ISSN: 2321-7782 (Online)

Volume 4, Issue 3, March 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

A Review on Image Encryption Using DNA Based Cryptography Techniques

Sarbjeet Kaur[1]
Student, CSE Department
Sri Guru Granth Sahib World University
Fatehgarh Sahib, India

Sheenam Malhotra[2]
Assistant Professor, CSE Department
Sri Guru Granth Sahib World University
Fatehgarh Sahib, India

Abstract: In today's period as the rate of information storage and transformation is rising day by day; so as information security is becoming more essential. Network security concerned with security which prevent data from misuse and modification. The Protection of information can be done with encryption. Many traditional mathematical algorithms used for encrypting the information or data but they have limitations.DNA (Deoxyribonucleic acid) cryptography is also new promising technique for security to information. The paper discuss about the technology DNA cryptography which promises secure the data from attacks. There are large amount of DNA researchers have been performed to secure the information from attacks and general introduction about cryptography and RLE data compression technique.

Keywords: Cryptography, DNA cryptography, DNA sequence, Run-length encoding, Image Encryption, Decryption.

I. INTRODUCTION

Now a day's, providing security is one of the great challenges because of the improvement in digital communication technology, development of computer power and storage. Image security becoming more and more important with the fast growth of information exchange via internet.

Cryptography is a secret text. It means to keep the messages secret during communication i.e., hiding of information from untrusted and unpredictable elements. Cryptography is the most vital component part of the infrastructure of communication security and computer security [18]. A cryptography technique needs some algorithm for encryption of data.

Mainly there are two main type of cryptography: Secret-key cryptography and Asymmetric-key cryptography.

Secret key cryptography uses one key for encryption and decryption. Asymmetric key cryptography uses two keys; one for encryption and another is for decryption [17].

In recent years, a lot of image encryption approaches have been proposed. Encryption is a usually employed method to protect the image data [6]. Among various protection techniques, the most efficient and common technique for the protection of image is image encryption technique. Many traditional encryption algorithms, such as DES, IDEA and AES etc. are not exact for image encryption [11]. DNA cryptography is promising as a new cryptographic field where DNA is used to carry the information [4]. DNA chain have a very large scale of parallelism and DNA computing speed could reach 1 billion times per second [18] .The ability for huge storage space ,ultra-low power consumption and parallelism are making it suitable for image encryption. Image encryption methods try to convert original image to another image that is hard to know; to remain the image secret between users, in other words it is essential that nobody could get to know the content without a key for decryption [16].

A DNA sequence include a four nucleic acid bases C (cytosine), T (thymine), A (adenine), G (guanine), where A and T are complementary, and G and C are complementary. Mathematically, this means we can use this 4 letter alphabet $\Sigma = \{A, G, C, T\}$ to encode data, which is more than a enough amount considering that an electronic computer wants only two digits, 1 and 0, for the identical reason. The four nucleic acid base C, T, A and G to denote 00, 01, 10, 11. Each 8-bit pixel value of the image can be representing as a nucleotide sequence with encoding method of length four [4]. With the development of DNA computing biological and algebraic operations are presented by researchers with DNA sequence [11]. In image encryption method, DNA is used to convert the pixel value of the image into DNA sequencing using DNA rules.

Data compression implies transfer or store a smaller number of bits. Compression is the decrease in size of data to save space. Compression can be divided into two types: Lossy compression and Lossless compression methods. Lossy compression method reduces the size of information. Lossy compression reduces a file by permanently eliminating certain data, especially redundant data. With lossless compression method, every single bit of information that was originally in the file remains same after the file is uncompressed. Whole of the information is completely restored [9].

Run-length encoding (RLE) is an easy type of lossless data compression whose original method is replacing any sequence of repeated duplicate symbols is with the first symbols and a repeat length. This is useful on data that have many runs. Thus the sequence “AAAAAATTTTCCCG” is replaced with “A5T3C2G”. The run-length code represents the original 14 characters in 7 only [7].

There are so many image encryption algorithms are available to protect the image from different attacks which is described in Literature survey section.

II. Literature Survey

Xing-Yuan Wang a, n, et al. [1] presented a Novel image encryption scheme using DNA (Deoxyribonucleic acid) sequence operations and chaotic system. In their scheme firstly, plain image is encoded by using the DNA encoding rule. Then DNA-level permutation and confusion operations are applied. To remove the ability of resisting plaintext attack they proposed an extended hamming distance. Finally, ciphered image is obtained after decoding. From experimental and theoretical analysis they demonstrate that the scheme has an extraordinarily high security and resist attacks.

Shreya Gupta, et al. [2] proposed an improved and efficient algorithm to encrypt a gray scale image of any size based on DNA approach. There are two phases for encrypting the original image. Firstly, DNA sequence matrix and masking matrix is obtained a intermediate cipher. In the second phase, pixel values of the image are scrambled to make it more robust. By using this way the original image is encrypted. Their results show that scheme not only can attain good encryption but can also attacks. All these attributes show that algorithm is appropriate for image encryption and security.

Saranya M R, et al. [3] presented a new method based on genetic algorithm, logistic map and DNA sequence for image encryption. In the first stage of algorithm, a chaotic sequence was generated with the help of logistic map function and secret key calculate the initial value.DNA mask was generated. To encrypt the digital image these mask along with chaotic sequence were used. At last, Genetic algorithm was implementing and best DNA mask was obtained. The obtained result show that proposed system shows high resistance to various types of attacks. The system possesses wide key space.

Ritu Gupta, et al. [4] presented a symmetric-key encryption algorithm using DNA approach. Firstly, DNA sequence generates a secret key. Then each pixel value of the image undergoes the encryption process using key and DNA computation methods. In encryption process, DNA addition and complement combined with the variable key expansion makes the method sufficiently secure. There is no need to send a long key over the channel. The proposed method has been experimentally evaluated in terms of brute-force attack, sensitivity analysis, avalanche effect and acceptable results have been established.

M.Amr Mokhtar, Sameh N.Gobran, et al. [5] introduced a stream cipher algorithm for image encryption. The image pixel is confused and diffused by chaotic logistics map and then DNA sequence used as a one-time-pad (OTP) to change pixel value. Introduced algorithm gives almost complete security, high sensitivity as well as high efficiency to resist statistical and differential attacks.

Ranu Soni, Arun Johar, et al. [6] proposed a new image encryption and decryption algorithm using DNA sequence addition operation. Four phases are implementing. In the first phase, image is renovating into binary matrix. Then matrix is apportioning into equal blocks. Second phase, each block is encoded into DNA sequence and add these blocks with DNA sequence addition operation. Added matrix is achieved by using two logistic maps for the result. Then decoding the DNA sequence matrix is complemented and encrypt that result by using DES then encrypted image is obtained. Algorithm includes a novel encryption method for providing security to image.

Jichao Ouyang, et al. [7] introduced a new compression method based on Run-Length-Encoding (RLE) and Delta encoding method. Compression methods like bio compress, DNA compress, CFact, CTW+LZ, and DNADP are not suitable for compress the DNA sequence. These compression methods can achieve high compression ratio but sacrifice too much of time. Thus, RLE Significantly improves the running time of the DNA compression methods.

Manimurugan.S, et al. [8] in encryption process, optimization techniques are used to separate the input image into of shares. Shares are compressed by modified RLE method. To retrieve the original image the reverse process has been taken in decryption process. Using this technique, there is no expansion of the image pixel and original quality of image is reconstructed and proved in the experiment results.

Ruchita Sharma, et al. [9] proposed a data security using compression and cryptography methods. Cryptography protects users by provide functionality for the encryption of data, authentication and privacy to other users. It shows basic information about cryptography, and compression & their methods are applied on text files. The data was first compressed using compression technique and then encrypt that compressed data.

Qiang Zhang, et al. [10] proposed a new image encryption algorithm based on DNA sequence addition operation. Firstly, original image is encoding and a DNA sequence matrix is obtained. Then divide DNA sequence matrix into some equal blocks. Thirdly, bring out DNA sequence complement operation using two logistic maps for the result of added matrix. Finally, DNA sequence matrix is decoding and encrypted image is obtained. The results show that algorithm can resist most known attacks, such as exhaustic attacks, statistical attacks and so on.

Qiang Zhang, et al. [11] proposed an image encryption scheme using DNA sequence addition operation and chaos. First, the original image is encoded and a DNA sequence matrix is obtained. The obtained matrix is divided into some equal blocks and to add these blocks DNA sequence addition operation is used. Next, DNA sequence complement operation is performed. Finally, DNA sequence matrix is decoded and we get the encrypted image. The experimental results show that the algorithm can resist most known attacks. All the features show that algorithm is very suitable for image encryption.

III. Conclusion and Future Scope

In this paper, we have surveyed existing work on image encryption with different techniques. We conclude that all techniques are used for encrypting and decrypting the image with DNA cryptography and lossless data compression methods. Each technique has different algorithms for Encryption and Decryption of the information. All techniques are useful for real time image encryption and decryption. The DNA cryptography is the art of securing the data using DNA sequence. The paper gives general introduction about network security, cryptography, DNA sequence and RLE. A novel encryption technique for providing security to data is proposed. In future, a security of data based on DNA sequence with RLE as a new method to improve the ability of resisting different attacks will be developed.

References

1. Wang, X., a, Zhang, Y., a, b, nn, Bao, X., a, "A novel chaotic image encryption scheme using DNA sequence operations," Optics and Lasers in Engineering, ISSN: 0143-8166, Vol. 73, pp.: 53-61, March 2015.
2. Gupta, S., Jain, A., "Efficient Image Encryption Algorithm Using DNA Approach," International Conference on computing for Sustainable global Development (INDIACom), ISSN: 1511-0054, pp.: 726 – 731, March 2015.

3. Saranya, M. R., Mohan, A. k., Anusudha, K., “Algorithm for enhanced images security using DNA and genetic algorithm,” International Conference on Signal Processing, informatics, communication and Energy System (SPICES), pp.:1-5, Feb. 2015.

4. Gupta, R., Jain, A., “A New Image Encryption Algorithm based on DNA Approach,” International Journal of Computer Applications, ISSN: 0975 – 8887, Vol.85, Issue No.18, pp.: 27-31, January 2014.

5. Mokhtar, A, M., Gobran, N, S., EI-Badawy, M., “colored image Encryption algorithm using DNA code and chaos theory,” International Conference on computer communication and Engineering (ICCCE), ISSN: 1490-5079, pp.: 12 – 15, Sept. 2014.

6. Soni, R., Johar, A., Vishakha Soni, “An Encryption and Decryption Algorithm for Image Based on DNA,” International Conference on communication systems and network technologies (CSNT), pp.:478-481, April 2013.

7. Ouyang, j., Feng, p., Kang, j., “Fast Compression of Huge DNA Sequence Data,” International Conference on Biomedical Engineering and Informatics (BMEI), pp.: 885-888, Oct.2012.

8. Manimurugan, S., Ramajayam, N., “Visual Cryptography Based On Modified RLE Compression without Pixel Expansion,” International Journal of Engineering and Innovative Technology (IJEIT), Vol. 2, Issue 3, pp.:135-138, September 2012.

9. Sharma, R., Bollavarapu, S., “Data Security using Compression and Cryptography Techniques,” International Journal of Computer Applications (IJCA), ISSN: 0975 – 8887, Vol. 117, Issue 14, pp.:15-18, May 2015.

10. Zhang, Q., Guo, L., Xue, X., Wei, X., “An Image Encryption Algorithm Based on DNA Sequence Addition Operation, “Fourth International conference on Bio-inspired computing, pp.:75-79, Oct. 2009.

11. Zhang_, Q., Guo, L., Wei X., “Image encryption using DNA addition combining with chaotic maps,” International Conference on Bio-Inspired Computing: Theory and Applications, vol.52, issue no.11-12, pp.:2028-2035, Dec 2010.

12. Saada, B., Zhang, J., “DNA Sequences Compression Algorithm Based on Extended-ASCII Representation,” Proceedings of the World Congress on Engineering and Computer Science, ISSN: 2078-0966, vol.2, pp.:2-5, October 2015.

13. Saada, B., Zhang, J., “DNA Sequences Compression Algorithms Based on the Two bits Codation Method,” International Conference on Bioinformatics and Biomedicine (BIBM), pp.:1684-1686, 2015.

14. Saranya, M, R., Mohan, K, A., Anusudha, K., “A Hybrid Algorithm for Enhanced Image Security Using Chaos and DNA theory,” International Conference on Computer Communication and Informatics (ICCCI), pp.:1-4, Jan. 2015.

15. S.Jeevidha, Dr.M.S.Saleem Basha, Dr.P.Dhavachelvan, “Analysis on DNA based Cryptography to Secure Data Transmission,” International Journal of Computer Applications, ISSN: 0975 – 8887, Vol. 29, Issue No.8, September 2011.

16. Peng, J., Jin, S., Liang Lei and Qi Han, “Research on a Novel Image Encryption Algorithm Based on hybrid of Chaotic Maps and DNA Encoding,” International Conference on cognitive informatics & cognitive computing(ICC*CC),ISSN:1382-3660, pp.:403-408, July 2013.

17. Patel, D, K., Belani, S., “Image Encryption Using Different Techniques: A Review,” International Journal of Emerging Technology and Advanced Engineering (IJETAE), ISSN: 2250-2459, Vol.1, Issue 1, pp.:30-34, November 2011.

18. Zhang, Y., Fu, B, H, L., “Research on DNA Cryptography,” Applied Cryptography and Network Security, pp.:357-376, March 2012.

19. Zhang,Q., Guo, L.,Wei,X., “A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system,” International Journal for Light and Electron Optics (IJLEO), Vol.124, Issue 18,pp.:3596-3600, September 2013.