A Survey On Dna Cryptographic Techniques, Challenges And Future Trends

Nidal M. Turab[1] , Mwaffaq Abu-Alhaija[2] , Hamza Abu Owida[3] , Jamal I. Al-Nabulsi[4]

[1]Department of Networks and Information Security, Faculty of Information Technology, Al-Ahliyya Amman University. Amman, Jordan.

[2]Department of Networks and Information Security, Faculty of Information Technology, Al-Ahliyya Amman University. Amman, Jordan.

[3]Medical Engineering Department, Faculty of Engineering Al-Ahliyya Amman University, Amman, Jordan.

[4]Medical Engineering Department, Faculty of Engineering Al-Ahliyya Amman University, Amman, Jordan.

Received March 25, 2022; Accepted March,30, 2022
ISSN: 1735-188X

Abstract

DNA Cryptography is one of the speedily growing technologies in the world as unbreakable algorithms, as well as to design and implement more complex and resistant to differential attack crypto algorithms. DNA computing had more speed, minimal required storage, and lower power consumption. DNA cryptography participates well-known cryptographic techniques and the characteristics of DNA. Nowadays, there exist several DNA cryptosystems proposed either as an algorithmic approaches or as an integral part of data secrecy applications. Algorithmic approaches were studied by very few researches that integrate both biological and arithmetic operations to gratify the necessity of system optimality. In addition, DNA cryptosystems provide layered security in applications besides other traditional cryptographic algorithms. This study provides a review of DNA cryptographic techniques and algorithm approaches proposed by recent researchers. This study aims to provide a review of DNA cryptographic techniques, algorithms, and approaches proposed by recent researchers, it aims also used to classify which approaches fulfil most of the evaluation parameters, and which is a lightweight cryptography. Most recent publications on DNA cryptographic approaches were reviewed from 2018 to 2022; using a keyword such as “DNA LWC”, “DNA Encryption” among different scientific databases. The findings of this study showed that most articles on DNA cryptography techniques neither provide complete security analysis nor built on mathematical methods. The researchers mostly demonstrated the proposed system model and tested the approaches using computer simulations. Nonetheless, no DNA computation implantations of the surveyed techniques were carried out. This study will assist researches as a reference for researches in future.

Keywords

DNA cryptography; DNA-based Cryptographic system; Lightweight Cryptography (LWC); DNA computing; steganography.

Introduction

The large spread of wireless devices connected to the Internet and cloud, besides the rapid advances in the new emerging Internet of Things (IoT), gain increasingly attention of researchers in different domains.

IoT consists of objects or sensors used to control many larger entities, generate and transfer data to/from other devices and systems over the Internet or other through wireless networks (Wortmann & Flüchter, 2015). The expectation of cloud computing is to grow from USD 80 billion dollars in 2016 to 320 billion dollars in 2030 (Abu-Alhaija, Turab, & Hamza, 2022; Intelligence, 2020), while IoT growth is to reach 24.1 billion in 2030.

IoT heterogeneous devices and applications generate large amounts of data that need to be secured. The main challenge is the constrained resources of IoT devices. The fact that more security requires more resources and processing power is a pivotal challenge for IoT devices and applications (Li, Song, & Iqbal, 2019; Turab & Kharma, 2019). Hence, securing IoT devices leads to the emersion Lightweight Cryptography (LWC) algorithm within the research community.

LWC families are encryption methods that assembly with low computational complexity. With the intention to enable devices with constrained resources to encrypt data. The National Institute of Standards and Technology (NIST) initiated LWC, where the performance of current NIST cryptographic standards is not acceptable for resource constrained devices (Toshihiko, 2017). A variety of LWCs had been invented; they should have relatively small key size, data block size, minimum power consumption, small number of rounds, and simple key generation, but still with acceptable strong security structure and good immunity to security attacks (Thakor, Razzaque, & Khandaker, 2021)Some of the approved LWCs by NIST are: Camellia, TWINE, Trivium, PRESENT, PICALO, LEX, CLEFIA SIMON and SPECK (Turab & Kharma, 2019).

Recent researches adopted deoxyribonucleic acid DNA computing to satisfy the need for sufficient and robust data confidentiality. Molecular biology, hardware, and biochemistry are used in DNA computing rather than electronic chip electronic computing. Instead of the binary digits 1 and 0 currently used by traditional computers, DNA computing represents data using four nitrogen bases that encode the genetic information, namely: A for Adenine, G for Guanine , C for Cytosine, and T for Thymine(Adleman, 1994). The ability to create short sequences of artificial DNA that used for encryption algorithm inputs. Due to the fact that one gram of DNA can store up to 108 terabytes of data leading to the probable field of enormous one-time pads and introducing new cryptographic methods(Gehani, LaBean, & Reif, 2003). Figure1 shows the DNA structure with a description of the main components (Ivanchuk, 2019).

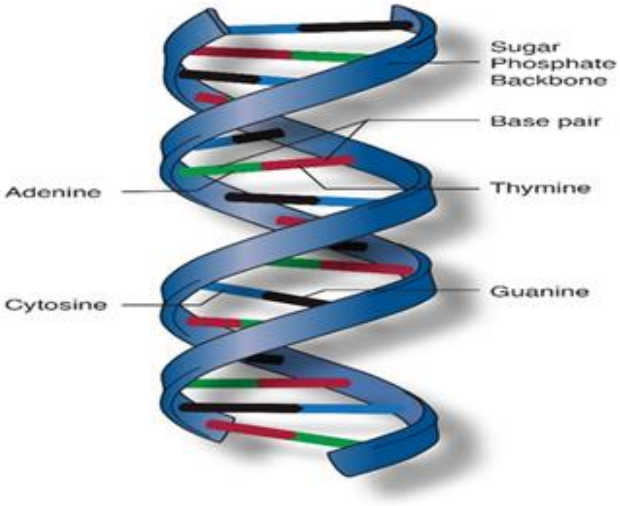

Figure 1: DNA structure

Therefore, in recent years, the area of DNA research is attracting increased attention from the research community. The main focus of this review paper is DNA cryptography; from the algorithms used, to the various parameters used to evaluate the proposed algorithm performance such as: correlation, entropy, Peak Signal -to-Noise Ratio (PSNR), Unified Averaged Changing Intensity (UACI) and finally the Number of Pixels Change Rate (NPCR).

The histogram of the image can be used to determine the entropy (Thum, 1984). The histogram is an indicator of possible grey levels in the image, with a typical value of eight.

The correlation indicates the relationship between two adjacent pixels (horizontal, vertical, and diagonal); the smaller values of correlation coefficients, the greater attack resistance (Akiwate, 2021).

The PSNR (dB) measures the ratio of peak power in the encrypted image with respect to that of the original image.

The cipher immunity against differential attacks is measured by both NPCR and UACI. The NPCR and UACI evaluate the number of changed pixels between the original and encrypted images, respectively. Whenever there is a single bit change between plaintext images, their values are in the range (0-1) and usually given as percentages (Wu, Noonan, & Agaian, 2011).

This study aims to provide a review of DNA cryptographic techniques, algorithms, and approaches proposed by recent researchers. Three research questions were framed in this study; these are:

1. What are the encryption algorithms used in DNA encryption approaches?
2. Which algorithm fulfils the most of the evaluation parameters?
3. Which algorithm is LWC algorithm?

To answer the aforementioned questions, 35 publications on DNA cryptographic approaches were reviewed from 2018 to 2022; using a keyword such as “DNA LWC”, “DNA Encryption” among different scientific databases such as Google Scholar and Scopus.

DNA BASED CRYPTOGRAPHY TRENDS

Some research work is being done on DNA Computing either using biological test tubes, but the majority of researches are computer simulations of the operations of DNA (Jacob, 2013). In this section, we will review the latest researches from a different perspectives and then we will compare their obtained results.

Basam and his team (Al-Shargabi & Al-Husainy, 2020) proposed a new symmetric block cipher DNA-based encryption technique, and they utilized the DNA sequence to generate a random and strong secret key, which is rigid to be broken by attackers. The generated DNA key is used to encrypt the source images. Their proposed algorithm is composed of substitution and transposition operations. They evaluated the effectiveness of their proposed DNA based encryption algorithm from encryption time, key size, and proportion of alterations prospective compared with two traditional encryption algorithms, namely: DES and AES. Their algorithm showed that the less the encryption time of the two algorithms they compared with. The PSNR was 8.687 dB compared to AES and DES algorithms. While the encryption time was about 125 ms.

Liu and his colleagues (M. Liu & Ye, 2021) proposed a symmetrical DNA based encryption that combines the Rivest-Shamir-Adleman (RSA) algorithm and DNA coding, RSDA generates the initial values of the hyperchaotic system. Then, they performed permutation at pixel level to attain message confusion according to the generated chaotic sequences. Finally, dynamical DNA encryption is used. Their experimental results showed that for 512*512 image, entropy was 7.994 while the correlations between adjacent V, H, and D pixels were -0.0014, -0.0011 and 0.0043; while the NPCR and UACI were 99.6136% and 33.4665% respectively.

For IoT devices with constrained resources, R. Al-Dwairi (Al-Dwairi, 2021) proposed a LWC. DNA tapes with some logical operations were used to generate keys for multi encryption rounds. He compared the proposed algorithm with AES and 3DES. The calculated entropy was 7.99902; while the correlation coefficient and PSNR were 0.083 and 6.184 dB, respectively.

Uddin et al. (Uddin, Jahan, Islam, & Rakib Hassan, 2021) generated large key form short key DNA-based for image encryption. Their obtained results showed that the entropy was 7.9998949; while the correlation values were −0.00012 for H, V, and D. Their proposed method achieved PSNR of 88.5642 dB.

Liu and his team proposed a remote image sensing encryption method in (H. Liu, Zhao, & Huang, 2019). The proposed algorithm is based on DNA; initially, they encoded a plain image with DNA, the encrypted image undergoes through different stages: DNA addition with DNA mask (that was generated using 2-D logistic map), 2-D logistic map with DNA bases is executed to mitigate differential attacks. Pixel-level rearrangement is the final stage. Their experimental result showed that the algorithm had encryption speed 0.651308 Mbit/s, entropy of 7.997, and the correlation coefficients were 0.00297, 0.0025 and 0.0054 for H, V and D respectively. Their proposed method achieved NPCR and UACI of 99.6231% and 33.495%, respectively.

Based on the use of the DNA Chen’s hyper-chaotic map, a secure image encryption technique was proposed by Khamy and Mohamed (El-Khamy & Mohamed, 2021). Their proposed algorithm involved extracting basic DNA images A, C, G, and T from an original image. Hyper chaos sequence diffusion of DNA images were used. Their obtained experimental results showed that the correlation coefficients were 0.0012, 0.0025, and 0.0011for H, V, and D, respectively. The highest entropy achieved was 7.9995, while the PSNR was 26.5214 dB and the NPCR and UACI were 99.65%, 33.45%, respectively.

Alsaffar and colleagues (Alsaffar, Mohaisen, & Almashhdini, 2021) combined DNA and AES 256 algorithms to encrypt messages, they used GZIP compression to reduce the encrypted message length; their obtained PSNR was 67.86 dB. The NPCR and UACI were 98.29% and 34 %, respectively.

Hadi and colleagues (Hadi, Ali, & Jawad, 2021) proposed a multistage image encryption process. Initially, the image was divided into blocks of n×n pixels. Then the n x n blocks were encrypted using the anticipated key. They generated a mask encryption key using the quadratic chaotic system. Their calculated results showed that the entropy was 0.9998 and the correlation coefficient was −0.0010. The NPCR and UACI were approximately 50%.

An image cipher is presented by Gan et al. (Gan et al., 2021), where the original image is firstly processed by self-updating transformation based on dynamic image filtering (STDIF). Afterwards, they used a chaotic system to encrypt the plain image according to the DNA rules. They used the SHA-256 hash function to choose keystreams from the obtained chaotic sequences. Their simulated results showed that the entropy was 7.9969, PSNR was 34.8909 dB, and the correlation values were - 0.0014, - 0.0029, and 0.0015 for V, H and D respectively. The average values of NPCR and UACI were 99.606% and 33.39 %.

Alshammari et al (B. Alshammari, R. Guesmi, T. Guesmi, H. Alsaif, & A. Alzamil, 2021) proposed a lightweight cryptosystem dedicated for highly constrained IOT devices. The algorithm is based on Advanced Encryption Standard (AES) and chaotic S-box. Their simulation showed that the correlation values were - 0.0499, 0.0059, and 0.1754 for V, H, and D, respectively, and the entropy value of 7.9460.

Al-Husainy et al. (Al-Husainy, Al-Shargabi, & Aljawarneh, 2021) proposed a flexible lightweight encryption system with random encryption key for IoT devices. Their experiment obtained an entropy of 7.9460 and PSNR of 8.11 dB.

Peng et al. (Peng, Cui, & Song, 2021) proposed an algorithm that increased the key space using chaos map. Their algorithm was divided into two parts: data and parameter encryption algorithm, they obtained experimental entropy of 7.9376 and 90.15 %, 1.3% for NPCR and UACI, respectively.

AVG3 encrypting technique built on the consolidation of DNA encryption and Rubik’s cube was proposed by Kaushik et al.(Kaushik, Thada, & Singh, 2021). Their experimental simulations showed that the encryption time for the 512 * 512 images was 38.6 seconds and NPCR was approximately 99.6%.

Akiwate and Parthiban (Akiwate, 2021) proposed a Secure And Efficient Image Cryptography (SEIC) method using Chaos and DNA encoding. The experimental results showed that UACI and NPCR were 49.75% and 99.62%, respectively, with the correlation coefficients for H, V, and D were 0.000901, 0.004058 and 0.000790 respectively.

Sujarani et al. proposed (Sujarani, Manivannan, Manikandan, & Vidhyacharan, 2021) a lightweight bio-cryptosystem. They generated random key series by computing a 2D_Logistic Sine Map. Afterthought, they divided the images into odd and even images. Each image is confused using a different chaotic key. Then, they merged the resultant images. Finally, DNA encryption using random keys was applied to the resultant confused image. Their computed results showed that NPCR= 99.58%, UACI= 33.56%, entropy =7.9894, PSNR= 45.5446, and correlation =0.9985.

One-dimensional composite chaos, hyperchaos and DNA coding technologies were used by Yujie Wan and colleagues in (Wan, Gu, & Du, 2020).They used seven keys in their proposed algorithm, resulting in a key space of 2364. The key entropy was 0.0020; the correlation of the neighboring pixels in the encrypted image was 7.9971. The PSNR was 41.7268 dB; the UACI and NPCR were 33.5211% and 99.6130%

Image steganography scheme based on DNA and chaos based on random bit generation was proposed by Mondal in (Mondal, 2020). The proposed scheme used generated random DNA sequences from cross-coupled chaotic. The encoded message was shielded using Least Significant Bit (LSB) substitution method. The obtained results showed that the entropy was 7.5733, correlation= 0.0096, and PSNR = 99 dB.

In (Meftah, Pacha, & Hadj-Said, 2020), Meftah et al. adopted Huffman coding for a new symmetric DNA encryption. Huffman coding was used to extract the secondary key from the main key. Then diffusion with a permutation box was used. Their obtained results showed that the NPCR = 99.6032 %, UAIC = 33.607%, the Correlation coefficients for H, V, and D were - 0.0132, 0.0027 and -0.0083 respectively while the entropy was 7.9957.

Alshammari et al. (B. M. Alshammari, R. Guesmi, T. Guesmi, H. Alsaif, & A. Alzamil, 2021) proposed a LWC algorithm based on the standard AES chaotic Boolean functions based S-box and the Hilbert curve. Their calculated results showed that the entropy values of 7.9460 the correlation coefficients for D, H, and V were 0.1754, 0.0059 and −0.0499, respectively.

A LWV image encryption algorithm based on logistic tent map and crossover operator with a genetic algorithm proposed to generate the random key was proposed by Gupta et al. (Gupta et al., 2021). Their experimental results showed that Entropy was 7.9968, NPCR 99.60%, UACI 33.46, and correlation coefficients for H, V and D 0.0059, and 0.0061 and 0.0415 respectively.

Al-Shargabi and his colleagues (Al-Shargabi & Al-Husainy, 2022) proposed multi round encryption for COVID-19 data. They used DNA key multi round encryption, a random key is selected within each round based on DNA and mapping table to ensure a high level of confusion and diffusion. They obtained the following simulated values: 7.998982 entropy and 6.533 dB PSNR.

Ferdush and his team (Ferdush, Begum, & Uddin, 2021)proposed Chaotic LWC image encryption using Arnold map. They calculated the NPCR as 99.67%, UACI as 34.19%, PSNR as 7.5785 dB, 7.9851 entropy, and 0.9831, 0.9806 and 0.9685 correlation coefficients for H, V and D respectively.

Xie et al. (Xie, Zhang, Zhang, & Li, 2021) proposed a medical image encryption method based on hyperchaos and DNA encoding. Firstly, images can be extracted and some important pixels can be encrypted. Secondly, hyperchaotic sequences are used to reduce the pixel correlation. Thirdly, they use DNA encoding. The simulated results were 99.64%, 33.81% for NPCR and UACI, PSNR 30.62287 dB, entropy 7.99060, the correlation coefficients for H, V and D were 0.0241, -0.0365 and 0.0345 respectively.

Hasan et al. (Hasan et al., 2021)proposed an efficient LWC algorithm for secure healthcare applications. They calculated the PSNR of 27 dB and the entropy of 7.98.

Babaei and his colleagues proposed a cryptosystem based on DNA and RCA (Recursive Cellular Automata) in (Babaei, Motameni, & Enayatifar, 2020). The encryption composed of two stages: diffusion and permutation, they used the logistic map to generate random numbers to shift the pixel values. Their obtained results showed that the entropy value was 7.9994 while the correlation coefficients were -0.0014,-0.002and -0.0012 for H, V, and D, respectively. They obtained NPCR of 99.6143% and UACI of 33.4675 %.

Abed et al. (Abed & Boyaci, 2020) proposed a LWC algorithm for smart cities and IOT security with different key and block sizes and nine rounds. The proposed algorithm is a mixture of Feistel structure and Substitution-Permutation Network (SPN) structure. Their performed simulations showed that the correlation was 0.0001 and the entropy was 7.9976.

Athira and Basu propped (Athira & Basu, 2020) an image encryption technique that uses transform-based scrambling and DNA based multi-chaotic encoding structure. The proposed technique involved Arnold transformation and DNA encoding scheme. They obtained NPCR= 99.62% and UACI=29.48

Vidhya and Rathipriya (Vidhya & Rathipriya, 2020)used genetic operators and Diffie-Hellman key exchange algorithm for DNA cryptography. Their experimental setup showed that the entropy was 1.4.

Akkasaligar and Biradar proposed a medical image encryption using dual hyperchaos map and DNA sequencing in (Akkasaligar & Biradar, 2020). In the proposed method, the permutation and diffusion process are performed on selected pixels of digital images. Their simulated results obtained an NPCR near to 99.68% and the value of UACI is 33.55%, PSNR around 5.72 dB, and the entropy of 7.8466.

A modified version of AES (DNAES) was proposed by Bahig and Nassr (sBahig & Nassr, 2019). Their experiments showed that the average of the CPU time taken by DNAES encryption selected samples for text, video, images, data files were 2.37,98.93, and 187.23 seconds, respectively.

Dagadu and colleagues (Dagadu, Li, & Addo, 2019) proposed an image encryption scheme. Their proposed scheme consists of two main phases: permutation and diffusion. They found that the correlation coefficients were 0.86654, 0.75873, and 0.72618 for H, V, and D, respectively, with entropy of 7.35830 NPCR of 99.6%, UACI of 33.489% and PSNR of 35.1889 dB.

Singh and Mahajan (Singh & Mahajan) proposed DNA based elliptic curve technique and DNA based encryption cryptography technique that improved the encryption speed. The entropy was around 5.3378.

Hazara and colleagues proposed a DNA cryptography algorithm based on DNA and involves the Fusion of Symmetric-Key techniques, DNA nucleotides, and XOR operation (Hazra, Ghosh, & Jash, 2018). There were two levels of security in the algorithm since two levels of substitution were applied to the encryption key, their mathematical calculations showed that there is a one per million possibility of key discovery.

Maddodi implemented a heterogeneous chaotic generator using neural network in (Maddodi, Awad, Awad, Awad, & Lee, 2018). The heterogeneity of the generator was obtained by alternating two different chaotic maps; Logistic and Piece Wise Linear Chaotic Map (PWLCM). In addition, the chaotic generator was used as an input for the encryption algorithm. The entropy value for their proposed algorithm were 7.9989 for color image. Adjacent pixel correlations were −0.0026, 0.0023 and −0.0022 for H, V, and D, respectively.

Ahgue et al. (Ahgue et al., 2018) proposed a symmetrical image encryption system that relies on One-Time Password (OTP) generated encryption key based on PWLCM chaotic equations and DNA encoding rules. Adjacent pixel correlation for grayscale, plain, and encrypted images was 0.00188452, −0.00169 and -0.00644 for H, V, and D respectively, NPCR of 99.62% and UACI of 99.6155%

An algorithm that first encrypted the message using DNA sequence rules and the key were both generated dynamically depending on the edge detection points that are produced by Canny algorithm, and then hides the encrypted text in one after another of the eight of the cover image blocks in reverse order except the edge points was proposed by Al-Saffar (al-Saffar, 2018). The obtained results showed that PSNR was 77.108 dB.

Ibraheem et al. (Ibraheem, Hamad, & Jalal, 2018) proposed a secure messaging utilizing both RSA (Rivest–Shamir–Adleman) and DNA computation for Message Queuing Telemetry Transport (MQTT) protocol. RSA is used to convert each character in the message sequence of numbers; those numbers are converted to binary encoded using DNA to code words. The correlation coefficient was 0.0625.

Abu-Alhaija in (Abu-Alhaija, 2019), proposed steganography security of information based on the LSB method, the proposed algorithm skins AES pre-encrypted private data as a text or image into image files. The proposed algorithm achieved PSNR of 96.3 dB and MSE of 0.00408.

RESULTS AND DISCUSSION

We had categorized the surveyed algorithms and methods into three categories: Image encryption DNA-based algorithm (Table 1), LWC DNA-based algorithm (Table2), and General DNA-based algorithm (Table 3); column 2 in each table answers research question no. 1.

For each table, we compared the algorithms for each category using different evaluation parameters. Keeping in mind that, when the correlation coefficients are extremely low and are near to zero, they indicate that there is no correlation between the encrypted and original images. The negative correlation coefficients show that the encryption scheme is key sensitive, the entropy value should ideally be 8. If the entropy is less than 8, there exists a certain threat of predicting the original message from the original message [25]. High PSNR indicate that the encrypted image is closer to the original message. In general, a higher PSNR value indicates a higher quality image. Higher NPCR/UACI value is inferred as a high resistance to differential attacks, so it is needed to get higher values of NPCR and lower values for UACI.

Table 1: Image encryption DNA-based algorithm

Ref.	Algorithm used	PSNR (dB)	NPCR (%)	UACI (%)	Correlation coefficients for V, H and D	Entropy
12	Choas and DNA encoding	✕	99.62	49.75	0.004058 , 0.000901 and 0.000790	✕
19	DNA Encryption using 2-D and 3-D logistic maps.	✕	99.6231	33.495	0.0025, .00297 and .0054	7.997
20	DNA Chen's hyper-chaotic map	26.5214	99.65	33.45	0.0025, 0.0012 and 0.001	7.9995
21	Combination of DNA and AES 256	67.86	98.29	34	✕	✕
20	Binary Image Encryption Based on Chaotic and DNA Encoding	✕	50	50	−0.0010	0.9998
23	Self-updating transformation based on dynamic image filtering (STDIF)	34.8909	99.606	33.39	- 0.0014, - 0.0029 and 0.0015	7.9969
27	Consolidation of DNA encryption and Rubik's cube	✕	99.6		✕	✕
29	(one-dimensional composite chaos and hyperchaos	41.7268	99.6130	33.5211	0.0020	7.9971
30	A cross-coupled chaotic map to generate random DNA sequences	99	✕	✕	0.0096	7.5733
38	Recursive Cellular Automata	✕	99.6143	33.4675	-0.002 - 0.0014, and -0.0012	7.9994
40	Multi chaotic encoding structure	✕	99.62	29.48	✕	✕

42	Dual hyperchaos map	5.72	99.68	33.55	✕	7.8466
50	RSA and DNA computation for Message Queuing Telemetry Transport	✕	✕	✕	0.0625	✕
51	Protection of information according to the LSB method	96.3	✕	✕	✕	✕

When examining table 1, we notice that Ref. [40] has highest NPCR/UACI (3.3792402), for PSNR Ref. [30] has highest value (99 dB), for entropy Ref. [20] has the highest value (7.9995). Moreover, It worth mentioning that Ref. [20], Ref. [23] and Ref. [30] evaluate all performance parameters (this answers research question 2). Figure 2 illustrates the PSNR calculated for each reference in table1.

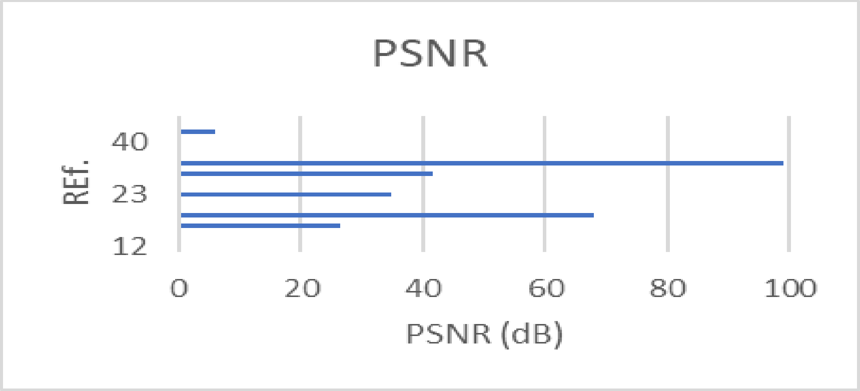

Figure2. PSNR from table 1

For table 2, Ref. [33] has highest NPCR/UACI (2.976688583), for PSNR Ref. [49] has highest value (77.108 dB), for entropy Ref. [15] has the highest value (7.99902). For LWC algorithms, Ref. [28], Ref. [36], Ref. [35] and Ref. [44] performed experimental evaluation for all parameters. In addition, Table 2 answers research question 3.

Table2: LWC DNA-BASED ALGORITHMS

Ref.	**Algorithm used**	**PSNR (dB)**	**NPCR (%)**	**UACI (%)**	**Correlation coefficients for V, H and D**	**Entropy**

15	block cipher DNA	8.687	×	×	×	×
17	block cipher DNA	6.184	×	×	0.083	7.99902
24	advanced encryption standard (AES) and a new chaotic s-box	×	×	×	- 0.0499, 0.0059 AND 0.1754	7.9460.
25	a variable block size DNA encryption.	8.11	×	×	×	7.9460
28	2d_logistic sine map for key generation	45.5446	99.58	33.56	0.9985	7.9894
30	standard AES	×	×	×	−0.0499 , 0.1754, AND 0.0059 AND	7.9460
33	logistic-tent map and crossover operator of a genetic algorithm	×	99.60	33.46	0.0061, 0.0059 and 0.0415.	7.9968
35	chaotic lec	7.5785	99.67	34.19	0.9806 , 0.9831, AND 0.9685	7.9851
36	Hyperchaos and DNA encoding	30.62287	99.64	33.81	-0.0365 , 0.0241 AND 0.0345	7.99060
37	TWO PERMUTATION TECHNIQUES	27	×	×	×	7.98
39	FEISTEL STRUCTURE AND SUBSTITUTION-PERMUTATION NETWORK				0.0001	7.9976
44	BASED ON PSEUDO RANDOMLY ENHANCED LOGISTIC MAP	35.1889	99.6	33.489	0.75873, 0.86654 AND 0.72618	7.35830
47	HETEROGENEOUS CHAOTIC GENERATOR	×	×	×	0.0023, −0.0026 −0.0022	7.9989

48	One Time Password generated encryption key based on PWLCM chaotic equations and DNA	✕	99.62	99.6155	−0.00169 , 0.00188452 and - 0.00644	✕
49	encryption and steganography	77.108	✕	✕	✕	✕

Figure 3 shows the illustrates PSNR calculated for each reference in table2.

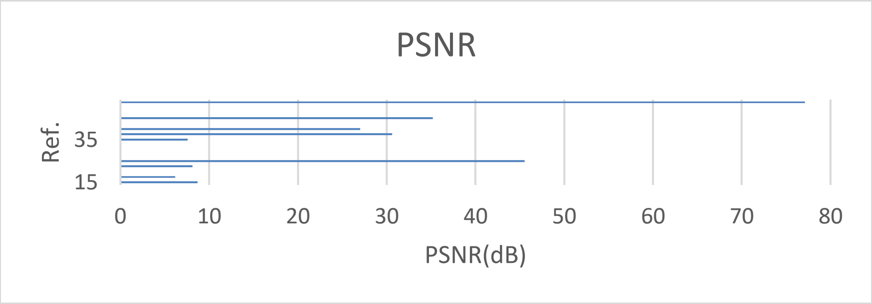

Figure 3. PSNR f table 2

Table3. General DNA-based algorithms

Ref.	Algorithm used	PSNR (dB)	NPCR (%)	UACI (%)	Correlation coefficients for V, H and D	Entropy
16	Combination of the RSA algorithm and DNA coding	✕	99.6136	33.4665	-0.0014, -0.0011 and 0.0043	✕
18	Large DNA based key is generated from a short key	88.5642	✕	✕	−0.00012	7.9998949
26	confusion mapping methods to increase the key space	✕	90.15	1.3	✕	7.9376
31	Huffman coding method	✕	99.6032	33.607	0.0027,-.0132, and - 0.0083	7.9957
34	DNA key multi-round encryption	6.533	✕	✕	✕	7.998982

41	genetic operators and Diffie-Hellman key exchange algorithm	✕	✕	✕	✕	1.4
43	modified AES based on DNA sequence	✕	✕	✕	✕	✕
45	DNA based elliptic curve technique	✕	✕	✕	✕	5.3378
46	FUSION OF SYMMETRIC-KEY TECHNIQUES	✕	✕	✕	✕	✕

When examining table 3 above, we notice that Ref. [26] has highest NPCR/UACI (69.34615385), for PSNR and entropy Ref. [18] has highest values (88.5642 dB and (7.9998949). Finally, Ref. [31] carried out experiments to evaluate most of the parameters. Figure 4 illustrates the PSNR calculated for each reference in table3.

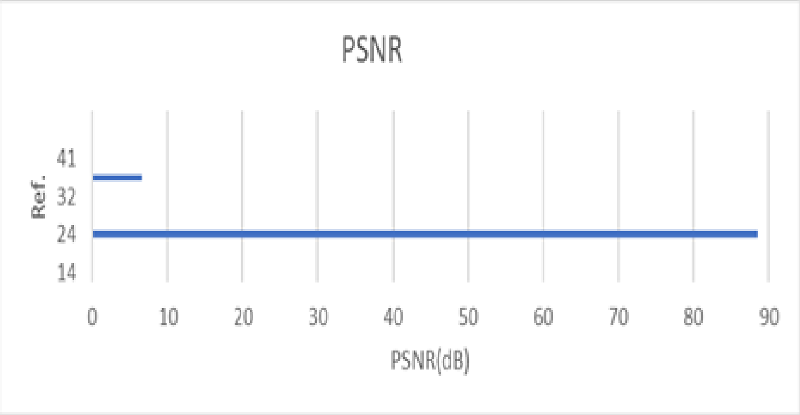

Figure 4. PSNR from table 3

CONCLUSIONS

Recently, there exist several DNA cryptosystems proposed either as an algorithmic approaches or as an integral part of data secrecy applications. Algorithmic approaches were studied by very few researches that integrate both the biological and arithmetic operations to gratify the necessity of system optimality. In addition, DNA cryptosystems provide layered security in applications besides other traditional cryptographic algorithms.

Most articles on DNA cryptography techniques indeed neither provide complete security analysis nor built based on mathematical methods. The researchers mostly demonstrated the proposed system model and tested the approaches using computer simulations. Nonetheless, no DNA computation implantations of the surveyed techniques were carried out.

This study will assist researches as a reference for researches in future. Therefore, this paper can help researchers to improve more on the current limitations of DNA cryptography.

Conflict of Interest

The authors declare that they have no conflicts of interest to report regarding the present work.

Funding Statement

This work is supported and sponsored by Al-Ahliyya Amman University.

References

Abed, A. M., & Boyaci, A. (2020). A lightweight cryptography algorithm for secure smart cities and IOT. Electrica, 20(2), 168-176.

Abu-Alhaija, M. (2019). Crypto-Seganographic LSB-based System for AWS-Encrypted Data. (IJACSA) Inter. J. of Advanced Computer Science and Applications, 10(10), 55-60.

Abu-Alhaija, M., Turab, N. M., & Hamza, A. (2022). Extensive Study of Cloud Computing Technologies, Threats and Solutions Prospective. COMPUTER SYSTEMS SCIENCE AND ENGINEERING, 41(1), 225-240.

Adleman, L. M. (1994). Molecular computation of solutions to combinatorial problems. science, 266(5187), 1021-1024.

Ahgue, A. O., De Nkapkop, J. D., Effa, J. Y., Franz, S., Adelis, P., & Borda, M. (2018). A DNA-based chaos algorithm for an efficient image encryption application. Paper presented at the 2018 International Symposium on Electronics and Telecommunications (ISETC).

Akiwate, B. (2021). Secure and Efficient Image Cryptography Technique using Choas and DNA Encoding Methodology. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(2), 2754-2764.

Akkasaligar, P. T., & Biradar, S. (2020). Selective medical image encryption using DNA cryptography. Information Security Journal: A Global Perspective, 29(2), 91-101.

Al-Dwairi, R. J. (2021). A New Symmetric Lightweight Encryption Algorithm Based on DNA for Internet of Things Devices مادختساب ءايشلأا تنرتنإ ةزهجأب صاخ لثامتم ديدج ريفشت ماظن يوونلا ضمحلا ةيصاخ. Middle East University.

Al-Husainy, M. A. F., Al-Shargabi, B., & Aljawarneh, S. (2021). Lightweight cryptography system for IoT devices using DNA. Computers & Electrical Engineering, 95, 107418.

al-Saffar, A. (2018). Cryptography with Dynamic DNA Depending on Edge Detection. Ibn AL-Haitham Journal For Pure and Applied Science, 31(2), 186-192.

Al-Shargabi, B., & Al-Husainy, M. A. F. (2020). A New DNA Based Encryption Algorithm for Internet of Things. Paper presented at the International Conference of Reliable Information and Communication Technology.

Al-Shargabi, B., & Al-Husainy, M. A. F. (2022). Multi-round encryption for COVID-19 data using the DNA key. International Journal of Electrical & Computer Engineering (2088-8708), 12(1).

Alsaffar, Q. S., Mohaisen, H. N., & Almashhdini, F. N. (2021). An encryption based on DNA and AES algorithms for hiding a compressed text in colored Image. Paper presented at the IOP Conference Series: Materials Science and Engineering.

Alshammari, B., Guesmi, R., Guesmi, T., Alsaif, H., & Alzamil, A. (2021). Implementing a Symmetric Lightweight Cryptosystem in Highly Constrained IoT Devices by Using a Chaotic S-Box. Symmetry 2021, 13, 129: s Note: MDPI stays neu-tral with regard to jurisdictional clai-ms in ….

Alshammari, B. M., Guesmi, R., Guesmi, T., Alsaif, H., & Alzamil, A. (2021). Implementing a symmetric lightweight cryptosystem in highly constrained IoT devices by using a chaotic S-box. Symmetry, 13(1), 129.

Athira, A., & Basu, P. (2020). A novel technique for image encryption using transform based scrambling and DNA based multi chaotic encoding scheme. Paper presented at the AIP Conference Proceedings.

Babaei, A., Motameni, H., & Enayatifar, R. (2020). A new permutation-diffusion-based image encryption technique using cellular automata and DNA sequence. Optik, 203, 164000.

Dagadu, J. C., Li, J.-P., & Addo, P. C. (2019). An image cryptosystem based on pseudorandomly enhanced chaotic DNA and random permutation. Multimedia Tools and Applications, 78(17), 24979-25000.

El-Khamy, S. E., & Mohamed, A. G. (2021). An efficient DNA-inspired image encryption algorithm based on hyper-chaotic maps and wavelet fusion. Multimedia Tools and Applications, 80(15), 23319-23335.

Ferdush, J., Begum, M., & Uddin, M. S. (2021). Chaotic lightweight cryptosystem for image encryption. Advances in Multimedia, 2021.

Gan, Z., Chai, X., Zhi, X., Ding, W., Lu, Y., & Wu, X. (2021). Image cipher using image filtering with 3D DNA-based confusion and diffusion strategy. Neural Computing and Applications, 33(23), 16251-16277.

Gehani, A., LaBean, T., & Reif, J. (2003). DNA-based cryptography Aspects of Molecular Computing (pp. 167-188): Springer.

Gupta, M., Gupta, K. K., Khosravi, M. R., Shukla, P. K., Kautish, S., & Shankar, A. (2021). An intelligent session key-based hybrid lightweight image encryption algorithm using logistic-tent map and crossover operator for internet of multimedia things. Wireless Personal Communications, 121(3), 1857-1878.

Hadi, S. A., Ali, S. A., & Jawad, M. J. (2021). Binary Image Encryption Based on Chaotic and DNA Encoding Next Generation of Internet of Things (pp. 295-312): Springer.

Hasan, M. K., Islam, S., Sulaiman, R., Khan, S., Hashim, A.-H. A., Habib, S., . . . Kamil, S. (2021). Lightweight encryption technique to enhance medical image security on internet of medical things applications. IEEE Access, 9, 47731-47742.

Hazra, A., Ghosh, S., & Jash, S. (2018). A new DNA cryptography based algorithm involving the fusion of symmetric-key techniques Advanced Computational and Communication Paradigms (pp. 605-615): Springer.

Ibraheem, S. S., Hamad, A. H., & Jalal, A. S. A. (2018). A Secure Messaging for Internet of Things Protocol based RSA and DNA Computing for Video Surveillance System. Paper presented at the 2018 Third Scientific Conference of Electrical Engineering (SCEE).

Intelligence, G. M. (2020). Global Cloud Computing Market :Based On Mode Of Deployment, Based On Cloud Service, By End Users With COVID-19 Impact | Forecast Period 2017-2030. from https://www.goldsteinresearch.com/report/cloud-computing-market-outlook-2024-global-opportunity-and-demand-analysis-market-forecast-2016-2024

Ivanchuk, B. (2019). DNA structure on a white background with a description of the main components. from https://www.dreamstime.com/dna-structure-white-background-description-main-components-simple-infographic-image135124647

Jacob, G. (2013). DNA based cryptography: An overview and analysis. International Journal of Emerging Sciences, 3(1), 36.

Kaushik, A., Thada, V., & Singh, J. (2021). VG3 Cipher for Secure Image Transmission. Paper presented at the Journal of Physics: Conference Series.

Li, S., Song, H., & Iqbal, M. (2019). Privacy and security for resource-constrained IoT devices and networks: Research challenges and opportunities: Multidisciplinary Digital Publishing Institute.

Liu, H., Zhao, B., & Huang, L. (2019). A remote-sensing image encryption scheme using DNA bases probability and two-dimensional logistic map. IEEE Access, 7, 65450-65459.

Liu, M., & Ye, G. (2021). A new DNA coding and hyperchaotic system based asymmetric image encryption algorithm. Mathematical Biosciences and Engineering, 18(4), 3887-3906.

Maddodi, G., Awad, A., Awad, D., Awad, M., & Lee, B. (2018). A new image encryption algorithm based on heterogeneous chaotic neural network generator and dna encoding. Multimedia Tools and Applications, 77(19), 24701-24725.

Meftah, M., Pacha, A. A., & Hadj-Said, N. (2020). DNA encryption algorithm based on Huffman coding. Journal of Discrete Mathematical Sciences and Cryptography, 1-14.

Mondal, B. (2020). A Secure Steganographic Scheme Based on Chaotic Map and DNA Computing Micro-Electronics and Telecommunication Engineering (pp. 545-554): Springer.

Peng, W., Cui, S., & Song, C. (2021). One-time-pad cipher algorithm based on confusion mapping and DNA storage technology. Plos one, 16(1), e0245506.

sBahig, H. M., & Nassr, D. I. (2019). DNA-based AES with silent mutations. Arabian Journal for Science and Engineering, 44(4), 3389-3403.

Singh, E. R., & Mahajan, E. S. Improved Elliptic Curve Cryptography with RFID Protocol Based on DNA Technique.

Sujarani, R., Manivannan, D., Manikandan, R., & Vidhyacharan, B. (2021). Lightweight bio-chaos crypt to enhance the security of biometric images in internet of things applications. Wireless Personal Communications, 119(3), 2517-2537.

Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access.

Thum, C. (1984). Measurement of the entropy of an image with application to image focusing. Optica Acta: International Journal of Optics, 31(2), 203-211.

Toshihiko, O. (2017). Lightweight cryptography applicable to various IoT devices. NEC Technical Journal, 12(1), 67-71.

Turab, N., & Kharma, Q. (2019). Secure Medical Internet of Things Framework based on Parkerian Hexad Model.

Uddin, M., Jahan, F., Islam, M. K., & Rakib Hassan, M. (2021). A novel DNA-based key scrambling technique for image encryption. Complex & Intelligent Systems, 1-18.

Vidhya, E., & Rathipriya, R. (2020). Key Generation for DNA Cryptography Using Genetic Operators and Diffie-Hellman Key Exchange Algorithm. Computer Science, 15(4), 1109-1115.

Wan, Y., Gu, S., & Du, B. (2020). A new image encryption algorithm based on composite chaos and hyperchaos combined with DNA coding. Entropy, 22(2), 171.

Wortmann, F., & Flüchter, K. (2015). Internet of things. Business & Information Systems Engineering, 57 (3), 221-224.

Wu, Y., Noonan, J. P., & Agaian, S. (2011). NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT), 1(2), 31-38.

Xie, H., Zhang, Y., Zhang, H., & Li, Z. (2021). Novel Medical Image Cryptogram Technology Based on Segmentation and DNA Encoding.