EasyChair Preprint

№ 5923

A New DNA Based Encryption Algorithm for Internet of Things

Bassam Al-Shargabi and Mohammed Abbas Fadhil Al-Husainy

June 27, 2021

A New DNA Based Encryption Algorithm for Internet of Things

Bassam Al-Shargabi[1] and Mohammed Abbas Fadhil Al-Husainy[2]

[1, 2] Faculty of Information Technology ,Middle East University, Amman-Jordan
bshargabi@meu.edu.jo, dralhusainy@gmail.com

Abstract : Nowadays, with the widespread of the Internet of Things (IoT) applications in every aspect of our lives. It's urgent to protect the sensitive data such as images generated by IoT devices transmitted through the wireless network. Furthermore, IoT devices are considered constraint devices regarding limited computation resources such as processing and memory size. Thus, classical encryption methods are not appropriate due to their complex computation resources. Therefore, in this paper, we proposed a new lightweight encryption algorithm based on the DNA sequence to be adequate for IoT device's resources. In the proposed algorithm, we utilized the DNA sequence random nature to generate a strong secret key, which is hard to be broken by attackers. The DNA key is used to encrypt images by two simple and robust substitution and transposition operations where they meet the requirements of IoT computation resources and the protection of the transmitted images. Moreover, the experimental results show outstanding results regarding key size, encryption time, and preparation of distortion compared with other encryption algorithms.

Keywords: Internet of Things, Data Encryption, DNA Sequence, Image Encryption, Security, Privacy.

1 Introduction

Due to the rapid development of Information, Communication Technologies (ICT), and the huge spread of Internet wireless network applications. New Internet of Things (IoT) technologies emerged and attracted much attention in academia and industry. The IoT devices can be defined as a set of objects or sensors that generate data and transfer data through the wireless network[1]. The IoT devices' main purpose is to collect, process, and pass data via communication channels and periodically control many larger units. The IoT trend is supposed to continue growing, with a rating of 26 billion network-connected devices through the year 2025[2]. IoT numerous applications span different aspects of human life, such applications extend from smart building, healthcare monitoring, smart home, smart city, and more. One of the issues in IoT applications is to handle and protect the huge amount of data generated from IoT heterogeneous devices.

The generated data from IoT devices become an attractive objective to those wishing to gain access to such data such as hackers. The solution is through using crypto-

graphic methods to provide security for valuable data, such as only authorized persons could decode the data. The classical cryptographic methods and techniques such as the Data Encryption Standard (DES) and Advanced Data Encryption (AES) algorithms cannot be used to encrypt and protect the security of generated data from the IoT device. [2–5]. The IoT devices are considered as constrained devices, where they have limited computation resources regarding processing and memory size capabilities. Therefore, classical encryption methods that require more computation resources and capabilities are not suitable for IoT devices. Therefore, the need for a lightweight encryption model or system for the IoT constrained devices that taking advantage of combining the features given by the latest appealing encryption mechanisms in order to provide sufficient and robust data confidentiality, through adapting simply to emerging and converging technologies such as DNA computing.

The merits of DNA computing such as huge parallelism, huge storage, and low-level power consumption also been exploited for introducing new cryptography methods[6, 7] . The encryption methods based on DNA computing mostly rely on the use of logistic maps and simple biological operations on DNA sequence such as logical XOR, subtraction, and addition were exploited[8, 9]. Other encryption methods exploited DNA sequence operations along with the use the chaos-based to encrypt data such as images along with the use of SHA 256 hash function[10] while another encryption approach, relying on a set of rules for transposition operation based on DNA sequence rules, to encrypt images while the encryption key was generated from images [11, 12]. Unfortunately, most of these encryption methods do not fit the resources of IoT device computational resources nor the weak nature of how the encryption key was generated.

In this paper, we are proposing a new lightweight encryption algorithm based on the DNA sequence that fits the computation resources of IoT devices. The key generation of the proposed algorithm is completely random based on the DNA sequence, which makes it very difficult to break. Moreover, the generated key is used to make simple, logical, and strong confusion and diffusion on the plain image based on the randomness nature of the DNA sequence and its which satisfies IoT computation capabilities.

The rest of the paper is structured as follows: The topic background and related work were discussed in section 2. The proposed DNA encryption algorithm was described in Section 3. The experimental results and discussions were presented in section 4, and finally, the conclusion was drawn in Section 5.

2 Background and Related work

Cryptography is a specified domain of science which compact with the encoding of data for the goal of concealing messages content. It plays a vital function in the infra-

structure of communication security. The latest advances in cryptography had shown the capability of exploiting DNA computation. This opens the way for DNA Computing as a new technique to boost producing a new cryptography system that meets the computation capabilities of IoT devices.

2.1 IoT and Encryption

Cryptographic algorithms introduced in the literature for IoT constrained devices could be categorized into the symmetric and asymmetric algorithms. Symmetric algorithms utilize the same key for both encryption and decryption. The strength of the symmetric algorithms is actually based on how the key was securely exchanged between the sender and receiver[13–15]. Asymmetric algorithms actually avail two various keys involving the public and private keys. The private key is never transmitted via the network and then it is secure. The public key is sent via the network to the receiver. Through encryption, the sender encrypts the plaintext utilizing the public key of the receiver and sends the resultant ciphertext to the receiver utilizing the network. Even if the public key was known to the hacker, he couldn't read the scrambled message because the secret key was not recognized for him. through decryption, the receiver will utilize the private key to decrypt the ciphertext. Asymmetric algorithms were more complex to implement and utilize more resources than symmetric algorithms. Therefore, most of the applications of IoT utilize symmetric algorithms in order to provide security to the transmitted data. Further, they are simple to execute, and utilize fewer resources with low overhead, and are secure as long as the key is hard for attackers to break [16].

Numerous encryption algorithms have been proposed recently to ensure the security of transmitted data through the IoT network, such as Tiny Encryption Algorithm (TEA) and Secure IoT (SIT) methods. The TEA methods are the most attractive due to its lower memory utilization and ease of implementation on both hardware and software scales [17]. on the other hand, SIT is a 64-bit block cipher and requires 64-bit key to encrypt the data. The architecture of the algorithm is a mixture of festal and a uniform substitution-permutation network[18], but in this paper, the DNA based encryption algorithm specifically designed to provide strong and secure data encryption that meets limited IoT computing resources.

DNA encryption is preferred instead of digital encryption because most of the cryptographic techniques have been cracked at least partially by the new computer generation such as the Quantum Computing[19]. Moreover, regarding the key generation issue, the randomness and complexity of DNA sequence attached an additional layer of security for DNA based encryption methods [20]. The DNA sequence consists of four alphabets(A, C, G, and T), where each alphabet is associated with a nucleotide. The DNA sequence is usually quite long and the publicly available DNA sequences are to be around 55 million. The DNA sequence is mainly used for a secret key generation where it must only be known by the sender and the receiver[21].

2.2 Related Work

A lightweight cryptographic (LWC) algorithm proposed in [22], which used a digital file of any type (text, image, audio, and video) as a seed in order to generate the secret key. Their method works on a 32-bit block size and a key of any length and type of digital data. It created a 16×16 exchange table of bytes, thus, a key space of 2048 was utilized. In addition, part of the key was embedded in the encrypted image.
Ciphertext-policy attribute-based encryption (CP-ABE) scheme [23] was introduced but it was not appropriate for lightweight IoT devices because they produced more computation overhead while implementing encryption and decryption operations. Another study in [24] proposed a hybrid DNA-encoded ECC (Elliptic curve cryptography) scheme which extends multi-level security. The DNA sequence was chosen, and utilizing a sorting algorithm, a unique set of nucleotide sets was assigned. These were instantly converted to binary sequence and then encrypted utilizing the ECC; so, granting double-fold security. algorithm analysis proved that DNA added with Elliptic Curve Cryptography (ECC) can provide better security compared to ECC alone. Results showed good performance for IoT technologies but it needs more computation resources more than the resources available in IoT devices. In another approach in [21], they used two levels of encryption where DNA encoded ECC to reduce processing time and memory size to be more adequate to IoT devices.
A stream cipher depends on DNA encryption and decryption was introduced in [25], where they encrypt text and data produced by image sensors. They integrated the compressive sensing algorithm with DNA encoding and decoding based stream cipher to perform the secure compressive sensing. but the computation overhead was minimal but also does not match the real computation of IoT devices.

3 Proposed DNA Encryption Algorithm

The proposed DNA based encryption algorithm for IoT devices is presented in this paper is a new DNA block cipher symmetric algorithm. The DNA sequence is exploited to generate an encryption secret key(Skey), where the generated Skey is completely random and used through encryption two main robust and strong substitution and transposition operations that fit the limited computation resources of IoT constrained devices. The proposed DNA based encryption algorithm as illustrated in figure 1 includes the next main operations:

- ***Key generation*** :The key generation of the proposed algorithms is extracted from any DNA sequence that is taken within any size, where DNA sequence contains a series of letters, and every four consecutive letters represent a series of randomly arranged bits. Each letter representing two bits as shown in table 1. The DNA sequence is then segmented into segments of 1 byte (K1, K2,...Kn) from the four DNA letters (A, C, G, T), where these segments represent the Secret Key (SK).

Table1. Binary representation of DNA Sequence letters

DNA letters	Binary representation
A	00
T	01
C	10
G	11

- ***The encryption process***: The proposed DNA based algorithm is a block cipher that involves substitution and transposition operations on the bytes of Source Image (SImage) as depicted in Figure 1. The two operations are described below:

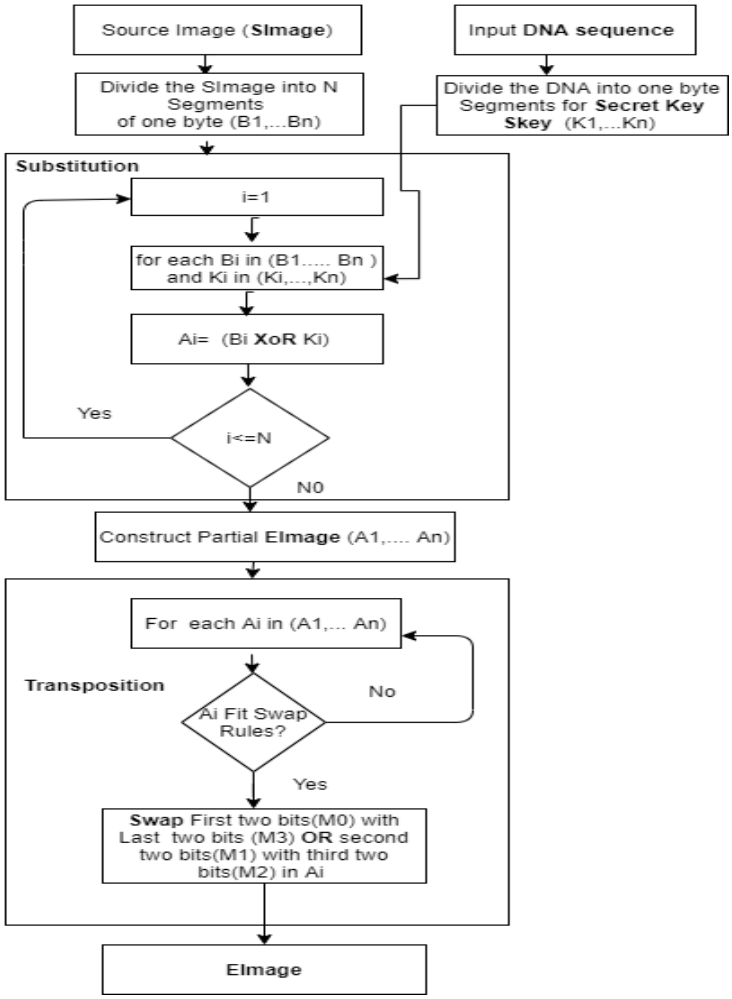

Fig. 1. The proposed DNA based encryption process

1. *substitutions phase*: Before applying the substation phase, the SImage must be segmented into N segments where each segment size is 1 byte (B1, B2,..., Bn). Thereafter, applying XOR operation between I byte (B1, B2...Bn) of SImage segments and DNA segments of Sk (k1,k2,...,kn) . The results of the XOR operation will form new bytes (A1, A2,..., An), and this operation repeated N times. The output of the whole operation will form new A_i bytes.

2. *Transposition phase*: The transposition phase involves swapping bits of the resulted Ai bytes. The bits swapping process executed on A (A1, A2,...., An) is based on the Sk bytes generated from the DNA sequence and set of rules as shown in table 2. For example, if the first two bits in A1 is 00 (DNA letter A) and the last two bits is 01 (DNA letter T) then don't swap them and if the third and fourth bits of A1 were 01 and 11 then swap these bits as shown in figure 2, where A1 represents one byte of the result substitution and AT1 byte represents the result of transposition operation. This process continues until the whole SImage is encrypted (EImage).

Tabl2. Swapping Rules

DNA sequence letter	DNA sequence letter	Operations
A	T	Don't Swap
C	G	Don't Swap
T	T	Swap
T	G	Swap
G	G	Swap
A	T	Don't Swap

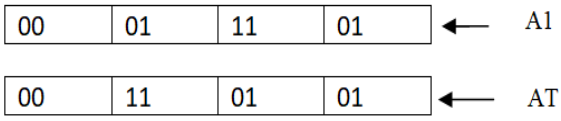

Fig. 2. Transportation Example

- The decryption process begins in a reverse way, as it begins with transposition then substitution. The decryption process starts from the last byte of the encrypted image (EImage) and gradually to the first byte of the encrypted image. The transposition phase returns the swapped bits to its original position based on swapping rules in table 2 as these rules must be shared among the sender and receiver of the image. At the end of the transposition phase, the substitution phase begins with applying XOR operation by taking the last byte of EImage and the last byte of the DNA sequence where the sender of EImage stopped substitution operation. The substitution continues until the First byte of EImage. At the end of the substitution phase, the original image SImage will be restored.

4 Experimental Result and Discussion

To evaluate the effectiveness of the proposed lightweight DNA based encryption algorithm for IoT constraints devices. We have implemented the proposed algorithm and compared its effectiveness regarding key size, encryption time, and proportion of distortion to well know encryption algorithms such as DES and AES as standards encryption algorithms. We have used several images with different size, content as illustrated in figure 3 .

a) Balloon (424*283) b) Petra (256* 256) C)Aqsa (381*254)

Fig. 3. Different types of images used in the experiments

The first evaluation metric is the key size used in the proposed DNA based encryption algorithm, to achieve high protection for the encrypted image the key must be large in size and completely random to be unbreakable by attackers. To overcome the computation resources of IoT devices, the key size for the proposed DNA-based algorithm for the encryption process is 8 bits' as shown in table 3. Due to the fact that during the encryption process, the SImage was divided into small segments (just one byte), and for each segment of SImage we applied XoR operation with 8 bits of the secret key generated from four-letter of DNA sequence until the last segment of the SImage . The Skey size is relatively relying on the size of SImage and considerably fits the memory size of IoT devices. In addition, it's not easy to break by an attacker due to the random nature of the DNA sequence.

Table3. Key size of proposed DNA algorithms, DES, and AES

Encryption System	Size of the Key (bit)
DNA algorithm	8
AES	256
DES	56

Regarding the second metric encryption time where it usually plays a significant role in different communication applications and its related encryption algorithms especially for IoT devices and its application. In the proposed DNA algorithm, the use of logical XOR substitution and transposition rules operations reduced the time needed to encrypt SImags (time in millisecond ms). This means less pro-

cessing time and memory that fit IoT computation resources compared to other algorithms as shown in table 4, where the encryption time on average for the three images for the proposed DNA algorithm was 125 ms, which is less in the other algorithms.

Table 4. Encryption Time

Image	Proposed DNA algorithm	DES	AES
POOL	203.125	2625	2609.375
PETRA	62.5	1421.85	1421.875
AQSA	109.375	2093.75	2125

Regarding, the proportion of distortion in EImage compared to SImage is based on Peak Signal-to-Noise Ratio (PSNR) metric. The PSNR value measures the impact of confusion and diffusion between the SImage and the EImage, where it is calculated in decibels using equation (1 and 2) . The experiments PSNR values indicate that the proposed algorithm achieved a comparable proportion of distortion in the EImage compared to other algorithms as shown in Table 5. .

$$NMAE = \frac{\sum_{k=0}^{SSize-1}|S(k)-E(k)|}{SSize} \times 100 \quad (1)$$

$$PSNR_{db} = 10.\log_{10}\left(\frac{Max_I^2}{NMAE}\right) \quad (2)$$

Where: Max_I is the maximum possible byte value of the data $\boldsymbol{S}$. And *db* refer to a decibel.

Table 5. PSNR value

Image	Proposed DNA algorithm	DES	AES
POOL	8.528	8.369	8.355
PETRA	7.786	7.648	7.667
AQSA	8.687	8.594	8.587

5 Conclusion

The proposed lightweight encryption algorithm in this paper is based on the DNA sequence for exploiting the random nature of the DNA sequence. The proposed algorithm also uses simple, strong, and robust substitution and transposition as the two main operations for the encryption process. The key generation and encryption processes were designed to be more adequate to meet the limited resources in terms of processing and memory size for IoT devices. The experimental result shows outstanding results regarding key size and its random nature which will make it hard for the attacker to break the key. The proposed algorithm also shows a comparable PSNR value compared to AES and DES.

As future work, we will study the effects of segmenting DNA and images into variable sizes regarding different computation resources of the IoT device's processing and memory size.

Acknowledgment

The author is grateful to the Middle East University, Amman, Jordan for the financial support granted to cover the participation in the conference and the publication fee of this research article

References

1. Al-Shargabi, B., Sabri, O.: Internet of Things: An exploration study of opportunities and challenges. In: 2017 International Conference on Engineering & MIS (ICEMIS). pp. 1–4. IEEE (2017).
2. Abualese, H., Al-Rousan, T., Al-Shargabi, B.: A New Trust Framework for E-Government in Cloud of Things. International Journal of Electronics and Telecommunications. 65, 397–405 (2019). https://doi.org/10.24425/ijet.2019.129791.
3. Hussain, I., Negi, M.C., Pandey, N.: A secure IoT-based power plant control using RSA and DES encryption techniques in data link layer. In: 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS). pp. 464–470. IEEE (2017).
4. Pawar, A.B., Ghumbre, S.: A survey on IoT applications, security challenges and counter measures. In: 2016 International Conference on Computing, Analytics and Security Trends (CAST). pp. 294–299. IEEE (2016).
5. Chourasia, S., Singh, K.N.: An efficient hybrid encryption technique based on DES and RSA for textual data. In: Information Systems Design and Intelligent Applications. pp. 73–80. Springer (2016).
6. Chai, X., Gan, Z., Yang, K., Chen, Y., Liu, X.: An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations. Signal Processing: Image Communication. 52, 6–19 (2017).
7. Wang, X., Hou, Y., Wang, S., Li, R.: A new image encryption algorithm based on CML and DNA sequence. Ieee Access. 6, 62272–62285 (2018).
8. Wen, H., Yu, S., Lü, J.: Breaking an image encryption algorithm based on DNA encoding and spatiotemporal chaos. Entropy. 21, 246 (2019).
9. Chai, X., Gan, Z., Yang, K., Chen, Y., Liu, X.: An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations. Signal Processing: Image Communication. 52, 6–19 (2017). https://doi.org/10.1016/j.image.2016.12.007.
10. Guesmi, R., Farah, M.A. Ben, Kachouri, A., Samet, M.: A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2. Nonlinear Dynamics. 83, 1123–1136 (2016).

11. Liu, Y., Lin, T., Wang, J., Yuan, H.: Bit image encryption algorithm based on hyper chaos and dna sequence. Journal of Computers. 29, 43–55 (2018).
12. Malik, M.G.A., Bashir, Z., Iqbal, N., Imtiaz, M.A.: Color Image Encryption Algorithm Based on Hyper-Chaos and DNA Computing. IEEE Access. 8, 88093–88107 (2020).
13. Maram, B., Gnanasekar, J.M., Manogaran, G., Balaanand, M.: Intelligent security algorithm for UNICODE data privacy and security in IOT. Service Oriented Computing and Applications. 13, 3–15 (2019).
14. Aly, M., Khomh, F., Haoues, M., Quintero, A., Yacout, S.: Enforcing security in Internet of Things frameworks: A systematic literature review. Internet of Things. 6, 100050 (2019).
15. Abbas Fadhil Al-Husainy, M., Al-Shargabi, B.: Secure and Lightweight Encryption Model for IoT Surveillance Camera. International Journal of Advanced Trends in Computer Science and Engineering. 9, 1840–1847 (2020).
16. Khan, M.A., Salah, K.: IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems. 82, 395–411 (2018).
17. Rajesh, S., Paul, V., Menon, V.G., Khosravi, M.R.: A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices. Symmetry. 11, 293 (2019).
18. Usman, M., Ahmed, I., Imran, M., Khan, S., Ali, U.: SIT: A Lightweight Encryption Algorithm for Secure Internet of Things. International Journal of Advanced Computer Science and Applications. 8, 1–10 (2017). https://doi.org/10.14569/ijacsa.2017.080151.
19. Fernández-Caramès, T.M., Fraga-Lamas, P.: Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE Access. 8, 21091–21116 (2020).
20. Omran, S.S., Al-Khalid, A.S., Al-Saady, D.M.: A cryptanalytic attack on Vigenère cipher using genetic algorithm. In: 2011 IEEE Conference on Open Systems. pp. 59–64. IEEE (2011).
21. Barman, P., Saha, B.: DNA encoded elliptic curve cryptography system for IoT security. International Journal of Computational Intelligence & IoT. 2, (2019).
22. Mohammed A. Fadhil Al-Husainy, H.A.A.-S. and S.R.M.: Lightweight Cryptosystem for Image Encryption Using Auto-Generated Key. ournal of Engineering and Applied Sciences. 13, 7418-7425. (218)AD.
23. Pasupuleti, S.K., Varma, D.: Lightweight ciphertext-policy attribute-based encryption scheme for data privacy and security in cloud-assisted IoT. In: Real-Time Data Analytics for Large Scale Sensor Data. pp. 97–114. Elsevier (2020).
24. Tiwari, H.D., Kim, J.H.: Novel method for DNA-based elliptic curve cryptography for IoT devices. ETRI journal. 40, 396–409 (2018).
25. Aishwarya, R.U., Sreerangaraju, M.N.: Enhanced Security using DNA Cryptography. (2019).