I. J. Computer Network and Information Security, **2016, 7, 1-9**
Published Online July 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2016.07.01

DNA-Genetic Encryption Technique

Hamdy M. Mousa
Faculty of Computers and Information, Menoufia University, Egypt
E-mail: hamdimmm@hotmail.com

Abstract—In this paper, we propose DNA-Genetic Encryption Technique (D-GET) in order to make the technique more secure and less predictable. In this technique, binaries any type of digital data and convert it to DNA sequencing, reshape, encrypt, crossover, mutate and then reshape. The main stages of D-GET are repeated three times or more. Transmit the encrypted data in text/image format file. In other side, the receiver uses the D-GET to decrypt the received data and reshape it to original format. This Technique also transforms the text into an image and vice versa to improve security and multiple key sequences to increase the degree of diffusion and confusion, which makes resulting cipher data difficult to decipher and makes to realize a perfect secrecy system. Experimental results demonstrate that proposed technique has multilayer protection stages against different attacks and higher level of security based on the multi-stages and genetic operations. Decrypted data are acceptable because of there is absolutely difference between it and secret data.

Index Terms—DNA Technique, cryptography, bit exchange, Genetic Algorithm.

I. Introduction

Cryptography technique is used to hide or represent information so nobody but authorized parties can decode it. Cryptography is the studies of mathematical techniques of information security such as confidentiality, data integrity, and authentication [1]. Ancient Egyptians are the oldest who encrypted text. The Internet provides essential communication and uses as a tool for many applications, i.e. secure commerce and payments to private communications and access control and so forth. Symmetric and Asymmetric key are two categories Cryptographic algorithms. In Symmetric algorithm, a common key is shared between the sender and the receiver. The other involves public and private keys that are mathematically related [1, 2].

There are many traditional cryptographic algorithms that used to encrypt and decrypt secret information. The paper proposed symmetrical encryption algorithm to protect data of Wireless Sensor Networks. It adopts minor encryption rounds, shorter data packet and simplified scrambling function. So, its calculation and resource cost are very low. Interpolation method is used to produce Child-Key by adopting longer-bit Key [3]. In [4], the symmetric cryptography algorithm is proposed for encryption and decryption the real-time audio signal. It is compared with the well-known RSA technique. The results showed that the suggested algorithm produces higher quality audio signal than the RSA method exact signal as the original one.

The traditional cryptographic algorithms are not enough to achieve very high level of security and hastily growing bio-molecular computation so that Bio-molecular computation uses in cryptographic field and DNA cryptography is a new cryptographic prototype.

DNA is a nucleic acid that contains the genetic instructions. The four bases found in DNA are adenine (A), cytosine (C), guanine (G) and thymine (T). A gene is a sequence of DNA that contains genetic information of all living organisms [5]. Three techniques to convert data from binary form to DNA (or RNA) form to amino acids form and the reverse are explained [5].

Nowadays, many research papers are proposed based on DNA encryption schemes that use biological properties of DNA sequences [6, 7, 8]. In the last few years, DNA Cryptography seems to be a promising strategy for fulfilling the current information security needs.

There are different processes to encode data and different DNA cryptography methodology that are used for secure data transmission like Polymerase chain reaction, bio-molecular, one-time-pad [9]. The most advantage of DNA cryptography is parallel processing capabilities.

DNA-based bio-molecular cryptography approach is designed. It based on DNA and carbon nanotube message that is used to transfer data between DNA and conventional binary storage [10]. The parallel DNA cryptography technique is introduced based on one time pad, DNA digital coding technique and DNA hybridization technique [11]. Parallelism DNA encryption technique based on matrix manipulation and secure key generation scheme is proposed [12]. DNA cryptographic based on implementation of YAEA encryption algorithm is proposed. It is symmetric key DNA cryptographic called Yet Another Encryption Algorithm (YAEA) and combined the mathematical model of the algorithm with the DNA to define key sequences [13]. DNA cryptography for Securing Ad hoc Networks based on the DNA digital coding and DNA fragmentation with symmetric system algorithm is proposed [14]. A new symmetric key DNA cryptographic algorithm based on the DNA key features and amino acid coding is proposed to enhance the security level of classical OTP cipher [15].

Public-key system using DNA as a one-way function for distribution is proposed. In this system, message is

Copyright © 2016 MECS

encoded by two primers using Polymerase Chain Reaction amplifications [16]. DNA public key cryptosystem, an asymmetric encryption and signature cryptosystem is proposed [17, 18]. A novel generation key scheme based on DNA is proposed to increase computational based on key expansion matrix depended on DNA scheme using random key generation scheme speed [19].

Data hiding is type of security of information. The two categories of data hiding are digital watermarking and steganographic applications. Data hiding aims to hide secret information in cover media without detectable [20]. Cryptography and steganography technique to encrypt and hide data using one-time-pad technique and DNA sequences technique [21]. The authors proposed symmetric DNA encryption algorithm to hide data based on DNA sequence [22].

The authors used Block cipher and Index of string for encrypting message into DNA sequences. DNA encryption algorithm searches the key sequence and writes in index number [23].

A novel and unique biological simulation based technique for DNA encryption and decryption is proposed. The plaintext is divided into two halves equally and transformed to DNA sequences using unique encoding table generation for every session. After that the cipher text is generated after applying proposed technique steps [24]. Some existing works on DNA Cryptography are discussed and compared [9].

An encryption method is composed of DNA synthesis and the hypothesis of conventional cryptography. The DNA Digital coding is also used as the plaintext pre-process stage. For more security protection, it is also used the fundamental keys that are the normal DNA successions [25]. Biotic Pseudo DNA based secret key cryptographic mechanism is proposed based on the genetic information of biological system using bio-molecular computation that is vast parallelism and energy efficiency. To improve security, it is also used of splicing system and random multiple key sequence [26]. Novel DNA cryptography algorithm is proposed based upon a secured symmetric key generation. This encryption algorithm is composed of three stages encryption, random key generation and decryption. In encryption stage, text is converted to ASCII then to DNA code. By using random key generated DNA sequences, this initial cipher is transformed to final cipher [27].

In this paper, DNA-Genetic Encryption Technique (D-GET) is proposed. In this technique, the secret data converted into binary and then into DNA sequences. In addition, the D-GET is an iterative algorithm. Iteration is called a round, and the number of rounds is three or more. Each round has four operations and it is iterative in nature. Iteration consists of encryption, reshaping process and genetic operations. In addition to that the symmetric key is used. Any data type format can be used as secret data i.e. text, word document, image pixels, audio and video. Experimental results prove that reconstructed data is typical copy of secret data. And they also demonstrate that proposed technique maintains the perfect security. The remaining of the paper is organized as follows: in section 2, proposed technique is introduced in detail, and then in section 3, the experimental results are provided, discussed and proved that it satisfies the presented security. Finally, some concluding remarks are given in the last section.

II. D-GET TECHNIQUE

The traditional cryptography is not sufficient due to the need of security increases and developing of cryptanalytic techniques. In recent years, DNA cryptography is a new field of cryptography. DNA cryptography seems to be a promising strategy for fulfilling the current information security needs.

This paper proposes DNA-Genetic Encryption Technique (D-GET) that is an iterative algorithm in order to enhance information security. Any type of data (i.e. message, image, video or signal) can be encrypted. The main steps of proposed technique are pre-processing, symmetric key encryption, reshaping and crossover and mutation [28]. They are explained as following.

A. Pre-processing Stage

After reading secret data, this data must be preparing depending into its type. In case text file, it is converted into ASCII values. Group them into 8-bits Binary data. Every two adjacent bits are transferred to the four bases; adenine (A), cytosine (C), guanine (G) and thymine (T), found in DNA. For example: according to Table 1.

Table 1. DNA and Representation of bits

Bits	DNA
00	A
01	C
10	G
11	T

In case of gray image, read pixels of image data into 8-bits Binary data. Every two adjacent bits are transferred to the four bases; adenine (A), cytosine (C), guanine (G) and thymine (T), found in DNA.

In RGB image, first, it is separated to three components. In case of Video data, determine the properties of the video file, including the duration, frame rate, format, height, and width and store them. As we know, a typical video contains many frames. Separate one frame at a time to save it into memory. Applying the same steps of gray image for every RGB components and each video frames.

Any type of data can be represented in a binary form (message, image, video or signal). Binary data divides to 8-bits group. Every two adjacent bits are transferred to the four bases; A, C, G and T, found in DNA. For better understanding, consider any secret data as a binary bit file. Decompose the bit file of any size onto group of bytes. For example:

Binary form of secret data:
…… 10 10 00 01 11 10 00 10 00 11 ……

Convert Binary form to DNA bases:
…… G G A C T G C G A T …….

B. Encryption stage

There are two categories of cryptographic algorithms that called Symmetric and Asymmetric key algorithms. In Symmetric scheme, the sender and the receiver are shared a common key. Asymmetric schemes involve public and private of keys which are mathematically related. The main advantage of symmetric cryptographic algorithm is high speed cryptography technique and more suitable to encrypt large amount of data [1, 2, 29]. So, the symmetric key is used in the proposed technique that based on DNA-based cryptography algorithm.

After conversion binary data to DNA sequencing then encrypt using key. The key may be DNA sequence or binary string. The key has variable length. If one or both of data and DNA sequence key DNA sequence, it will convert to binary form then, perform an exclusive OR operation on the corresponding elements of them and convert back to DNA sequence. For example:

Binary form of secret data:
…… 10 10 00 01 11 10 00 1000 11 …….

Binary form of Key:
…… 00 10 11 11 11 11 00 1110 01 …….

XOR Result:
…… 10 00 11 10 00 01 00 0110 10 …….

C. Reshaping Stage

After Encryption, A basic genetic algorithm is composed of three operators; reproduction, crossover and mutation [28]. To produce genetic material that pass to the next operation and iteration in the form of chromosome population, the Reshaping stage is used. In this stage, first number and length of chromosome are determined. These values may be constant are varied for every round. Reshape it by align the DNA sequence into rows to construct parents' chromosomes (chromosome population) with pre-defined length.

For example:

Secret data:
……..GCCCGCACCGGAACAACGGGCG
TTCCGTCCGACCCCTTTCAACTATCAGTCTTGTCA
GGCTACCGATTATCAATGCGCT ……
….

Chromosome population
……
GCCCGCACCGGAACAACGG
GCGTTCCGTCCGACCCCTTT
CAACTATCAGTCTTGTCAGG
CTACCGATTATCAATGCGCT
…….

D. Crossover Stage

After constructing parents' chromosomes, the next operation is crossover. There are two types of crossover. These may be sequentially used in technique rounds. In the first one, the parents are selected in the mating pool. A single-point crossover point is selected between the first and last bits of the parents' chromosomes then, creating two new offspring by exchanging the heads of parent1 and parent2. Consequently the offspring contain portions of the DNA codes of both parents as shown in figure 1.

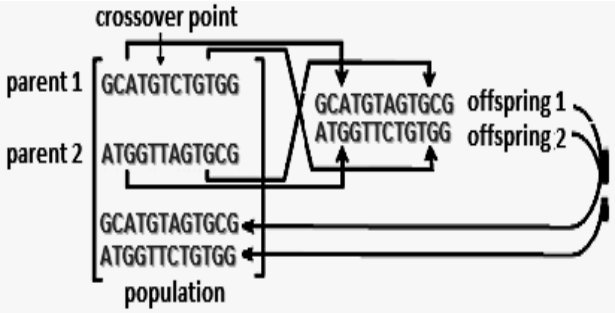

Fig.1. Two Parents Mate to produce two Offspring

The second type of crossover is rotation, after align the DNA sequence into rows to construct chromosome population. Rotate left / right with predefined value. For example:

Secret data:
…… 0 1101 1010 0101 0101 111 …….

Apply rotate Crossover:
…… 0 1010 1111 0110 1101 001 …….

Apply one point Crossover:

Two parents:
…… 11 0110 0100 1001 0010 11 …….
…… 10 0100 0111 1011 1110 01 …….

Two offsprings:
…… 11 0110 0100 1011 1110 01…….
…… 10 0100 0111 1001 0010 11…….

E. Mutation Stage

After crossover process, the chromosomes are subjected to mutation. Mutation is the alteration of string elements. Two types of mutation are used. In the first one, convert data to binary vector and define two mutation points between the first and last bits then complement bits in between i.e. single point mutation changes a 1 to a 0, and vice versa. In the second mutation type, convert each four bits to two bases of DNA (1010 → CG), for example: according to Table 2. After conversion, reshape it to DNA bases vector and define two points between the first and last bases then alter DNA bases to another one (i.e., C → G).

Copyright © 2016 MECS

Table 2. DNA bases and Representation of bits

DNA	Bits	DNA	Bits	DNA	Bits	DNA	Bits
TA	0000	GA	0100	CA	1000	AA	1100
TC	0001	GC	0101	CC	1001	AC	1101
TG	0010	GG	0110	CG	1010	AG	1110
TT	0011	GT	0111	CT	1011	AT	1111

The following example demonstrates the mutation operations of proposed technique. For example:

Apply complement Mutation:

Before mutation:
…… 11 0110 0100 1001 0010 11 …….

After mutation:
…… 11 0101 1011 0110 1010 11 ……..

Apply Alter Mutation:

Before mutation:
…… G G A C T G C G A T …….

After mutation:
…… A A G T C A T A G C ……..

The probability frequency of crossover and mutation operation is 100%. Encrypt and reshape data to pass to next round. The number of rounds depends on a predefined number of iterations. Transmit the encrypted data in text/image format file. At the receiver side, binaries received data and convert it to DNA sequencing and reshape, decrypt, crossover, mutate, decrypt and reshape to original format. The sequence of stages D-GET is illustrated in figure 2 (b). Figure 2 (a) illustrates the scenario of the stages of D-GET.

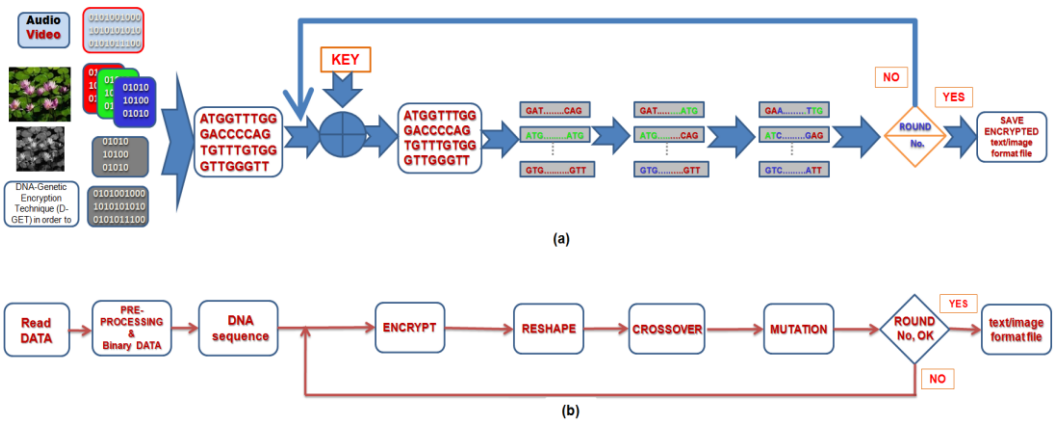

Fig.2. Stages of D-GET

The Pseudocode of Encoding and Decoding secure D-GET are shown in figure 3 and figure 4.

Input: Read Secret data (text/Image)
Output: encrypted (text/Image) file
BData1 ← Binarize the secret data.
Reshape Bdata1
Group each two adjacent bits.
DNA bases ← Bdata1
While (Round No not equal to Zero) do
Encrypt Bdata2 with key.
Reshape Bdata2
Crossover operation
Mutation.
End while
Reshape Bdata2
Save encrypted (text/Image) file
Transmit file.

Fig.3. Pseudocode of Proposed Encoding D-GET

In the previous explanation of D-GET, the pre-processing stage is complicated that means for each type of data file and format, it is wide-ranging among to conversion to ASCII values, reading pixels of image, separating components or frame and getting the properties of the video file as mentioned above to solve this problem, generalize D-GET technique. The Generalization technique is composed of the same stages of D-GET but the read data and pre-processing stage is replace with a simple Read Binary File command (fread) using 8-bit unsigned integer (uint8) and specified parameters that describe the format of the secret data.

Input: encrypted (text/Image) file
Output: secret data
BData ← Binarize encrypted (text/Image) file
Reshape Bdata
While (Round No not equal to Zero) do
Mutation
Crossover operation
Reshape Bdata
Decrypt Bdata with key.
End while
Reshape Bdata
Save reconstracted (text/Image) file

Fig.4. Pseudocode of Proposed Decoding D-GET

Copyright © 2016 MECS

III. Implemntation and Evaluation Results

The D-GET is implemented using MATLAB 2012 on Windows 8.1 64-bit Operating system in AMD Athlon(tm) II X2 220 Processor, 2.80GHz and 4 GB RAM. We perform experiments to test the effectiveness of the proposed technique and run it with different types of secret data.

In the first part, some experiments are carried out to prove the efficiency of the proposed D-GET with different formats of gray and color images. We choose some known test images and others as test images. First, read image. In case of RGB image, separate firstly it to three components, then each component passes through the processes of D-GET to encrypt it. After encoding, gathering, reshape and save encrypted data in image or text file format.

Four typical examples among them are shown in figure 5. The original images and encrypted-images in image format and DNA string are shown in figure 5. The processing time for encrypting 256x256 gray image file is approximately 26 seconds/3 rounds.

In case of image format, one of the most important factors for examining the quality of encryption technique is the visual inspection of encrypted image. The features of the image are disappeared and there is no visual relation between original and encrypted one as shown in figure 5. This means that D-GET is the good encryption technique.

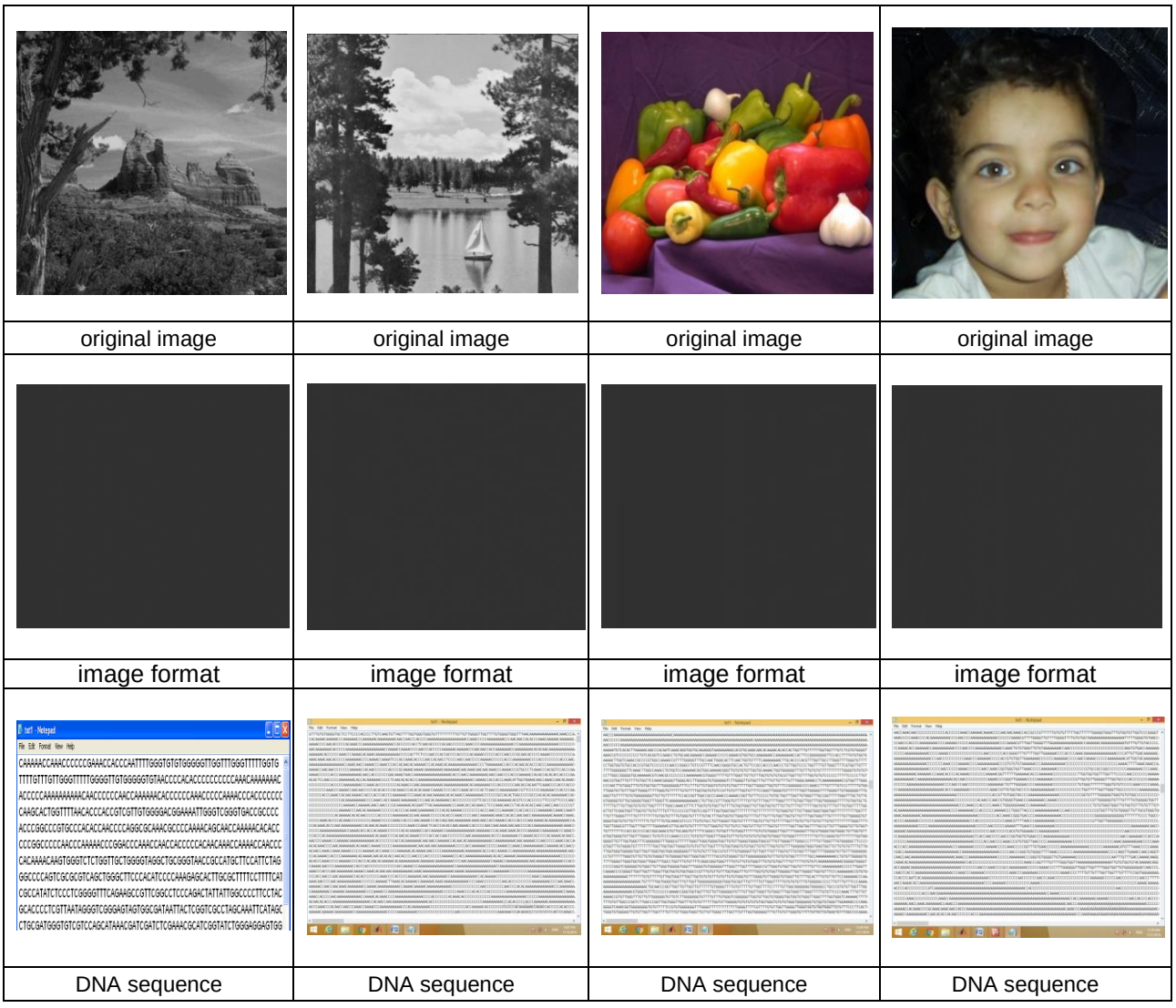

Fig.5. The Original Secret Images and Encrypted Images

For testing the proposed D-GET, second type of binary form is text file. Group of experiments is conducted to encrypt text and save the encrypted-data in DNA sequence and image format. One typical example among them is shown in Figure 6.

For more testing of the proposed D-GET, third type of binary form is audio file with different format. Encryption time for mp3 audio file with duration equal 30 seconds is about 5.5 seconds. Encryption time is approximately 36 seconds for 4 minutes mp3 audio file. Group of experiments is conducted to encrypt audio files and save the encrypted-data in DNA sequence and image format.

The last type of binary form is video file with different

format for testing the proposed D-GET. Encryption time is around 104 seconds for Movie Clip (xylophone.mpg) file with the following properties: Duration: 4.702 seconds, Bits/Pixel: 24, Frame Rate: 29.9700, Number of Frames: 141, Frame rate: 29 frames/second, Height: 240, Width: 320, Video Format: 'RGB24', audio Bit rate: 64kbps, audio sample rate: 44 kHz and channels: 2 (stereo). Some of experiments are conducted to encrypt video with duration less than 10 seconds and save the encrypted-data in DNA sequence and image format.

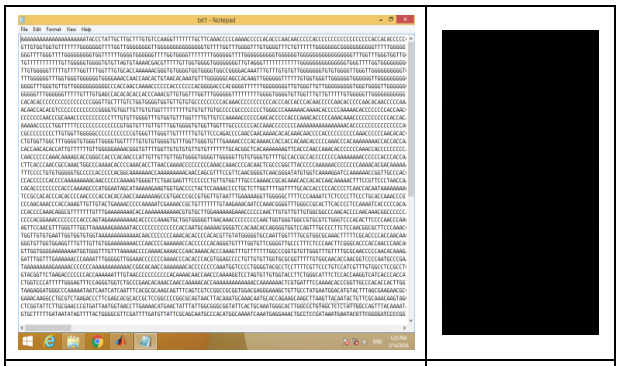

Fig.6. Part of Encrypted Text in DNA Sequence

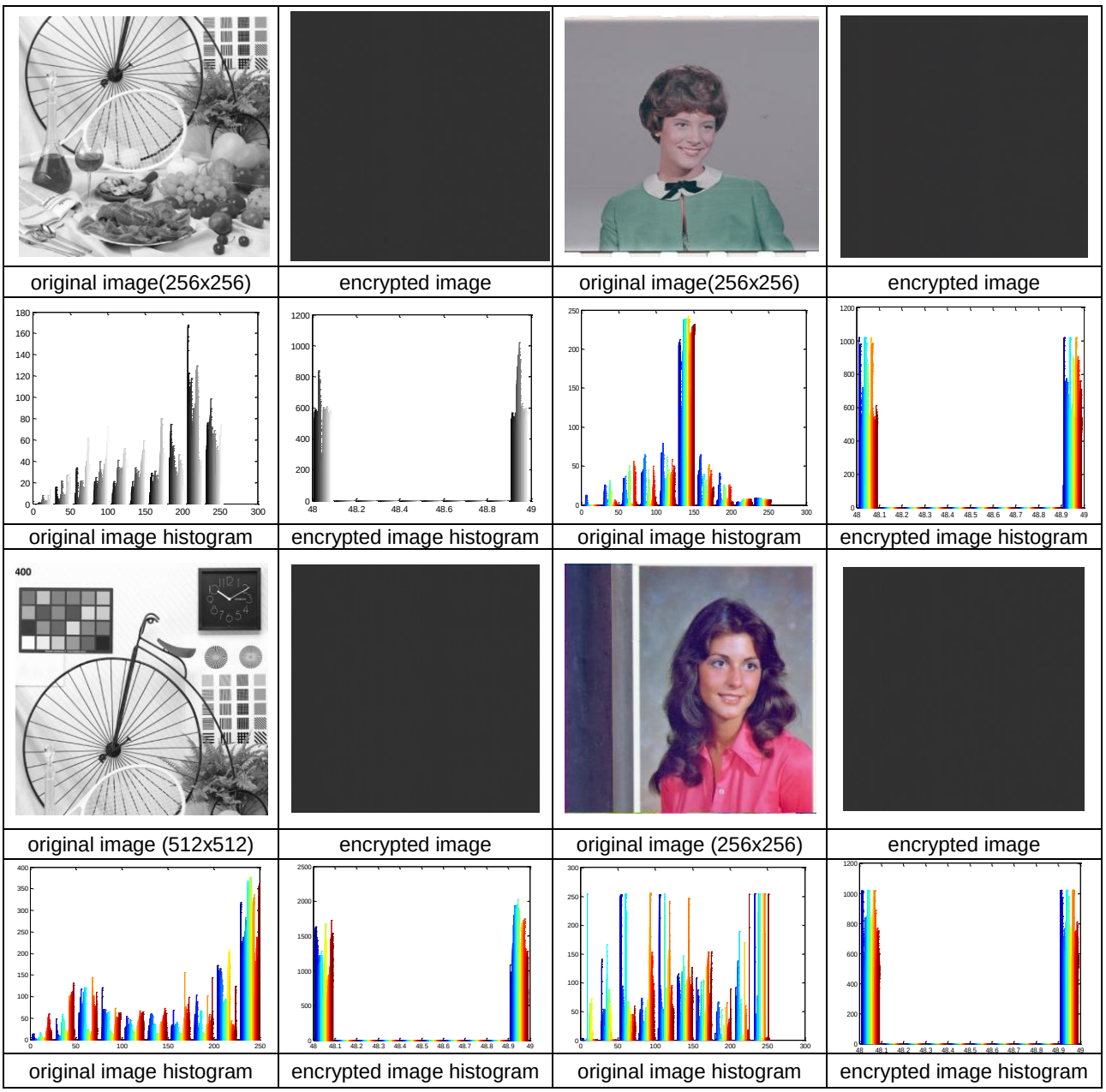

Fig.7. The Histograms of Secret Image and its Corresponding Cipher Images

IV. Experimental Results Analysis

Cryptanalysts attack any encrypted data to discover its contents using all kinds of cryptanalytic, statistical and brute-force attacks [30]. A good encryption procedure should be robust against them. So there are some features must be achieved. There is no relation between sensitive data values before encryption and encrypted data values after encryption. Encryption should mix around the different parts of the secret data so that nothing is presented in its original place.

The encrypted image is examined with the naked eye to identify and revealed any data that can help attackers to discover the original one. The visual inspection is not enough for judging the quality of encryption technique. So, other evaluation metrics are considered to estimate the efficiency of encryption technique. For example, the histogram of the original and ciphered image must be absolutely different to avoid statistical attacks, and the values of key can't predict and large enough to avoid brute force attacks.

A. Histogram Analysis

In case of image format, the attacker examines encrypted data (cipher-image) with the naked eye to identify any obvious inconsistencies. Visual attacks are the simplest and most important types of steganalysis.

The histograms of several original images and their encrypted images are analyzed. Four typical examples among them are shown in figure 7. The first and third rows in figure 7 show the secret image and its corresponding cipher images. But, the second and fourth rows show the histograms of secret image and its corresponding encrypted images. It is clear that the histograms of the encrypted image and the original one are significantly difference. So the encrypted image does not provide any indication to utilize any statistical attack on the D-GET, which makes statistical attacks difficult.

In case of image and text to DNA string, text file to image, the relationship between them is negligible.

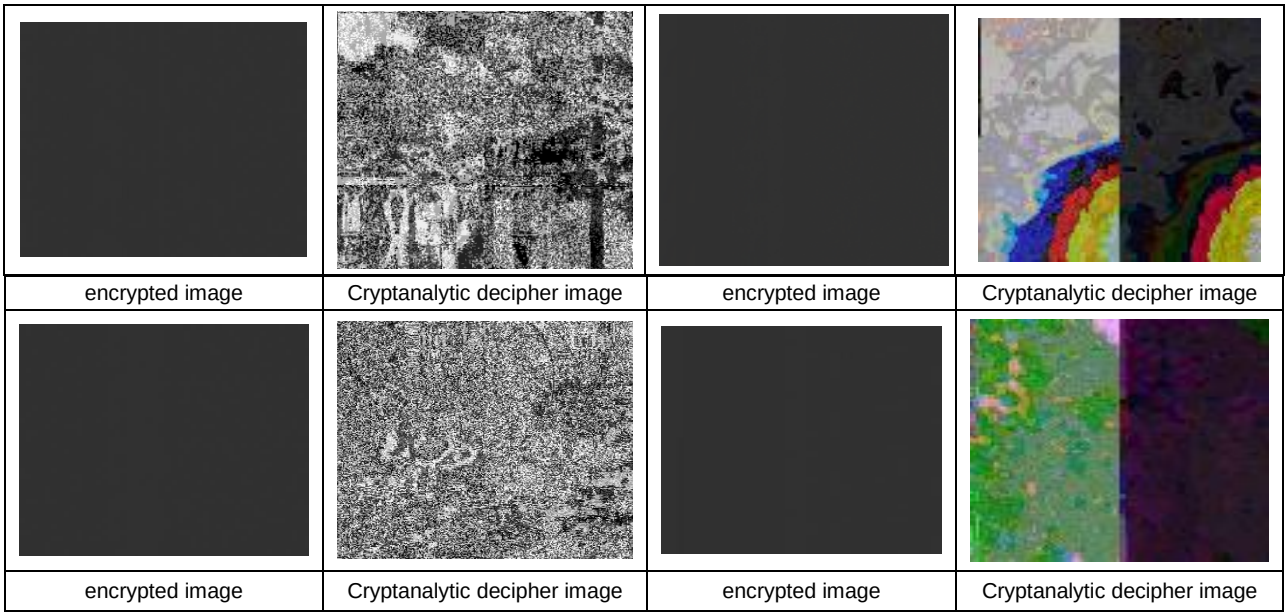

Fig.8. Cipher Data and its Corresponding Cryptanalytic Decipher Images

B. Key Space Analysis

The D-GET has large key space that making brute force attack is infeasible. It has DNA and binary sequence types of the secret keys and different combinations of them. So it resists the exhaustive of brute force attacks.

C. Attacker Tries

Attacker tries to discover any knowledge from the cipher-data that help him to find any relationship between cipher-data and the original data, by studying how differences in an input can affect the resultant difference at the output in an attempt to derive the key. If the cipher-data is image, attacker tries to make a slight change such as modifying one pixel of the encrypted image; attacker observes the change of the plain-image. If a hacker any how decrypts the image then he gets another image, which further confuses him whether the actual information is in DNA sequence or in image format. If hacker notes that all values of encrypted image is 0 and 1 hexadecimal values and convert adjacent 8 pixels to single pixel and reconstructs image. Figure 8 shows sample of output.

Thus, the D-GET makes larger statistical changes in the transmitted images. Cryptosystem is secure if it cannot be discovered even with full knowledge of the decryption algorithm. Experimental results demonstrate that proposed technique can defeat many existing steganalytic attacks. Its output is DNA sequence that making prediction of original secret is very complicated. It has a higher level of security against some existing

Copyright © 2016 MECS

attacks based on the multi-operations, encrypted keys, genetic operations and multi-rounds. In general, encrypted data size is bigger than original data size and increase of computing time. But it achieves better encryption.

V. Conclusions

In this paper, D-GET is implemented. The D-GET that is more secured encryption technique based on multi-iterations and genetic operations. It is also included operations, encryption, rotation, crossover, mutation and reshapes that increase encryption quality. This Technique transforms the DNA sequence text into an image and vice versa and confuses whether the secret message is in text or in image format. The results show the resistance of the D-GET technique against different steganalytic attacks based on multiple key sequences, D-GET operation and changes in size and format original data. The negligible relationship in both the secret data and its encrypted-data reduces the possibilities of cryptanalysis and breaking the cipher.

Furthermore, technique has multilayer protection stages that achieves confidentiality and gives more security, effectiveness and robustness to data and protects against detection.

In future work, we will be standardizing D-GET and try to reduce the transmitted data size and the encryption time.

References

[1] William Stallings, "Cryptography and Network Security: Principles and Practice", Prentice Hall, 2011.

[2] Keith M. Martin," Everyday Cryptography Fundamental Principles and Applications", Oxford University Press Inc., New York, 2012.

[3] Jingli Zheng, Zhengbing Hu and Chuiwei Lu, "A Light-weight Symmetric Encryption Algorithm Based on Feistel Cryptosystem Structure", MECS, I.J. Computer Network and Information Security, pp. 16-23, Vol. 1, 2015.

[4] M.I.Khalil, "Real-Time Encryption/Decryption of Audio Signal ", MECS, I. J. Computer Network and Information Security, Vol., 2, pp. 25-31, 2016.

[5] Mona Sabry, Mohamed Hashem and Taymoor Nazmy, "Three Reversible Data Encoding Algorithms based on DNA and Amino Acids' Structure", International Journal of Computer Applications (0975 – 8887) Volume 54– No.8, September 2012.

[6] C. T. Celland, V. Risca and Bancroft C. "Hiding messages in DNA microdots," Nature, vol. 399, pp. 533–534, 1999.

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

[8] Mohammadreza, Najaftorkaman, Nazanin Sadat Kazazi, "A Method to Encrypt Information with DNA-Based Cryptography", International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(3): pp. 417-426, 2015.

[9] T. Anwar, Dr. S. Paul, and S. Singh, "Message Transmission Based on DNA Cryptography: Review", International Journal of Bio-Science and Bio-Technology, Vol.6, No.5, pp.215-222, 2014.

[10] Chen Jie, "A DNA-based bio molecular cryptography design," Proceedings of IEEE International Symposium, Vol. 3, pp. 822-825, 2003.

[11] Pramanik Sabari, and Sanjit Kumar Setua, "DNA cryptography," In Electrical & Computer Engineering (ICECE), 7th IEEE International Conference on, pp. 551-554, 2012.

[12] Tushar Mandge, Vijay Choudhary. "A DNA encryption technique based on matrix manipulation and secure key generation scheme", International Conference on Information Communication and Embedded Systems (ICICES), 21-22 Feb. 2013.

[13] Sherif T. Amin, Magdy Saeb, Salah El-Gindi, "A DNA based Implementation of YAEA Encryption Algorithm," International Conference on Computational Intelligence (CI 2006), San Francisco, Nov. 20, 2006.

[14] A. K. Verma, Mayank Dave, R.C. Joshi, "Securing Ad hoc Networks Using DNA Cryptography", IEEE International Conference on Computers and Devices for Communication (CODEC06), pp. 781-786, Dec. 18-20, 2006.

[15] Fatma E. Ibrahim, M. I. Moussa and H. M. Abdalkader, "A Symmetric Encryption Algorithm based on DNA Computing", International Journal of Computer Applications (0975 – 8887) Volume 97– No.16, pp. 41-45, July 2014.

[16] Kazuo Tanaka, Akimitsu Okamoto, and Isao Saito, "Public-key system using DNA as a one-way function for distribution". Biosystems, Vol. 81, pp. 25-29, 2005.

[17] Lai, XueJia, "Asymmetric encryption and signature method with DNA technology", Science China Information Sciences 53.3, pp. 506-514, 2010.

[18] Cui, Guangzhao, Liming Qin, Yanfeng Wang, and Xuncai Zhang, "An encryption scheme using DNA technology", In Bio-Inspired Computing: Theories and Applications, IEEE International Conference on, pp. 37-42, 2008.

[19] Lai Xin-she, Zhang Lei, "A novel generation key scheme based on DNA", International conference on Computational Intelligence and security, pp. 264-266,13-17 Dec. 2008.

[20] Seyyed Amin Seyyedi and Nick Ivanov,"Statistical Image Classification for Image Steganographic Techniques", MECS, I.J. Image, Graphics and Signal Processing, pp. 19-24, Vol. 8, July 2014.

[21] Deepak Kumar, and Shailendra Singh, "Secret data writing using DNA sequences," In Emerging Trends in Networks and Computer Communications (ETNCC), IEEE International Conference on, pp. 402-40, 2011.

[22] Zhang Yunpeng, Zhu Yu, Wang Zhong and Richard O. Sinnott, "Index-based symmetric DNA encryption algorithm", 4th International congress on image and signal processing, pp. 2290 - 2294, 2011.

[23] Yunpeng Zhang, Bochen Fu, and Xianwei Zhang, "DNA cryptography based on DNA Fragment assembly", International Conference on Information Science and Digital Content Technology (ICIDT), Vol. 1, pp. 179-182, 2012.

[24] Noorul Hussain Ubaidur Rahman, Chithralekha Balamurugan, and Rajapandian Mariappan, "A Novel DNA Computing based Encryption and Decryption Algorithm", Procedia Computer Science 46 pp. 463 – 475, 2015.

[25] Shima Ramesh Maniyath, Thani kaiselvan V , "A Novel DNA based Encryption Algorithm for Multimedia information", An international journal of advanced computer technology, Volume 5 (1), pp. 2036 - 2045, January – 2016.

[26] E. Suresh Babu, C. Naga Raju, and Munaga H M Krishna

Prasad, “Inspired Pseudo Biotic DNA Based Cryptographic Mechanism against Adaptive Cryptographic Attacks”, International Journal of Network Security, Vol.18, No.2, PP.291-303, Mar. 2016.
[27] Bonny B. Raj, J. Frank Vijay and T. Mahalakshmi, “Secure Data Transfer through DNA Cryptography using Symmetric Algorithm”, International Journal of Computer Applications, Volume 133 – No.2, pp. 19-23 ,January 2016.
[28] M. Mitchell, “An Introduction to Genetic Algorithms”, MIT Press, 1998.
[29] Simon Johnson, “Cryptography for Developers”, Syngress Publishing, 2007.
[30] Mark Stamp and Richard M. Low, “APPLIED CRYPTANALYSIS Breaking Ciphers in the Real World”, John Wiley & Sons, Inc., Hoboken, New Jersey, 2007.

Authors’ Profiles

Hamdy M. Mousa received the B.S. and M.S. in Electronic Engineering and Automatic control and measurements from Menoufia University, Faculty of Electronic Engineering in 1991 and 2002, respectively and received his PhD in Automatic control and measurements Engineering (Artificial intelligent) from Menoufia University, Faculty of Electronic in 2007. His research interest includes intelligent systems, Natural Language Processing, privacy, Security, embedded systems, GSP applications.

How to cite this paper: Hamdy M. Mousa,"DNA-Genetic Encryption Technique", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.7, pp.1-9, 2016.DOI: 10.5815/ijcnis.2016.07.01