A DNA-Based Security solution Using Aggregated Chaos Cross and Cubic Map

Zeeshan Ahmad[1], Hafiz Umar[2], Chundong Li[3], and Ling Chen[3]
[1]School of Electronic Engineering and Optoelectronic Technology Nanjing University of Science and Technology, China
[2]Department of Computer Science, Ghazi University, Pakistan
[3]College of Electronic and Information Engineering, Southwest University, China

Abstract: *DNA, cryptography and chaos, can be combined as a whole aggregated DNA, chaos-based and cryptography Discrete Chaotic Cryptography (DCC) to encrypt and decrypt data simultaneously. A new image encryption scheme based on chaotic system and DNA encoding has been proposed in this paper. Firstly the image is permuted by mixing the horizontally and vertically adjoint pixels with the help of Cross Chaotic Map (CCM). Afterwards, the permuted image is divided into Least Significant Bits (LSB) and Most Significant Bits (MSB). Each LSB and MSB is further divided into two blocks and encoded by DNA sequence. The encoded blocks are combined and XOR operation is performed to get a diffused image. Finally the diffused image is permuted by a cubic chaotic map to accomplish the confusion phase and cypher image is obtained. Simulation results show that the proposed scheme can achieve good encryption and also provide resistance against different kind of attacks.*

Keywords: *Chaos Theory, DNA, Image Encryption, Cryptography.*

Received June 17, 2014; accepted August 16, 2015

1. Introduction

Chaos, cryptography and DNA, are three different kinds of disciplines, but they are closely related with different aspects. The research framework generated by the combination of these three disciplines is called Discrete Chaotic Cryptography (DCC). Cryptography or cryptology is taken from three Greek words, kryptos which means "hidden, secret", graphein means "writing" and logia means "study". Normally Cryptography studies the mathematical techniques of secrecy or information security such as confidentiality, data integrity, entity authentication and data origin authentication [10]. Consequently researchers pay more attention to confidentiality and security of the multimedia information [13]. Traditional encryption methods are not suitable for image encryption so a new method of image encryption obligatory. The chaos-based encryption [8] was first proposed in 1989. Since then, a lot of chaos-based encryption algorithms had been proposed by the researchers. It has been long debated in the literature whether Chaos theory play a significant role in image encryption. Unique characteristics of chaotic map attract prevalent attention from the cryptographers all over the world to develop new algorithms. The algorithm based on the chaos are easier to realized as compared to the traditional cryptosystems [15], which make it more suitable for large scale data analysis, images, audio and video data. The above described intrinsic features are directly related to confusion and diffusion which are the basic properties of an ideal cypher.

One-dimension discrete chaotic map was first introduced by Mathews to generate a sequence of pseudo-random numbers in cryptography [17].The confusion and diffusion based architecture was firstly proposed by Fridrish [3]. He used one dimensional and two dimensional logistic chaotic maps for image encryption. In traditional chaotic symmetric image encryption, confusion and diffusion normally use the one dimensional Piecewise Linear Chaotic Map (PWLCM) and logistic map described by Equation 1 and 2 [3].

$$x_{i+i} = \begin{Bmatrix} X / P_0 & X\hat{I}[0,P] \\ (x - P_o) / (0.5 - P_o) & x\hat{I}[P,0.5] \\ (1 - x_i) & \end{Bmatrix} \quad (1)$$

$$x_{i+1} = \mu x_i (1 - x_i) \quad (2)$$

In this paper, we have proposed a new methodology to scramble an image using Cross and cubic chaotic maps. Chaotic map is utilized to generate the more complicated pseudo random sequence with the help of binary key to generate the initial values and parameters. The key is modified after every step of encryption. We map the image pixels with the cross chaotic sequence and after scrambling, divide the permuted image into Least Significant Bits (LSB) and Most Significant Bits (MSB). Furthermore, the LSB and MSB are divided into two blocks each, which are

L1, L2 and M1, M2. These blocks are then encoded by the DNA addition. Simulations results show the validity and superiority of the proposed methodology.

2. Related Work

Unlike the chaotic cryptography which achieve the current research hotspot, the relationship between the DNA data hiding techniques and cryptography are seldom studied [19]. In 1994 Adleman [1] perform first time experiment on DNA computing, DNA coding has some intrinsic qualities like huge storage and massive parallelism which make difficult to distinguish the real DNA sequence and the fake one [6]. Over 163 million sequences are publically available for cryptography [5]. A novel confusion and diffusion method for image encryption was proposed in [7].The arrays generated by Piecewise PWLCM permute the rows and columns of original grayscale image. Each pixel of the original image was encoded by using four nucleotides of DNA sequence. Empirical analysis shows that the scheme did not achieve good encryption result, except the large key space. [11, 20] proposed two Image encryption algorithms by using the XOR operation, bit shift, DNA addition and subtraction operation, based on the 1-D or 2-D Logistic map to generate the chaotic sequence. Gehani *et al*. [4] presented an algorithm based on one time pad cryptography with DNA strands. In his algorithm, he pointed out that DNA has extra ordinary information density and suitable for huge data storage. In the current digital era the need for multimedia security is becoming the hot issue. Clelland and Risca [2] proposed a novel encoding method where nucleotide are used as a quaternary code and each latter is denoted by three nucleotides. Different categories of data need different kind of security requirements .Among all types of data, digital data has great importance. Our security solution depends on digital image captured by the digital camera. Distribution of the image data from different organization such as military, medical, using different communication channels require strong security mechanism with certain facts like huge volume of data, high redundancy and real time processing. To make practical the secure transmission of multimedia data, many proposed approaches require extraordinary resources because of complex computation [18]. A great deal of exertion on encryption has been thru but numerous anticipated scheme flop to deliver a reasonable security. Our dissertation emphasis on image encryption based on image encryption based on DNA and chaos that is a blustering issue to prompt the firm development of image encryption. It is apparent from the above discussion that the combination of DNA with the encryption is an ongoing trend for researchers which will be helpful to open the new dimension for implementation in real-world applications.

3. Cross Chaotic Map

The DNA and chaos based encryption oriented approach [7] did not get the desired results. To enhance the encryption security and increase the calculation efficiency we use cross chaotic map. Among the chaotic maps Cross Chaotic Map (CCM) has invariant natural density and discussed in [14]. CCM exhibits a great diversity of dynamics behaviour [12]. Figure 1 shows the permuted image by cross chaotic map.

$$\begin{cases} X_{i+1} = 1 - \mu . Y_i . Y \\ Y_{i+1} = cos[k cos^{-1} x_i]; \end{cases} ,x,y \in [-1,1] \quad (3)$$

To reduce the computational complexity we change the Equation 5 to one dimensional.

$$x_{i+i} = 1 - \mu (cos(k \cos^{-1} x_i)^2 \quad (4)$$

Where μ and k are the control parameters of the systems, μ=2 and k=6. The system show great diversity of dynamic behaviour.

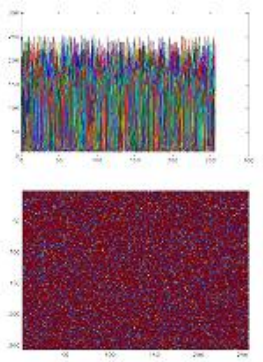


Figure 1. Permuted image by cross chaotic map

4. Characteristics of Cross-Chaos

CMM is chosen because of its higher degree of chaos-complexity [16]. Lyapunove exponent of the cross chaotic map is greater as compare the other maps. The Lyapunove Comparison (LC) value of cross map is 1.503 while that of logistic map is 0.6826. The group of time series changes in the pattern direction is quantitatively determined by the approximate entropy [14]. The approximate entropy is smaller if it is close to the time series model and size of similar probability and if the pattern of time sequence is not similar then the approximate entropy is bigger. The approximate entropy of the Cross map is 1.653140 and that of Logistic map is 0.718837. The bigger approximate entropy of cross-chaos shows high chaos-complexity.

4.1. Cubic Map

In our image encryption approach we use cubic map because of special cases, complicated dynamics and complex expression the cubic map have the unique

characteristics for implementation [11]. Cubic map is one of the simplest polynomial maps of the desired type when a is restricted to the range $0 \leq a \leq 4$ then f maps the interval Z = [1, -l].the equation of the cubic chaos map has high invariant density. Figure 2 describe the bifurcation diagram of the cubic map.

$$f(x) = ax^3 + (1-a)x$$

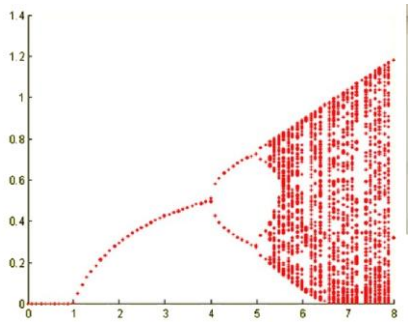


Figure 2. Bifurcation diagram of cubic map

4.2. Cross Cascade Permutation

Two-dimension Circulation Encryption Algorithm (TECEA) [21] implement group encryption method and define two kinds of rotations to rotate the column or rows in cyclic manner. The main deficiency of this scheme is that there is no full confusion mechanism to spread the whole image.

We use the cross chaotic map to define the mapping rule from original position to pseudorandom position (in plain to cipher image). Confusion and diffusion converts the plain image into the cipher image. The traditional confusion process relocates the pixel in a pseudorandom manner to decrease the correlation of neighbouring pixel and with the help of diffusion we spread small modification in the plain image to almost all the pixels in the cipher image. In only permutation process the cipher cannot provide the sufficient security and cryptanalyzed by the known plaintext attacks.

In our proposed Cross Code Permutation (CCP), different steps are carried out in the permutation phase to prepare the information utilize diffusion from the different directions:

- *Step 1*. Set the initial value of the X0, μ and k which we get from the generated secret key, to iterate the Equation 6.
- *Step 2*. Sort and index the pseudorandom numbers sequence in 1D array and transformed the 2D image in to 1D array. The size of both arrays should be same.
- *Step 3*. Map the values of Image array with the index of the sorted array of CCM.

In the second diffusion round of CCP, we involve MSB and LSB DNA encoding by using different rules. After combining the image we apply XOR algebraic operation and permute the image again by cubic map to obtain the random positions of the already scrambled pixels in previous process.

5. DNA Addition and Subtraction Rule

Cryptography attracts extensive concerns from both public and government sides in recent years. Among various technologies we can use Biotechnological methods for cryptography. Unlike cryptography which received much attention, the relationship between DNA and Cryptography is seldom studied [9]. The leading approach shows how DNA binary strands can be used for steganography, useful technique of encryption and decryption. It is observed that DNA steganography based on DNA binary strands is safe under the hypothesis that an interceptor has the same technological capabilities as sender and receiver of encrypted messages.

The transformation of data from digital to DNA bases is called encoding and the reverse process is called decoding. In cryptography of digital images, different cryptographic methods based on DNA binary strands exist. There are three kinds of data hiding methods based upon the DNA sequence properties which are insertion method, complementary pair method and substitution method [12]. Researchers used DNA complementary rules for encoding and decoding to incorporate the simple diffusion at early stage of algorithm. The most common techniques to select one of the 8 rules for encoding and another rule from remaining 7 rules for decoding of all pixels of an image which reduces the capabilities of DNA transformation for early diffusion process [21].

In confusion phase we convert the permutated image into binary image and divide the pixels into LSB and MSB blocks. Each block of the permutated image is encoded by the DNA encoding rule from Table 1. L1 is encoded by rule 2 and L2 is encoded by rule 3. M1 is encoded by the rule 6 and M2 is encoded by the rule 7.

Next step is the DNA encoding phase. We add the L1 and L2 by using Table 2 and obtain a DNA sequence L-DNA and M-DNA next to combine them we apply the XOR algebraic operation with the help of key k2. Finally cipher image is obtained. Finally cipher image is obtained. Similarly, subtraction rules are given in Table 3.

Table 1. DNA encoding rules.

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

Table 2. Addition for DNA sequence.

+	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 3. Subtraction for DNA sequence

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

6. Propose Image Encryption

According to the Figure 3, the proposed encryption scheme is summarized as below:

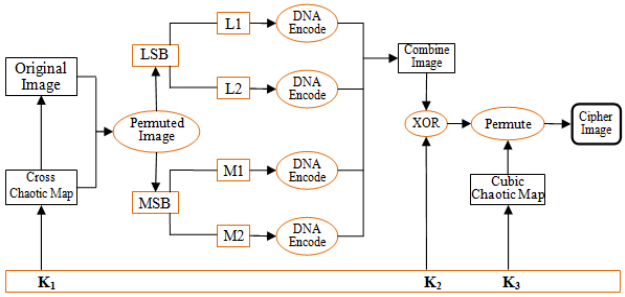


Figure 3. Graphical description of the image encryption algorithm.

- *Step 1*. Initial conditions are calculated using 96 bit long external key. The key is divided into twelve blocks of 8 bits.

$$K=K1, K2, K3, K4 \ldots K12 \quad (6)$$

Here, each *K* represents the 8 bit of the secret key.

- *Step 2*. To calculate *X*0, we choose the three blocks of the key.

B=*K*7, *K*8, *K*9

K71	K72	K73	..	K78	K81	K82	..	K88	K91	K92	K93	..	K98

Here *K*ij is the binary representation of the i[th] block; we compute the real number *X*01 using the following formula.

$$X1 = (K71 \times 20 + K72 \times 21 + \ldots\ldots K78 \times 27 + K81 \times 28 + K82 \times 29 + \ldots\ldots K88 \times 215 + K91 \times 216 + K92 \times 217 + \ldots\ldots K98 \times 223)/224 \quad (7)$$

- *Step 3*. Another real number *Y* is calculated using the blocks K4, K5 and K6 as below:

$$X_2 = \left[\sum_{i=23}^{0} (K_i x 2^i) \right] / 2^{24} \quad (8)$$

$$X0 = (X1 + X2) mod 1 \quad (9)$$

- *Step 4*. Permute the image 'I' by using cross chaotic map Equation 5 and initial condition *X*0 and control parameters μ=2 and *K*=6 obtained from Equation 6.
- *Step 5*. The permuted image I is converted into binary image 'B'. Divide each pixel of the permutated image 'B' into LSB and MSB.
- *Step 6*. LSB and MSB are further divided into L1, L2 and M1, M2 respectively.
- *Step 7*. Encode each bit of L1 to obtain a sequence LY'_1 by selecting DNA rules from encoding group of Table 1 and repeat the process for L2, M1 and M3.
- *Step 8*. Combine all LSB and MSB to get a new sequence C.
- *Step 9*. Chaotic sequence is generated by CMM to permute the key.
- *Step 10*. XOR operation is applied on the combined image using the permuted key.

The key *K*1 is modified to *K*12 for the XOR operation.

$$(K_i)_{10} = ((K_i)_{10} + (K_{12})_{10}) mod\ 256 \quad (10)$$

7. Result and Analysis

For any good encryption scheme it is necessary that it should be robust against all kind of well-known attacks. This section presents the simulation analysis of the proposed image encryption method. Parameters such as Statistical attack and sensitivity analysis is carried out to prove that the proposed system is efficient and secure.

7.1. Resistance to Exhaustive Attacks

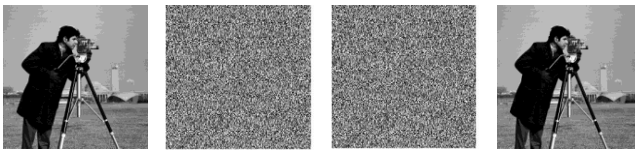
7.1.1. Key Space

In our proposed encryption scheme, cross and CCM are used to encrypt the image. The key space should be enough large to make any attack infeasible. The proposed architecture has 2128 different combinations of the key. We can increase the key size but longer key increase the computational time for encryption and decryption that will not be suitable. Here, we use the CCM that is highly sensitive to initial condition, so we calculate the initial condition by using the secret key. The secret key is modified after encryption of the each block of the image.

7.1.2. Key sensitivity analysis

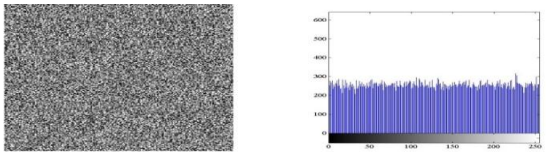
The initial conditions of chaotic map are generated by a secret key. Chaotic map is highly sensitive to initial conditions. So, minor change in key will generate a completely changed sequence yielding a totally different result.
Plain text =P
Cipher text image C1=Enc (P, K1)
Cipher text image C2=Enc (P, K2)
Decipher text image D1=Dec (C1, K1)
Decipher text image D2=Dec (C1, K2)
Decipher text image D3=Dec (C1, K3)
Difference only for one bit K1 ≠ K2 ≠ K3

Results in Figures 4 and 5 shows that the proposed DNA insertion rule based security solution is sensitive to the encryption key for both processes encryption and decryption with good confusion properties.



a) Original image. b) Encrypted image. c) Decrypted Image with different initial value. d) Decrypted image with correct initial value.

Figure 4. Impact of initial value on decryption

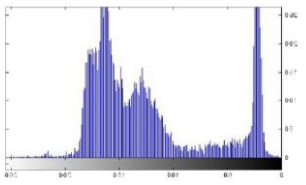


a) Decrypted Image with different key space b) Corresponding Histogram

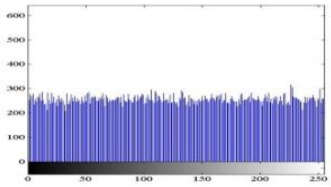
Figure 5. Impact of key space on decryption.

7.2. Histogram Analysis

Histogram analysis is the most important parameter to illustrate the encryption quality of the image. For a good encryption method it is necessary that Pixels of the image should be uniformly distributed to resist against any statistical attack. Applying our proposed encryption scheme, frequencies of gray levels in the encrypted image are fairly flat as compared the original histogram. This effect is illustrated in Figure 6 given below.



a) Grey histogram of original Image.



b) Grey histogram of encrypted image.

Figure 6. Histogram analysis of image.

7.3. Pixel correlation coefficient

The connection between two adjacent pixels in three different dimensions is studied in this segment. One property of the digital image data is high information redundancy so we need to break the high correlation between neighbouring pixels. According to the special relation of a pixel and adjacent pixel where x-axis denotes the intensity of one randomly selected pixel and y axis denotes the corresponding adjacent pixel. It is clear that by encryption process high correlation between the adjacent pixels are completely broken in all directions [21]. Where x and y are the gray scale values of two adjacent pixels in the image. By using the Equation 11, 12, 13 and Equation 14 we calculate the correction coefficient of each pair [21].

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{11}$$

$E(x)$ is estimation of mathematical expectation of x.

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left[x_i - E(x)\right]^2 \tag{12}$$

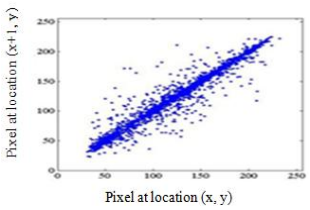
$D(x)$ is the estimation of the variance of x [22].

$$COV(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left[x_i - E(x)\right]\left[y_i - E(y)\right] \tag{13}$$

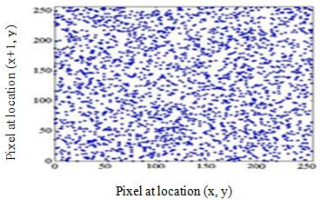
$COV(x, y)$ is the estimation of covariance of two adjacent pixels in vertical, horizontal and diagonal directions [23].

$$\gamma(x,y) = \frac{COV(x,y)}{\sqrt{D(x)g\sqrt{D(y)}}} \tag{14}$$

We select randomly 1024 pairs of neighbour pixels for both cipher text and plain text of image. The x-axis denotes the intensity of randomly selected pixels and y-axis denotes the intensity of its corresponding adjacent pixels. Correlation visualization for 1024 randomly selected pixels in both plain and cipher image are shown below in Figure 7.



a) Original image.



b) Encrypted Image.

Figure 7. Correlation of two horizontally adjacent pixels.

Table 4 list the correlation coefficients of two adjacent pixels.

Table 4. Correlation coefficient of two adjacent pixels.

Position	Plain Image	Encrypted Image
H	0.9368	0.0051
V	0.69659	0.0057
D	0.8791	0.0018

7.4. NPCR and UACI Test

Generally to evaluate the difference between two cipher texts and to measure the resistance against the differential attacks, NPCR and UACI are commonly used quantities. NPCR stands for number of changing pixel rate and UACI for unified average change intensity. NPCR measure the percentage of different pixel number between the two images. NPCR [21] is calculated by Equations 15 and 16:

$$NPCR = \frac{\sum_{ij} D(i,j)}{M \times N} \times 100\% \quad (15)$$

Where D (i, j) is the difference function can be defined as [21]:

$$D(i,j) = \begin{cases} 1, if c^1(i,j) \neq c^2(i,j) \\ 0, if c^1(i,j) = c(i,j) \end{cases} \quad (16)$$

$C1$ and $C2$ are the two cipher image UACI [21] is defined by Equation 17:

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C1(i,j) - C(i,j)|}{255}\right] \times 100\% \quad (17)$$

In our proposed image scheme, we use two plain images. One is original $C1$ and the other is $C2$ which is obtained by changing the bit position. The two plain images are encrypted several times by the proposed scheme. NPCR is 99.52 % and UACI is 32.60% for the corresponding cipher image obtained by using the proposed methodology.

8. Conclusions

DNA cryptography might become a practical application in the context of classification organic and inorganic materials with DNA 'barcodes'. In this paper we propose an image encryption algorithm. We use different kind of DNA rule for the LSB and MSB encoding and decoding and plain image is permuted by the cross chaotic map. Then, apply XOR operation with the key permuted by cubic map. The experimental results and security analysis describe that our algorithm has improved encryption quality and highly sensitive for secret key. Moreover proposed scheme can also repel the exhaustive attack, statistical attack, and differential attack. All above discussed features shows that our image encryption scheme is suitable for encryption.

Acknowledgment

This work was supported by Natural Science Foundation of China (grant no: 61374078). It was also supported by the Fundamental Research Funds for the Central Universities under Grant XDJK2015C079 and Grant SWU115015.

References

[1] Adleman L., "Molecular Computation of Solutions to Combinatorial Problems," *Science*, vol. 266, no. 5187, pp. 1021-1023, 1994.

[2] Clelland C. and Risca V., "Hiding messages in DNA microdots," *Nature*, vol. 399, pp. 533-534, 1999.

[3] Fridrich J., "Symmetric Ciphers Based on two Dimensional Chaotic Maps," *International Journal of Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259-1284, 1998.

[4] Gehani A., Bean T., and Reif J., "DNA-Based Cryptography," *Lecture Notes in Computer Science* , vol. 2950, pp. 167-188, 2014.

[5] Guo C., Chang C., and Wang Z., "A New Data Hiding Scheme Based on DNA sequence," *International Journal of Innovative Computing, Information and Control*, vol. 8, no. 1, pp. 139-149, 2012.

[6] Head T., Rozenberg G., Bladergroen R., Breek C., Lommerse P., and Spaink H., "Computing with DNA by Operating on Plasmids," *Biosystems*, vol. 57, no. 2, pp. 87-93, 2000.

[7] Liu H., Wang X., and Kadir A., "Image Encryption Using DNA Complementary Rule and Chaotic Maps," *Applied Soft Computing*, vol. 12, no. 5, pp. 1457-1466, 2012.

[8] Matthews R., "On the Derivation of a "Chaotic" Encryption Algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29-42, 1989.

[9] Mousa H., Moustafa K., Abdel-Wahed W., and Hadhoud M., "Data Hiding Based on Contrast Mapping Using DNA Medium," *The International arab journal of information technology*, vol. 8, no. 2, pp. 147-154, 2011.

[10] Rivest R., *Cryptology* Handbook of Theoretical Computer Science, MIT Press, 1990.

[11] Rogers T. and Whitley D., "Chaos in the Cubic Maping," *Mathematical Modeling*, vol. 4, no.1, pp. 9-25, 1983.

[12] Shiu H., Ng K., Fang J., Lee R., and Huang C., "Data Hiding Methods Based Upon DNA Sequences," *Information Sciences*, vol. 180, no. 11, pp. 2196-2208, 2010.

[13] Stallings W., *Cryptography and Network Security*: *Principles and Practices*, Prentice Hall, 1999.

[14] Wang L., Ye Q., Xiao Y., Zou Y., and Zhang B., "An Image Encryption Scheme Based on Cross Chaotic Map," *in Proceeding of Image and Signal Processing*, Sanya, pp. 22-26, 2008.

[15] Wang X., Chen F., and Wang T., "A New Compound Mode of Confusion and Diffusion for block Encryption of Image Based on Chaos," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 9, pp. 2479-2485, 2010.

[16] Xiaojun T., Yang L., Miao Z., and Hongyu S., "New Chaotic Image Encryption Algorithm Based on Cross-Mapping," *Wuhan University Journal of Natural Sciences*, vol. 17, no. 6, pp. 461-467, 2012.
[17] Yeung M. and Pankanti S., "Verification Cryptosystems Issues and Challenges," *Journal of Electronic Imaging*, vol. 9, pp. 468-476, 2000.
[18] Yeung S., John C., and David L., "A Multi-key Secure Multimedia Proxy Using Asymmetric Reversible Parametric Sequences: Theory, Design, and Implementation," *IEEE Transactions on Multimedia*, vol. 7, no. 2, pp. 330-338, 2005.
[19] Zhang Q., Guo L., and Wei X., "Image Encryption Using DNA Addition Combining with Chaotic Maps," *Mathematical and Computer Modelling*, vol. 52, no. 11-12, pp. 2028-2035, 2010.
[20] Zhang Q., Wang Q., and Wei X., "A Novel Image Encryption Scheme Based on DNA Coding And Multi-Chaotic Maps," *Advanced Science Letters*, vol. 3, no. 4, pp.447-451, 2010.
[21] Zhang Q., Xue X., and Wei X., "A Novel Image Encryption Algorithm Based on DNA Subsequence Operation," *The Scientific World Journa*l, vol. 2012, 2012.
[22] Zhu Z., Zhang W., Wong K., and Yu H., "A Chaos Based Symmetric Image Encryption Scheme using a Bit Level Permutation," *Information science*, vol. 181, no. 6, pp. 1171-1186, 2011.

Zeeshan Ahmad was born in Pakistan in 1988. He received the B.E. degree in electrical (telecom) engineering from the Bahria University Islamabad, Pakistan, in 2011 and M.E. degree in electronics and communication engineering from Chongqing University, Chongqing, China, in 2014. Currently, he is enrolled in Nanjing University of Science and Technology, Nanjing, Jiangsu Province, China as a PhD Student.
His research interests include array signal processing, ultra wideband and wideband beam forming, radars, adaptive arrays, GPS and satellite navigation systems.

Hafiz Gulfam Ahmad Umar was born in Pakistan in 1984. He received Ph.D and M.Sc degree in Computer Science from Chongqing University, China and Bahauddin Zakarya University Multan, Pakistan, in 2015 and 2005 respectively. From 2007 to 2014 he served as a lecturer in Agriculture University Faisalabad. Currently he is an Assistant professor with department of Computer science, Ghazi University, D.G.Khan, Punjab, Pakistan. His research interest includes image encryption, intrusion detection systems, data mining, information security and cloud computing.

Ling Chen got her B.Sc. from Kun ming University of Science and Tec hnology, Kunming, China in 2010. She got her Ph.D. from Chongqing University, Chongqing, China.Now she is an assistant professor at the College of Electronic and Information Engineering, SouthwestUniversity,Chongqing, China, 400715. Her research interests include artificial neural netwowrk, memristor, nonlinear system and image pro cessing etc.

Chuandong Li received his B.S.de gree in Applied Mathematics from Sichuan University, Chengdu, China in 1992, and M.S. degree in operational research and control theory and Ph.D degree in Computer Software and Theory from Chongqing University, Chongqing, China, in 2001 and in 2005, respectively. He is a Professor at the College of Electronic and Info rmationEngineering, Southwest University, Chongqin g, China, 400715, now. He has been the IEEE Senior member since 2010. From November 2006 to November 2008, he serves as a research fellow in the Department of Manufacturing Engineering and Engineering Management, City University of Hong Kong, Hong Kong, China. He has published about more than 200 journal papers. His current research interest covers computational intelligence, artificial neural networks, memristive systems, chaos control and synchronization, and impulsive dynamical systems.