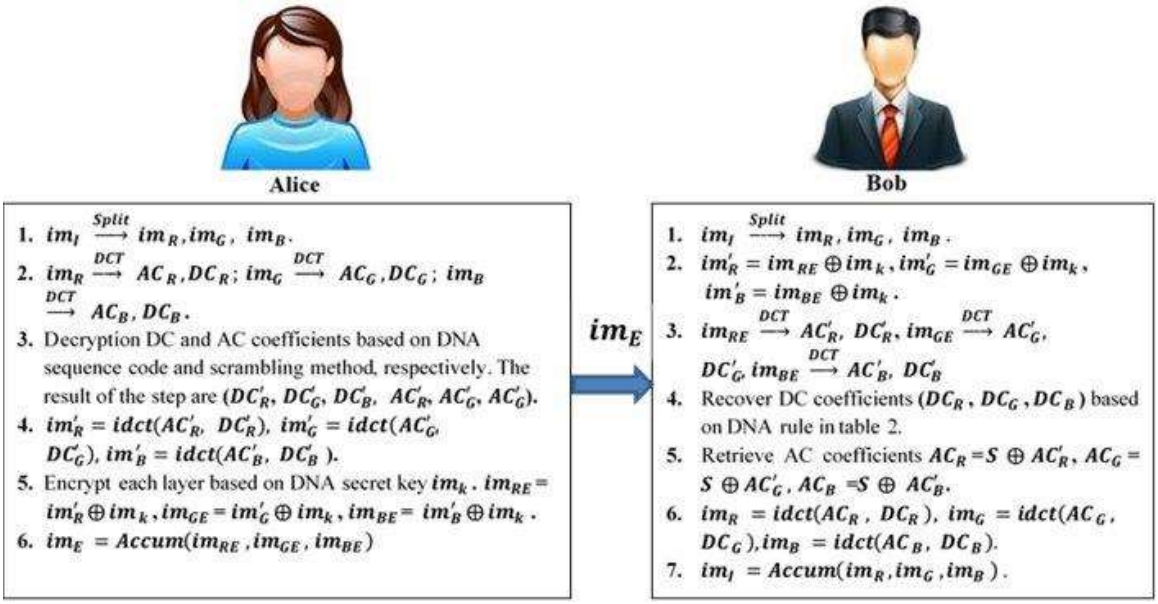


Figure 4. Encryption and decryption of our proposed scheme

Proposition 2. Our proposed scheme can withstand Chosen/known plain image attack.

Proof. There are several significant points that connected with our proposed scheme to avoid this malicious attack as below:

1. The permutation diffusion process is realized in one phase according to scrambling method that has been applied in our proposed scheme, we use the scrambling method in partial manner as follows.
   a. $im_R \xrightarrow{DCT} AC_R, DC_R$; $im_G \xrightarrow{DCT} AC_G, DC_G$; $im_B \xrightarrow{DCT} AC_B, DC_B$.
   b. The scrambling is applied on each layer of AC matrices (AC_R, AC_G, AC_B) with sequence S : $AC'_R = S \oplus AC_R$, $AC'_G = S \oplus AC_G$, $AC'_B = S \oplus AC_B$.
2. The DNA encryption sequence is applied on DC coefficients (DC_R, DC_G, DC_B) of input image (im_I) for obtaining DNA sequences matrices (DC'_R, DC'_G, DC'_B) based on the secret key (im_k) and DNA rules in Table 7. Additionally, we use crpto-hash function for each 512 pixels of im_r that gains our proposed scheme strong secure against this attack.
3. The encrypted image is transformed and rounded to $im_k \in [0..255]$ for each layer ($im_{RE} = im'_R \oplus im_k$, $im_{GE} = im'_G \oplus im_k$, $im_{BE} = im'_B \oplus im_k$) in the encryption process ($im_E = Accum(im_{RE}, im_{GE}, m_{BE})$.

Table 7. One time key in encryption process

Key	Layer	Correlation
Key 1 Vs. Key2	R	0.0034
	G	0.00087
	B	0.00267
Key 2 Vs. Key3	R	0.0022
	G	0.00076
	B	0.00156

In a chosen plain image attack, the cryptanalyst refers that there is temporal access at encryption equipment and he can select a color image for encryption and attempt to find the image secret key (im_k) based on the following important points:

1. He selects a random image and split into three layers $im_I \xrightarrow{Split} im_R, im_G, im_B$.
2. He tries to build im_k or eavesdrops it from the last session of encrypted image between Bob and Alice.
3. He compute $im_R \xrightarrow{DCT} AC_R, DC_R$; $im_G \xrightarrow{DCT} AC_G, DC_G$; $im_B \xrightarrow{DCT} AC_B, DC_B$.
4. The cryptanalyst is facing severe difficulties to encrypt DC and AC coefficients because he should know the DNA sequence rule and scrambling sequence, respectively to generate (DC'_R, DC'_G, DC'_B, AC'_R, AC'_G, AC'_G). While the key has generated in the previous session worked once for each encryption phase. Therefore, we have different DNA and scrambling sequences for each plain image (im_I).

Proposition 3. Our proposed scheme can withstand entropy image attack.
Proof. The entropy controls the changeability of message/plaintext, i.e. it measures how much unrest generates the encryption function at output. If the scrambling process works well, we have high trouble in encrypted image, as a result, higher refers to entropy. Another situation, the encryption function is not adequately random and the cryptosystem may be applied the fruitful entropy attack because there occurs a certain degree of changeability of the encryption process. Herein, the performance of our proposed encryption process is tested and verified. Additionally, the entropy H(p) of plaintext (p) can be computed as follows:

$$H(p) = \sum_{i=1}^{2^N-1} Prob(p_i) log_2(1/Prob(p_i))$$

where N is the number of bits of the plaintext p, 2^N refers to all possible values, $Prob(p_i)$ denotes a probability of p_i, log_2 characterize the base 2 logarithm, and an entropy represents expressed in bits, If there is the plaintext p encrypted with 2^N possible values, the entropy must be $H(p) = N$ perfectly. The true image has 8 bits per layer (Red, Green, Blue), i.e.$N = 8$ at element layer. Consequently, the maximum entropy of each element in true image is 8. Table 8 demonstrates the results of entropy and a comparison with modern related works. The value of entropy is close to 8, so, the scrambling and DNA sequences process are good and obtaining high unrest at output.

Table 8. Correlation coefficient of encrypted image

Color Image	Layer	Our Proposed Scheme	Murillo-Escobar et al.[24] (2015)	Zhou et al. [16] (2014)	Zhang et al. [25] (2013)
256×256	R	7.9922	7.9949	7.9976	
	G	7.9911	7.9953		
	B	7.9909	7.9942		
512×512	R	7.9933	7.9974	7.9993	7.9993
	G	7.9922	7.9975		
	B	7.9911	7.9969		
1024×1024	R	7.9922	7.9978	7.9998	
	G	7.9923	7.9976		
	B	7.9943	7.9976		

3.5. Computation cost

We computed the costs of the different process (Setup of secret key, DCT transform, encryption process and decryption process) in the proposed scheme based on Table 9. Table 10 explains the time processing of our proposed scheme.

Table 9. Description of time processing

Notation	Description
T_h	Time of Process hash function
T_{DNA}	Time of DNA Process
T_{dct}	Time of discrete cosine transform (dct)
T_{idct}	Time of inverse discrete cosine transform ($idct$)
$T_{Enc/Dec}$	Encryption and Decryption process

Table 10. Computational cost

Process	Time
Setup of Secret Key	$T_h + T_{DNA}$
DCT transform	$3\ T_{DNA}$
Encryption Process	$3\ T_{DNA} + 3\ T_{dct} + 3\ T_{Enc} + 3\ T_{idct}$
Decryption Process	$3\ T_{DNA} + 3\ T_{dct} + 3\ T_{Dec} + 3\ T_{idct}$
Total	$T_h + 10\ T_{DNA} + 6\ T_{dct} + 6\ T_{idct} + 6\ T_{Enc/Dec}$

4. CONCLUSION

In this paper, we have proposed a robust and an efficient encryption scheme for color image. We used DCT, DNA, ands scrambling method to achieve a good balance between strong security and time processing of proposed scheme. The security analysis approves that the color image encryption has a good performance and safe against many well-known attacks such as MITM attack, entropy attack image attack, differential attack, static attack, chosen/known plain image attack. Additionally, our work enjoys several strong characteristics as follows: (1) the decryption error is very low to recover the original image; (2) Once key for each encryption process and if the user wants to use the same key in many times, our proposed scheme supports secret key sensitivity; (3) the encrypted image is null based correlation value.

REFERENCES

[1] Shuqin Zhu and Congxu Zhu, "Secure Image Encryption Algorithm Based on Hyperchaos and Dynamic DNA Coding," *Entropy*, vol. 22, no. 7, pp. 772, 2020, https://doi.org/10.3390/e22070772.

[2] D. Huo, X. Zhu, G. Dai, H. Yang, X. Zhou and M. Feng, "Novel image compression-encryption hybrid scheme based on DNA encoding and compressive sensing," *Applied Physics B.*, vol. 126, no. 3, pp. 1-9, 2020.

[3] Kang Xuejing and Guo Zihui, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system," *Signal Processing: Image Communication*, vol. 80, 2020, https://doi.org/10.1016/j.image.2019.115670.

[4] S. Zhou, Q. Zhang, X. Wei and C. Zhou, "A summarization of image encryption," *IETETech. Rev.*, vol. 27, no. 6, pp. 503-510, 2010, DOI: 10.4103/02564602.2010.10876783.

[5] F. B. Muhaya, M. Usama and M. K. Khan, "Modified AES using chaotic key generator for satellite imagery encryption," *Emerg. Intell. Comput. Technol. Appl.*, vol. 5754, pp. 1014-1024, 2009, DOI: 10.1007/978-3-642-04070-2_107.

[6] A. J. Menezes, P. C. van Oorschot and S.Vanstone, "Handbook of Applied Cryptography," CRCPress, BocaRaton, FL, USA, 1996.

[7] T. Shah, T. U. Haq and G. Farooq, "Improved SERPENT Algorithm: Design to RGB Image Encryption Implementation," in *IEEE Access*, vol. 8, pp. 52609-52621, 2020, doi: 10.1109/ACCESS.2020.2978083.

[8] G. Chen, Y. Mao, C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749-761, 2004.

[9] V. Patidar, N. Pareek, G. Purohit, K. Sud, "Modified substitution-diffusion image cipher using chaotic standard and logistic maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 15, no. 10, pp. 2755-2765, 2010, https://doi.org/10.1016/j.cnsns.2009.11.010.

[10] X. Wang, L. Teng, X. Qin, "A novel colour image encryption algorithm based onchaos," *Signal Process*, vol. 92, no. 4, pp. 1101-1108, 2012, DOI: 10.1016/j.sigpro.2011.10.023.

[11] C. Li, Y. Zhang, R. Ou, K.-W. Wong, "Breaking a novel colour image encryption algorithm based on chaos," *Nonlinear Dyn.*, vol. 70, no. 4, pp. 2383-2388, 2012, DOI: 10.1007/s11071-012-0626-5.

[12] C. Li, S. Li, K.-T. Lo, "Breaking a modified substitution-diffusion image cipher based on chaotic standard and logistic maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 16, no. 2, pp. 837-843, 2011, https://doi.org/10.1016/j.cnsns.2010.05.008.

[13] Q. Zhang and L. Guo, "An image encryption algorithm based on DNA sequence addition operation," in *2009 Fourth International on Conference on Bio-Inspired Computing*, pp. 75-79, 2009, doi: 10.1109/BICTA.2009.5338151.

[14] X.L. Xue and Q. Zhang, "An image fusion encryption algorithm based on DNA sequence and multi-chaotic maps," *J. Comput. Theor. Nanosci.*, vol. 7, no. 2, pp. 397-403, 2010, DOI: https://doi.org/10.1166/jctn.2010.1372.

[15] M. A. Murillo-Escobar, F.Abundiz-Pérez, C. Cruz-Hernández and R. M. López-Gutiérrez, "A novel symmetric text encryption algorithm based on logistic map," in *Proceedings of the 2014 International Conference on Communications, Signal Processing and Computers*, pp.49-53, 2014.
[16] Y. Zhou, L. Bao, C. Philip Chen, "A new1d chaotic system for image encryption," *Signal Process*, vol. 97, pp. 172-182, 2014, https://doi.org/10.1016/j.sigpro.2013.10.034
[17] P. Gaborit and O. D. King, "Linear constructions for DNA codes," *Theor. Comput. Sci*., vol. 334, pp. 99-113, 2015, doi:10.1016/j.tcs.2004.11.004.
[18] O. D. King and P. Gaborit, "Binary templates for comma-free DNA codes," *Discrete Appl. Math*., vol. 155, no. 6-7, 831-839, 2007, https://doi.org/10.1016/j.dam.2005.07.015.
[19] E. Z. Dong, Z. Q. Chen, Z. Z. Yuan and Z. P. Chen, "A chaotic image encryption algorithm with the key mixing proportion factor," in *2008 International Conference on Information Management, Innovation Management and Industrial Engineering*, pp. 169-174, 2008.
[20] A. Bakhshandeh and Z. Eslami, An authenticated image encryption scheme based on chaotic maps and memory cellular automata," Optics and Lasers in Engineering, vol. 51, no. 6, pp. 665-673, 2013.
[21] M. C. Dufourny, "MPEG-4 Style Object-based Codec with Matlab," TFE Department, Umea University, Sweden, 2006.
[22] S. Bahrami and M. Naderi, "Encryption of multimedia content in partial encryption scheme of DCT transform coefficients using a lightweight stream algorithm," *Optik-International Journal for Light and Electron Optics*, vol. 124, no. 18, pp. 3693-3700, 2013, https://doi.org/10.1016/j.ijleo.2012.11.028.
[23] Ymgerman, "Dna Molecules Binary Code 3d Render Stock Illustration 255618778," shutterstock.com, available: https://www.shutterstock.com/image-illustration/dna-molecules-binary-code-3d-render-255618778 (accessed Oct. 15, 2020).
[24] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez, O. R. Acosta Del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos," *Signal Processing*, vol. 109, pp. 119-131, 2015, https://doi.org/10.1016/j.sigpro.2014.10.033.
[25] W. Zhang, K. W. Wong, H. Yu, Z.-L. Zhu, "An image encryption scheme using reverse2-dimensional chaotic mapand dependent diffusion," *Commun. Nonlinear Sci. Numer. Simul*., vol. 18, no. 8, pp. 2066-2080, 2013, https://doi.org/10.1016/j.cnsns.2012.12.012.