Journal of Computing and Communication Vol.1 , No.2 , PP. 9-23 , 2022

Secure Image encryption algorithm based on DNA Encoding and Chaos map for cloud computing

Diaa Salam Abd Elminaam*[a,b] , Menna Allah Wafik[a], Mohamed Abdelfatah[a]

[a] Information Systems Department, Faculty of Computers and Artificial Intelligence, Benha University, 12311, Egypt
[b]Department of Computer Science, Misr International University, Cairo, Egypt

*Corresponding Author: Diaa Salam Abd Elminaam [Diaa.salama@fci.bu.edu.eg]

ARTICLE DATA

Article history:
Received 08 Mar 2022
Revised 03 Aug 2022
Accepted 09 Aug 2022
Available online

Keywords:
DNA Encoding
cloud computing
Image encryption

ABSTRACT

Cloud computing is rapidly expanding in the IT business today, providing a new approach to handling various information systems. The fast advancement of technology necessitates the usage of this technology and reaping its benefits. Understanding and expertise for using algorithmic security in processes and data systems are rising as awareness and concerns about cloud services and information security risks. The major goal of this project is to conduct a security analysis and performance evaluation of a novel lightweight cryptographic method for improving data security in cloud computing. A series of experiments on several test photos were used to verify the efficacy of the suggested technique. Compared to existing schemes, the numerical results show that the suggested algorithm works incredibly well and gives better encryption results despite the larger key sensitivity. Nonetheless, the suggested approach is more resistant to known statistical, differential, and exhaustive attacks.

1. Introduction

Cloud computing is a notion in internet technology that provides different internet-based remote services, including infrastructure, data storage, and applications. This includes enacting various regulations, measures, and restrictions to safeguard cloud computing technology's assets, software, and related resources. [1].

Cloud computing comprises software, hardware, networks, applications, and customer service interfaces. The main concept of the cloud is virtualization, which can be accomplished by pooling and sharing resources. Virtualization's main characteristics are extensibility, flexibility, and multiple leasing. Customers can choose from several cloud computing service models, including infrastructure as a Service (IAAS), Platform as a Service (PAAS), and Software as a Service (SAAS) [2].

The cloud computing paradigm comprises three functional parts, which are stated below: cloud services are classified into four categories: public cloud, private cloud, hybrid cloud, and community cloud. A cloud service provider creates the public cloud, which is available to all end users. A certain company built the private cloud for its exclusive purpose. The hybrid cloud has the potential to increase the scalability of enterprises. The groups could work together to build their cloud within a community cloud [3].

- **Cloud Service Provider**

An entity in charge of running a Cloud Storage Server (CSS) with a large storage capacity for customer data and powerful computing capabilities.

- **Customer / Owner**

A single consumer or business keeps large amounts of data in the cloud and depends mostly on the cloud for data maintenance and computation.

- **User**

A device is registered to the owner and utilizes data saved in the cloud by the owner. The user may also be the owner [3].

According to the security of cloud computing, the following requirements should be included:

- **Confidentiality**: refers to only authorized individuals having access to information.
- **Integrity**: The communication's receiver must ensure that the message has not been tampered with while in transit. The attacker cannot be able to substitute a false message with a valid one.
- **Availability**: Authorized workers must access information and computers [4].

The use of encryption, cryptography and authentication procedures reduces security risks [4-5]. Encryption is used to conceal and securely keep information from attackers so that only the people who need it may access and safely distribute it.

There are various symmetric and asymmetric cryptographic methods available to ensure text data security, including Advanced Encryption Standard (AES), IDEA (International Data Encryption Algorithm), and RSA (Proposed by Rivest, Shamir, and Adleman). However, the survey shows that these techniques are unsuitable for picture encryption because image data properties such as pixel correlation, bulk space, and substantial redundancy among pixel values make image encryption more difficult than text encryption [6].

Chaotic image encryption relies on a dynamic mechanism to deliver quick and safe data security methods. There are two types of chaotic systems: one-dimensional (1D) chaotic systems and high-dimensional (HD) chaotic systems. At the moment, typical 1D chaotic systems employed in information encryption include logistic maps, tent maps, Hénon maps, and sine maps [7–11]. However, the aforementioned chaotic systems still have several flaws, such as a tiny key space, inadequate complexity, and low security, which allows the decryption process to be readily accomplished. Much research has been conducted to improve the present 1D chaotic system [12–17]. However, a 1D chaotic system is insufficient for picture encryption since it is easily hacked.

Due to the huge parallelism and remarkable information density of DNA molecules, researchers have merged DNA technology with chaos to build high-efficiency and safe encryption techniques [18-24]. The basic theory of DNA is utilized. In [19] to overcome the drawbacks of picture encryption based on chaotic maps and DNA cryptography. The basic theory of DNA and DNA sequence operation is applied to achieve picture encryption. The suggested approach in [24] scrambles the pixel values of an image's RGB components using DNA addition and then encrypts the scrambled pictures. However, adding is the only action of DNA encoding in this study.

The primary goal of adopting encryption methods is to safeguard or store large amounts of data in the cloud. Inspired by previous discussions, we present a hybrid method that uses encryption to improve cloud data security. This work combines DNA encoding and chaotic logistic maps to improve cloud security. **The following are the significant contributions of the proposed work:**

- Proposal for an image security method for cloud storage applications.
- The use of DNA and chaotic maps to create lightweight but efficient pixel diffusion.
- Image cryptography with a large key space to resist brute force attacks.
- Execution of various attack analyses to demonstrate the efficacy of cryptography.

The article's novelty is as follows:

- The lower dimensions and structure of many contemporary chaos-based DNA designs are flawed. Consequently, to boost cipher unpredictability, a unique sort of diffusion level is created that uses pseudo-random values to disperse the DNA sequences instead of binary operations.
- The scheme is applied to higher-dimensional chaotic systems to achieve the diffusion level.
- The cryptography work is extremely sensitive to key settings, with a high recovery rate from noisy impacted images.

2. Related Work

Data security has been improved by the author's proposal of a framework that integrates cryptographic techniques, the "Advanced Encryption Standard (AES)" algorithm, and the "Hash function," SHA-2 [25]. "The researcher developed and implemented safe cloud storage systems for small and medium-sized organizations (SMEs)" [26].

When transferring data to the cloud, this research employed the strategy of merging the encryption algorithm (AES) with the hash function (MD5) to achieve data integrity and anonymity. The author has also presented a technique for securely sending data to a cloud storage device utilizing Erasure encoding (RSA) and AES encryption algorithms. [27].

To maximize the security of cloud computing data, the research recommended using hybrid encryption methodologies such as RSA Digital Signature, RSA algorithm, Blowfish algorithm encryption/decryption, Feistel, and (XOR) operating algorithms. [28] discussed the Symmetric Data Encryption Standard (DES), and it was also shown how to combine two independent methods, DES and (RSA), to eliminate the security difficulties associated with Cloud Storage.

A lightweight 64-bit block-size cryptosystem with a 128-bit key was developed, iterated in 32 rounds, and performed two sorts of operations: (XOR) and left or right rotations [30].

Other research examined the efficiency of DES (AES), RC2, BLOWFISH, and RC6 based on numerous simulation performances and concluded that the techniques should be widely known for better results. " [31].

X. Chai et al. [32] offer a medical picture encryption technique that performs diffusion and permutation operations using the (PRN) sequence produced by the 4D chaotic map. They employ Latin square pixel permutation and bi-directional adaptive diffusion for improved encryption effects. As an initial condition of the 4D map, the system calculates the (SHA-256) value, making it resistant to known and chosen plaintext assaults. Their scheme outperforms state-of-the-art techniques in terms of performance.

S. S. Asker et al. [33] provide an image security framework based on a 2D economic map and a logistic map. They use the logical (XOR) function to dilute image pixels and illustrate a vital generating approach. The technique's efficiency is evaluated, and it is concluded that it has a high degree of protection to resist any attack.

T. Li et al. [34] propose a logistic and 2D Lorenz map-based image cryptography approach. The logistic and sine map equations, and the modulus function, are combined. The technique has a key space of 10112 and is theoretically ideal (NPCR) and (UACI) values.

They also propose an encryption method based on the (LLSS) map, the Qi hyper-chaotic map, and DNA encryption. LLSS is a 1D chaotic map developed by Y. Wan et al. [35]. The resulting map has no time window and corresponds exactly to the bifurcation graph range [0, 4]. The Fibonacci transform and DNA block coding increase the scheme's security. However, the performance of the above schemes has not been validated on clinical images with high contrast between intensity levels.

Kumar et al. [38] proposed a two-layer RGB image encryption approach that used pixel diffusion and a Deoxyribose Nucleic Acid (DNA) complementary rule with an Elliptic curve public key.

According to Wu et al. [39], the logistic map was used to generate the key, and the DNA-XOR process accomplished the image diffusion. Also, other related work can be found in [40-50] has been proposed in recent years to address the cryptography and security of cloud computing

The remainder of the paper is arranged as follows: was formulated as follows: preliminaries are introduced in Section 3. Section 4 includes the proposed scheme DNA & Chaos map, while Security analysis and simulation findings are presented in Section 5. Section 6 addresses the proposed algorithm's contribution, then contrasts it with other techniques. Finally, the conclusion is reached in Section 7.

3. Preliminaries

3.1. DNA Coding

DNA is an important aspect of the genetic sciences that have already been widely employed in various uses. DNA coding [34] is a mature coding system with significant parallelism and ultra-low power consumption, making it ideal for cryptography. The DNA series contains four nucleic acids: A (adenine), T (thymine), C (cytosine), and G (guanine). A can pair with T, and C can pair with G thanks to the complementary base pairing theorem. Table 1 lists DNA encoding/decoding laws to satisfy the Watson-Crick base pairing law. As seen in Table 1. A digital image's pixel value is a number between 0 and 255 that an 8-bit binary sequence may represent. Every pixel value of the picture may be turned into a DNA molecular sequence of four bits using DNA coding principles. Furthermore, various DNA sequences with distinct coding rules can be generated for the same binary sequence.

To generate distinct binary sequences, different encoding and decoding techniques are employed. The plaintext picture and chaotic sequences used for encryption are often translated into DNA molecular sequences in line with DNA coding principles in the encryption technique. The two DNA sequences then perform the DNA operation to

produce the diffusion operation. Using DNA coding principles, the encrypted DNA sequence is decoded and restored to the pixel level to produce the final cipher.

Table 1
Rules of DNA encoding and DNA decoding

	Rules							
Rules	Rule (1)	Rule (2)	Rule (3)	Rule (4)	Rule (5)	Rule (6)	Rule (7)	Rule (8)
00	A	A	T	T	C	C	G	G
01	C	G	C	G	A	T	A	T
10	G	C	G	C	T	A	T	A
11	T	T	A	A	G	G	C	C

3.2. Operations of DNA

Applying operations of DNA to the encryption algorithm increases its strength. Table 2. Presents the operation of DNA addition. Table 3. Presents the operation of DNA subtraction.

Table 2
Operation of DNA addition

+	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G
T	T	A	G	C

Table 3
Operation of DNA subtraction

-	A	G	C	T
A	A	T	C	G
G	G	A	T	C
C	C	G	A	T
T	T	C	G	A

3.3. Chaotic logistic map

Chaos is a deterministic, random-like phenomenon that occurs in nonlinear and bounded dynamical systems. Furthermore, it depends on its initial condition and parameters [35]. A chaotic map is a discrete-time dynamical system that is described by equation (1):

$$x_{k+1} = f(x_k), x \in (0,1), k = 0,1,2,3 \quad (1)$$

When the initial conditions are different and distributed over the entire area, the chaotic sequences $x_k, k = 0,1,2,3$ are uncorrelated. Equation (2) defines a logistic map as one of the simplest chaotic maps.

$$x_{k+1} = f(x) = \mu(x_k)(1 - x_k)$$

$$\mu \in (0,4), x_k \in (0,1) \quad (2)$$

As shown in Figure1, the map is chaotic when $\mu \in (3.569945,4)$ it is used. Chaotic signals can be employed in communication because they have some statistical features with white noise; we may also convert chaotic real-valued sequences to chaotic binary sequences using Equation (3).

$$f(X) = \begin{cases} 0, & 0 < Xn \leq 0.5 \\ 1, & 0.5 < Xn < 1 \end{cases} \quad (3)$$

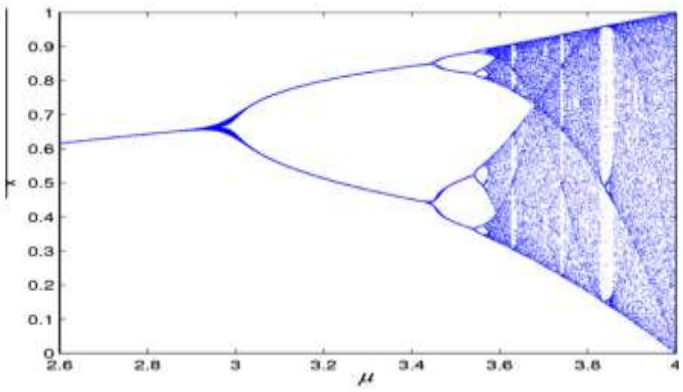


Figure1 The logistic map's bifurcation diagram.

4. Cryptosystem

Because cloud computing offers its clients a high storage capacity, it is critical to preserve this data. There are several encryption techniques, yet anybody may compromise the bulk of these techniques' security. As a result, strengthening security measures is crucial. This is why we offered our plan, showing its efficacy and anonymity by the results obtained. We introduce a unique encryption technique for cloud-sensitive information security in this study. The data owner encrypts the sensitive information on the client side before transferring it to a web-based cloud storage provider. Because of its great speed, acceptable computation, and good security, the Chaos algorithm for encryption is deemed good. We proposed a new approach to obtain a secure encrypted image that uses chaotic logistic mapping and DNA encoding. The initial conditions of this map are incredibly important. We've also used DNA encoding in this study, which helps to make encryption significantly more complicated and random. The technique of encoding pixel values into a DNA sequence of nucleic acid bases A, T, G, and C is known as DNA encoding.

As a web-based cloud storage provider, we chose Google Drive. Google Drive is a simple, long-lasting, and scalable data storage service with a simple web interface that allows users to save and retrieve any amount of data at any time and from any location on the internet. After creating a folder in Google Drive regions, we upload items to the Google Drive folder.

4.1. Approach to Encryption

The following are the encryption processes for the specific steps:

Input: Plain image

Step 1: Transform image to decimal matrix D_ I $(m\times n\times 3)$, then to binary matrix **bin-I,** $(m\times n\times 3\times 8)$ the row and column image dimensionalities are m and n, etc.

Step 2: Two chaotic logistic maps are used in the condition where initial values are g_0 =0.154, g_1 =0.769, and control parameters of the system are μ_0 =4, μ_1 =4 to create two chaotic sequences x_n, x'_n with length **L, L'** equal to the length of binary matrix **bin-I** using Equation (2):

$$x_{k+1} = f(x) = \mu(x_k)(1 - x_k)$$

$$\mu \in (0,4)\ ,\ x_k \in (0,1) \qquad (2)$$

Step 3: Transform two chaotic sequences x_n, x'_n into binary sequences B_x_n, B_y_n , then merge them as one matrix **bin-S** $(m\times n\times 24)$:

$$f(x) = \begin{cases} 0, & 0 < x_n \le 0.5 \\ 1, & 0.5 < x_n < 1 \end{cases} \qquad (3)$$

Step 4: Encode the matrix **bin-I** and **bin-S** based on the DNA encoding rule selected by random key1 ∈ [1:8] to obtain DNA sequence matrices DNA_I $(m\times n\times 12)$ and DNA_S $(m\times n\times 12)$ based on table 1

Step 5: Perform DNA addition operations between DNA_I and DNA_S based on table 2.

Step 6: Using the DNA rule chosen by key1, decode the matrix, which is the result from step (5) to get the first decoded matrix

Step 7: Execute the third logistic chaotic map used in the condition where the initial value is g_2 =0.01 and the control parameter of the system μ_2 =4 to create one chaotic sequence x''_n with length L" equal to the length of the decoded matrix, which results from step 6 using Equation (2).

$$x_{k+1} = f(x) = \mu(x_k)(1 - x_k)$$

$$\mu \in (0,4)\ ,\ x_k \in (0,1) \qquad (2)$$

Step 8: Perform XOR operation between the matrix generated from step 6 and chaotic sequences generated from step 7 to get **the second decoded matrix**

Step 9: Create a Random key matrix the same size as the matrix resulting from **step 8**.

Step 10: Perform XOR operation between the matrix generated from step 8 and key values generated from step 9 to get the cipher image.

Output: Cipher image

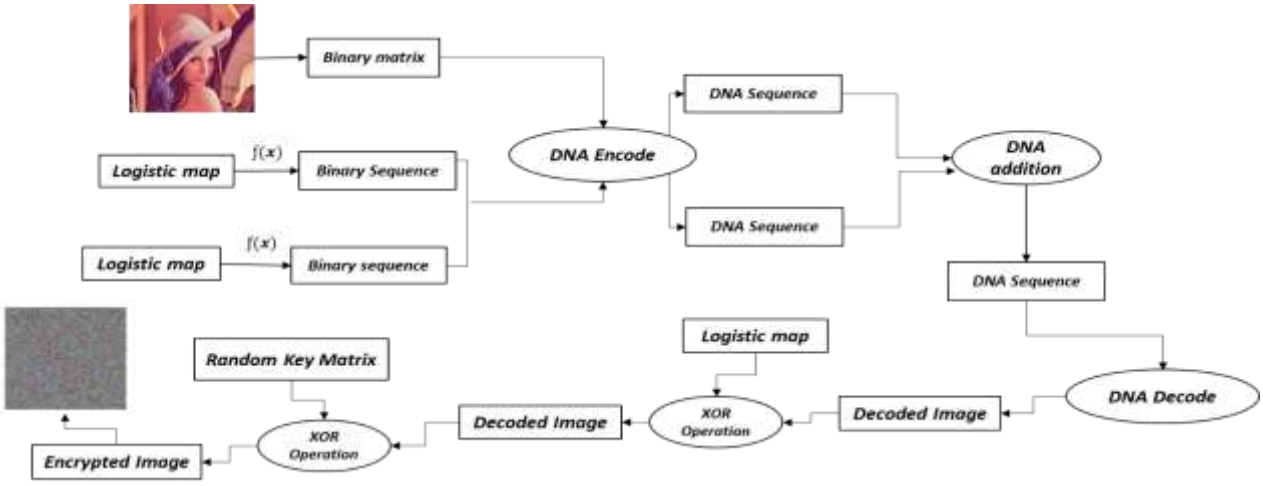


Figure 2. The suggested encryption algorithm's flow chart.

4.2. Approach to Decryption

Input: Cipher image

Step 1: Transform image to decimal matrix D_ I $(m \times n \times 3)$, then to binary matrix **bin-I,** $(m \times n \times 3 \times 8)$ the row and column image dimensionalities are m and n, etc.

Step 2: Create a Random key that equals the size of the given image in step 1.

Step 3: Perform XOR operation between the matrix generated from step 1 and key values generated from step 2 to get the first decoded matrix.

Step 4: Execute the third logistic chaotic map is used in the condition where the initial value is g_2 =0.01 and the control parameter of the system μ_2 =4 to create one chaotic sequence x''_n with length L" equal to the length of the decoded matrix, which results from step 3 using Equation (2).

$$x_{k+1} = f(x) = \mu(x_k)(1 - x_k)$$

$$\mu \in (0,4)\ ,\ x_k \in (0,1) \qquad (2)$$

Step 5: Perform XOR operation between the decoded matrix generated from **step 3** and the chaotic sequence generated from step 4 to get the second decoded matrix which will be converted to a binary matrix bin-I_2.

Step 6: Two chaotic logistic maps are used in the condition where initial values are g_0 =0.154, g_1 =0.769, and control parameters of the system are μ_0 =4, μ_1 =4 to create two chaotic sequences x_n, x'_n with length L, L' equal to the length of binary matrix bin-I_2 using Equation (2):

Step 7: Transform two chaotic sequences x_n, x'_n into binary sequences B_x_n, B_y_n , then merge them as one matrix bin-S $(m \times n \times 24)$:

$$f(x) = \begin{cases} 0, & 0 < x_n \le 0.5 \\ 1, & 0.5 < x_n < 1 \end{cases} \qquad (3)$$

Step 8: Encode the matrix bin-I_2, and bin-S based on the DNA encoding rule selected by random key1 ∈ [1:8] to obtain DNA sequence matrices **DNA_I2** $(m \times n \times 12)$ and **DNA_S** $(m \times n \times 12)$ based on table 1.

Step 9: Perform DNA subtraction operations between **DNA_I2** and **DNA_S** based on table 3.

Step 10: Using the DNA rule chosen by key1, decode the matrix, which is the result from step (9), to get the plain image

Output: Plain image

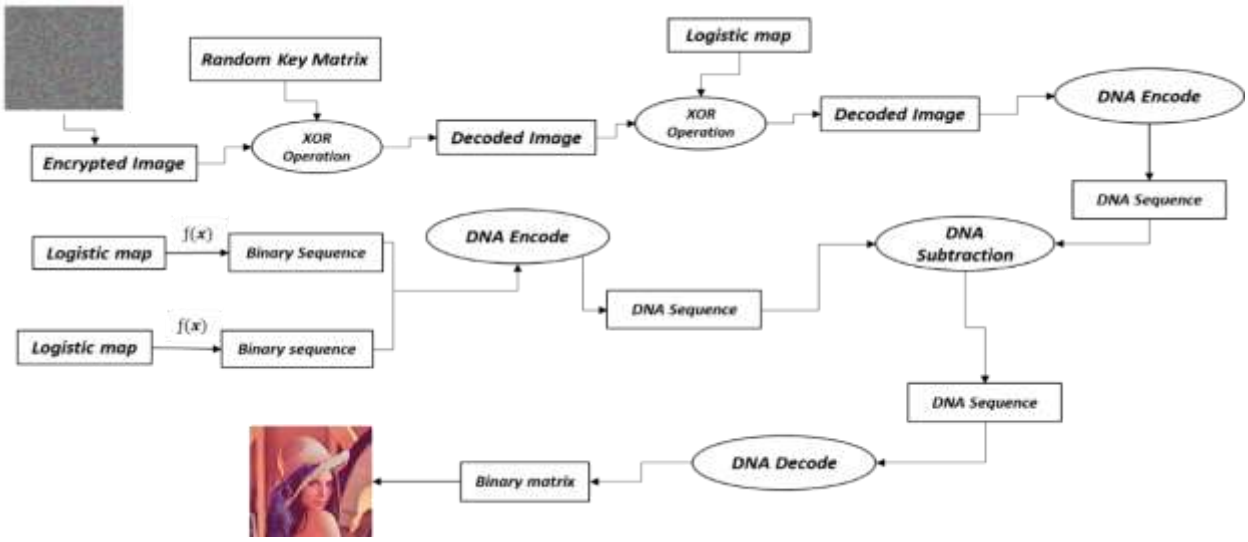


Figure 3. The suggested decryption algorithm's flow chart

5. Simulation results and Security Analysis

Simulates the encryption and decryption processes from various perspectives. The suggested method was put through a series of tests to ensure its stability and quality. We tested many images such as (Lena, Baboon, and Peppers) all of them with size (256 ×256), using some well-known parameters that have been used by various authors [32–36] to compare the efficiency of various cryptographic algorithms under initial conditions: g_0 =0.154, μ_0=4, g_1 =0.769, μ_1 =4, g_2 =0.01, μ_2 =4, MATLAB 2015b runs all of the tests on a 2.60 GHz CPU with 4 GB of RAM.

5.1. Ability to resist statistical attack

5.1.1 Histogram analysis

The gray histogram is more logical, and it has high visibility. The pixel intensity must be evenly dispersed after encryption to declare that the picture is impulsive. A close-to-ideal distribution of pixel intensities indicates that the reaction is flat and improves anti-attack behavior. Figure. 4 depicts plain- images with size 256×256, such as Lena and Baboon, with a focus on a few pixel values. Cipher-images, on the other hand, have a more uniform distribution. . The x-axis indicates grayscale values ranging from 0 to 255, while the y-axis shows the number of pixels in the figure's corresponding grayscale.

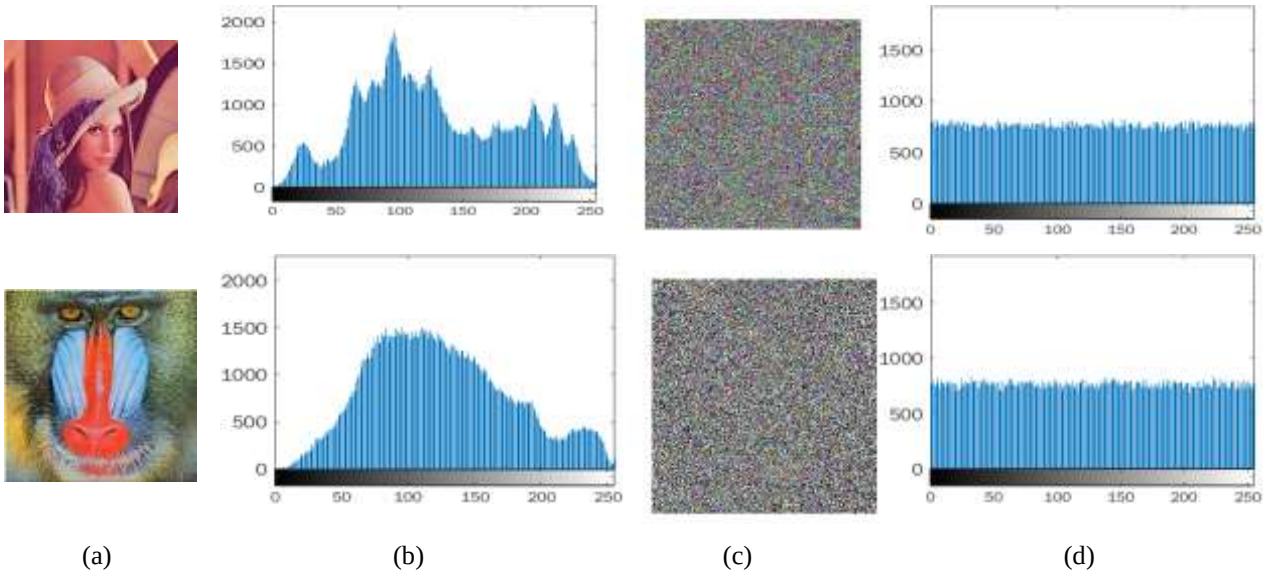


Figure 4. Histograms analysis. (a) plain-images (b) histogram of plain-images (c) cipher-images (d) histogram of cipher-images.

5.1.2 Correlation analysis

The correlation coefficient (CC) quantifies the redundancy of the pixels in a picture. The raw image has a significant level of redundancy, but the encrypted image should have a very low CC value. This indicates that the encrypted picture has the least amount of redundancy. Equation (4) defines the correlation coefficient.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{S}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2$$

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right)$$

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (4)$$

S is the total number of pixels picked from the picture, where x, and y are the pixel values of neighboring pixels. E(x) represents the estimation of mathematical expectations. D(x) represents the estimation of x's variance. $Cov(x,y)$ Represents the covariance estimation between x and y, and r_{xy} indicates the image's correlation coefficient. The paper randomly selects 2000 pairs of adjacent pixels for the correlation test in the horizontal, vertical, and diagonal directions. Figure.5 shows the correlation distributions for plain and cipher in horizontal and vertical directions. Plain-image correlation distributions are concentrated, while cipher-image correlation distributions are fairly uniform. According to the results, the proposed cryptosystem effectively reduces the correlation between two adjacent pixels in the horizontal, vertical, and diagonal directions. Table 4 shows the correlation coefficient results. Plain-image

correlation coefficients are 1, while cipher-image correlation coefficients are 0. As a result, by using correlation analysis to break up the cryptosystem, the attacker would be unable to obtain valuable correlation information.

Table 4.
Correlation coefficient results

Image (256 ×256)	CC of Plain Image				CC of Cipher Image		
	Horizontal	Vertical	Diagonal		Horizontal	Vertical	Diagonal
Lena	0.9806	0.9601	0.9383		-0.0070	0.0011	0.0007
Baboon	0.8199	0.8903	0.9039		0.0048	-0.0003	0.0013
Peppers	0.9027	0.9442	0.9430		0.0015	-0.0027	-0.0016

5.1.3 Information Entropy

The entropy of information is an important statistic for assessing the strength of a cryptographic algorithm. The ensemble's entropy is an acceptable measure of its average information content. The theoretical description of entropy is given in Equation (5).

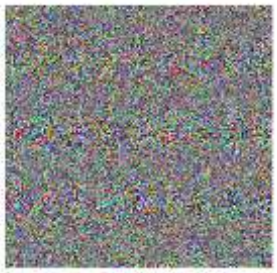
$$H(s) = -\sum_{i=0}^{2^n-1} p(s_i)\, log_2\, p(s_i) \qquad (5)$$

The optimal information entropy for the cipher-image is equal to 8, where the symbol's probability equals $P(s_i)$. A higher information entropy indicates less information content. The proposed cryptosystem's information entropy of plain images and associated encrypted images Table 5 demonstrates this. According to the findings, the encryption algorithm only discloses a limited bit of image information.

Table 5.
Shows the result of Information entropy.

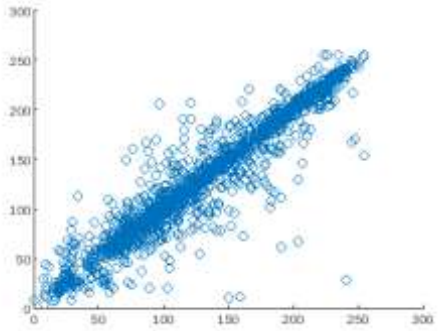
Plain Images (256×256)	The entropy of plain images	The entropy of cipher images (Our Algorithm)
Lena	7.7598	7.9990
Baboon	7.2630	7.99913
Peppers	7.7300	7.99912

(a)Plain Image

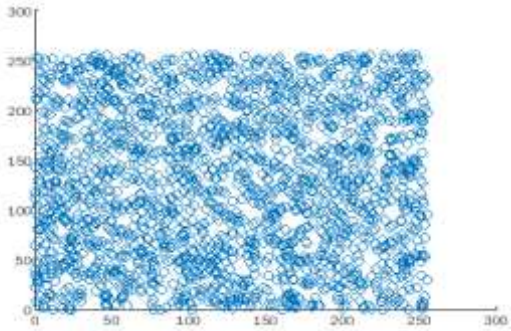


(b) Cipher Image

Pixels distribution in horizontal

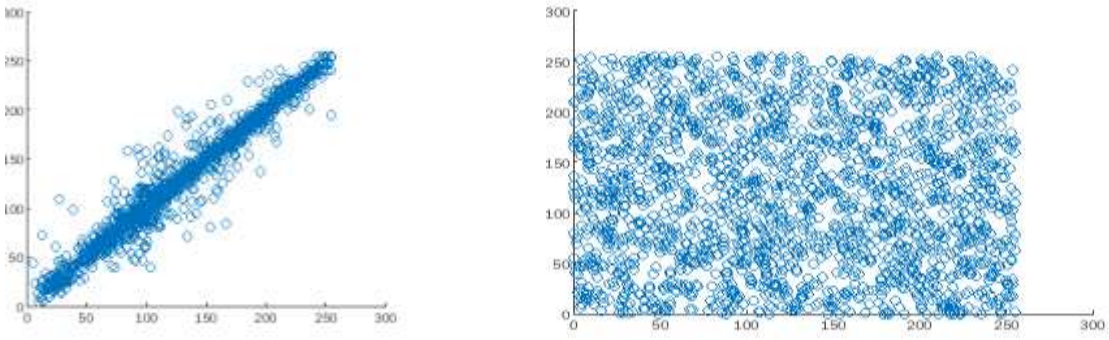


(c)



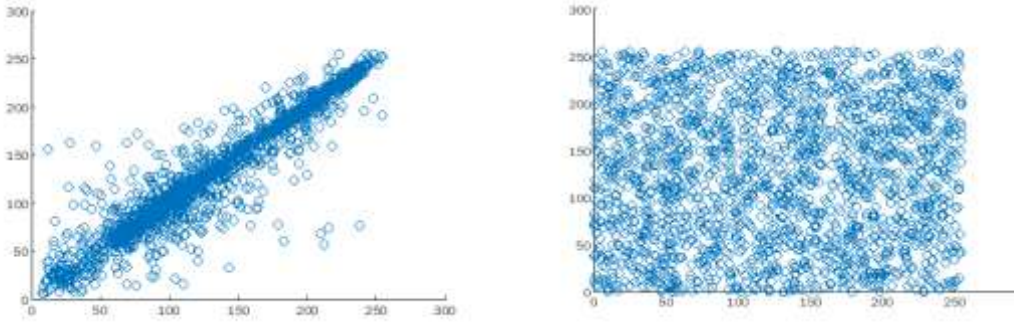
(d)

Pixels distribution in vertical



(e) (f)

Pixels distribution in diagonal



(g) (h)

Figure 5. Shows the correlation distributions for plain and cipher in horizontal, vertical, and diagonal directions

5.1.4 Differential Attack

By measuring the difference of the corresponding cipher-image, the differential attack is an efficient method for detecting statistical patterns in the distribution of plain images. An attacker would often make a tiny alteration to the plain picture before using cryptographic techniques to encrypt the image before and after any changes. They then try to figure out how the plain picture and the cipher image are related. The main objective of the differential analysis is to figure out how sensitive the plain image is. The unified average changing intensity (UACI) and the number of pixels changes rate (NPCR) are two main parameters used to compare cipher images. (NPCR) calculates the difference in pixel counts among both two cipher-images as a percentage. (UACI) calculates the average intensity of difference between two cipher images. (NPCR) and (UACI) are defined by equations (7) and (8), respectively.

$$D(i,j) = \begin{cases} 0, & C(i.j) = C(i,j)' \\ 1, & C(i.j) \neq C(i,j)' \end{cases} \quad (6)$$

$$NPCR = \frac{\sum_{ij} D(i,j)}{\mathrm{M}\times\mathrm{N}} \times 100\% \quad (7)$$

$$UACI = \frac{1}{M\times N}\left[\sum_{ij} \frac{|C(i.j)-C(i,j)'|}{255}\right] \times 100\% \quad (8)$$

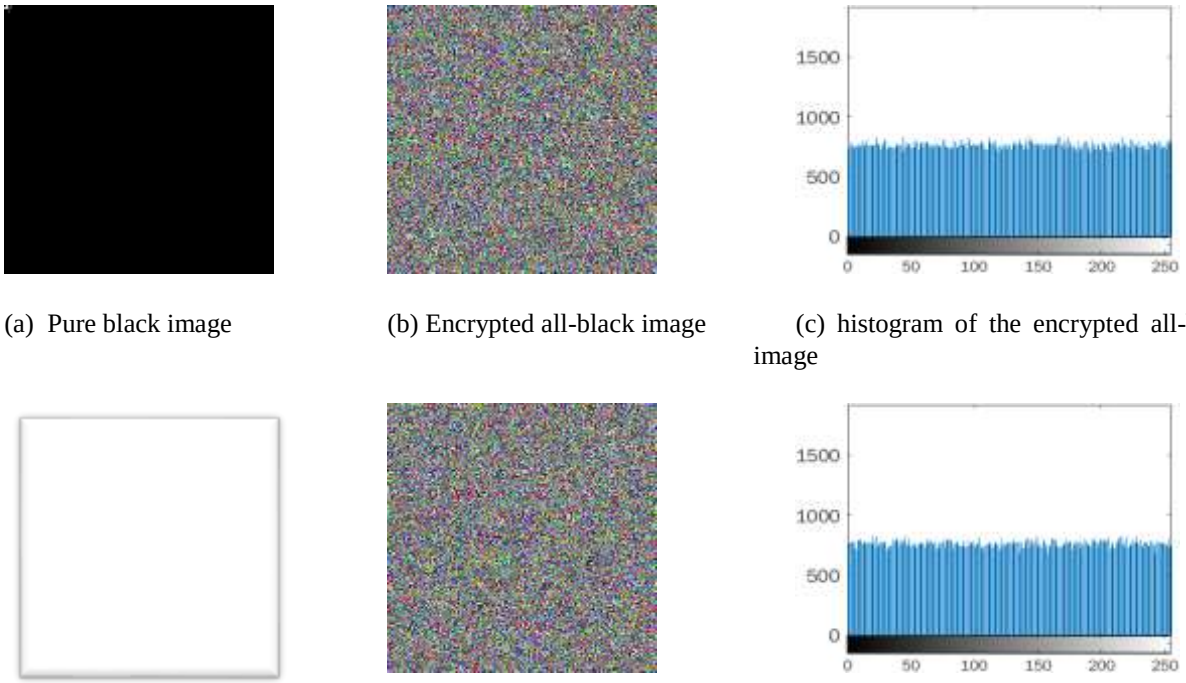
The size of the cipher-images C and C` is denoted by M×N. Table 6 shows the average NPCR and UACI results for a 1-bit modification in a plain image pixel close to the perfect 99.6094% and 33.4635%. The research results show that the algorithm is resistant to differential attacks.

Table 6.
Shows the average NPCR and UACI results.

Images	NPCR (%)	UACI (%)
Lena	99.60 %	33.43%
Baboon	99.54 %	28.75 %
Peppers	99.54%	28.73%

5.1.5 Chosen-Plaintext Attack

Kirchhoff's' cryptographic principles assert that encryption and decryption techniques in a cryptosystem are known or visible. As a result, the cryptosystem's security is determined by the key rather than the encryption scheme itself. The attacker acquires the valid equivalent key by investigating the relationship between the key and the cipher-text or the plaintext and cipher-text. The primary approaches are the cipher-text-only attack, KPA, CPA, and selected cipher-text attack (CCA). CPA is acknowledged as the most powerful assault method among these; hence the capacity of the existing algorithm to withstand CPA is examined here. This whole encryption technique yields both "pure white image" and "pure black image" pictures of the encrypted photos and the related histograms, as illustrated in figure 6. Figure 6's histogram is uniformly dispersed. Table 7's information entropy is 7.9991. The correlation coefficients are near zero. It can be demonstrated that selecting pure white or black pictures makes it difficult for an attacker to assess the corresponding key. To summarise, the suggested technique is resistant to the selected plaintext attack.



(a) Pure black image (b) Encrypted all-black image (c) histogram of the encrypted all-black image

(d) Pure white image (e) Encrypted all-white image (f) histogram of the encrypted all-white image

Figure 6. Test results with pure black and pure white images

Table 7.
The information entropy and correlation coefficients of the test images.

Images	The entropy	Correlation Coefficients		
		Horizontal	Vertical	Diagonal
Pure black image	0	-	-	-
Encrypted Pure black image	7.99914	-0.0071	0.0060	0.0046
Pure white image	0	-	-	-
Encrypted Pure white image	7.99911	0.0025	-0.0043	0.0021

5.2. Ability to resist exhaustive attack

5.2.1 Key Space Analysis

A good encryption algorithm should have sufficient key space to withstand exhaustive attacks. The suggested algorithm's key consists of six keys: g_0, μ_0, g_1, μ_1, g_2, μ_2. To facilitate comparison, the index portion is expressed as a positive value following the international standard IEEE 754. Because the significant digit of a double-precision floating-point type is 52 bits, the size of the control parameter's key pace will be $2^{52\times6} = 2^{312}$ greater than 2^{128}. The results reveal that it is nearly impossible to accurately attack the method using brute force, indicating that the encryption technique can withstand attacks.

5.2.2 Key sensitivity analysis

Encryption efficiency is important for assessing the encryption scheme's overall performance. Multiplying floating point numbers takes the most time in computations for analysis of chaos-based encryption schemes. Key sensitivity analysis is a standard attack technique that encrypts plain images with pairs of security keys linked by a slight difference. Statistical insights are obtained by measuring the differences between the related cipher images. The cipher images are different when an encryption algorithm encrypts the same plain image with two slightly different keys. Using the (NPCR) equation (7) and the (UACI) equation (8), the difference may be calculated. Table 8 shows the results of (NPCR) and (UACI) for key sensitivity analysis, indicating a major difference between the two cipher images.

Table 8.
Shows the results of NPCR and UACI for key sensitivity analysis

Image	g_2	μ_2	NPCR (%)	UACI (%)
Lena (256×256)	0.01	3.950000000000001	99.619%	33.450%
	0.010000000000001	3.95	99.615%	33.481%

5.3. Computational complexity analysis

The computational complexity of an encryption algorithm has a large impact on its performance. The time complexity in each step is presented below to help evaluate the computational complexity of the proposed approach. The first stage is the breakdown of the picture matrix. As a result, the temporal complexity is

$O(M \times N \times 3)$, where M and N are the picture dimensions. The DNA-based operations are the prominent module of the technique provided here, with the complexity for DNA encoding and decoding and for DNA addition and XOR $(M \times N \times 3 \times 4)$. As a result, the suggested technique has an overall computational complexity of O $(M \times N \times 12)$.

6. Discussion

The research offers a unique image encryption system based on DNA bases probability and a three-dimensional logistic map for secure image storage and transmission. The suggested method was put through a series of tests to ensure its stability and quality. According to the experimental results, the suggested algorithm may resist several known attack methods against images. Employing three one-dimensional logistic maps with DNA bases probability, we design a unique approach to generate a close link between the plain image and its cipher image to avoid chosen-plaintext attack and differential assault. Table 9 shows that the proposed cryptosystem effectively reduces the correlation between two adjacent pixels in the horizontal, vertical, and diagonal directions, according to the results of comparisons. Tables 10, Table 11, and Table 12 show that the algorithm suggested in this research is close to the ideal value and performs better than other algorithms discussed in other literature, showing that it has a great encryption effect. Table 13 shows that when the proposed algorithm is compared to previous approaches [37-39], the suggested

method has reduced computational complexity. When entropy is compared, the proposed algorithm performs better in terms of protection than other algorithms. As a result, our proposed encryption algorithm is resistant to differential attacks, and the encryption's security performance is excellent.

Table 9.
Correlation Coefficients for Lena image comparison

Plain Image		**Cipher Image**					
Lena (256×256)		Proposed	X. Chai et al. (2019) [32]	S. S. Asker et al. (2019) [33]	T. Li et al. (2020) [34]	Y. Wan et al. (2020) [35]	J. Ferdush et al. (2021) [36]
Horizontal	0.9806	-0.0070	0.0070	0.0005	0.0044	0.0020	0.0414
Vertical	0.9601	0.0011	-0.0102	0.0017	0.0015	0.0105	-0.0342
Diagonal	0.9383	0.0007	0.0030	-0.0025	0.0019	0.0019	0.1083

Table 10.
Comparison of Entropy values

Image (256×256)	**Proposed scheme**	S.S.Askar et al. (2019) [33]	T. Li et al. (2020) [34]	Y. Wan et al. (2020) [35]	J. Ferdush et al. (2021) [36]	NLCA 2021[1]
Lena	7.9990	7.9981	7.9894	7.9974	7.9974	7.9970
Baboon	7.99913;2	7.9973	7.9893	-	-	7.9973

Table 11.
Comparison of NPCR values

Image (256×256)	**Proposed scheme**	J. Ferdush et al. (2021) [36]	NLCA 2021[1]
Lena	99.60	99.37	99.5758

Table 13.
Comparison of Complexity analysis

Parameter	**Proposed scheme**	[37]	[38]	[39]
Complexity	O (M × N × 12)	O (M × N × 12)	O (M × N × 12)	O (M × N × 24)

7. Conclusion

With the advancement of advanced cloud computing technologies, security remains one of the most pressing issues in the cloud computing world. Use security mechanisms and apply them correctly and consistently to keep end users safe. These cryptographic techniques play an important role in communication reliability, where encoding and decoding time. Only the authorized user has access to the data in our proposed work. If an unauthorized user obtains data by accident or on purpose, he must decode it at each level, which is a challenging process in the absence of a valid key. To increase the complexity and security, we offer three levels of security. Multilevel encryption is believed to give greater security than single-level encryption; hence we provide three levels of encryption based on distinct source procedures to increase complexity and security. DNA encoding and chaotic logistic maps ensure customer data's safety and confidentiality compared to other algorithms.

References

[1] Thabit, F., Alhomdy, S., & Jagtap, S. (2021). Security analysis and performance evaluation of a new lightweight cryptographic algorithm for cloud computing. Global Transitions Proceedings, 2(1), 100–110. doi:10.1016/j.gltp.2021.01.014.

[2] Mahmood, L. G. S. (2017). Data security protection in cloud computing by using encryption. Kirkuk University Journal-Scientific Studies, 12(4), 276-286.

[3] Che, J., Duan, Y., Zhang, T., & Fan, J. (2011). Study on the security models and strategies of cloud computing. Procedia Engineering, 23, 586-593.

[4] Pansotra, E. A., & Singh, E. S. P. (2015). Cloud security algorithms. International journal of security and its applications, 9(10), 353-360.

[5] Parameshachari, B. D., Kiran, R. P., Rashmi, P., Supriya, M. C., Rajashekarappa, M. B., & Panduranga, H. T. (2019, January). Controlled partial image encryption based on LSIC and chaotic map. In ICCSP (pp. 60-63).

[6] Xuejing, K., & Zihui, G. (2020). A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system. Signal Processing: Image Communication, 80, 115670.

[7] Pareek, N. K., Patidar, V., & Sud, K. K. (2006). Image encryption using chaotic logistic map. Image and vision computing, 24(9), 926-934.

[8] Mondal, B., Singh, S., & Kumar, P. (2019). A secure image encryption scheme based on cellular automata and chaotic skew tent map. Journal of information security and applications, 45, 117-130.

[9] Ping, P., Xu, F., Mao, Y., & Wang, Z. (2018). Designing permutation–substitution image encryption networks with Henon map. Neurocomputing, 283, 53-63.

[10] Asim, M., & Jeoti, V. (2007, November). On improving an image encryption scheme based on chaotic logistic map. In 2007 International Conference on Intelligent and Advanced Systems (pp. 758-763). IEEE.

[11] Yang, B., & Liao, X. (2018). A new color image encryption scheme based on logistic map over the finite field ZN. Multimedia Tools and Applications, 77(16), 21803-21821.

[12] Li, R., Liu, Q., & Liu, L. (2019). Novel image encryption algorithm based on improved logistic map. IET Image Processing, 13(1), 125-134.

[13] Chen, J. X., Zhu, Z. L., Fu, C., Yu, H., & Zhang, L. B. (2015). A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. Communications in Nonlinear Science and Numerical Simulation, 20(3), 846-860.

[14] Jolfaei, A., & Mirghadri, A. (2011). Image encryption using chaos and block cipher. Computer and Information Science, 4(1), 172.

[15] Meng, L., Yin, S., Zhao, C., Li, H., & Sun, Y. (2020). An Improved Image Encryption Algorithm Based on Chaotic Mapping and Discrete Wavelet Transform Domain. Int. J. Netw. Secur., 22(1), 155-160.

[16] Evans, A. N., & Rooney, B. J. (2010). Human characteristics; evolutionary perspectives on human mind and kind. SciTech Book News, 1.

[17] Han, C. (2019). An image encryption algorithm based on modified logistic chaotic map. Optik, 181, 779-785.

[18] Akhavan, A., Samsudin, A., & Akhshani, A. (2017). Cryptanalysis of an image encryption algorithm based on DNA encoding. Optics & Laser Technology, 95, 94-99.

[19] Zhang, Q., Guo, L., & Wei, X. (2010). Image encryption using DNA addition combining with chaotic maps. Mathematical and Computer Modelling, 52(11-12), 2028-2035.

[20] Chai, X., Fu, X., Gan, Z., Lu, Y., & Chen, Y. (2019). A color image cryptosystem based on dynamic DNA encryption and chaos. Signal Processing, 155, 44-62.

[21] Enayatifar, R., Guimarães, F. G., & Siarry, P. (2019). Index-based permutation-diffusion in multiple-image encryption using DNA sequence. Optics and Lasers in Engineering, 115, 131-140.

[22] Sokouti, M., & Sokouti, B. (2018). A PRISMA-compliant systematic review and analysis on color image encryption using DNA properties. Computer Science Review, 29, 14-20.

[23] ur Rehman, A., Liao, X., Ashraf, R., Ullah, S., & Wang, H. (2018). A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2. Optik, 159, 348-367.

[24] Liu, Y., Tang, J., & Xie, T. (2014). Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map. Optics & Laser Technology, 60, 111-115.

[25] Gastermann, B., Stopper, M., Kossik, A., & Katalinic, B. (2015). Secure implementation of an on-premises cloud storage service for small and medium-sized enterprises. Procedia Engineering, 100, 574-583.

[26] Vanishreeprasad, S., & Pushpalatha, K. N. (2015). Design and implementation of hybrid cryptosystem using AES and Hash Function. IOSR Journal of Electronics and Communication Engineering, 10(3), 18-24.

[27] Meenakumari, M., & Athisha, G. (2014). Improving message authentication by integrating encryption with hash function and its VLSI implementation. Int. J. Innov. Res. Electr. Electron. Instrum. Control Eng.

[28] Panda, M. (2016, October). Performance analysis of encryption algorithms for security. In 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES) (pp. 278-284). IEEE.

[29] Khan, S. S., & Tuteja, R. R. (2015). Security in cloud computing using cryptographic algorithms. International Journal of Innovative Research in Computer and Communication Engineering, 3(1), 148-155.

[30] Gong, Z., Nikova, S., Law, Y. W., Juels, A., & Paar, C. (2012). RFID. Security and Privacy: 7th International Workshop, RFIDSec 2011, Amherst, USA, June 26-28, 2011, Revised Selected Papers.

[31] Princy, P. (2015). A comparison of symmetric key algorithms DES, AES, Blowfish, RC4, RC6: A survey. International Journal of Computer Science & Engineering Technology (IJCSET), 6(05).

[32] Chai, X., Zhang, J., Gan, Z., & Zhang, Y. (2019). Medical image encryption algorithm based on Latin square and memristive chaotic system. Multimedia Tools and Applications, 78(24), 35419-35453.

[33] Askar, S. S., Karawia, A. A., Al-Khedhairi, A., & Al-Ammar, F. S. (2019). An algorithm of image encryption using logistic and two-dimensional chaotic economic maps. Entropy, 21(1), 44.

[34] Li, T., Du, B., & Liang, X. (2020). Image encryption algorithm based on logistic and two-dimensional lorenz. IEEE Access, 8, 13792-13805.

[35] 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.

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

[37] Chidambaram, N., Raj, P., Thenmozhi, K., & Amirtharajan, R. (2020). Advanced framework for highly secure and cloud-based storage of colour images. IET Image Processing, 14(13), 3143-3153.

[38] Kumar, M., Iqbal, A., & Kumar, P. (2016). A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography. Signal Processing, 125, 187-202.

[39] Wu, X., Kurths, J., & Kan, H. (2018). A robust and lossless DNA encryption scheme for color images. Multimedia Tools and Applications, 77(10), 12349-12376.

[40] AbdElminaam, D. S., Kader, H. M. A., Hadhoud, M. M., & El-Sayed, S. M. (2013). GPS test performance: Elastic execution applications between mobile device and cloud to reduce power consumption. International Journal of Computer Science and Network Security (IJCSNS), 13(12),

[41] Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M. (2009). Energy efficiency of encryption schemes for wireless devices. *International Journal of Computer Theory and Engineering*, *1*(3), 302.

[42] Salama, D., Kader, H. A., & Hadhoud, M. (2011). Wireless network security still has no clothes. *International Arab Journal of e-Technology*, *2*(2), 112-123.

[43] Abd Elminaam, D. S., Abdual-Kader, H. M., & Hadhoud, M. M. (2010). Evaluating The Performance of Symmetric Encryption Algorithms. *Int. J. Netw. Secur.*, *10*(3), 216-222.

[44] Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M. (2009). Tradeoffs between energy consumption and security of symmetric encryption algorithms. *International Journal of Computer Theory and Engineering*, *1*(3), 325.

[45] Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M. (2009). Analyzing the energy consumption of security algorithms for wireless lans. *International Journal of Computer Theory and Engineering*, *1*(4), 334.

[46] Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M. (2009). Measuring and Reducing Energy Consumption of Cryptographic Schemes for Different Data Types. *International Journal of Computer Theory and Engineering*, *1*(3), 1793-8201.

[47] Elminaam, D. A., Kader, H. A., & Hadhoud, M. M. (2009). Evaluating the Effects of Cryptography Algorithms on power consumption for wireless devices. *International Journal of Computer Theory and Engineering*, *1*(3), 1793-8201

[48] Taha, A. A., Elminaam, D. S. A., & Hosny, K. M. (2018). An improved security schema for mobile cloud computing using hybrid cryptographic algorithms. *Far East Journal of Electronics and Communications*, *18*(4), 521-546.

[49] Abdul, D. S. (2018). 'Reliable the resources of mobile devices in cloud computing. Int. J. Adv. Comput. Technol., 10(1), 61-70.

[50] AbdElminaam, D. S., Toony, A. A., & Taha, M. (2020). Resource Allocation in the Cloud Environment Based On Quantum Genetic Algorithm Using Kalman Filter with ANFIS. IJCSNS, 20(10), 10.