Secured Image Encryption Scheme Using both Residue Number System and DNA Sequence

M. I. Youssef, A. E. Emam, S. M. Saafan, M. Abd Elghany

Abstract— This paper proposes a new image encryption scheme that uses DNA sequences and Residue number system. The design of this scheme is based on the binary to residue data message conversion, then impeding the message secretly inside the DNA sequence. This merge will be leaded to perform multilayer encryption with different keys to increase the security and more flexibility, with less complexity. As the security is one of the most important issues in communication systems, the evolvement of cryptography and cryptographic analysis are considered as the fields of ongoing research. Thus, a straight forward algorithm that achieves efficiency as multi-layer encryption techniques are implemented.

Index Terms—DNA, Image, Encryption, Residue number system

I. INTRODUCTION

Data encryption is important to the security and integrity of information to be transmitted through a network. The need for a secured communication is more profound than ever, recognizing the fact that the conduct of almost all our business and personal matters are carried out today by computer networks [1]. Hence, in an environment where data encryption applications are fast-evolving, an algorithm that offers efficient and low-complexity encryption can provide security for information against intrusion and sophisticated threats that abound now. Moreover, the information that has to be transmitted must be encrypted to reduce the size of the data and increase processing speed.

This is done by designing a system using residue number system and inserting the image in a DNA based encryption schemes [2 - 4]. From this sequence a several useful properties could be shown:

a. There is almost no difference between a real DNA sequence and a faked one.
b. There are a large number of DNA sequences publicly available in various web-sites.

A rough estimation would put the number of DNA sequences publicly available to be around 55 million. [5, 6]

By using the above facts, we provided in this paper a RNS-DNA based encryption method that convert the image to a RNS based system then insert it to a secret reference DNA sequence. Only the sender and the receiver are aware of this reference sequence including the selected moduli, which are used to convert from binary to RNS, the moduli order (arrangement) and the selected DNA sequence in order to increase the security issues.

Manuscript received October, 2013.

M. I. Youssef, is with the Al-Azhar University, Cairo, Egypt.
A. E. Emam, is with the Al-Azhar University, Cairo, Egypt.
S. M. Saafan, is with the Higher technological Institute, Egypt.
M. Abd Elghany, is with the Al-Azhar University, Cairo, Egypt.

II. BASIC BACKGROUNDS

A. Residue Number System (RNS)

A residue number system (RNS) [7 - 9] represents a large integer using a set of smaller integers, so that computation may be performed more efficiently. It relies on the Chinese remainder theorem (CRT) [9] of modular arithmetic for its operation, a mathematical idea from Sun Tsu Suan-Ching (Master Sun's Arithmetic Manual) in the 4th century AD.

The residue number system is defined by the choice of v positive integers m_i ($i = 1, 2, \ldots v$) referred to as moduli. If all the moduli are pair-wise relative primes, any integer N, describing a non-binary message in this letter, can be uniquely and unambiguously represented by the so-called residue sequence ($r_1, r_2 \ldots r_v$) in the range $0<N<MI$,where $r_i = N \pmod{m_i}$ represents the residue digit of N upon division by m_i, and $M_I = \Pi\, m_i$ is the information symbols' dynamic range. Conversely, according to the Chinese Reminder Theorem, for any given v-tuple ($r_1, r_2 \ldots r_v$) where $0 \le r_i < m_i$; there exists one and only one integer N such that $0 \le N < M_i$ and $r_i = N \pmod{mi}$ which allows us to recover the message N from the received residue digits.

Residue number system has two inherent features that render the RNS attractive in comparison to conventional weighted number systems, such as for example the binary representation. These two features are [8]: The carry-free arithmetic and Lack of ordered significance amongst the residue digits.

The first property implies that operations related to individual residue digits of different moduli are mutually independent. The second property of the RNS arithmetic implies that some of the residue digits can be discarded without affecting the result, provided that a sufficiently "high dynamic range" is retained in the "reduced" system in order to unambiguously contain the result.

B. Bimolecular Technology

DNA, the major support of genetic information (genetic blueprint) of any organism in the biosphere, is composed of two long strands of nucleotides, each containing one of four bases (A – adenine, C – cytosine, G – guanine, T – thymine), a deoxyribose sugar and a phosphate group. The DNA strands have chemical polarity, meaning that on each end of a molecule there are different groups (5' – top end and 3' – bottom end) [6].

The four alphabets: A, C, G and T that consist in a DNA sequence is described in Table 1, each alphabet is related to a nucleotide. It is usually quite long. For instance, the DNA sequence of "Litmus", its real length is with 2856 nucleotides long. [5, 6]

- Table 1 -

Alphabet	Binary representation
A	00
C	01
G	10
T	11

A DNA molecule has double-stranded structure obtained by two single-stranded DNA chains, bonded together by hydrogen bonds: A = T double bond and C ≡ G triple bond. The double helix structure is configured by two single antiparallel strands as seen in Fig. 1. The DNA strands that bond each other through A-T and C-G bonds are known as complementary strands.

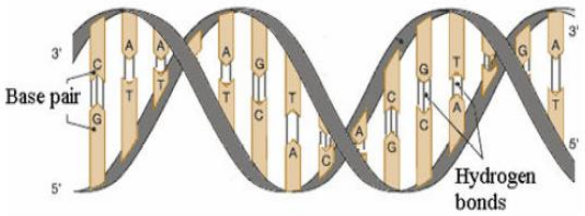

Fig. 1: DNA Structure

The DNA strands can be chemically synthesized using a machine, known as DNA synthesizer. The single-stranded chains obtained artificially with the DNA synthesizer are named oligonucleotides having usually 50-100 nucleotides in length.

III. PROPOSED ENCRYPTION SCHEME

In this paper different DNA encryption schemes are utilized together with residue number system in order to provide a more secure and flexible encryption system for image secure transmission.

Two main methods are used; insertion and complementary pair approach methods. These two methods were originally introduced in previous work [10 - 11], and we modified these techniques with merge by layer which concern about image converted to residue number system. In the following the two methods are explained.

A. Modified Insertion method:

Starting with the simplest approach called the insertion approach. Suppose the secret 64x64 bit image (M), let S be the real DNA code sequence.

The coding steps are as follows:

1) Using a secret RNS system [15 13 11], encrypt the transmitted image M'.
2) Choose the segmentation scheme for the DNA code. Suppose k is 3.
3) Depending on the length of the modified message M' and the selected segmentation scheme k, the sequence S length are selected.
4) Divide S into segments whereby each segment contains k bits.
5) Insert bits from M', once at a time, into the beginning of segments of S.
6) We use the binary code scheme to produce the following faked DNA sequence.
7) We send the above sequence S' to the receiver.

This proposed scheme has two layers of encryption as seen in Fig. 2, first conversion of the image to RNS system, and the second is the insertion of the RNS message secretly in the DNA sequence.

Each one of these two layers has its own security levels, where in the first step the conversion to RNS, the security is implemented in the number of modules used, values of the selected moduli and in the order of these moduli's. While in the second step were the faked DNA sequence is generated, the security is achieved in the DNA code selected, the located of the inserted bits inside the DNA code, and finally in the segmentation used.

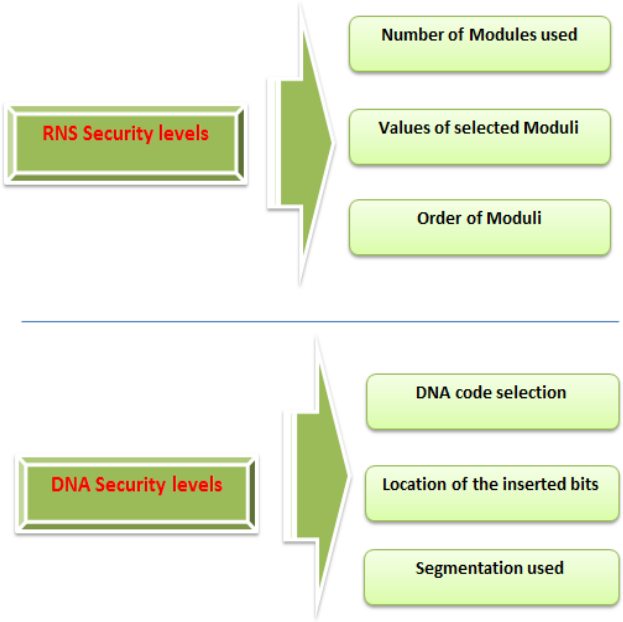

Fig. 2: Implemented Security Layers Using Insertion method

B. Modified Complementary Pair Approach:

Suppose the secret image M, the coding steps are as follows:

1) Using a secret RNS (15, 13, 11), convert the image to another binary form M'.
2) Generate a DNA sequence consisting of A, C, G and T only.
3) Divide M into segments such that each segment contains even number of bits.
4) Generate set of complementary strings with length k and insert them into L. The number of complementary strings depends on the image size.
5) Insert the first (second) alphabet of the secret message one alphabet before the first (second) complementary string.
6) Use a random number generator to select two positive integers j and i. Insert substrings S[j,j+i], and S[2j,2j+i] one alphabet after the first and second complementary substrings.
7) We send the above sequence L' to the receiver.

In this scheme we have four layers of encryption as seen in Fig. 3, first conversion of the image to RNS system, the second is the generation of the complementary pairs in the DNA code, the third is the insertion of the RNS message secretly in the DNA sequence and the fourth is the usage of a random number generator that is also added to the DNA code to generate the transmitted faked DNA code.

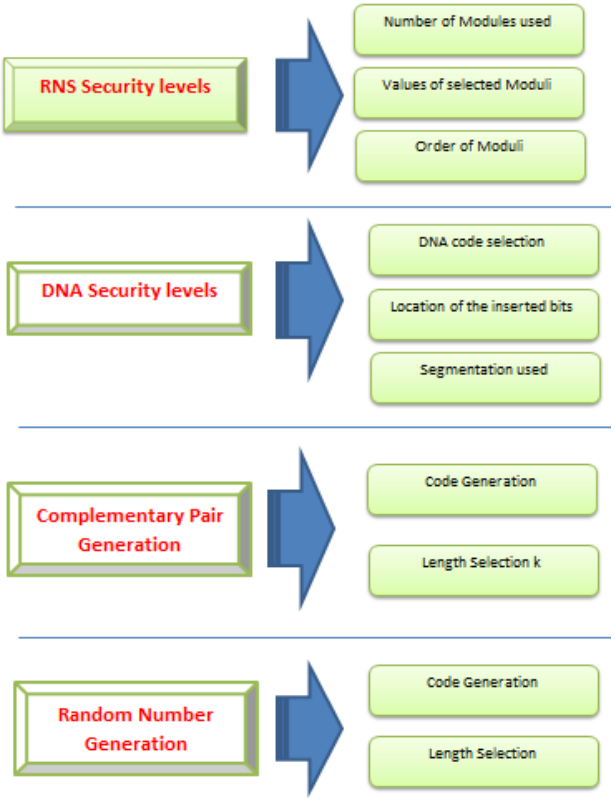

Fig. 3: Implemented Security Layers using the complementary approach

IV. SYSTEM MODEL

In this section basic transmission system shown in Fig. 4, is proposed and analyzed when the system is designed with and without RNS.

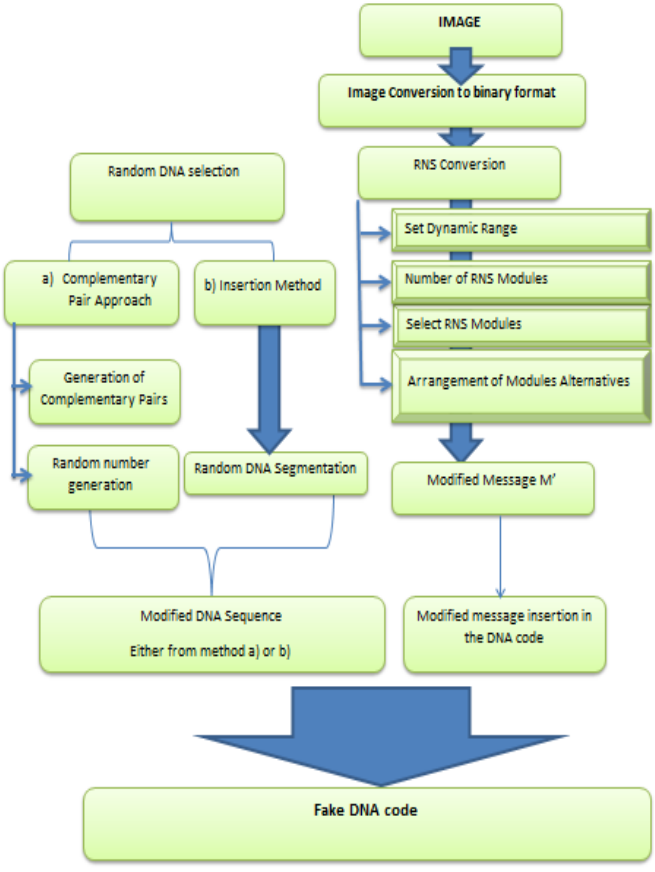

Fig. 4: DNA Encryption System

V. PARAMETERS FOR EVALUATION IMAGE ENCRYPTION SCHEME

An important issue in image encryption algorithms is the evaluation of the quality of encryption. Earlier studies on image encryption were based on visual inspection to judge the effectiveness of an encryption technique [12, 13].

An image encryption algorithm is good, if it is able to conceal a large number of image features. In some scenarios, visual inspection is sufficient but it does not give an indication about the amount of information concealed. To judge the quality of encryption a number of measuring techniques are proposed in this section, using these parameters the efficiency and security of an image encryption scheme can be evaluated.

A. Correlation Coefficient:

Correlation determines the relationship between two variables. In other words, correlation is a measure that computes degree of similarity between two variables. Correlation coefficient is a useful measure to judge encryption quality of any cryptosystem [14]. Any image cryptosystem is said to be good, if encryption algorithm hides all attributes of a plaintext image, and encrypted image is totally random and highly uncorrelated [14 – 16].

If encrypted image and plaintext image are completely different then their corresponding correlation coefficient must be very low, or very close to zero. If correlation coefficient is equal to one, then two images are identical and they are in perfect correlation. In case of perfect correlation (correlation coefficient is equal to 1); encryption process completely fails because the encrypted image is same as the plaintext image. When correlation coefficient is -1 then encrypted image is negative of original (plaintext) image.

Let x and y be the gray-scale values of two pixels in the same place in the plaintext and ciphertext images. Then mathematically correlation coefficient can be written as:

$$C.C = Cov(x,y)/(\sigma_x \sigma_y) \quad (1)$$

$$\sigma_x = \sqrt{(VAR(x))},\ \sigma_y = \sqrt{(VAR(y))} \quad (2)$$

$$VAR(x) = 1/N\ \Sigma(x_i - E(x))^2 \quad (3)$$

$$Cov(x,y) = 1/N\ \Sigma(x_i - E(x))\ (y_i - E(y)) \quad (4)$$

Where;
C.C is correlation coefficient,
Cov is covariance at pixels x and y,
VAR(x) is variance at pixel value x in the plaintext image,
σ_x is standard deviation,
E is the expected value operator,
N is the total number of pixels for N x N matrix.

B. Information Entropy Analysis

Entropy of a source gives idea about self-information i.e., information provided by a random process about itself [17]. The concept of entropy is very important for analyzing an encryption scheme. Information entropy is the main feature of uncertainty. It shows the degree of uncertainties in any communication system. The entropy, H(m) of any message can be calculated as:

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \times \log_2 \frac{1}{p(m_i)} \quad (5)$$

Where; $p(m_i)$ represent the probability of occurrence of the symbol m_i.

In general, the entropy value of the source is smaller than the ideal value, due to the fact that a real information source rarely transmits random messages. For a cryptosystem to

resist the entropy attacks, the entropy of the cryptosystem should be close to ideal value [18–20].

C. Pixel Deviation Measurement

The deviation in pixel values between original image and encrypted image is a good parameter to express the quality of encryption [20]. Randomness introduces in the encrypted image helps to conceal the features of plaintext image. The encryption quality is good, if deviation (changes) of pixels is maximum and irregular between the plaintext image and encrypted image. With the above discussion it is clear that deviation (change in pixel values) can be taken as a parameter to evaluate the quality of an image encryption scheme.

a. Maximum Deviation: By measuring the maximum deviation between the plaintext image and the corresponding encrypted image, the quality of encryption can be accessed.
b. Irregular Deviation: Histogram deviation is a good parameter to judge the quality of an encryption algorithm, but we cannot depend on this factor alone. The irregular deviation measures how much the statistical distribution of histogram deviation is close to uniform distribution. If Irregular deviation is close to uniform distribution then the encryption algorithm is said to be good.
c. Peak Signal-to-Noise Ratio (PSNR): Peak signal-to noise ratio can be used to evaluate an encryption scheme. It is a measurement which indicates the changes in pixel values between the plaintext image and the ciphertext image.

$$PSNR = 10 \times \log_{10} \left[\frac{M \times N \times 255^2}{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (P(i,j) - C(i,j))^2} \right] \quad (6)$$

Where;
M is the width and N is the height of digital image.
P(i; j) is pixel value of the plaintext image at grid (i; j)
C(i; j) is pixel value of the ciphertext image.
The lower value of PSNR represents better encryption quality.

All the above parameters will be utilized in the proposed scheme seen in sections 3, 4 and measured as stated in section5 to check and evaluate this given model.

VI. DECRYPTION PHASE

On the other hand, image decryption as seen in Fig. 5 retrieves the original image from the encrypted one. Where the processed encrypted bitstream (digital image data encoded with RNS-DNA sequence) is received and recognized. Then depending on the DNA encryption scheme, we extract the image bit stream from the DNA sequence, finally the decoder with correct moduli set used to decode the encrypted bitstream back to binary or decimal to re-construct the original image.

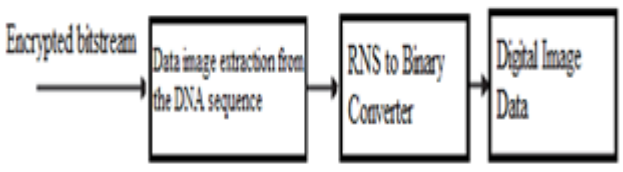

Fig. 5: DNA Decryption System

The decryption algorithm will be shown in details in subsections *A* and *B*:

A. Modified Insertion method:

The de-coding steps are as follows:

1) Generate numbers *k*'s by using the same random number generator with the same seed of the encoding scheme.
2) For a DNA sequence *S*' of the set, code *S*' into a binary sequence by using the binary coding used by the sender and use 1+ *k*' to divide the binary sequence into binary segments.
3) For each segment of the first *p* segments of *S*', extract the first bit, called m_i.
4) For each segment of the first *p* segments of *S*', extract the last k_i bits, called s_i.
5) Concatenate all m_i's to be M'and all s_i's, to be S_1.
6) Transform S_1 to be a DNA sequence by using the same rule. If S_1 is not a prefix of *S*, go to Step 2.
7) Using a secret RNS system [15 13 11], decrypt the received image M'.
8) Return *M*.

B. Modified Complementary Pair Approach:

The de-coding steps are as follows:

1) For the next DNA sequence *L*" in the set, use the dynamic programming strategy to find out all complementary substrings. If the substrings are not of the correct lengths or no such strings are found, go back to Step 1.
2) Select two positive integers *j* and *i* by using the same random number generator used in Algorithm 3.1. For each pair of complementary substrings a_g and a_g', check whether the substring with length *i*-1 starting from one alphabet after a_g' is the same with $S[j_g, j_{g+i}]$ or not. If not the same, ignore *L*", go to Step1.
3) For each pair of complementary substrings a_g and a_g', extract the alphabet one alphabet before a_g, called m_g.
4) Concatenate all m_g 's to be M'.
5) Using a secret RNS system [15 13 11], decrypt the received image M'.
6) Return *M*.

VII. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

In this section, we will demonstrate firstly in subsection *A* the encryption technique using RNS coding only , then provide the encrypted image and the Histogram of our proposed technique based on the merging between RNS and DNA sequences in subsection *B* and finally evaluating this scheme through different measuring parameters as will be seen in sections *C, D, E and F*.

A. RNS Coding Schemes:

A 64x64 bit Lena Image and its histogram is seen in Fig. 6 is encrypted using RNS modules [15 13 11]. The Histogram of the image after adding each RNS base is analyzed in addition to the Histogram of the RNS modules as a whole to see the encryption effect on the image when adding the RNS as seen in Fig. 7.

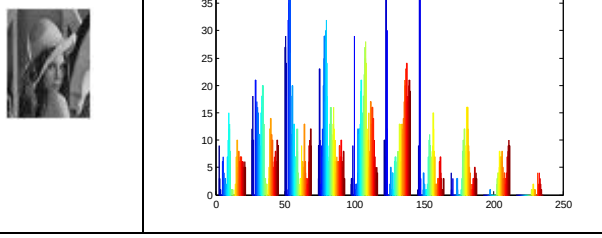

Fig. 6: Lena Image and Histogram before Encryption

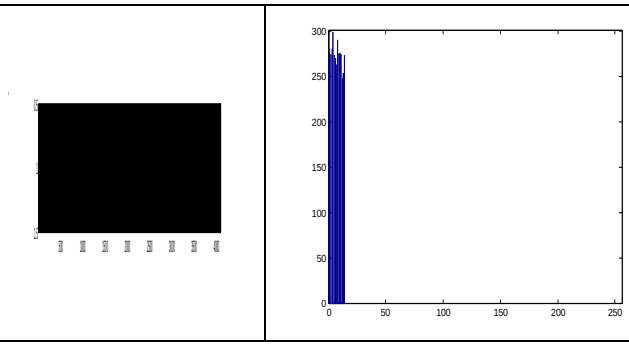

Fig. 7.a: Image and its Histogram after adding RNS Base15

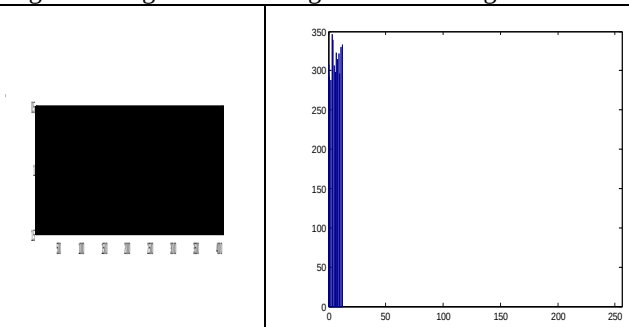

Fig. 7.b: Image and its Histogram after adding RNS Base 13

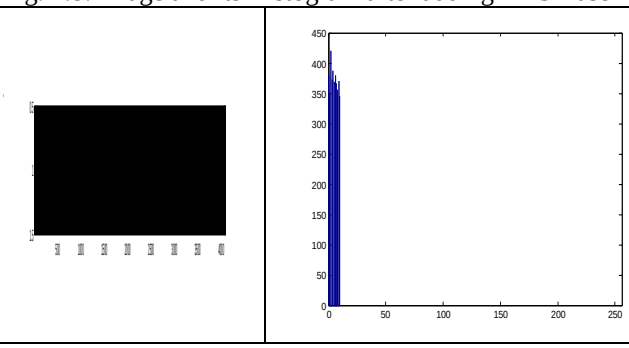

Fig. 7.c: Image and its Histogram after adding RNS Base 11

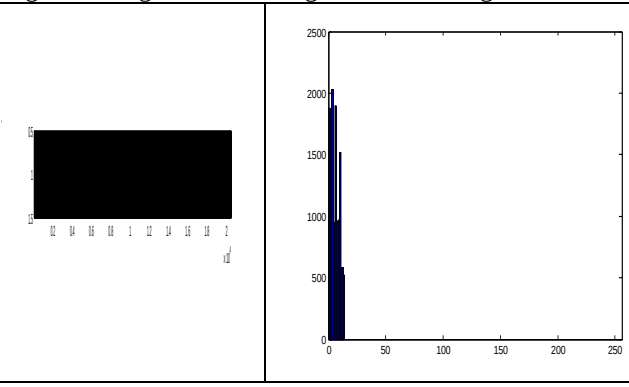

Fig. 7.d: Image and its Histogram after Encryption Using RNS[15 13 11]

As shown in Fig. 7.a, 7.b, 7.c & 7.d, the image is totally encrypted using RNS and the histogram shows the distribution of the encrypted image pixels which had been compressed, this histograms still show the maximum number of each module and we could expect its associated residue number system. This is a weak point of only using RNS as a standalone encryption system.

B. Histograms of Real and faked DNA sequences:

The faked DNA sequence generated from the insertion and complementary pair approach methods with and without RNS encryption using Lena image shown in Fig. 6 and also using Cameraman, baboon, rabbit images shown in Fig. 8, 9, & 10 are analyzed and compared with that of the real DNA sequence.

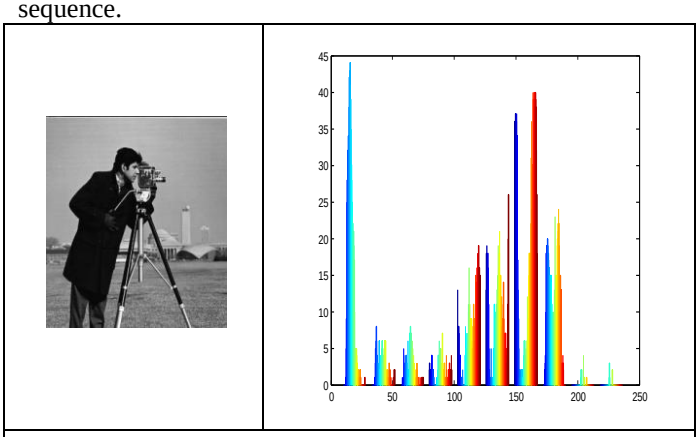

Fig. 8: Cameraman Image and Its Histogram before Encryption

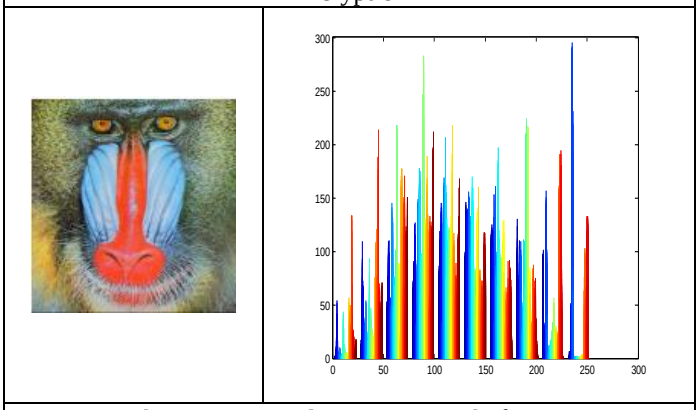

Fig. 9: Baboon Image and Its Histogram before Encryption

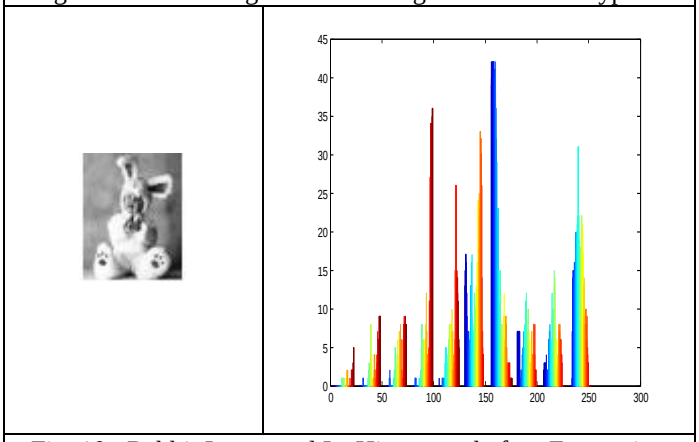

Fig. 10: Rabbit Image and Its Histogram before Encryption

In Fig. 11, the Histograms of the real DNA sequence using insertion method and complementary pair approach method are shown;

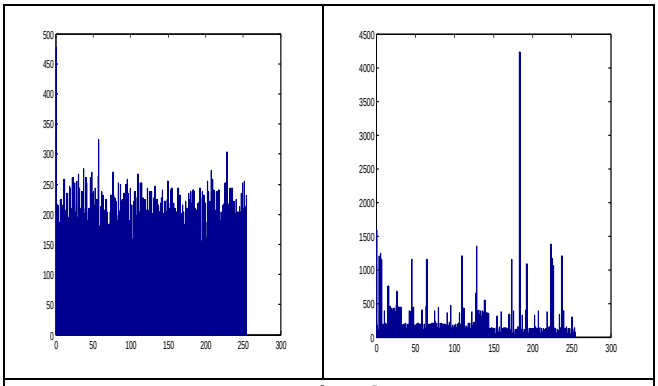

Fig. 11: Histogram of Real DNA sequence using Insertion method, Complementary pair approach method

In subsection *B.1* and *B.2*, the Histograms of the DNA sequence generated after inserting the 64x64 images are shown;

B.1 Using Insertion Method

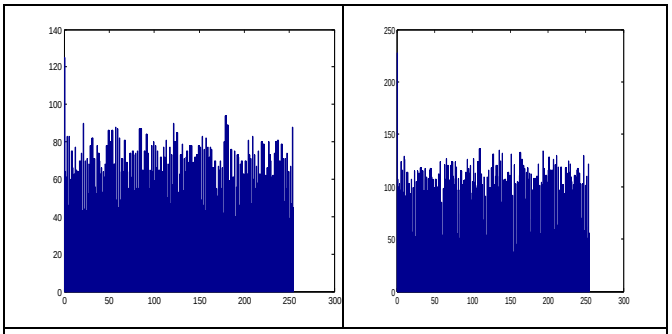

Fig. 12: Histogram of faked DNA sequence (Encrypted message) Without and with using RNS

B.2 Using Complementary Pair approach

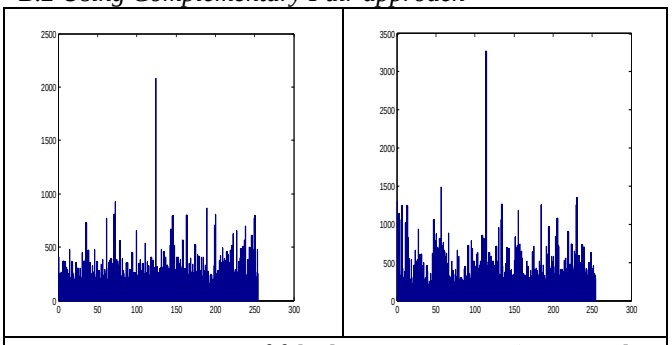

Fig. 13: Histogram of faked DNA sequence (Encrypted message) Without and with using RNS

Finally, in Fig. 14 the encrypted images are shown with and without using RNS;

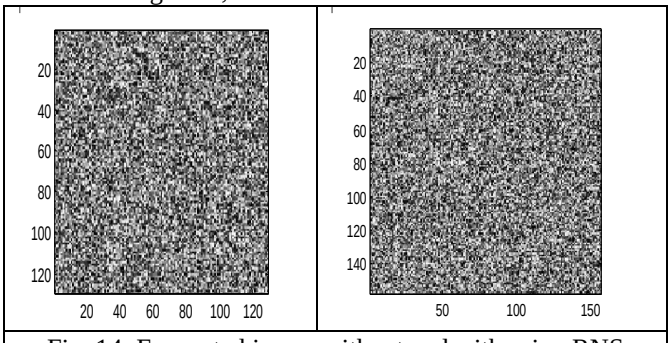

Fig. 14: Encrypted image without and with using RNS

As seen from Fig. 11, 12, and 13, the histograms of the real and faked DNA sequences (after image insertion) are similar and thus the intruder could not distinguish easily between a real and a faked DNA sequence transmission.

Now, we will evaluate our proposed encryption scheme through measuring its correlation, peak signal to noise and entropy values as seen in sections *C*, *D*, *E* and *F*.

C. Cross correlation property:

In this section we will measure the cross correlation values for the insertion and complementary pair approach methods with and without RNS encryption using Lena Image shown previously in Fig. 6.

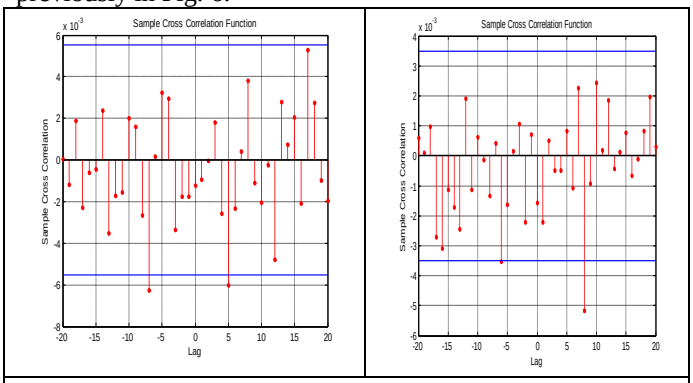

Fig. 14: Cross correlation of encrypted system using Insertion method without and with RNS

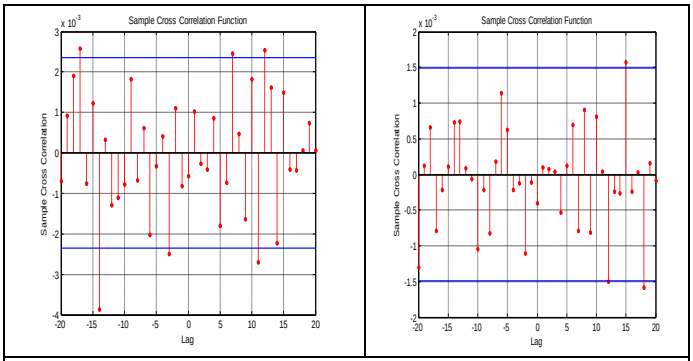

Fig. 15: Cross correlation for encrypted system using complementary method without and with RNS

The cross correlation property could be summarized in the next table;

- Table 2 -

Max Cross-correlation property		
DNA Method	Without RNS	With RNS
Insertion method	0.00527438	0.00242796
Complementary Pair approach	0.00257191	0.00157679

As seen from table 2, the RNS implementation improves the cross correlation property of the system and thus enhances the security aspect. Also, the utilization of the complementary pair approach improves the cross correlation property compared to the insertion method.

D. Correlation Coefficient Analysis:

Correlation is a measure that computes degree of similarity between two variables. In this section, we present correlation coefficient analysis before and after Encryption with and without RNS. The correlation coefficient between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in original and cipher image were tested.

Tests were performed in addition to Lena image shown in Fig. 6, images of Cameraman, Baboon and Rabbit were also

introduced as seen in Fig. 8, 9 & 10. The size of all the four images was 64_64 pixels.

- Table 3 -

Direction of adjacent pixels	Correlation coefficient – Lena Image		
	Before Encryption	After Encryption Without RNS	After Encryption With RNS
Between Horizontal pixels	0.3907728	0.039989	0.040982
Between Vertical pixels	0.32940076	0.039003	0.043732
Matrix Form	0.1300406	0.047092	0.0497963

- Table 4 -

Direction of adjacent pixels	Correlation coefficient – Cameraman Image		
	Before Encryption	After Encryption Without RNS	After Encryption With RNS
Between Horizontal pixels	0.552828	0.0433912	0.04082
Between Vertical pixels	0.521895	0.0397180	0.043146
Matrix Form	0.3972451	0.04532978	0.048249

- Table 5 -

Direction of adjacent pixels	Correlation coefficient – Baboon Image		
	Before Encryption	After Encryption Without RNS	After Encryption With RNS
Between Horizontal pixels	0.421120	0.04109	0.04021
Between Vertical pixels	0.371623	0.0414710	0.0395040
Matrix Form	0.221849	0.048830	0.0438510

- Table 6 -

Direction of adjacent pixels	Correlation coefficient – Rabbit Image		
	Before Encryption	After Encryption Without RNS	After Encryption With RNS
Between Horizontal pixels	0.397395	0.0423598	0.044304
Between Vertical pixels	0.443347	0.04048921	0.040685
Matrix Form	0.205258	0.0467574	0.046946

As seen from tables 3, 4 5 and 6, for plaintext images (before encryption), the value of correlation coefficient in all directions is close to 1 and is comparable to that provided using traditional encryption schemes as Advanced Encryption Standard (AES) & Compression Friendly Encryption Scheme (CFES). Also, using RNS would decrease the PSNR value and thus enhance the encryption

.

The ciphertext images obtained using the DNA algorithm has correlation coefficient close to zero all directions. After encryption the autocorrelation value decreased to 1/10 its value before encryption, this means that encrypted image is uncorrelated in horizontal direction. Similar results for diagonal and vertical directions were obtained.

E. Peak Signal-To-Noise Ratio (PSNR) for varies Encryption Schemes

The PSNR value is measured for the insertion and the complementary pair approach methods with and without using the residue number system. Table 7 summarizes the results seen in these different encryption schemes:

- Table 7 -

PSNR in db		
DNA Method	Without RNS	With RNS
Insertion method	7.795 db	7.74 db
Complementary Pair approach	8.088 db	7.73 db

As seen from this table that both Insertion and complementary pair approach methods provide a PSNR in the order of 8 db which is lower compared to that provided using the Advanced Encryption Standard (AES) that provide a PSNR in the order of 9 db, and thus provides better encryption scheme. Also, using RNS would decrease the PSNR value and thus enhance the encryption.

F. Information Entropy Analysis

As discussed in Section 5.2, ideally the information entropy should be 8 bits for gray scale images. If an encryption scheme generates an output cipher image whose entropy is less than 8 bits, then there would be a possibility of predictability, which may threaten its security. Information entropy is calculated by using Eq. 6. Simulation results for entropy analysis are shown in Table 8.

- Table 8: Entropy results –

	Mutual Information	Joint Entropy
Insertion Method Without RNS	2.194892405	13.76551256
Insertion Method With RNS [15 13 11]	1.714374634	14.22392371
Insertion Method With RNS [15 13 11 8 7]	1.179927146	14.71998888
Complementary Pair Approach Method Without RNS	0.545971091	14.71153461
Complementary Pair Approach Method With RNS [15 13 11]	0.385810102	15.04949237
Complementary Pair Approach Method With RNS [15 13 11 8 7]	0.229541399	15.19839599

From table 8, it is shown that using RNS decrease significantly the mutual entropy and thus enhance the security of the encryption system. Also, it is clear that the complementary pair approach method provide better encryption scheme compared to the insertion method.

VIII. CONCLUSIONS AND FUTURE WORK

In this paper, we introduced the merging between the DNA sequence and RNS to encrypt an image which added more permutation and combination that provide more security, flexibility with less complexity.

Two methods (insertion and complementary approaches methods) had been proposed and demonstrated, which is based upon a reference sequence known only to the sender and the receiver. This reference sequence can be selected from any web-site associated with DNA sequences. Since there are many web-sites and roughly 55 million publicly available DNA sequences, it is virtually impossible to guess this sequence.

We applied different parameter evaluation like correlation coefficient, entropy and peak signal to noise ratio analysis to measure the quality of our algorithm which had been found to provide comparable results to conventional schemes like the Advanced Encryption Standard (AES) and Compression Friendly Encryption Scheme (CFES).

We used the proposed encryption and decryption scheme for different image formats such as Lena, cameraman, baboon and rabbit. This means that the proposed scheme is reliable and valid.

Also, it was noticed that the complementary Pair approach provided additional improvements in the cross correlation and entropy properties compared to that using Insertion method.

REFERENCES

[1] A. Ammar, A.Al Kabbany, M. Youssef and A. Emam, "A Secure image coding scheme using Residue Number System", in proceedings of the 18th National Radio science conference, Egypt, pp. 339- 405, March 2001.

[2] Clelland, C. T., Risca, V. and Bancroft, C., Hiding Messages in DNA Microdots, Nature, Vol. 399, 1999, pp.533-534.

[3] Leier, A., Richter, C., Banzhaf, W. and Rauhe, H., Cryptography with DNA Binary Strands, BioSystems, Vol. 57, 2000, pp.13-22.

[4] Shimanovsky, B., Feng, J. and Potkonjak, M., Hiding Data in DNA, Revised Paper from the 5th International Workshop on Information Hiding, Lecture Notes in Computer Science, Vol. 2578, 2002, pp.373-386.

[5] European Bioinformatics Institute, URL: http://www.ebi.ac.uk

[6] M. Schena, "Microarray Analysis", Wiley-Liss, July 2003.

[7] K. W. Watson, "Self-checking computations using residue arithmetic," Proc. IEEE, vol. 54, pp. 1920–1931, Dec. 1966.

[8] E. D. D. Claudio, G. Orlandi, and F. Piazza, "A systolic redundant residue arithmetic error correction circuit," IEEE Trans. Computers, vol. 42, pp. 427–432, Apr. 1993.

[9] H. Krishna and J. D. Sun, "On theory and fast algorithms for error correction in residue number system product codes," IEEE Trans. Computers, vol. 42, pp. 840–852, July 1993.

[10] H. Z. Hsu and R. C. T. Lee, "DNA Based Encryption Methods", the 23rd workshop on combinatorial Mathematics and Computation theory.

[11] H. J. SHIU Et Al, "Data hiding methods based upon DNA sequences", Information sciences, 2010.

[12] H. Elkamchouchi and M. Makar, "Measuring encryption quality for bitmap images encrypted with rijndael and kamkar block ciphers," in Radio Science Conference, 2005. NRSC 2005. Proceedings of the Twenty-Second National. IEEE, 2005, pp. 277–284.

[13] H. Ahmed, H. Kalash, and O. Allah, "Encryption efficiency analysis and security evaluation of rc6 block cipher for digital images," in Electrical Engineering, 2007. ICEE'07. International Conference on. IEEE, 2007, pp. 1–7.

[14] I. Elashry, O. Allah, A. Abbas, S. El-Rabaie, and F. El-Samie, "Homomorphic image encryption," Journal of Electronic Imaging, vol. 18, p.033002, 2009.

[15] N. El-Fishawy and O. Zaid, "Quality of encryption measurement of bitmap images with rc6, mrc6, and rijndael block cipher algorithms," International Journal of Network Security, vol. 5, no. 3, pp. 241–251, 2007.

[16] S. Kamali, R. Shakerian, M. Hedayati, and M. Rahmani, "A new modified version of advanced encryption standard based algorithm for image encryption," in Electronics and Information Engineering (ICEIE), 2010 International Conference On, vol. 1. IEEE, 2010, pp. V1–141.

[17] R. Gray, Entropy and information theory. Springer Verlag, 2010.

[18] H. Ahmed, H. Kalash, and O. Allah, "Implementation of rc5 block cipher algorithm for image cryptosystems," International Journal of Information Technology, vol. 3, no. 4.

[19] R. Enayatifar, "Image encryption via logistic map function and heap tree," Int. J. Phys. Sci, vol. 6, no. 2, p. 221, 2011.

[20] Z. Han, W. Feng, L. Hui, L. Da Hai, and L. Chou, "A new image encryption algorithm based on chaos system," in Robotics, Intelligent Systems and Signal Processing, 2003. Proceedings. 2003 IEEE International Conference on, vol. 2. IEEE, 2003, pp. 778–782.