Increasing Randomization of Ciphertext in DNA Cryptography

Maria Imdad[1], Sofia Najwa Ramli[2]
Center of Information Security Research
Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia, Batu Pahat, Malaysia

Hairulnizam Mahdin[3]
Center of Intelligence and Autonomous Systems
Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia, Batu Pahat, Malaysia

Abstract—**Deoxyribonucleic acid (DNA) cryptography is becoming an emerging area in hiding messages, where DNA bases are used to encode binary data to enhance the randomness of the ciphertext. However, an extensive study on existing algorithms indicates that the encoded ciphertext has a low avalanche effect of providing a desirable confusion property of an encryption algorithm. This property is crucial to randomize the relationship between the plaintext and the ciphertext. Therefore, this research aims to reassess the security of the existing DNA cryptography by modifying the steps in the DNA encryption technique and utilizing an existing DNA encoding/decoding table at a selected step in the algorithm to enhance the overall security of the cipher. The modified and base DNA cryptography techniques are evaluated for frequency analysis, entropy, avalanche effect, and hamming weight using 100 different plaintexts with high density, low density, and random input data, respectively. The result introduces good performances to the frequency analysis, entropy, avalanche effect, and hamming weight, respectively. This work shows that the ciphertext generated from the modified model yields better randomization and can be adapted to transmit sensitive information.**

Keywords—DNA cryptography; avalanche effect; frequency test; entropy; hamming weight

I. Introduction

With the amazing development of Deoxyribonucleic Acid (DNA) computing, DNA cryptography is a new advancement in cryptography. DNA molecules are an integral part of a cell and act as genetic information carriers, but when applied in modern cryptography, it serves as a data manipulation tool [1].

The design of an encryption/decryption algorithm should be complex enough to stand for a long time against a security attacks. The best way to reach such complexity in a system is to work towards scalability because this will ultimately lead to large-scale complexity. The main idea to increase the complexity in the system by augmenting its size is to achieve the desired security that will require tremendous efforts to attack the system successfully. These desired properties can be achieved by DNA cryptography as it offers huge parallelism and storage capacity simultaneously [2]. The power of DNA encryption is not only in the molecules or encoding but in the positions where we want to save our data to protect it from attacks for a longer time [3] . Cryptography is the procedure to create such algorithms, whereas; cryptanalysis is the procedure where attackers or the algorithm developers validate the cipher for its vulnerabilities and improve it by giving insight for future directions [4]. Randomness [5], avalanche effect [6], and entropy per bit [7] are some of the desired properties to evaluate the ciphertext. A cryptographic solution should satisfy this criterion, at least to ensure safety.

Avalanche effect [5] is a compelling test, whereby changing one bit in plaintext or key will change at least 50% of the bits in the ciphertext. This research work focuses on the change in ciphertext from a plaintext perspective. A detailed study of DNA cryptographic encryption algorithm as in [8] indicates that the avalanche effect is considerably less, leading to security vulnerabilities. Specifically, the conversion of the binary data into DNA bases (00 to A, 01 to G, 10 to C, 11 to T) exhibits poor avalanche effect or randomization of the ciphertext. This may cause an attacker to establish a relationship between plaintext and its ciphertext. In this paper, a modified DNA encryption technique with an existing DNA encoding table used in [9] are introduced to the existing algorithm to overcome the mentioned security vulnerability. The proposed encryption technique allows the user to send encrypted information with an extra fold of security. The experimental results have endorsed the effectiveness of the proposed technique by performing a statistical analysis between the base technique and the proposed technique.

The overall structure of the study takes the form of six sections, including this introductory section followed by a literature review in Section 2. Section 3 gives an insight on the encryption algorithm using base and the proposed technique. Section 4 explains the list of tests to measure the randomness in technique. Section 5 has a detailed analysis of results validating the effectiveness of the proposed technique. Section 6 discusses the concluding remarks considering improvements and limitations followed by cited references in a separate section.

II. Related Work

DNA computing is an increasingly important area in applied cryptography where the inherited property of storing huge data is adopted along with DNA replication to introduce randomness in the cipher. DNA computing can be applied in various forms during the encryption-decryption process; it can either be used as complement operation, digital coding, polymerase chain reaction, or as a security alternative [10]. A large volume of published studies describes the role of DNA in cryptography. This research focuses on DNA digital coding only with detailed insight into its security impact in cryptographic techniques. In 2012, Noorul Hussain [9] introduced a new concept based on DNA digital coding, where a dynamic DNA encoding table was presented. This encoding table is a 24∗4 matrix of 96 American Standard Code for Information Interchange (ASCII) characters consisting of alphabets, numbers, and special characters. Later this table was used and extended by other researchers [11]-[13]. It is evident that the utilization of this table in an algorithm has improved the randomness of ciphertext and consequently enhanced the system security.

An extended version of the ASCII table was introduced with 256 ASCII character encoding [11]. For a dynamic sequence, table creation, all characters are initially allocated randomly to DNA base sequences followed by an iterative rearrangement using a mathematical pattern, whereas in the encryption process, the plaintext is first converted into DNA bases using the sequence table, followed by the creation of data chunks to encrypt them using an asymmetric cryptosystem and finally to merge the chunks as the ciphertext. The system of dynamic encoding coupled with asymmetric cryptosystem naturally raises the degree of data confidentiality. It is proved by comparison with existing techniques and a statistical suit of randomness defined by the National Institute of Standards and Technology (NIST).

In [12], a network traffic and intrusion detection system is proposed using DNA sequences, where DNA bases are used to encode the 41 attributes of the network. The next attributes have been analyzed for experimentation purposes, and the results indicate a 15% improvement in accuracy, whereby a more complex encoding can effectively improve the accuracy of the intrusion detection system. In [13] and [14], a Dynamic DNA sequence table is used in combination with OTP to improve data security. The attacker must execute all possible DNA sequence variations before getting original data, which is supposed to be very difficult. The proposed technique provides better security than other techniques, in particular against brute force attacks. The algorithm aims to transmit the One-time-pad (OTP) securely, but execution time has been increased as compared to other similar techniques.

Interestingly a cryptographic system is designed, where the authors in [8] apply a delayed Hopfield neural network to generate the cryptographic key before DNA encryption-decryption process. Specifically, the chaotic neural network generates a binary sequence, passed on to the permutation function yielding the first level key for encryption. The system's strength lies in the random selection of trajectories for neural networks, delay function, and DNA cryptography. The authors claim that changing one byte can change 32 out of 128 bits in the ciphertext, which is significantly less than the expected change, where changing one bit in plaintext or key should bring more than 50% change in the ciphertext.

All these research works endorse the fact that DNA encryption using DNA encoding can significantly improve the security of the cryptographic solution. A similar approach in [8] is extended with the existing DNA encoding table at a carefully selected location. The subsequent section explains the encryption process for the base technique followed by the improved technique with an additional layer of the dynamic sequence table.

III. Methodology

A. Base Technique

The Hybrid chaotic neural network as in [8] generates the key while the DNA cryptography algorithm encrypts/decrypts the original data. However, this paper only discusses the application of DNA cryptography, so it primarily discusses encryption/decryption without going into details of the key generation process. Plaintext, key, and ciphertext are of equal length, i.e., 128 bits. Following are the steps involved in the encryption process:

1) Take plaintext from the user and divide it into fixed-length sub-sequences R_j.

2) A random binary sequence S_j of equal length is produced using a key generation.

3) R_j is permuted using left cyclic shift yielding R_j' where the number of bits to be shifted V_j is pre-calculated by key generation part.

4) S_j is subjected to right cyclic shift producing S_j' using V_j.

5) To produce the 1st level encrypted text C_j'', an XOR operation is performed between R_j' and S_j', as given below:

$$C_j'' = R_j' \oplus S_j'$$

6) The second level of encryption is performed on binaries obtained from $C_{j'}$. Applying "00" to "A", "01" to "G", "10" to "C", and "11" to "T", yielding C_j is the DNA encoded ciphertext.

The decryption process is the reverse of the encryption process where DNA decoding produces D_j' and thus D_j'' as below:

$$D_j'' = D_j' \oplus S_j'$$

This D_j'' undergoes permutation and cyclic shift to give the plaintext.

B. Proposed Technique

The proposed algorithm works the same way as far as the key generation is concerned in [8], but there is an improvement for encryption and decryption part as in Fig.1.

1) The user enters the plaintext, which goes directly to the DNA sequence table and gets encoded.

2) Then binary coding is applied as $A = 00$, $T = 01$, $C = 10$, and $G = 11$.

3) Conversion into corresponding decimal values.

4) Conversion of decimal values into ASCII characters.

5) Split each string into equal size blocks R_j.

The encryption process continues as the same steps, 3-6 in the base technique. Fig. 1 gives a pictorial representation of the system for the encryption-decryption process. The encryption process is illustrated in green, the key generation process in yellow, and the decryption process is in blue. These steps are similar to the original algorithm, and the improvements are added as new layers (in red) and displayed distinctively in the encryption and decryption process. Table I indicates the DNA encoding/decoding table being introduced to the algorithm as applied in [9].

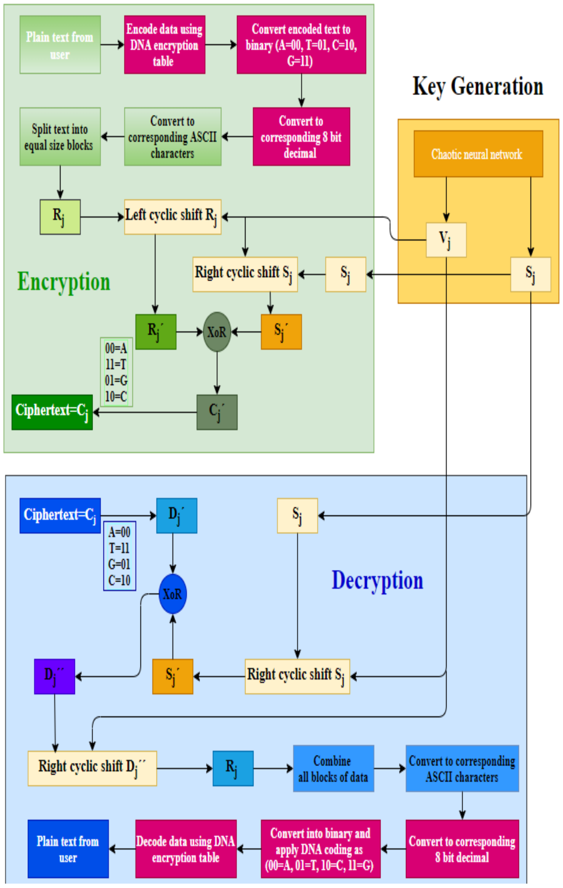
Plain text from user
Encode data using DNA encryption table
Convert encoded text to binary (A=00, T=01, C=10, G=11)
Key Generation
Split text into equal size blocks
Convert to corresponding ASCII characters
Convert to corresponding 8 bit decimal
Chaotic neural network
R_j
Left cyclic shift R_j
V_j
Encryption
Right cyclic shift S_j
S_j
S_j
R_j'
XoR
S_j'
00=A
11=T
01=G
10=C
Ciphertext=C_j
C_j'
Ciphertext=C_j
D_j'
S_j
A=00
T=11
G=01
C=10
XoR
Decryption
D_j''
S_j'
Right cyclic shift S_j
Right cyclic shift D_j''
R_j
Combine all blocks of data
Convert to corresponding ASCII characters
Plain text from user
Decode data using DNA encryption table
Convert into binary and apply DNA coding as (00=A, 01=T, 10=C, 11=G)
Convert to corresponding 8 bit decimal

Fig. 1. The Proposed Technique with Detailed Encryption and Decryption

TABLE I. DNA ENCODING/DECODING TABLE [9]

DNA Base Sequence				
ACAT-a	ACTC– q	CAAT– G	ATAA– W	ATTA- ,
ACTG- b	ACCG– r	CATG– H	ATTT– X	ATCC- .
ACCC- c	TCTC– s	CACG– I	ATCG– Y	TTTA- ?
ACGA– d	TCCC– t	CAGT– J	ATGC– Z	TTCG- /
TCAT– e	CCTT– u	GAAG- K	TTAA– 0	CTTC- :
TCTG– f	CCCC– v	GATA– L	TTTT– 1	CTCG- ;
TCCG– g	GCTA– w	GACG– M	TTCC– 2	GTTC– "
TCGT– h	GCCC– x	GAGG– N	TTGG- 3	GTCC– '
CCAG– i	AAAA– y	AATA– O	CTAT– 4	AGAG- {
CCTA– j	AATT– z	AACG– P	CTTG– 5	AGTA– [
CCCG– k	AACC–A	TATC– Q	CTCC– 6	AGCG- }
CCGG– l	AAGG- B	TACG– R	CTGA– 7	AGGG-]
GCAA– m	TAAT– C	CATC– S	GTAT– 8	TGAA- |
GCTT– n	TATG– D	CACC– T	GTTG– 9	TGTT- \
GCCG– o	TACC– E	GATT– U	GTCG– <	TGCG- +
GCGC– p	TAGA– F	GACC– V	GTGT- >	TGGC- =
CGAA--	CGCC-)	GGAT- ∗	GGCC- ∧	AGTT- $
CGTT-–	CGGG– (	GGTG- &	GGGA-%	AGCC- #
TGTA -@	TGCC- ¡	CGTA- ˜	CGCG- ‘	GGCG- £

IV. EVALUATION PARAMETERS

In this section, several tests from the literature are performed to evaluate the randomness of the ciphertext produced by the proposed algorithm and the base technique [5], [7], [15]-[17]. These tests can only be performed on binary sequences. Thus, the ciphertext is then converted from DNA sequence into binary to complete the evaluation. Three different datasets have been used as inputs to these tests, categorizing them as low density, high density, and random [18]-[20]. Low and high density are the biased datasets, where plaintext has all zeros and only one 1 bit in string. A high density is an exact opposite with all ones but only 1 zero. The purpose of using biased data is to identify the exact randomness in the ciphertext. For an algorithm being provided with random plaintexts, there are high chances that the generated ciphertext will also be random. On the other hand, for a non-random (biased) dataset, the probability of obtaining a random ciphertext is relatively low. Therefore, the use of different categories of datasets can establish confidence in the improved scheme from security perspectives.

A. Frequency (Mono Bit) Test

The frequency test calculates the number of a binary string, 0's and 1's appear in the ciphertext. This test determines that either the number of zeros and ones are equal or not, as this is one of the desired properties of a ciphertext [5]. Value 0.01 is the level of significance for this test which means that only 1 sample out of 100 will be rejected. Ideally, the resultant value should be "1", which means a perfect balance of 0 and 1 in the string. This test assesses the closeness of these values to 1/2 of the total numbers of binary string appeared in the ciphertext, as it is ideal for these values to be equal. For this test, the preliminaries are:

n the length of the bit string,

ε the sequence of bits in the string as $\varepsilon = \varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n$

S_{obs} the absolute value for summation of X_i.

$$X_i = 2\text{ε} - 1 = \pm 1 \tag{1}$$

$$S_n = X_1 + X_2 + \cdots \ldots + X_n \tag{2}$$

$$S_{obs} = \frac{|S_n|}{\sqrt{n}} \tag{3}$$

Finally, the tail probability, i.e., the p-value, is calculated in (4).

$$\text{p-value} = \operatorname{erfc}\left(\frac{S_{obs}}{\sqrt{2}}\right) \tag{4}$$

erfc is a complementary error function. This test evaluates the p-value, whereas if the computed value of p is less than 0.01, it is concluded that the given sequence is not random [15], [16]. On the other hand, if the p-value is more than 0.01, the string passed the test and can be declared as a random string.

B. Avalanche Effect

A small change in plain text or key yielding a significant change in the ciphertext is called the avalanche effect (5). It's a highly desirable property for algorithm design, such as the higher the avalanche effect, the better the algorithm [21]-[27].

Avalanche > 50% of an exemplary algorithm makes the cipher more random and less predictable for attackers.

$$\text{Avalanche Effect} = \frac{\text{Number of flipped bits in cipher text}}{\text{Total number of bits in cipher text}} \tag{5}$$

C. Entropy

Shannon introduced the concept of entropy in bits in 1948 [7] and is termed as uncertainty in the expected output bits. Uncertainty of the cipher is determined by the number of plaintext bits that can be recovered from scrambled ciphertext to get the original message [17] successfully. Moreover, entropy is the weighted average of optimal bit representation size, such as the average size of an encoded message. Mathematically, entropy can be defined as in (6).

$$H(X) = -\sum_{x\in X}(\Pr[X]log_2(\Pr[X])) \tag{6}$$

Here we are calculating the entropy of X with $X = \{0,1\}$. Calculating for both bases as in (7).

$$H(X) = -\left[P(0)log_2\big(P(0)\big) + P(1)log_2\big(P(1)\big)\right] \tag{7}$$

The highest uncertainty is only achieved when the values are equally distributed i.e.

$$H(X) = 1 \tag{8}$$

D. Hamming Weight

Two strings of equal length having different symbols at some positions; the total number of those positions is called hamming weight [21], [26]. A higher value of the hamming weight represents the better randomness of the binary sequence.

$$Hamming\ Weight = \frac{Total\ number\ of\ non\ zero\ bits}{Length\ of\ the\ cipher\ text} \tag{9}$$

V. Result and Discussion

Both techniques discussed in previous sections are implemented in Matlab 2019 to evaluate the randomness of the ciphertext. Tables II and III have results for all of the tests described in Section IV. The value of plaintext is changed by toggling bits across the string followed by a constant key. The plaintexts in Table II are 128 bits long. The key is set to "0001100010010101001001000010101110000110101001000110 001100001111110001101011000101111011110010010011111100 110110000011111100110010". The same key is used to produce the ciphertext for further evaluations. As the frequency is one of the tests by NIST [28] and the minimum required length of the string is 100 bits, the ciphertext bits are concatenated to apply this test. Here, we have 33 high density, 33 low density, and 34 random plain texts for evaluation, and, ultimately, the average value of all these observations is calculated.

A. Frequency Test

As mentioned in the previous section, the frequency test calculates the number of 0's and 1's that appear in the ciphertext. If the p-value calculated on the ciphertext is more than 0.01, the ciphertext is concluded as a random string, or else it is a non-random. Thus, Table II shows the p-value of the ciphertext produced by the base and the improved algorithm using (1), (2), (3), and (4). High density, low density, and random plaintexts are used as inputs to both algorithms.

TABLE II. Frequency Analysis, Avalanche effect and Hamming Weight Test for the base and the Improved Technique

Plaintext	Frequency Test		Avalanche Effect		Hamming Weight	
	Base	Improved	Base	Improved	Base	Improved
High density	0.8227	0.9872	38.06 %	52.9 %	62.3	63.5
Low density	0.8953	0.987	40.6 %	55.33 %	63.9	64.2
Random	0.7625	0.9891	37.99%	55.7%	63.5	63.9
Average	**0.8268**	**0.9877**	**38.55%**	**54.64%**	**63.23**	**63.87**

Based on Table II, both techniques have passed the NIST frequency test successfully with the average p-values (y-axis) for three variants of plaintexts are greater than 0.01. Each p-value (y-axis) of the ciphertext generated from those variants of plaintexts is also depicted in Fig. 2 and 3. The ideal p-value for this test is 1, and all the ciphertexts should have a value close to 1. Based on Fig. 2 and 3, it can be seen that there are specific outputs that have successfully achieved a p-value of 1. However, this ratio is minimal in case of the base technique compared to the improved technique. It can be seen from Table II that the average p-value of the improved technique (0.9877) is very close to 1.

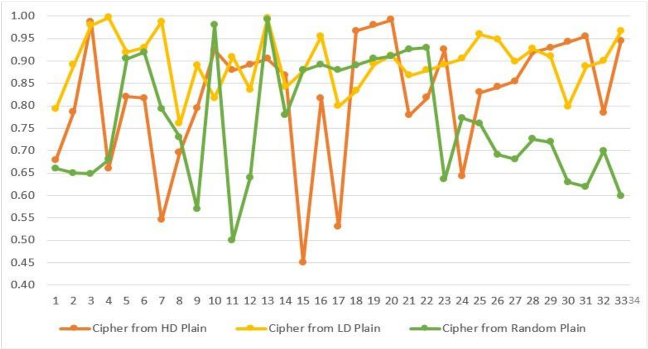

Fig. 2. Frequency Analysis of base Technique.

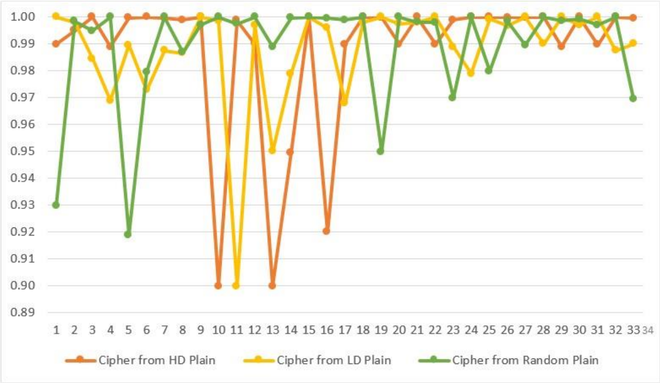

Fig. 3. Frequency Analysis of Improved Technique.

B. Avalanche Effect

The avalanche effect is a very desirable property when it comes to randomness in the ciphertext. As mentioned earlier, the higher the avalanche effect, the better the security. Any given scenario where the attacker has access to ciphertext tries to establish a relationship between ciphertext and its plaintext.

If changing one bit results in a change of more than 50% bits, it becomes challenging for the attacker to retrieve the original message. In Table II, the base technique has the avalanche effect values, which range from 37.99% for random to 38.06% and 40.6% for high and low density plaintext, respectively. Meanwhile, the improved technique has values ranging from 52.9% to 55.7%, significantly higher than the base technique.

These values are calculated using (5) and presented in Fig. 4 and 5. As depicted in Fig. 4, changing 1 bit in plaintext has generally introduced a difference from 8% to 65%. Whereas by looking at Fig. 5, it is evident that observed values range between 40% and 70%. Row 5 in Table II has the average value of avalanche effect, and it can be observed that this value is 38.55% in the case of the base technique and has significantly improved to 54.64% for the improved technique.

Example scenarios of avalance effect have been presented in Table III, where "CRYPTOGRAMMATIST" is the original plaintext, feed to the algorithm and the produced ciphertext is used as a reference to calculate the number of flipped bits. For example, changing one bit in the 40th location of the binary sequence in the plaintext yields 24 flipped bits in the ciphertext by the base technique. Thus, the avalanche effect is 18.755%, considering that the length of ciphertext is 128 bits. For the base algorithm, the result shows that the avalanche effects range from 12.5% to 32.0312%, with an average of 19.72% when changing one bit of the binary sequence in the plaintext at different locations (bold and underlined bit). Meanwhile, the improved technique has the avalanche effects range from 53.9% to 61.75%, with an average of 57.4175%. The average avalanche effect indicates a significant improvement of 37.69%. Thus, this new encryption/decryption technique can be used to improve security for an environment in which data sensitivity and randomness are essential.

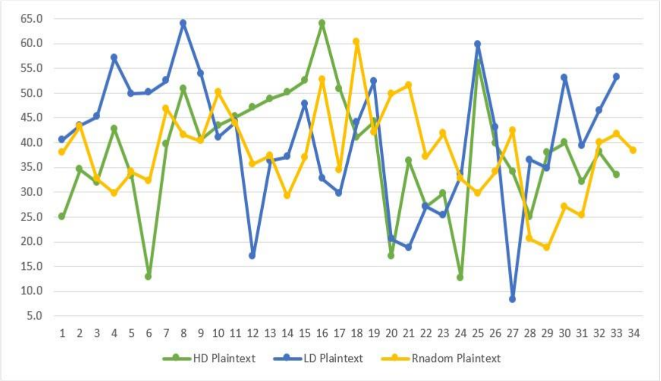

Fig. 4. Avalanche Effect of base Technique.

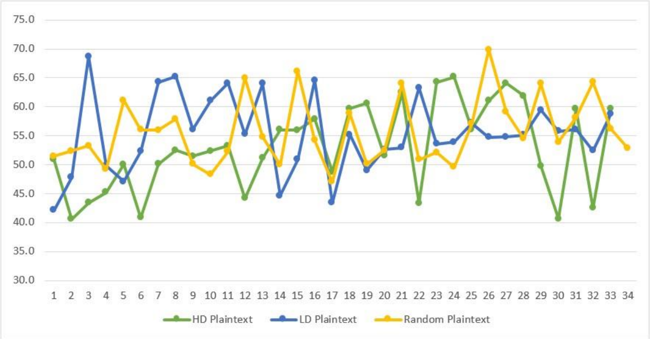

Fig. 5. Avalanche Effect of Improved Technique.

TABLE III. AVALANCHE EFFECT AND ENTRPOY FOR THE BASE AND IMPROVED TECHNIQUE

Plaintext	**Base Technique**			**Improved Technique**		
	Ciphertext	Avalanche effect	Entropy $H(X)$	Ciphertext	Avalanche effect	Entropy $H(X)$
CRYPTOGRAMMATIST	11001111001001101110011001101000 100011111000000001110101110111111 11010101111011111101100110000001 01000011010010011111010111100100	———	0.9914	00101100101001010100101011100001 00111011000010100110010111110000 00110100101111111110011011011111 11000110000101000101111010110110	———	0.9984
CRYP**<u>U</u>**OGRAMMATIST	11001111001001101110011001101000 100011111000000001110101110111111 11010101111011111100011001101010 0 00010110000011100101000001011000 1	24/128= 18.755%	0.9984	00101100100011111010010000001110 11000000101000011000101101011010 10001111000100000101110101110001 01010011010000001000000000101110 0	79/128 = 61.72%	0.9745
CRYPTO**<u>F</u>**RAMMATIST	11001111001001101110011001101000 100011111000000011011111011101010 10000000101110101000110011010100 00010110000011100101000001011000 1	41/128= 32.0312%	0.9972	10110011000100101010010000001011 11101100001101001111000000001101 01100001111010101001111011011111 11000011111010111111010101011101	78/128 = 60.93%	0.9956
CRYPTO**<u>E</u>**RAMMATIST	11001111001001101110011001101000 100011111000000001110101110111111 11010101111011111101100110000001 01000011010000100000101101011010	16/128= 12.50 %	0.9984	10110110010001111111000101011110 10111011110111110000101110100110 10001111000100000001100010111000 1 01111001000101000101111011100010	69/128 = 53.9%	0.9972
CRYPTOGRA**<u>L</u>**MATIST	11001111001001101110011001101000 100011111000000001110101110111111 11010101111011111101100110000001 01000011101100100000101101011010	20/128= 15.625%	0.9956	00100011000110101111000101011011 11000000101000011000101101010101 01100001111011111110011011011010 10010011010000001000010111110001 1	68/128 =53.12%	0.9998
Average	------	*19.72%*	*0.9963*	--------	*57.4175%*	*0.9931*

C. Entropy

Equation (6) and (7) are applied to find the entropy of ciphertext. In Table III, the entropy of the ciphertext has been calculated for the base and the proposed technique. It can be seen that the entropy of ciphertext in both cases is nearly equal, with a value of 0.9963 for the base technique and 0.9931 for the proposed technique, which is the information content per bit. So it can be said that the information content per bit has not decreased even for the improved technique but has sustained some optimum value throughout the observations. The ideal entropy in the given case is 1, as depicted in (8), but the observed entropy for both techniques is very close to one.

D. Hamming Weight

Hamming weight has been calculated using (9). In Table II, it is observed that hamming weight for base technique ranges from 62.3 to 63.9, whereas for improved technique, this value ranges from 63.5 to 64. The ideal expected value for hamming weight in a binary string of 128 bits should be 64. The average observed value of 100 plain texts for the base technique is 63.23, whereas, for the improved technique, it's 63.87.

In summary, Tables II and III confirm that the proposed technique performs better for frequency, avalanche effect, and hamming weight. The observed values are not only better than the base technique but are also nearly equal to ideal expected values. Whereas for entropy calculation, the value of the improved technique has not improved yet, the difference from the base technique is quite negligible. Hence, the improved technique is a better alternative to the proposed technique, where enhanced security is offered with all the security considerations of the base technique.

VI. Conclusion

DNA cryptography has served as a better alternative to traditional systems in recent times. Advancement in the study helps to identify the security vulnerabilities in the existing systems. This research highlights that by carefully examining the ciphertext produced by the base technique, in terms of avalanche effect can be further improved. The average avalanche effect is 38.55% when flipping one bit of binary sequence in the plaintext for 100 different plaintexts ranging from high density, low density, and random data set. On the other hand, the average avalanche effect of the proposed technique has increased to 54.64% by introducing a DNA encoding table. The work also includes the frequency, entropy, and hamming weight to test the overall security of the improved system. The results show that the improved technique is better in terms of the frequency's p-value, avalanche effect, and hamming distance than the base technique. For entropy, the value produced by both algorithms is approximately equal. Hence, the improved technique is a better alternative to the proposed technique, and this research. A good future direction of this work can be defining new trajectories in key schedules and analyzing the impact of key changes to the ciphertext.

Acknowledgment

The authors would like to thank all reviewers for their helpful comments. The authors would also like to thank the Ministry of Higher Education Malaysia for supporting the research under Fundamental Research Grant Scheme Vot No. FRGS/1/2019/ICT03/UTHM/03/1 and partially sponsored by Universiti Tun Hussein Onn Malaysia.

References

[1] X. Zhang, Z. Zhou, and Y. Niu, "An image encryption method based on the feistel network and dynamic DNA encoding," IEEE Photonics Journal, vol. 10, no. 4, pp. 1-14, 2018.

[2] S. Sadeg, M. Gougache, N. Mansouri, and H. Drias, "An encryption algorithm inspired from DNA," in 2010 International Conference on Machine and Web Intelligence, 2010, pp. 344-349: IEEE.

[3] H. M. Bahig and D. I. Nassr, "DNA-based AES with silent mutations," Arabian Journal for Science and Engineering, vol. 44, no. 4, pp. 3389-3403, 2019.

[4] B. M. Kumar, B. R. S. Sri, G. Katamaraju, P. Rani, N. Harinadh, and C. Saibabu, "File Encryption and Decryption Using DNA Technology," in 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), 2020, pp. 382-385: IEEE.

[5] Y. Zhang, "The image encryption algorithm based on chaos and DNA computing," Multimedia Tools and Applications, vol. 77, no. 16, pp. 21589-21615, 2018.

[6] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-allen and hamilton inc mclean va2001.

[7] C. E. Shannon, "A mathematical theory of communication," The Bell system technical journal, vol. 27, no. 3, pp. 379-423, 1948.

[8] S. S. Roy, S. A. Shahriyar, M. Asaf-Uddowla, K. M. R. Alam, and Y. Morimoto, "A novel encryption model for text messages using delayed chaotic neural network and DNA cryptography," in 2017 20th International Conference of Computer and Information Technology (ICCIT), 2017, pp. 1-6: IEEE.

[9] N. H. UbaidurRahman, C. Balamurugan, and R. Mariappan, "A novel DNA computing based encryption and decryption algorithm," Procedia Computer Science, vol. 46, pp. 463-475, 2015.

[10] Y. Niu, K. Zhao, X. Zhang, and G. Cui, "Review on DNA Cryptography," in International Conference on Bio-Inspired Computing: Theories and Applications, 2019, pp. 134-148: Springer.

[11] M. R. Biswas, K. M. R. Alam, S. Tamura, and Y. Morimoto, "A technique for DNA cryptography based on dynamic mechanisms," Journal of Information Security and Applications, vol. 48, p. 102363, 2019.

[12] F. E. Ibrahim, H. Abdalkader, and M. Moussa, "Enhancing the security of data hiding using double DNA sequences," in Industry Academia Collaboration Conference (IAC), 2015, pp. 6-8.

[13] A. Hazra, C. Lenka, A. Jha, and M. Younus, "A Novel Two Layer Encryption Algorithm Using One-Time Pad and DNA Cryptography," in Innovations in Computer Science and Engineering: Springer, Singapore, 2020, pp. 297-309.

[14] M. R. Biswas, K. M. R. Alam, A. Akber, and Y. Morimoto, "A DNA cryptographic technique based on dynamic DNA encoding and asymmetric cryptosystem," in 2017 4th International Conference on Networking, Systems and Security (NSysS), 2017, pp. 1-8: IEEE.

[15] A. S. Al-Wattar, R. Mahmod, Z. A. Zukarnain, and N. I. Udzir, "Generating a new S-Box inspired by biological DNA," International Journal of Computer Science and Application, vol. 4, no. 1, pp. 32-42, 2015.

[16] D. A. Zebari, H. Haron, S. R. Zeebaree, and D. Q. Zeebaree, "Multi-Level of DNA Encryption Technique Based on DNA Arithmetic and Biological Operations," in 2018 International Conference on Advanced Science and Engineering (ICOASE), 2018, pp. 312-317: IEEE.

[17] G. Ye, C. Pan, X. Huang, Z. Zhao, and J. He, "A chaotic image encryption algorithm based on information entropy," International Journal of Bifurcation and Chaos, vol. 28, no. 01, p. 1850010, 2018.

[18] H. Othman, Y. Hassoun, and M. Owayjan, "Entropy model for symmetric key cryptography algorithms based on numerical methods,"

in 2015 International Conference on Applied Research in Computer Science and Engineering (ICAR), 2015, pp. 1-2: IEEE.

[19] H. Shi, Y. Deng, and Y. Guan, "Analysis of the avalanche effect of the AES S box," in 2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), 2011, pp. 5425-5428: IEEE.

[20] C. P. Dewangan, S. Agrawal, A. K. Mandal, and A. Tiwari, "Study of avalanche effect in AES using binary codes," in 2012 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), 2012, pp. 183-187: IEEE.

[21] H. Agrawal and M. Sharma, "Implementation and analysis of various symmetric cryptosystems," Indian Journal of science and Technology, vol. 3, no. 12, pp. 1173-1176, 2010.

[22] S. Ramanujam and M. Karuppiah, "Designing an algorithm with high Avalanche Effect," IJCSNS International Journal of Computer Science and Network Security, vol. 11, no. 1, pp. 106-111, 2011.

[23] S. Vyakaranal and S. Kengond, "Performance analysis of symmetric key cryptographic algorithms," in 2018 International Conference on Communication and Signal Processing (ICCSP), 2018, pp. 0411-0415: IEEE.

[24] K. D. Muthavhine and M. Sumbwanyambe, "An analysis and a comparative study of cryptographic algorithms used on the Internet of Things (IoT) based on avalanche effect," in 2018 International Conference on Information and Communications Technology (ICOIACT), 2018, pp. 114-119: IEEE.

[25] S. T. Nadu, "A block cipher algorithm to enhance the avalanche effect using dynamic key-dependent S-box and genetic operations," International Journal of Pure and Applied Mathematics, vol. 119, no. 10, pp. 399-418, 2018.

[26] X. Chai, Z. Gan, Y. Lu, Y. Chen, and D. Han, "A novel image encryption algorithm based on the chaotic system and DNA computing," International Journal of Modern Physics C, vol. 28, no. 05, p. 1750069, 2017.

[27] M. Imdad, S. N. Ramli, H. Mahdin, B. U. Mouni, and S. Sahar, "An Enhanced DNA Sequence Table for Improved Security and Reduced Computational Complexity of DNA Cryptography," in EAI International Conference on Body Area Networks, 2020, pp. 106-120: Springer.

[28] A. Sharaieh, A. Edinat, and S. AlFarraji, "An enhanced polyalphabetic algorithm on vigenerecipher with DNA-based cryptography," in 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), 2018, pp. 1-6: IEEE.