Adaptive Key Length Based Encryption Algorithm using DNA Approach

Anchal Jain
CSE Department
Inderprastha Engineering College
Ghaziabad, India
anchalkiet@gmail.com

Navin Rajpal
School of Information and Communication Technology
Guru Gobind Singh Inderprastha University
Delhi, India
navin_rajpal@yahoo.com

***Abstract*— In recent years various DNA based symmetric cryptographic algorithms have been suggested to develop secure image encryption techniques but secrecy of key and key space is often compromised due to small size of key. In this regard, this paper proposes a new method of adaptive key length based image encryption using DNA approach. The proposed algorithm uses 72-bit external key to generate the initial condition for chaotic sequence and for expansion of key to the desired length using DNA replication and complement rule. The proposed algorithm has a huge key space generated using key expansion method although the original key sequence is small. The original image is then encrypted using DNA addition and DNA complementary rule guided by the chaotic sequence. Experimental results and security analysis show that the proposed algorithm has achieved the satisfactory computing-security level.**

Keywords—DNA Cryptography, Chaotic Map, Image Encryption

I. INTRODUCTION

The revolutionary growth of digital and communication technology has promoted the use of digital images and videos being transmitted over internet and wireless network very frequently. To prevent the data from unauthorized access security is an important issue for communication and storage of images. In symmetric key cryptography, same key is used for encryption and decryption.The security of such system depends on secrecy of the key. Though the key is shorter and encryption/decryption process is simple and faster but the key distribution process is a major challenge. Public key cryptosystem solves the key distribution problem by using different secret key for internal users. Thus key exchange between users is not required but the process involved in generating public key is very complex and time consuming. In recent years, various image encryption approaches have been proposed to overcome these problems and to find efficient algorithm for image/video encryption. In 1994 Adleman [1] did the first ever experiment on DNA computing and gave the new dimension to cryptographic field. Gehani [2] proposed a one-pad encryption based on the DNA encryption and decryption methods; Leier A et al. [3] designed two kinds of encryption scheme to fulfil information hiding based on DNA binary sequences applying DNA technology, Kazuo T [4] solved the problem of key distribution. At the same time, DNA encryption system based on symmetric encryption has also made progress [5,6]. Many DNA based encryption schemes have been suggested [7,8,9]. In DNA Encryption the DNA technique combined with cryptology, aim to produce new cryptography to give secure and efficient cipher services. This paper proposes a new method of image encryption using DNA approach. In section II, encryption process is explained step by step, in section III, security analysis is performed in terms of brute force attack, sensitivity analysis and statistical analysis and finally in section IV paper is concluded.

II. PROPOSED ENCRYPTION PROCESS

A. DNA Encoding Scheme

A DNA sequence contains four nucleic acid bases A (adenine), C (cytosine), G (guanine), T (thymine), where A and T are complementary, and G and C are complementary [2]. In the binary, 0 and 1 are complementary, so 00 and 11 are complementary, 01 and 10 are also complementary. In this paper, C, A, T , G denote 00, 01, 10, 11, respectively. For 8 bit grey level images, each pixel can be represented as a DNA sequence whose length is 4. For example, if the pixel value of the image is 114, convert it into a binary stream as [01110010], now by using the above DNA encoding rule, DNA sequence [AGCT] represents the pixel. Further, this DNA coding is reversible.

B. Key Generation and Expansion

The key generation process consists of following steps.

1) Algorithm uses a one-dimensional logistic map to generate pseudorandom sequence mathematically represented as

$$X_{n+1} = rX_n(1 - X_n) \quad (1)$$

where $0 \le r \le 4$ and $0 \le X \le 1$
In the proposed algorithm, the value of r is kept at 3.9999 which correspond to highly chaotic behavior.

2) The algorithm uses 72-bit external key entered in hexadecimal and then convert it into 9 blocks of 8 bits each as in (2).

$$k=k_1k_2\ldots\ldots\ldots\ldots k_9 \text{ (ASCII Mode)} \quad (2)$$

3) The first three keys k_1 to k_3 are used to generate initial condition for the logistic map as follows.

$$X_0 = \frac{\sum_{i=1}^{3} k_i}{256\times 3} \quad (3)$$

4) Now generate a sequence of real numbers $q_1, q_2 \ldots q_k$ in the range [0.1, 0.9] by iterating the logistic map (1) using the

978-0-7695-5013-8/13 $31.00 © 2013 IEEE
DOI 10.1109/ICMIRA.2013.34

initial condition obtained in step 3 and obtain 6 unique integer numbers in range 1 to 24 using (4).

$$N_k = int(\ 23\times (q_k - 0.1)/0.8) + 1 \quad (4)$$
$$N = \{\ N_1, N_2, N_3, N_4, N_5, N_6\ \} \quad (5)$$

for example N={1, 7, 6,15,11, 20}

5) Keys from k_4 to k_9 are encoded into DNA sequence as suggested in previous subsection A, each key being encoded into a string of 4 nucleic acids. Example shown as below

ACTC CTGC TACA TATC CTGA ATCG (6)

6) Now the DNA sequence is replicated three times. 6 random integer numbers generated in step 4 are used as two site positions in each replicated sequence to complement the values being between sites and thus generating a complete new 3 times expanded key of initial sequence. For example original sequence in (6) is copied as below and complementary sites are highlighted as per values of N_k where k=1to 6 in (5).

ACTC CTGC TACA TATC CTGA ATCG
A ***CTC CTG*** *C TACA TATC CTGA ATCG (*1and 7)
ACTC CT ***GC TACA TAT*** *C CTGA ATCG (*6 and 15)
ACTC CTGC TAC ***AT ATCC TGA*** *ATCG (*11 and 20)

Hence the new sequence of expanded key is

ACTC CTGC TACA TATC CTGA ATCG
A ***GAG GAC*** *C TACA TATC CTGA ATCG*
ACTC CT ***CG ATGT ATA*** *C CTGA ATCG*
ACTC CTGC TAC ***TATAG GACT*** *ATCG* (7)

7) Finally the substrings each of length 4 from expanded key DNA sequence (7) is converted back into the decimal numbers. Thus now 24 keys are available for encryption process.

$$K = \{K_1, K_2, K_3 \ldots\ldots K_{24}\} \quad (8)$$

The benefit of this expansion is that there is no need to send large key over he channel and still a long key can be generated having sufficiently large key space.

C. Encryption

8) *First Round:* The value of initialisation vector IV used in (9) is chosen as the last value in the decimal format of key i.e. K_{24}. The first round is performed as in (9)

$$\left.\begin{aligned} C_1 &= [(IV \oplus P_1) \times K_1]\ mod256 \\ C_i &= [\ C_{i-1} \oplus P_{i-1}) \times K_i]\ mod256 \end{aligned}\right\} \quad (9)$$

where $P_i \in P$, $P = \{P_1, P_2, \ldots\ldots\ldots, P_{mn}\}$ pixel values of original image in range 0 to 255, $m\times n$ is the total no of pixels in image matrix, intermediate cipher values are $C = \{ C_1, C_2, C_3, \ldots\ldots\ldots C_{16}\}$ and i varies from 2 to 16.

9) *Second Round:* Encode intermediate cipher values C_i each into strings of length 4 using DNA encoding as suggested in subsection A and generate the chaotic sequence of 16 real numbers (x,y) using 2-D logistic map (10)

$$\left.\begin{aligned} x_{i+1} &= \mu_1 x_i(1-x_i) + \lambda_1 y_i^2 \\ y_{i+1} &= \mu_2 y_i(1- y_i) + \lambda_2(x_i^2 + x_i y_i) \end{aligned}\right\} \quad (10)$$

where $2.75< \mu_1 \leq 3.4$, $2.75< \mu_2 \leq 3.4$, $0.15< \lambda_1 \leq .21$, $0.13< \lambda_2 \leq 0.15$, $\mu_1 = 3.2$, $\mu_2 = 3$, $\lambda_1 = 0.17$, $\lambda_2 = 0.14$. Initial conditions are calculated as

$$\left.\begin{aligned} x_0 &= \left(\frac{\left(mod\left(\sum_{i=1}^{m/2}\sum_{j=1}^{n} p_{ij}, 256\right)\right)}{256} + r_1\right) mod1 \\ y_0 &= \left(\frac{\left(mod\left(\sum_{i=m/2}^{m}\sum_{j=1}^{n} p_{ij}, 256\right)\right)}{256} + r_2\right) mod1 \end{aligned}\right\} \quad (11)$$

where $r_1 = \frac{\sum_{l=17}^{19} K_i}{256\times 3}$ and $r_2 = \frac{\sum_{l=20}^{22} K_i}{256\times 3}$, . Map the chaotic values x and y according to function in (12) and we get new mapped values of x and y in range 0 to 3.

$$f(z) = \begin{cases} 0, & 0 < z \leq 0.25 \\ 1, & 0.25 < z \leq 0.5 \\ 2, & 0.5 < z \leq 0.75 \\ 3, & 0.75 < z \leq 1 \end{cases} \quad (12)$$

Now for the final round of encryption, the complementary rule suggested in [10] combined with DNA addition [11] and guided by chaotic sequence is used. For complementary rule it must satisfies that, for each nucleotide m_i in the nucleotide string

$$\left.\begin{aligned} m_i &\neq B(m_i) \neq B(B(m_i)) \neq B(B(B(m_i))) \\ m_i &= B(B(B(B(m_i)))) \end{aligned}\right\} \quad (13)$$

where $m_i \in \{A, C, T, G\}$

$B(m_i)$ is the base pair of m_i, which can guarantee the complementary rule of injective mapping. There are total 6 groups legal complementary rules and any one of them for example (AT)(TC)(CG)(GA) can be applied to the proposed method. The addition and subtraction tables are shown in Table I and Table II. The encryption is performed as in (14).

for i = 2 to 15

$$\left.\begin{aligned} FC_1 &= comp_{x[1]}(\, Rot_{y[1]}(C_{16})) + C_1 \\ FC_i &= comp_{x[i]}(\, Rot_{y[i]}(FC_{i-1})) + C_i \\ FC_{16} &= comp_{x[16]}(\, Rot_{y[16]}(K_{23})) + C_{16} \end{aligned}\right\} \quad (14)$$

where FC_i denotes the final cipher value, $x[i]$ and $y[i]$ are the new mapped chaotic values using (12), $Rot_{y[i]}(FC_i)$ rotates the cipher FC_i $y[i]$ times to the left, The addition operator '+' denotes the DNA addition and

$comp_0(m) = m$
$comp_1(m) = B(m)$
$comp_2(m) = B(B(m))$
$comp_3(m) = B(B(B(m)))$

Same process is repeated for remaining pixels. Convert the sequence $FC = \{ FC_1, FC_2, \ldots FC_{mn} \}$ into two dimensional matrix of decimal values to get the encrypted image.

The decryption process is reverse of encryption process.

TABLE I. ADDITION TABLE

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

TABLE II. SUBTRACTION TABLE

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

TABLE III. CORRELATION COEEFICIENT ANALYSIS OF FIGURE 1

Image1	**Image2**	**Correlation coefficient**
Encryted image A (fig.1b)	Encryted image B (fig.1c)	0.094
Encryted image B (fig.1c)	Encryted image C (fig.1d)	0.0012
Encryted image C (fig.1d)	Encryted image A (fig.1b)	0.0132

III. SECURITY ANALYSIS

Security analysis is the major challenge in any cryptosystem. Here, the security analysis of the proposed algorithm is performed on the parameters such as brute-force attack, sensitivity analysis and statistical analysis.

A. Key Space analysis

In cryptosystem, the key space is calculated based on number of bits being used in key. For N bit key, the key space is 2^N bits. The larger the N is, larger is the key space. In this paper 72 bit key was used initially but by using a variable key expansion method based on DNA replication and complement rule, key can be expanded to any desirable length. As discussed in paper, after expansion 144 more bits were added increasing the key space from 2^{72} to 2^{216}. This key expansion ensures that key space is large enough and the system is more secured against brute force attack.

B. Sensitivity Analysis

The proposed algorithm shows sensitivity to slight change in key. The Fig.1 shows the original image and the corresponding encrypted images using slightly different keys and Table III shows corresponding correlation analysis.

C. Statistical Analysis

1) Histogram Analysis: Histogram is calculated and analysed for several encrypted images and their original grey level images with different sizes that have significantly different content. Fig.2 shows the performance of proposed technique in terms of histogram analysis for one example.

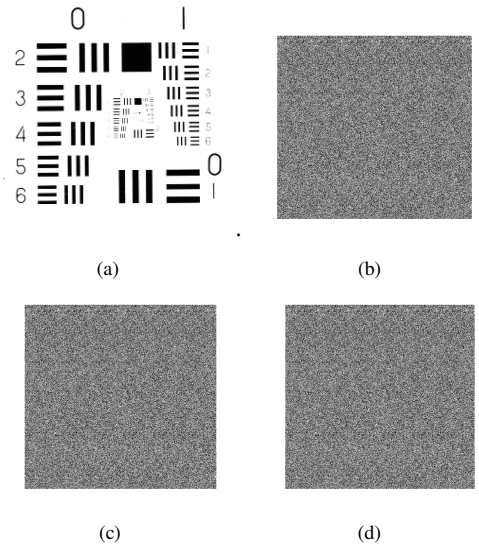

Figure 1. Key sensitivity test: Frames (a) and (b) respectively shows original image and its encrypted image using secret key '*A405FD2578CDE1FFCE* ' and frames (c) (d) respectively shows encrypted images of image in frame (a) with keys '***B****405FD2578CDE1FFCE*' and '*A405FD2578CDE1FFC****D***'.

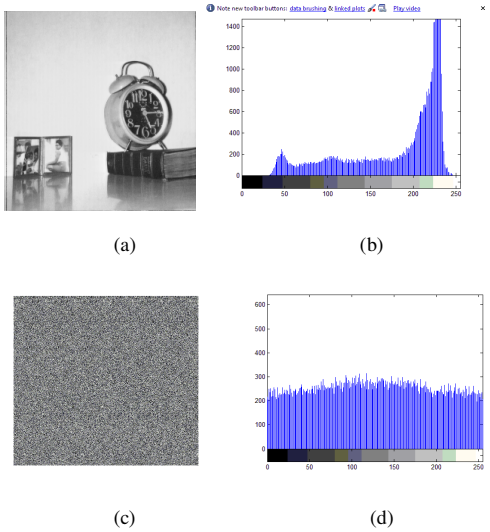

Figure 2. Histogram Analysis: (a) Original image clock.tiff (b) histogram of original image. (c) encrypted image of original image shown in frame (a) using proposed method and key 'A405FD2578CDE1FFCE' (in hexadecimal) (d) histogram of encrypted image in frame (c).

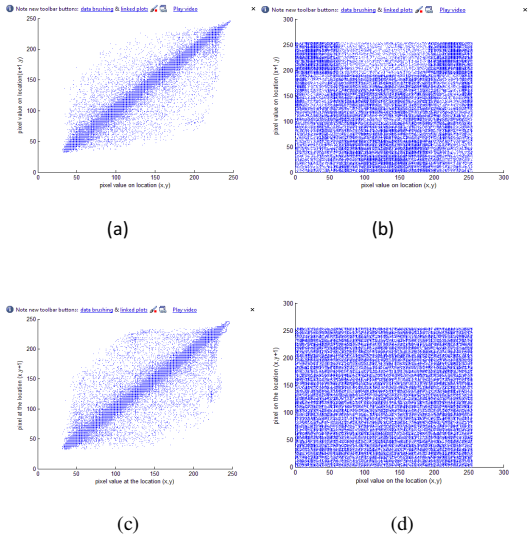

Figure 3. Correlation analysis of two adjacent pixels: Frames (a) and (b) show the distribution of horizontally adjacent pixels of original image shown in Fig. 2(a) and the corresponding encrypted image shown in Fig. 2(c). Frame (c) and (d) shows the distribution of vertically adjacent pixels of the original image shown in Fig. 2(a) and encrypted image shown in Fig. 2(c) respectively.

Key '*A405FD2578CDE1FFCE*' (in hexadecimal) is used for encryption. Fig. 2(d) shows that histogram of the encrypted image is scattered more uniformly over the entire pixel space than that of respective original image and appears significantly different from it. Thus, histogram analysis does not reveal any information of original image providing clue for statistical attack.

2) Correlation coefficient Analysis: Correlation coefficient is a measure of the strength and direction of the linear relationship between two variables. The correlation coefficient between two horizontally adjacent or vertically adjacent pixels in the original and encrypted images is calculated using (15).

$$C_r = \frac{N\sum_{j=1}^{N}\left(x_j \times y_j\right) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{\left(N\sum_{j=1}^{N} x_j^2 - \left(\sum_{j=1}^{N} x_j\right)^2\right) \times \left(N\sum_{j=1}^{N} y_j^2 - \left(\sum_{j=1}^{N} y_j\right)^2\right)}} \qquad (15)$$

The *x* and *y* are the values of two adjacent pixels and N is the number of pixels selected for the calculation. Fig. 3 shows the vertical and horizontal correlation plots of original image shown in Fig. 2(a) and corresponding encrypted image. Further, Table IV shows mathematical results in terms of correlation coefficients for the original and encrypted images. Digital images from USC-SIPI image database are used which is maintained by the University of Southern California primarily to support research in image processing, image analysis and machine vision.

It is clear from Table IV that negligible correlation exists between the vertically and horizontally adjacent pixels of the encrypted images.

TABLE IV. CORRELATION COEFFICIENT ANALYSIS

Image		**Original image**	**Encrypted Image**
clock.tiff	***Vertical***	0.9852	-0.0199
	Horizontal	0.9764	-0.0050
Boat.512.tiff	***Vertical***	0.8841	-.0001
	Horizontal	0.9454	-.0085

IV. CONCLUSION

In this paper, a symmetric-key encryption algorithm based on the DNA approach is proposed. The original key sequence is small but it can be expanded to the desired length using proposed key expansion method guided by chaotic sequence. The expanded key has sufficiently large key space and therefore there is no need of sending the large key over the channel. The chaotic encryption process combined with DNA addition and complement scrambles the pixel values of the image making the technique sufficiently secure. The proposed technique has been experimentally evaluated in terms of brute-force attack, sensitivity analysis and statistical analysis and acceptable results have been found.

REFERENCES

[1] Adleman, "Molecular computation of solutions of combinatiorial problems", Science , Vol.266, 1994 , pp. 1021-1024.

[2] G ehani A, LaBean T H, Reif J H. , “D N A -based cryptography”, Dismacs Series in Discrete Mathematics and Theoretical Computer Science 54 ,2000, pp. 233-249.

[3] Leier A, Richter C, Banzhaf W, et al. “Cryptography with DNA binary strands”,. Biosystem s, 2000, 5(7), pp. 113-22.

[4] Kazuo T, Akimitsu O, Isao S. Public-key system using DNA as a one way function for key distribution. Biosystems, 2005, pp.81 25-29.

[5] MX Lu, XJ Lai, GZ Xiao, L Qin, “Symmetric-key cryptosystem with DNA technology”, Science in China Series F: Information Sciences, 2007, 50(3), pp. 324-333.

[6] Kang Ning, “ A Pseudo DNA Cryptography Method”, CoRR 2009,abs/0903.2693.

[7] Qiang Zhang, Xianglian Xue, Xiaopeng Wei,” A Novel Image Encryption Algorithm based on DNA Subsequence Operation “,The Scientific World Journal, Volume 2012, Article ID 286741.

[8] Xiaopeng Wei,Ling Guo, Qiang Zhang, “A Novel Image Encryption Algorithm based on DNA sequence Operation and hyper chaotic system”, Journal of system ans software, Volume 85, Issue 2, 2012, pp. 290-299.

[9] Xiaopeng Wei,Ling Guo, Qiang Zhang, “A Novel Image Encryption Algorithm based on DNA sequence Operation and hyper chaotic system”, Journal of system and software, Volume 85, Issue 2, 2012, pp. 290-299.

[10] Hongjun Liu, Xingyuan Wang, Abdurahman kadir,“Image encryption using DNA complementary rule and chaotic maps”, Applied Soft Computing 12 ,2012, pp. 1457–1466.

[11] Q. Zhang, L. Guo, X.P. Wei, “Image encryption using DNA addition combining with chaotic maps”, mathemathematical and Computer modelling 52(11-12) 2010, pp. 2028-2035.