Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

# Secure Imaging in 6D Chaos: A DNA-Encoded Approach for Enhanced Privacy

**[1]Shantanu Ranjan, [2]Romil Singh, [3]Shivam Sharma, [4]Deependra Sinha**

*[1234]Department of Electroniccs and Communication, Galgotia's College of Engineering and Technology, India.*

**Abstract.** Images are encoded to prevent unauthorized access to sensitive data. Although chaos-based picture encryption algorithm is being widely utilized in many industries, the widespread use of low-dimensional chaos increases questions regarding the security of the encryption. The study suggests a framework for encrypting pictures that uses DNA Encryption and a 6D high-dimensional chaotic system to handle this. First, random chaos sequences are used to undergo diffusion and shuffling of the original image sequences, and then there is further diffusion and shuffling at the DNA level. An encrypted image is then created by combining the encoded sequences that are generated. The experiments' findings demonstrate that the recommended algorithm performs better in terms of picture complexity (key space over $2^{300}$), pixels correlations and image entropy (close to 8). Furthermore, in comparison to previous references, the algorithm demonstrates excellent encryption quality.

**Keywords:** Chaos Theory, DNA-Encoding, 6D Chaos, Encryption, Decryption.

## Introduction

In light of technological progress in communication, an immense volume of images is now circulated across public networks. Diverse sectors such as military image repositories and medical imaging platforms require a more robust and expedient security infrastructure to collect & transmit electronic pictures. [1-3]. Because of this, protecting the safety of online photos has emerged as a critical priority. Consequently, three main approaches have been suggested: steganography, encryption, and watermarking. [4]. Because of its high level of security, the encryption technique has emerged as a crucial tool in this regard. Many different methods have been used to introduce a multitude of image encryption techniques in recent decades. [5]. Numerous ciphers such as DES, IDEA, AES, RSA, among others, have been employed for encryption purposes. Nevertheless, most of these approaches are primarily suited for textual data and are ill-suited for image encryption. This limitation arises mainly from the inherent vulnerability of images, including inter-pixel correlation, extensive data volume, and redundancy. To tackle this challenge, researchers have introduced a diverse range of encryption schemes. [5–9]. Compared to traditional cryptology methods, chaos-based encryption procedures are more random, unpredictable, and non-periodic because of their susceptibility to the starting conditions and system factors. [10, 11]. As a result, advances in chaos-based algorithms for encryption have been made quickly. Diffusion operations in chaotic sequences are a common technique in picture encryption. Chaotic cryptosystems generally use sequences to reorganize the original pixel arrangement of an image.

Chaotic systems are classified as high-dimensional or low-dimensional. Multidimensional systems produce three or more chaotic streams, while low-dimensional systems usually produce one or two. Habustu et al. described picture encryption technique done on chaos theory in 1991 [12] This breakthrough ignited the proliferation of numerous chaos-based encryption algorithms. As an example, Hua Z created an image encryption method predicated upon the '2D Logistic-Sine coupling map'[13]. Pareek.N created a method for encryption that leverages a single-dimensional chaos logistic map that uses the encrypted key which is updated after encrypting every frame that consists of 16 image pixel[1]. Chanil Pak introduced a novel technique for encrypting colored pictures using a newly developed single-dimensional chaos map[14], Majority of low-dimensional chaos-based picture encryption methods were Outperformed by superior outcomes of several picture encryption techniques [15–17].

However, because of security concerns, encryption techniques that operate in low dimensions are unable to meet the requirements, which has led towards the faster development for encryption methods that can operate in large dimensions. Guarnong developed a novel picture encryption approach employing 3D chaotic Cat maps [2], which is a noteworthy development in the area of picture-based encryption techniques based on hyper-chaotic processes. Using a 3D baker map, Mao YB suggested a quick photo encryption method [9, 10], demonstrating better temporal complexity in comparison to the other techniques mentioned in his research. Adrian-Viorel Diaconu proposed a technique for scrambling color images using Pixel Transposition Digital Chaos and Knight's Moving Rules across RGB Channels [18].

Following the updated Henon map, Writer proposed a color picture encryption method [19]. In comparison to the previous Henon map, this upgraded version shows richer chaotic features and a greater degree of complexity, leading to better efficiency during encryption. Apart from these, numerous other researchers have developed a plethora of picture encryption techniques rooted on multidimensional chaotic systems [20–22]. Because DNA computing has some advantages over other computer platforms, including big data spaces, exceptionally minimal energy usage, and massive scale concurrent processing, encryption techniques centered on hyper-chaos and encoded DNA have gained popularity in recent years [15–17, 22]. In addition, because of the unique characteristics involving bit-level permutation, a lot of picture encryption methods employ it to jumble the association among pixels [19, 23, 24]. In addition, certain strategies matching a weak chaotic system with other ways can give excellent results. [25] devised an approach in 2022 that incorporated a complex system with Sub-block Spiral Scans. They also used Matrix Multiplication. Similarly, [26] put proposed a rapid picture encryption technique built on one-channel cryptography and chaotic systems.

The previously suggested approaches primarily focus on low-dimensional chaos systems, which often lack sufficient complexity. Alternatively, some methods rely on DNA coding, but they are frequently vulnerable to hacking. To overcome these limitations, we propose a color picture method of encryption based on the encoding of DNA and a six-dimensional hyper-chaotic system. The distinct role and novel advancements in this study are delineated as following. Initially, we utilize a hyper-chaotic system with six-dimensional of greater complexity as the source of randomized streams. The output consists of six unique chaotic streams, which are described by the key and evaluation of the raw image. Furthermore, this paper categorizes these streams into two distinct groups to account for permutation and diffusion. In order to enhance the power and safety of the permutation process, we employ pixel-level and DNA-level permutations, which result in a substantially reduced correlation between the initial picture and the image that was encrypted. Without a doubt, both of these permutation processes strengthen the algorithm's ability. We perform diffusion operations at the pixel and molecular level to the chaotic pictures after permutation. This paper evaluates the algorithm using key-space evaluation, key sensitiveness, correlation evaluation, and other techniques. The outcomes demonstrate that the algorithm we developed performs better than existing methods.

The reset organizing paper include; Chaotic System, DNA Encoding, Proposed Methodology, System Parameters, Histogram Analysis, Efficiency Measurement, Key space Synthesis, Correlation, Entropy Analysis and Encryption Quality.

## Chaotic System

Many academics nowadays have suggested using chaos-based picture encryption methods. While some of them employ hyper-chaotic systems in the encryption system, others use low-dimensional chaos to produce pseudo-random patterns for scrambling the original picture. Formula 1 represents the Lorenz Chaos system formula, which was developed in 1963 [27]. Formula 1 uses the Characters a, b, and c stand for initial conditions, whereas characters x, y, and z stand for system values.

$$L(x)\begin{cases}\dot{x} = a(y-x)\\ \dot{y} = cx - y - xz\\ \dot{z} = -bz + xy\end{cases} \tag{1}$$

As time passed, the standard Lorenz chaotic system became unable to meet the ever-increasing communication security needs. This resulted in the proposal. of using higher-dimensional chaotic systems. The traditional Lorenz system was modified in 2009 to incorporate both linear and non-linear feedback controllers, which resulted in the development of the ensuing 5D hyper-chaos system [28].

$$L(x)\begin{cases}\dot{x} = \sigma(y-x) + u\\ \dot{y} = rx - y - xz - v\\ \dot{z} = -\beta z + xy\\ \dot{u} = k_1 u - xz\\ \dot{v} = k_2\end{cases} \tag{2}$$

Five-dimensional hyper-chaos system is characterized from control parameters such as σ, r, k1, B, and k2, where k1 and k2 are both positive. The system develops a hyper-chaotic attractor featuring 3 positive Lyapunov coefficients alongside one equilibrium. In general, a system of chaos that has greater hyper-chaotic attractors generally more complicated. Therefore, it is comprehensible why the functioning of the five-dimensional hyper-chaos system tends to be more sophisticated compared to standard Lorenz system.

Nonetheless, the desire for safety is relentless. To augment the complication and unpredictability of in system, concept of six-dimensional hyper-chaos system was introduced. This work utilizes the six-dimensional hyper-chaos system introduced by [29]. It is produced by combining a one-dimensional linear system into a five-dimensional hyper-chaos system stated in formula number 3.

$$L(x)\begin{cases}\dot{x} = \sigma(y - x) + u \\ \dot{y} = cx - y - xz - v \\ \dot{z} = -\beta z + xy \\ \dot{u} = du - xz \\ \dot{v} = -ky \\ \dot{w} = hw + ly\end{cases} \quad (3)$$

Thirteen terms make 6D hyper-chaotic system that consists of a total of seven different factors. It also includes 6 system values. Among them, the constant parameters are a, b, c, and h; the coupling parameter is l; and the two control factors that affect the behavior of the system and its bifurcations are d and k. In contrast to the hyper-chaotic system in 5D, there are six Lyapunov exponents in the 6D version. Positive results from four of them indicate that the six-dimensional hyper-chaos system exceeds the 5D variant with respect to of complication and unpredictable nature. In Qigui Yang's study [29], the possible values of the other variables is given, and a, b, c, and h is identified as fixed variables.

## Dna Encoding

4 distinct base type i.e. adenine i.e. (A), thymine i.e. (T), cytosine i.e. (C), and guanine i.e. (G)—and dually parallel to one another strands are involved to make up a typical DNA molecule. With A connecting solely to T. Also, G is bonding only to C, these strands/bases show a supportive link. Encryption dependent on the use of DNA is often referred as biological encryption [30]. Since traditional biological encryption is bound by expensive prices and tight scientific specifications, pseudo-DNA technology has come to prominence as a crucial part of cryptography [31]. In Table 1. only eight of the four pairings of the 24 encodings tries Watson-Crick supplementing criteria.

**TABLE 1. Coding Conditions for $DNA_{encoding}$**

| Coding Number | One | Two | Three | Four | Five | Six | Seven | Eight |
|---|---|---|---|---|---|---|---|---|
| 00 | A | A | T | T | G | G | C | C |
| 01 | C | G | G | C | A | T | A | T |
| 10 | G | C | C | G | T | A | T | A |
| 11 | T | T | A | A | C | C | G | G |

Several binary operations were performed by DNA nucleoid that are demonstrated in Table 2. In this research, we apply simply the XOR operation. DNA encoding and decoding features were adeptly implemented in the encryption and decryption stages. So as the names of functions imply, DNA encoding converts a given picture data to closest DNA base, while DNA decoding does the opposite.

**TABLE 2.** XOR Conditions

| Rule | A | G | C | T |
|---|---|---|---|---|
| A | A | G | C | T |

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

## Proposed Methodology

Colour picture encryption method made in this study combines DNA encoding with a six-dimensional hyper chaos system. Three primary colour matrices make up the digital colour image: Red, Green, and Blue. As a result, all primary colour must be encrypted independently during the encryption process (encrypting R, G, and B). Fig. 1 shows the process diagram for the encryption scheme.

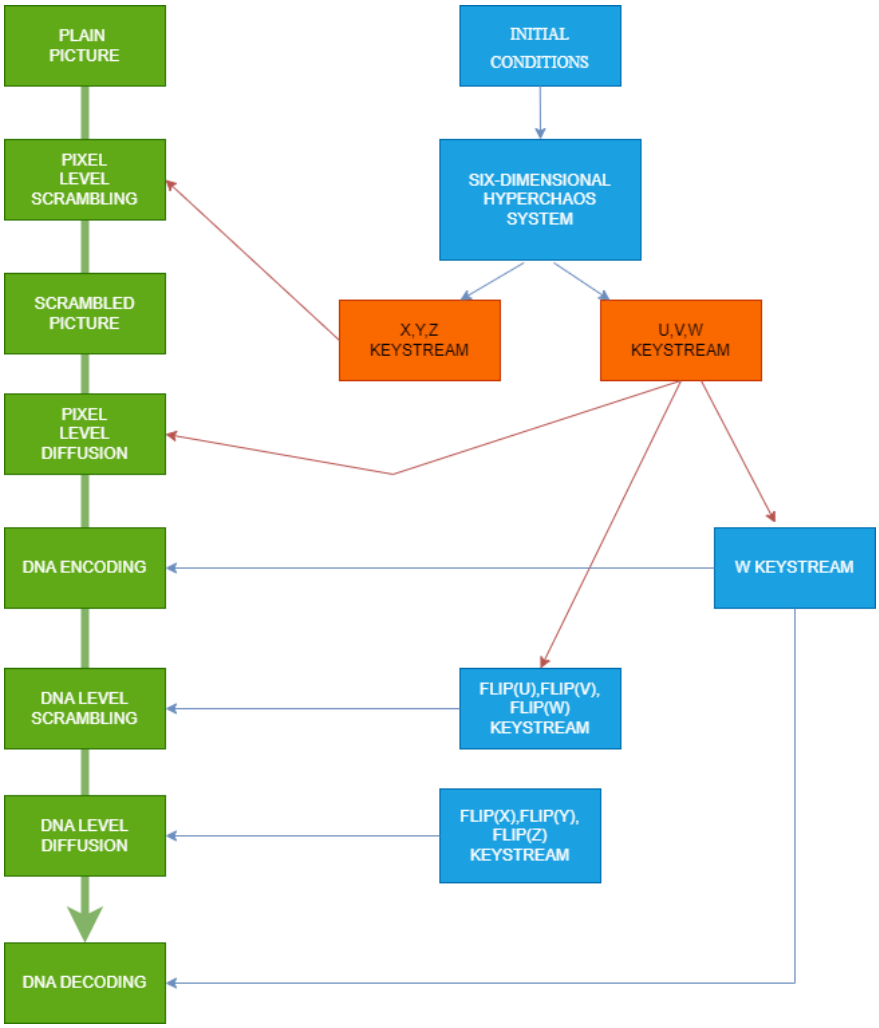



**FIGURE 1.** Proposed Methodology

### Algorithm (1): Picture Encryption

An M * N * 3 matrix, designated as P, represents a plain colour image at the start of the procedure for encrypting data, as shown in Fig. 1. The encryption algorithms matrix $A_1$ and this matrix match. The following is a breakdown of the encryption steps:

1. **Matrix Size Calculation (Step 1)**: Determine the dimensions of matrix $A_1$ by calculating its length (M) and width

(N).

2. **Initialization of System Values (Step 2):** Set the starting settings for system parameters (x, y, z, u, v, w) & key components, considering distortion from the system and sensitivity. Generate the system's values i.e. a, b, c, d, h, k, l utilising an unpredictable number generator inside the Monte Carlo approach, assuring unpredictability using the UNIX timestamp as the seed.

3. **Chaotic Sequence Generation (Step 3):** Transform the $A_1$ dimensions and the key into a six-dimensional hyperchaos system. Repeat procedure to construct sequences of chaos by repeating (threshold + max(M, N)) times, creating interference for boosting complexity.

4. **Chaos Sequence Derivation (Step 4)**: Compute six chaotic sequences using a specific formula, resulting in values x(t), y(t), z(t), u(t), v(t), and w(t).

$$\begin{cases} x(t) = |x(t-1) + i * (sin(x(t-1))), p| \\ y(t) = |y(t-1) + i * sin(y(t-1)) * sin(x(t-1)), p| \\ z(t) = |z(t-1) + i * sin(z(t-1)) * sin(y(t-1)) * sin(x(t-1)), p| \\ u(t) = |u(t-1) + i * sin(u(t-1)), p| \\ v(t) = |v(t-1) + i * sin(v(t-1) * sin(u(t-1)), p| \\ w(t) = |w(t-1) + i * sin(w(t-1)) * sin(v(t-1)) * sin(u(t-1)), p| \end{cases} \quad (4)$$

5. **Matrix Segmentation and Transformation (Step 5)**: Segment the chaotic sequences into two matrices ($S_1$ and $S_2$) and convert their data type from double to uint8. The resulting matrices $S_1$ and $S_2$ have dimensions M*$N$*3.

$$\begin{cases} S_1 = |floor(S_1, M * N) + 1, t \in [1, M * N * 3]| \\ S_2 = |floor(S_2, M * N) + 1, t \in [1, M * N * 3]| \end{cases} \quad (5)$$

6. **Decimal Permutation Operation (Step 6)**: Perform decimal permutation operations on matrix $A_1$ using chaotic matrix $S_1$. This operation involves segmenting $S_1$ into three parts ($S_1 1$, $S_1 2$, and $S_1 3$) to perform scrambling operations on each dimension (R, G, B) of the plain matrix A1.

$$\begin{cases} Swap(A_1 1(t), A_1 2(S_1 1(t)), t \in [1, M * N]) \\ Swap(A_1 2(t), A_1 2(S_1 2(t)), t \in [M * N, 2 * M * N]) \\ Swap(A_1 3(t), A_1 3(S_1 3(t)), t \in [2 * M * N, 3 * M * N]) \end{cases} \quad (6)$$

$$A_2(t) = A_1(t), t \in [1, M * N * 3] \quad (7)$$

7. **Decimal Diffusion Operation (Step 7)**: Apply decimal diffusion by carrying out bit XOR operation in the matrix $A_2$ and chaotic matrix $S_2$.

$$A_3 = bitxor(A_2(t), S_2)), t \in [1, M * N * 3] \quad (8)$$

8. **DNA Encoding (Step 8)**: Encode the diffused matrix $A_3$ into a DNA matrix $A_4$ using predefined coding rules from Table 1.

$$A_4 = DNA_{encoding}(A_3, w_i), w_i \in [1,8] \cap i \in [1,3 * M * N] \quad (9)$$

9. **DNA Scrambling (Step 9)**: Implement DNA scrambler on the DNA encoding matrix, utilizing iterative keystreams (flip(u), flip(v), flip(w)) to scramble the position of DNA bases.

$$Swap(A_4(t), A_4(S_4(t))), t \in [1, M * N * 3] \quad (10)$$

$$A_5(t) = A_4(t), t \in [1, M * N * 3] \quad (11)$$

10. **DNA Diffusion (Step 10)**: Conduct DNA level diffusion between matrix $A_5$ and DNA diffusion sequence $S_4$, applying defined XOR rules from Table 2.

$$A_6 = dnaxor(A_6(t), S_4(t)), t \in [1, M * N * 3]$$

(12)

11. **Decoding (Step 11)**: Transform the distributed DNA matrix $A_6$ into A using the decoding criterion and the decimal matrix generated by the chaotic sequence w. The encrypted picture is represented as Take C, where $w_i$ stands for the eight rules of permissible combinations. In the end, the function yields the encrypted image's decrypted decimal sequence or matrix.

$$C = DNA_{decoding}(A_6, w_i), w_i \in [1,8] \cap i \in [1,3 * M * N]$$

(13)

**Algorithm (2): Image Decryption**

The phases of the procedure for encryption are mirrored in the decryption process. To create chaotic sequences, the key is first fed into the hyperchaotic system. The decimal matrix is then created by encoding the cypher image into a DNA sequence using diffusion, permutation, and decoding operations. The plain image P is then recovered by performing the inverse operations known as decimal diffusion and decimal permutation.

## System Parameters

We have chosen the following crucial parameters, which have undergone thorough experimental validation: **Key: [x = four y = four z = three u = four v = five w = -2, a = ten b = 8/3, c = twenty-eight, d = two, h = 8.8]**. Furthermore, the level of interference has been set to 0.02, the initial number is 982451653, and the cutoff value is set to 700. Fig. 2 shows both the decryption and encryption procedures for colour images that are 512 By 512 pixels in size.

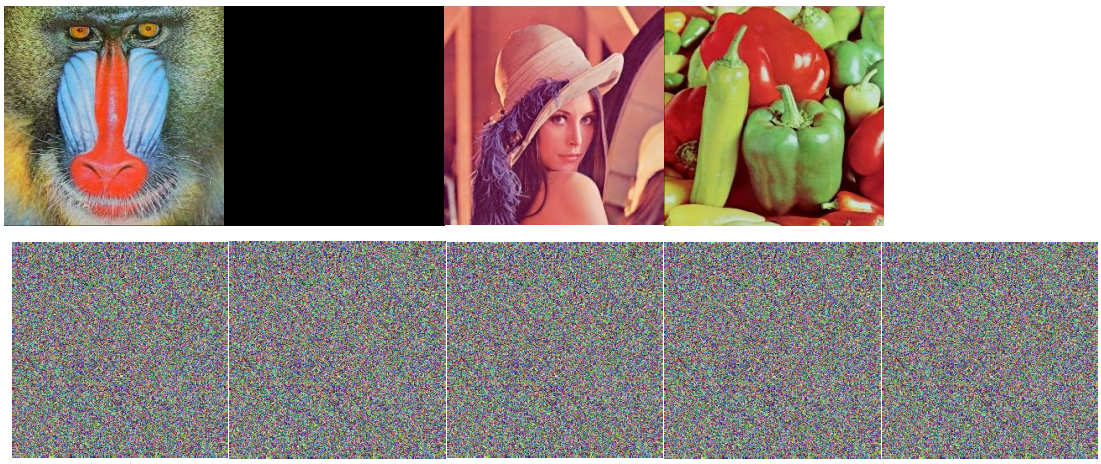
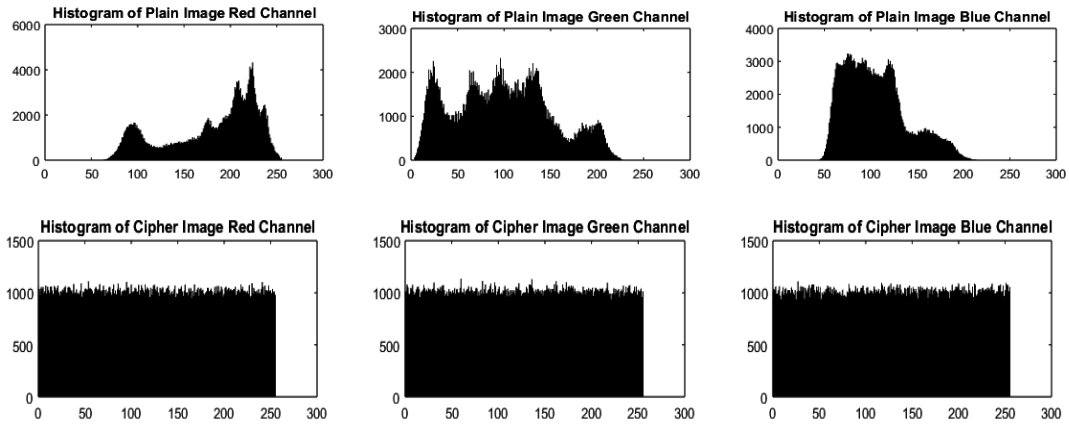


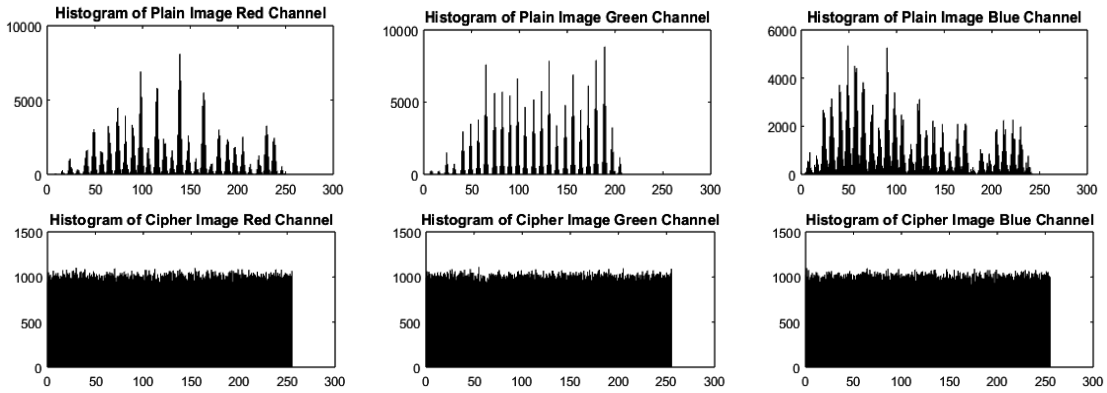
**FIGURE 2. a). Baboon (Plain & Cipher), b). Black (Plain & Cipher), c). Lena (Plain & Cipher), d). Peppers (Plain & Cipher), e). White (Plain & Cipher).**

## Histogram Analysis

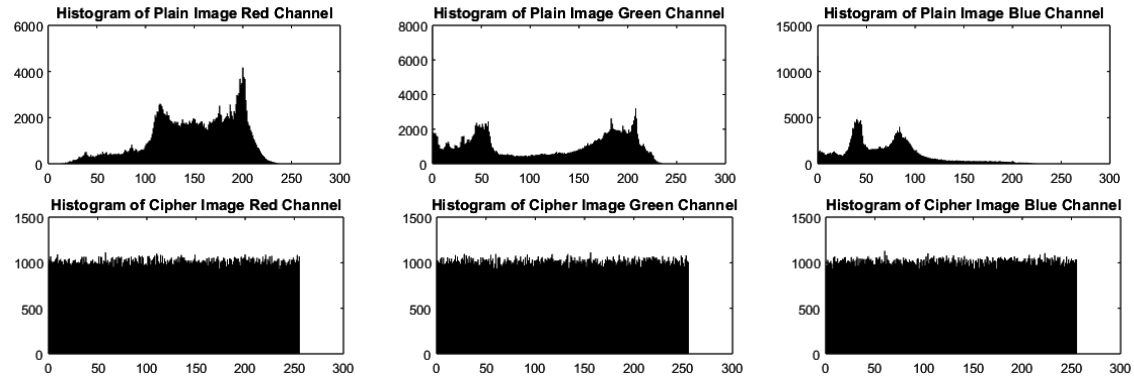
The cypher picture's graphical representation shows the variation of pixel information, that constitutes an essential way to ascertain if the method for encryption is capable of withstanding an attempt of statistical evaluation. A threat utilising statistical evaluation is one in which the attacker uses statistical evaluation to obtain the statistical features of encrypted pictures. It is the statistics of unique information that enable the chosen ciphertext attack. The three smoother histogram elements (R, G, and B) of the cypher picture in Fig. 3 indicate that it's unlikely for an intruder to decipher the data of the encrypted picture. Consequently, this makes the cypher picture less vulnerable to statistical attacks and more homogeneous. Three unique photos—"Lena," "Baboon," and "Pepper"—were chosen by the paper to be encrypted. Figure 3 illustrates the experimental findings. Taking into account the results, it is clear that each plain photo's initial histogram is erratic prior to encryption, as well as the related histogram illustrating the encrypted picture appears planar.




(a)




(b)




(c)

**FIGURE 3.** (a) RGB histograms for plain and cipher picture Lena, (b) RGB histograms for plain and cipher picture Baboon, (c) RGB histograms for plain and cipher picture Peppers.

## Performance Analysis

The Irrespective of the software's environment, the speed of execution of a picture's encryption technique is a crucial metric. The method was constructed using MATLAB and its speed capability was assessed on a laptop having Intel made Core i5-10300H CPU operating at 2.50 Gigahertz, 8GB of RAM, and Windows 11 as the OS. The references [18, 32] indicate that the data transfer rates for the proposed technique are 117.028 and 193.502 kilobytes per second (KB/s) correspondingly. The cost of the suggested approach on picture arrays of size 512x512 is 149.304 KB/s. Given the complexity of the technique presented in this study, together with other objective

criteria such as computer setup, it is very unlikely that the approach can consistently yield a significant improvement in image security. The algorithm's speed demonstrates its ability to achieve an appropriate equilibrium between safety and effectiveness.

## Key Space Synthesis

The term "key space" said to be a collection of valid and unique keys used in a certain encryption system. The level of security provided by an encryption system is closely correlated with the key space's size. An attacker attempting to forcibly unlock the data with every possible combination of keys will find it more difficult to compromise a monitored interaction with a larger value. The key space consists of all possible secret key combinations. There are six initial settings and seven system parameters in the concealed key of the picture encryption system. Since there are $10^{-15}$ details using a dependable laptop, equation (14) represents the first key space.

$$keyspace = \prod_{t=1}^{13} 10_t^{15} \quad (14)$$

The outcome of equation (14) is $10^{195}$, meaning it's substantially bigger than $2^{300}$. Its key space is sufficient for picture encryption approach, and it is more effective than several methods [19, 33, 34], namely $2^{160}$, $2^{256}$, and $10^{70}$. Hence, the recommended approach's key space is sufficient to repel a thorough attack.

## Correlation Analysis

Each of the pixels in a picture have a significant connection, and this relationship causes a picture to be simpler to break. More precisely, when adjacent pixels are correlated, it means that there is a connection. It should be imperative that the encrypted picture disrupt the relationship between neighbouring pixels in the original picture. Although it's not usually possible, in an ideal scenario there would be zero correlation within the encrypted image.

Random selections were made among 10,000 pairs of adjacent pixels for this purpose. We picked all 3 orientations and acquired encrypted photos. The mathematical equation is used to compute the coefficient of correlation in the following manner:

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \quad (15)$$

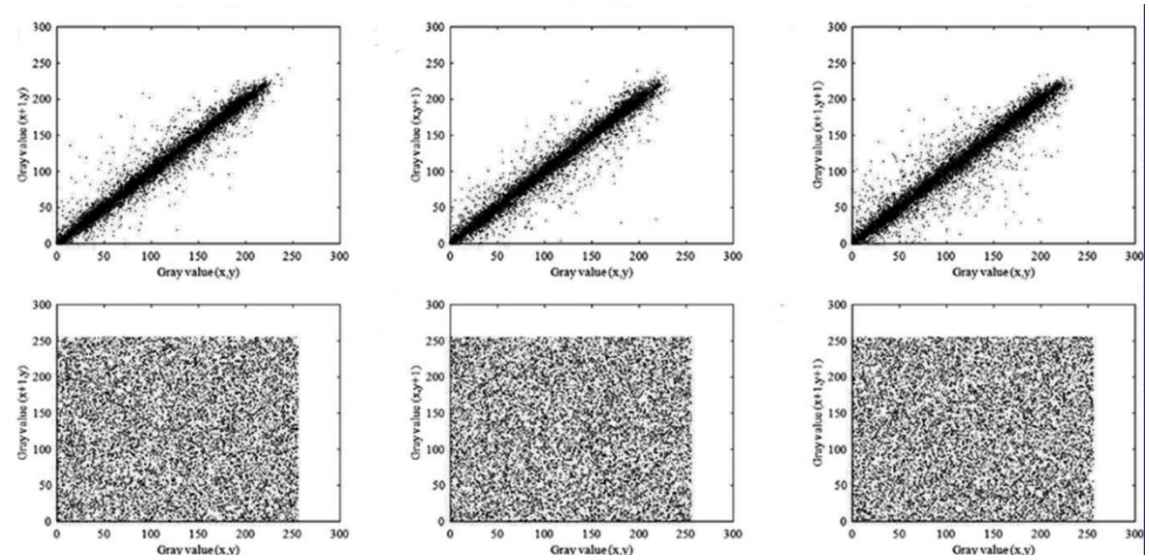
$$\rho X,Y \;=\; corr(X,Y) = \frac{cov(X,Y)}{\theta X \theta Y} = \frac{E[(X-\beta X)(Y-\beta Y)]}{\theta X \theta Y} \quad (16)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (17)$$

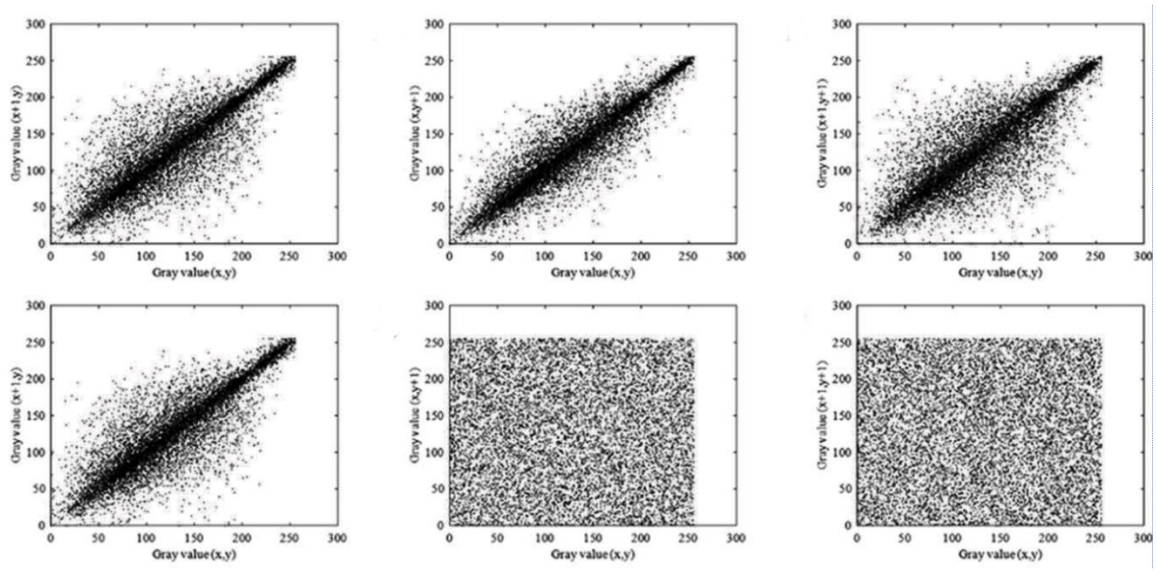
$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (18)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \quad (19)$$

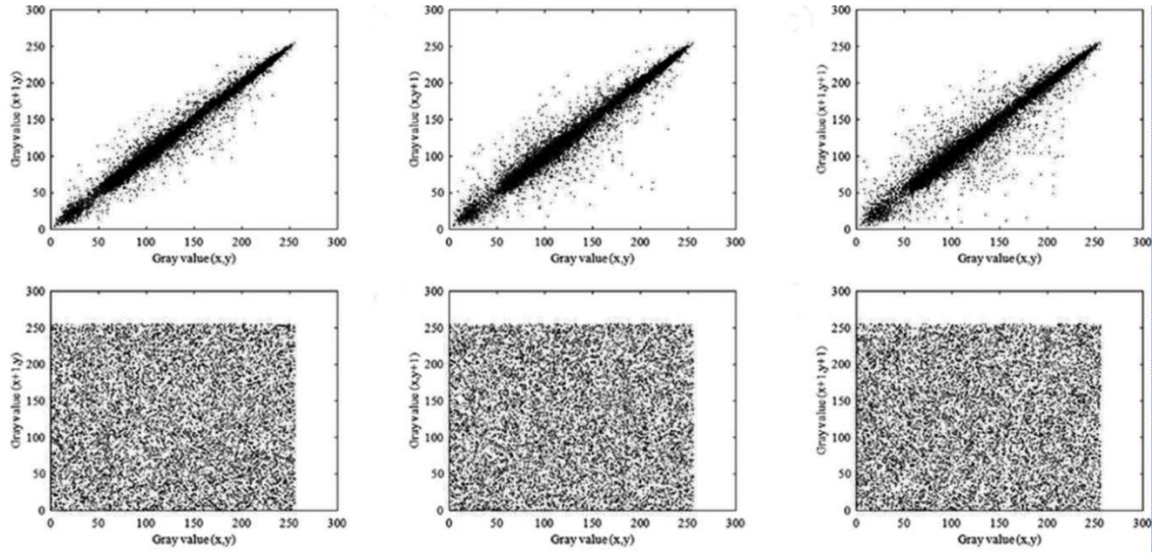
Fig. 4 demonstrate the relationship in the plain photo pattern & the encrypted photo pattern. The correlation coefficient values between the two adjacent pixels are shown in Table 3. indicating that there is almost no association between the pixels that are adjacent to one another.


Gray value (x,y)
Gray value (x+1,y)
Gray value (x,y+1)
Gray value (x+1,y+1)

(a)


Gray value (x,y)
Gray value (x+1,y)
Gray value (x,y+1)
Gray value (x+1,y+1)

(b)




(c)

**FIGURE 4. (a) Correlation graph for Plain and Cipher Lena, (b) Correlational graph for Plain and Cipher Baboon, (c) Correlation graph for Plain and Cipher Pepper**

**Table 3. Secured Images Correlation Index**

| Images | Positions | Plain Image | | | Encrypted Image | | |
|---|---|---|---|---|---|---|---|
| | | Red | Green | Blue | Red | Green | Blue |
| Lena | Hori. | 0.9891 | 0.9813 | 0.9564 | -0.0014 | -0.0012 | -0.0057 |
| | Vert. | 0.9793 | 0.9694 | 0.9330 | 0.0011 | -0.0097 | 0.0062 |
| | Diag. | 0.9713 | 0.9546 | 0.9174 | -0.0019 | -0.0045 | -0.0046 |
| White | Hori. | 0.000 | 0.000 | 0.000 | -0.0015 | -0.0015 | 0.0051 |
| | Vert. | 0.000 | 0.000 | 0.000 | 0.0030 | -0.0016 | 0.0048 |
| | Diag. | 0.000 | 0.000 | 0.000 | 0.0036 | 0.0079 | 0.0042 |
| Black | Hori. | 0.000 | 0.000 | 0.000 | -0.0045 | 0.0036 | -0.0011 |
| | Vert. | 0.000 | 0.000 | 0.000 | 0.0184 | -0.0038 | -0.0017 |
| | Diag. | 0.000 | 0.000 | 0.000 | -0.0189 | -0.0071 | -0.0046 |
| Baboon | Hori. | 0.8563 | 0.8005 | 0.8845 | 0.0067 | -0.0011 | 0.0019 |
| | Vert. | 0.9304 | 0.8950 | 0.9363 | 0.0090 | 0.0005 | 0.0056 |
| | Diag. | 0.8472 | 0.7702 | 0.8629 | -0.0023 | -0.0015 | -0.0002 |
| Pepper | Hori. | 0.9760 | 0.9891 | 0.9739 | -0.0091 | 0.0039 | 0.0073 |
| | Vert. | 0.9770 | 0.9884 | 0.9759 | -0.0059 | 0.0010 | -0.0067 |
| | Diag. | 0.9630 | 0.9819 | 0.9601 | -0.0011 | -0.0079 | 0.0047 |

The correlation scores between different encryption techniques for "Lena" photographs are displayed in Table 4. Prior to applying encryption, the pixel correlation of every image is readily apparent, as Table 3 shows in Fig. 4. However, after encryption is applied, the result is almost equal to 0. This illustrates that our method of encryption drastically breaks the link between pixels. Table 4. shows that the values obtained with our method

have a higher median than the values produced from [18, 35, 36], demonstrating that our strategy is more reliable. Particularly at horizontal green portion as well as diagonal red part, the suggested technique possesses the greatest effectiveness in upsetting the pixel correlation. As a result, the outcome suggests the low similarity in the next-to pixels in the cypher picture across the horizontal plane.

**Table 4. Encrypted Lena Correlation Comparison With Various Methods**

| Positions | Primary Color | [18] | [19] | [35] | [36] | Our Result |
|---|---|---|---|---|---|---|
| Horizontal | Red | 0.0063 | 0.0007 | 0.0060 | -0.0052 | -0.0015 |
| | Green | 0.0110 | -0.0035 | 0.0060 | -0.0052 | -0.0011 |
| | Blue | 0.0104 | 0.0015 | 0.0060 | -0.0052 | -0.0054 |
| Vertical | Red | 0.0004 | -0.0004 | -0.0209 | 0.0086 | 0.0011 |
| | Green | -0.0064 | 0.0023 | -0.0209 | 0.0086 | -0.0095 |
| | Blue | 0.003 | 0.0028 | -0.0209 | 0.0086 | 0.0063 |
| Diagonal | Red | -0.0020 | 0.0039 | 0.0055 | -0.0020 | -0.0018 |
| | Green | 0.0166 | -0.0079 | 0.0055 | -0.0020 | -0.0047 |
| | Blue | 0.0049 | 0.0010 | 0.0055 | -0.0020 | -0.0045 |

## Entropy Analysis

The entropy of data is a very significant measurement of unpredictability which assesses the randomness of random variables in theories of information. If encrypting does not generate sufficient chaos when it produces output, the encryption system may be the target of entropy attack. In an ideal world, the sufficient entropy of data of each RGB element picture is 8. With N being the total amount of bits in the message m, $2^N$ being every one of the potential values, $p(m_i)$ denoting a likelihood of $m_i$, $\log_2$, & value of entropy represented by bits, the description for the entropy H(m) for a picture m might be found as such.

$$H(m) = -\sum_{i=0}^{2^N-1} p(m_i \log_2(p(m_i))) \quad (20)$$

The entropy of simple pictures is provided in Table 5. Table 6 shows Encrypted Lena Entropy Comparison with various Methods.

**TABLE 5. Encrypted Data Entropy Analysis**

| Pictures | Lena | Pepper | Baboon | White | Black |
|---|---|---|---|---|---|
| Encrypted | 7.999 | 7.999 | 7.997 | 7.994 | 7.993 |
| Red Channel | 7.994 | 7.999 | 7.993 | 7.994 | 7.994 |
| Green Channel | 7.993 | 7.999 | 7.999 | 7.993 | 7.994 |

| | | | | | |
|---|---|---|---|---|---|
| Blue Channel | 7.995 | 7.999 | 7.999 | 7.994 | 7.994 |

Naturally, via calculation of data entropy, the mean value for the data entropy readings of these 6 picked RGB photos is extremely near to the perfect 8. Thus, the suggested technique is resistant towards the entropy exploit. The value of the final cypher picture, as shown in Table 5, is 7.999, meaning it's greater than [23, 35, 36].

**TABLE 6. Encrypted Lena Entropy Comparison with various Methods**

| Pictures | [19] | [23] | [35] | [36] | This paper |
|---|---|---|---|---|---|
| Encrypted Data | 7.998 | 7.981 | 7.992 | 7.996 | 7.999 |
| Red Channel | 7.997 | 7.979 | 7.993 | 7.996 | 7.993 |
| Green Channel | 7.997 | 7.980 | 7.992 | 7.995 | 7.992 |
| Blue Channel | 7.996 | 7.982 | 7.990 | 7.996 | 7.994 |

## Encryption Quality

Modifications made to the input image are immediately reflected in the cipher picture, making the plain and cipher versions of the picture clearly correlated. This sensitivity guarantees that harm in the plaintext result in observable variations in the ciphertext, making differential attacks ineffective. The differentiation of a 1-pixel shift on the encrypted picture is evaluated using two widely-used metrics: the Number of Pixel Change Rate (NPCR) & Unified Average Change in Intensity (UACI). These values help to quantify the degree to which encryption algorithms distribute changes throughout the ciphertext, thereby strengthening their defenses against attacks.

**TABLE 7. Quality Results**

| Pictures | NPCR | UACI |
|---|---|---|
| Lena | 99.663 | 36.256 |
| Baboon | 99.611 | 34.707 |
| Peppers | 99.596 | 33.306 |
| Black | 99.597 | 0.000 |

## Conclusion

In the past few years, several picture encryption techniques utilizing chaos systems have been presented. Simultaneously, the pseudo-DNA innovation has been advancing rapidly in the field of cryptosystems. However, the bulk of these models depend upon low-dimensional chaos system, that fails to meet the needs in unpredictability and resilience. The research proposes a digital colour picture encryption technique that utilizes a six-dimensional hyper-chaos system with encoded DNA technique to tackle this issue. The six-dimensional hyper chaos system demonstrates hyper chaos solution characterized by 4 positive Lyapunov coefficients throughout a

broad range of values for k. This encryption technique is achieved by means of DNA-level permutation and pixel-level diffusion. By applying permutations at both the pixel level along with DNA level, the original picture's location is scattered. Additionally, through a process known as diffusion, the connection between the initial picture and the encrypted version becomes extremely faint. This study conducts a variety of tests to evaluate the encryption method, including analysing the size and complexity of the key space, assessing the uniformity of key distribution, measuring the randomness of encrypted data, examining frequency distributions, checking for correlations between input and output, testing encryption quality and evaluating overall performance. The experimental outcomes reveal that the proposed method for encrypting coloured images demonstrates strong performance. Additionally, chaotic systems exhibit impressive capabilities in analysing bifurcation and assessing stability. In essence, the six-dimensional hyper chaos proves to be well-suited for integration into cryptographic systems.

This study introduces a novel approach to encrypting digital colour images, leveraging a six-dimensional hyper-chaos system alongside DNA encoding. While the proposed encryption system finds applicability across diverse domains, there remains scope for enhancing the efficiency of the six-dimensional hyper-chaotic algorithm within cryptographic contexts. Due to limitations in hardware resources and MATLAB efficiency, the encryption process currently lacks optimization for speed. Current efforts are focused on improving the algorithm's speed and intricacy.

Future research will prioritize the development of efficient techniques to counter attacks from supercomputers and quantum computers, as well as optimizing algorithmic performance.

## References

1. Pareek, Narendra & Patidar, Vinod & Sud, K.K.. (2006). Image encryption using chaotic logistic map. Image and Vision Computing. 24. 926-934. 10.1016/j.imavis.2006.02.021.
2. Chen, Guanrong & Mao, Ybin & Chui, Charles. (2004). A symmetric image encryption based on 3D chaotic cat maps. Chaos, Solitons & Fractals. 21. 749-761. 10.1016/j.chaos.2003.12.022.
3. Furht, B., & Kirovski, D. (Eds.). (2004). Multimedia Security Handbook (1st ed.). CRC Press. https://doi.org/10.1201/9781420038262
4. Digital image steganography: Survey and analysis of current methods, Signal Processing, Volume 90, Issue 3, 2010, Pages 727-752, ISSN 0165-1684, https://doi.org/10.1016/j.sigpro.2009.08.010.
5. HUSSAIN, U. Noorul; CHITHRALEKHA, T. Review of DNA Cryptology. Networking and Communication Engineering, [S.l.], v. 3, n. 13, p. 843-849, Oct. 2011. ISSN 0974 – 9616
6. Henry Ker-Chang Chang, Jiang-Long Liu, A linear quadtree compression scheme for image encryption, Signal Processing: Image Communication,Volume 10, Issue 4, 1997, Pages 279-290, ISSN 0923-5965, https://doi.org/10.1016/S0923-5965(96)00025-2.
7. Chen, Guanrong & Ueta, Tetsushi. (1999). Yet Another Chaotic Attractor. International Journal of Bifurcation and Chaos - IJBC. 9. 1465-1466. 10.1142/S0218127499001024.
8. Bourbakis, Nikolaos G. and Christos Alexopoulos. “Picture data encryption using scan patterns.” Pattern Recognit. 25 (1992): 567-581.
9. Subbiah, Geetha & Punithavathi, P & Infanteena, A & Sindhu, Sivatha. (2018). A Literature Review on Image Encryption Techniques. International Journal of Information Security and Privacy. 12. 42-83. 10.4018/IJISP.2018070104.
11. Mao, Y., Chen, G. (2005). Chaos-Based Image Encryption. In: Handbook of Geometric Computing. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-28247-5_8
12. Habutsu, Toshiki & Nishio, Yoshifumi & Sasase, I. & Mori, Shinsaku. (1991). A Secret Key Cryptosystem by Iterating a Chaotic Map. LNCS. 547. 127-140. 10.1007/3-540-46416-6_11.
13. Hua, Zhongyun & Jin, Fan & Xu, Binxuan & Huang, Hejiao. (2018). 2D Logistic-Sine-Coupling Map for Image Encryption. Signal Processing. 149. 10.1016/j.sigpro.2018.03.010.
14. Murillo-Escobar MA, Meranza-Castillón MO, López-Gutiérrez RM, Cruz-Hernández C. Suggested Integral Analysis for Chaos-Based Image Cryptosystems. *Entropy*. 2019; 21(8):815. https://doi.org/10.3390/e21080815

15. Babaei, Majid. (2013). A novel text and image encryption method based on chaos theory and DNA computing. Natural Computing. 12. 10.1007/s11047-012-9334-9.

16. Jain, Anchal & Rajpal, Navin. (2015). A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. Multimedia Tools and Applications. 29. 10.1007/s11042-015-2515-7.

17. Zhang, Qiang & Liu, Lili & Wei, Xiaopeng. (2014). Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps. AEU - International Journal of Electronics and Communications. 68. 186–192. 10.1016/j.aeue.2013.08.007.

18. Diaconu, Adrian-Viorel & Costea, Alexandru & Costea, Marius Aurel. (2014). Color Image Scrambling Technique Based on Transposition of Pixels between RGB Channels Using Knight's Moving Rules and Digital Chaotic Map. Mathematical Problems in Engineering. 2014. 10.1155/2014/932875.

19. Gao, Xiaohong. (2021). A color image encryption algorithm based on an improved Hénon map. Physica Scripta. 96. 10.1088/1402-4896/abed7d.

20. Zhang, Wei & Yu, Hai & Zhao, Yu-li & Zhu, Zhi-liang. (2016). Image encryption based on three-dimensional bit matrix permutation. Signal Processing. 118. 10.1016/j.sigpro.2015.06.008.

21. Li, Xiao & Cho, Sung & Kim, Seok. (2014). A 3D image encryption technique using computer-generated integral imaging and cellular automata transform. Optik - International Journal for Light and Electron Optics. 125. 10.1016/j.ijleo.2013.12.036.

22. Zhu Z-L, Zhang W, Wong K-w, Yu H (2011) A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf Sci 181(6):1171–1186

23. Liu, Hongjun & Wang, Xingyuan. (2011). Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Optics Communications. 284. 3895-3903. 10.1016/j.optcom.2011.04.001.

24. Pyle I (1967) Format effectors in iso7 and ascii. Commun ACM 10(3):137

25. Xian, Yongjin & Wang, Xingyuan & Wang, Xiaoyu & Li, Qi & Ma, Bin. (2022). A Chaotic Image Encryption Algorithm Based on Sub-block Spiral Scans and Matrix Multiplication. 10.1007/978-3-031-06791-4_25.

26. Gao, Xinyu & Mou, Jun & Xiong, Li & Sha, Yuwen & Yan, Huizhen & Cao, Yinghong. (2022). A fast and efficient multiple images encryption based on single-channel encryption and chaotic system. Nonlinear Dynamics. 108. 10.1007/s11071-021-07192-7.

27. Lorenz, E. N., 1963: Deterministic Nonperiodic Flow. *J. Atmos. Sci.*, **20**, 130–141, https://doi.org/10.1175/1520-0469(1963)020<0130:DNF>2.0.CO;2.

28. Hu, Guosi. (2009). GENERATING HYPERCHAOTIC ATTRACTORS WITH THREE POSITIVE LYAPUNOV EXPONENTS VIA STATE FEEDBACK CONTROL. International Journal of Bifurcation and Chaos. 19. 651-660.

29. Yang, Qigui & Osman, Waleed & Chen, Chuntao. (2015). A New 6D Hyperchaotic System with Four Positive Lyapunov Exponents Coined. International Journal of Bifurcation and Chaos. 25. 1550060. 10.1142/S0218127415500601.

30. Shalon D, Smith SJ, Brown PO. A DNA microarray system for analyzing complex DNA samples using two-color fluorescent probe hybridization. Genome Res. 1996 Jul;6(7):639-45. doi: 10.1101/gr.6.7.639. PMID: 8796352.

31. A.K. Verma, M. Dave, and R.C. Joshi, Journal of Discrete Mathematical Sciences and Cryptography 11, 393 (2008).

32. Wu, Y., Agaian, S. S., & Noo0.000, J. P. (2012). Sudoku associated two dimensional bijections for image scrambling. *arXiv preprint arXiv:1207.5856*.

33. Seyedzadeh, Seyed Mohammad & Mirzakuchaki, Sattar. (2012). A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. Signal Processing. 92. 1202-1215. 10.1016/j.sigpro.2011.11.004.

34. Liang Z, Qin Q, Zhou C, Wang N, Xu Y, Zhou W. Medical image encryption algorithm based on a new

five-dimensional three-leaf chaotic system and genetic operation. PLoS One. 2021 Nov 29;16(11):e0260014. doi: 10.1371/journal.pone.0260014. PMID: 34843485; PMCID: PMC8629275.

35. Shakiba, Ali. (2019). A Randomized CPA-Secure Asymmetric-Key Chaotic Color Image Encryption Scheme based on the Chebyshev Mappings and One-Time Pad. Journal of King Saud University - Computer and Information Sciences. 33. 10.1016/j.jksuci.2019.03.003.

36. Iqbal, Nadeem & Hanif, Muhammad & Abbas, Sagheer & Khan, Muhammad & Rehman, Zia. (2021). Dynamic 3D scrambled image based RGB image encryption scheme using hyperchaotic system and DNA encoding. Journal of Information Security and Applications. 58. 102809. 10.1016/j.jisa.2021.102809.