Received: April 28, 2024. Revised: June 12, 2024.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Image Cryptography Based on Confusion and Diffusion Using 6D Hyper Chaotic System and Fibonacci Q-matrix

Donia Fadil Chalob[1] **Rusul Hussein Hasan**[2]* **Rusul Fadhil Yaser**[3]

[1]*Mustansiriyah University, Department of Computer Science, Iraq*
[2]*University of Baghdad, Iraq*
[3]*Ministry of Education, Iraq*
* Corresponding author's Email: russl@colaw.uobaghdad.edu.iq

Abstract: The day-life calls for transferring millions of images between users, in the era of Information Technology. The security of these images essential using a well-known encryption techniques. The robust image cryptography relies on confusion and diffusion strategies. A new image cryptography algorithm is suggested multiple confusion-diffusion techniques based on 6D hyper chaotic system and Fibonacci Q-matrix. The plain image is confused employing random numbers produced using six- dimension hyper chaotic system across two different confusion phases. In diffusion phases, Fibonacci transformation, XOR operation and cyclic shift are applied. The security of the suggested algorithm is experimented via statistical attacks, differential attacks and brute force attacks. The proposed algorithm is succeeded in passing the security levels, where the key space was expanded to a relatively larger than 10^{176} and having property of high key sensitivity. The resultant cipher image is free of statistical features by means of histogram and entropy since the histogram is completely equal in all instances even with monochrome colour images. The proposed technique accomplishes 7.99% of average entropy. Furthermore, it showed 99.61% and 31.21 of average NPCR and UACI, respectively. Moreover, the proposed technique records average correlation coefficient values in horizontal, vertical, and diagonal orientations equal to 0.0030, 0.0024, and 0.0026, respectively.

Keywords: Image cryptography, Hyper chaotic system, Fibonacci Q-matrix, Six dimension.

1. Introduction

As a main carrier of information transmission and storage, the digital image is extensively utilized in life of people and in many fields including medical treatment, education, and environmental observing. Sensitive information could be attacked if it is transferred on an insecure channel. Thus, the security of image when transmitting has become a focal point and research [1]. The researchers recommended various cipher methods from a number of standpoints to ensure adequate security for the multimedia information. Utilizing Chaos theory of image cryptography is an outstanding method among these technologies. The reason is that chaos maps possess a substantial feature of sensitivity towards the control parameter and initial values and are defined via ergodicity and non- convergence [2]. The good cryptography algorithm follows the two important confusion-diffusion concepts [3, 4]. The confusion concept is done by randomly scrambling neighbouring pixels, while the diffusion concept can be acquired by scattering a small modify in the pixels of original image to all of the encrypted image [5].

Literatures about image cryptography algorithms based on 6D chaotic systems are reviewed. N. N. Jasem and S. A. Mehdi [6] proposed a new cipher algorithm that exploits a hyper six-dimension chaotic system. The algorithm combines switching, randomization, XOR operations, diffusion in a number of phases to warrant robust cryptography. Q. Zhang and J. Han [7] proposed color image encryption technique based on 6D hyper chaotic system, dynamic DNA coding and image hashing. The hash series is mined via image hashing algorithm and used as the control parameter and initial value of chaos system. Then, RGB levels of image are synthesized into a two-dimension array and the pixel replacement is achieved via the enhanced two-dimension chaos map. Lastly, the 6D hyper chaotic system is utilized to produce arbitrary sequences for DNA coding and arithmetic processes. A. A. Rashid and K. A. Hussein [8] presents an efficient method for grey and color images encryption based on logistic 6D chaotic system and image density to create keys and encrypt the image via exclusive OR process. S. Sun [9] presented an image encryption based on random signal insertion and 6D hyper chaos system, where inserting some randomized indications into the chaotic system variables through repetition. The totality value of all original pixels is utilized in generation of the initial values of the chaos system. Then, splitting a pixel into two equivalent portions and procedure a bigger array. Cycle shift, confusion and diffusion are functioned on the new array. S. A. Mehdi and Z. latif Ali [10] presents an image encryption and decryption scheme relied on a new six-dimension hyper chaotic system. The cipher algorithm involves of four phases: chaotic sequence production, Latin square, confusion and diffusion. X. Wu et al. [11] constructed a new image cryptography scheme via two- dimension DWT and six dimensional hyper chaotic system in both spatial and frequency domains, where the key sequence is depend on the chaotic system and the plain image. H. Mondal et al. [12] introduced a sparse depiction method and 6D chaos system besides RC6 for a greyscale image to cipher non-zero sparse component through the assistance of a well-trained thesaurus. S. A. Yassir and H. R. Shakir [13] suggested an approach consists of elliptic-curve cryptography and 6D hyper chaos system started with a key acquired via the hash algorithm of type SHA-256. S. Sun [14] introduced image encryption method based on 6D hyper chaos system and randomize signals insert using some randomize signal into the chaos system values throughout repetition. The addition result of entirely original pixels is utilized to yield the preliminary variables of the chaotic system. F. Yu *et al* [15] studied a new memoristive Hopfield neural network 6D fractional order by using the memoristor to mimic the convinced existing, and the bifurcation features and concurrence attractor features of fractional memoristor Hopfield neural network to generate a random values and employ it in image encryption. M. Naim and A. A. Pacha [16] introduced a new image cryptography based on a mixture of 6D hyper chaos system along with advanced Hill cipher. Whole zero pixels are swapped by pixels of value 256 using the prime number 257 as modulo. S. John and S. N. Kumar [17] implemented a hyper chaotic system as a cipher key along with 6D, each dimension with its range values and employed it for the encryption of medical images and the 3D printed model.

Furthermore, some literatures on image encryption algorithms based on Fibonacci matrix are reviewed: O. Dişkaya, et al. [18] proposes a new cryptography scheme based on Fibonacci polynomial matrices. In every cycle, the Fibonacci polynomials matrices in confusion and diffusion are considered contrary. While in every cycle, the matrix of the column shuffle phase in the AES algorithm is similar. A. M. Cyriac and B. M. K. Sheeja [19] introduced encryption and decryption scheme based on optical scanning holography and Fibonacci- Lucas transformation. The first phase includes a point spread function contrived optic scan cryptography system using a new key based on fused biometric matrix. A digital cryptography approach is applied after this stage. C. Maiti, et al. [20] introduced a new image cryptography technique, where the confusion phase is achieved via Fibonacci Transformation, and Tribonacci Transformation alters the pixel value. The Fibonacci and Tribonacci values are decided via hashing the original image. X. Hu, et al. [21] proposed a color image cryptography method based on a cloud model Fibonacci chaos system and a matrix convolution process. The method engages the cloud model and the general Fibonacci, forming more complex chaotic system that satisfies the dynamic randomization difference of chaotic sequences. Y. Zhou, et al. [22] introduced a new image cryptography method via a mixture of parametric bit-plane dissolve in addition to bit- plane scrambling and resizing, and data mapping. The algorithm employs the P-code Fibonacci for image bit- plane dissolve and the two dimensional P-Fibonacci convert because they are parametric dependent. H. Wen et al. [23] proposed a chaotic image cryptography based on the “diffusion-confusion-diffusion” structure, adopting a plaintext correlation technique to produce chaos PRNS and the cipher text feedback diffusion mechanism to enhance the security. Z. Tang et al. [24] propose a new image cryptosystem via conjointly developing arbitrary overlapping block divider, double spiral scan, Henon map and Lu map. The original image is partitioned into intersecting blocks, for each block the pixels are shuffled via double spiral scan. The start point is randomly chosen under the control of Henon map in spiral scans. Next, image components are generated based on undisclosed keys and applied to control the Lu map for computed an undercover array similar as the input image size. The cipher image is acquired via scheming XOR process between the secret array and corresponding components of the shuffled image.

The hyper chaotic mechanism has the ability to form key sequences that possess a huge key space. The exploitation of hyper chaotic system advances security performance. The colour image contains extra information as compared to the grey image. Thus, it is great challenge to encrypt colour image with high competence in substantial time. The weaknesses of small key space motivated the authors to utilize a six dimensions hyper chaotic system to cipher colour images. The first phase is confused the positions of pixels in the original image using the 6D hyper chaotic system. Second, the Fibonacci Q-matrix and Exclusive OR are developed in the diffusion phase. The contribution of this work is summarized as:

1. Develop image cryptosystem security based on 6D hyper chaotic system. Implementing multiple confusion- diffusion structure to ensure robust security.
2. Decent resistance to brute force attacks because of the large key space of 6D hyper chaotic system.
3. Ensure the efficiency of the image cryptosystem, where one chaotic system is utilized and more rationalized procedures are applied to ensure lower complexity.

The next sections are organized as follows: The mathematical basics of the 6D hyper chaotic system and Fibonacci Q- matrix obtainable in Section 2. The suggested cryptography algorithm is obtainable in Section 3. In Section 4, experiments and results are considered. Comparison of Performance is introduced in Section 5. Section 6 is presented the conclusion.

2. Mathematical foundation

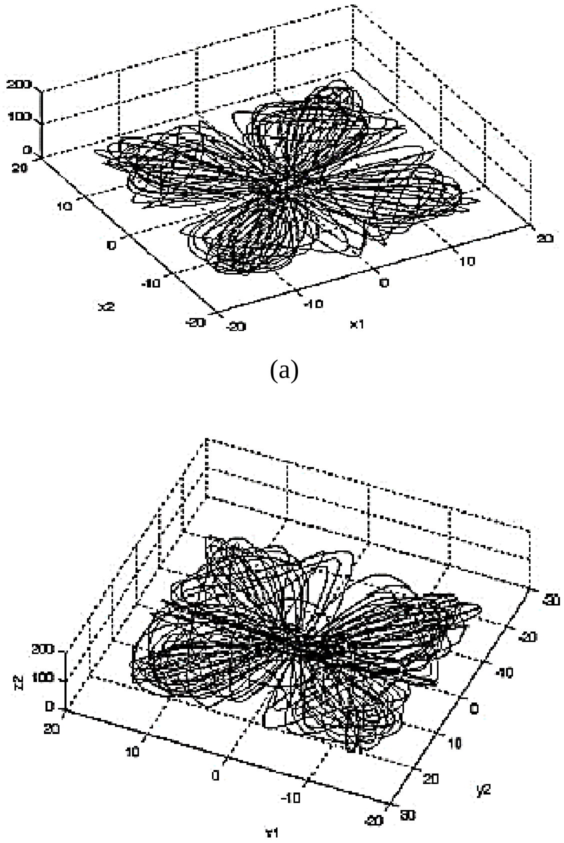
The conventional cryptography algorithms are unsuitable using directly for ciphering image. It differs from text encryption because of essential structures of images like redundancy, big volumes, and correlation in neighbouring pixels. Besides, the classical algorithms require long time, often needed a robust mathematical substance, and had key management problem, such as in securing key exchange mechanism. Chaos theory has been recorded a significant improvement in mathematical precision, key management, security and applications, thanks to its properties that are similar to cryptography requirements. The background knowledge of 6D hyper chaotic system and Fibonacci transformation is studied in the following two subsections.

2.1 Hyper chaotic system

A Four-wing hyper chaotic attractors is obtained by coupling two identical Lorenz systems [25], as in Eq. (1). Lorenz system shows the famous butterfly attractor for δ = 10, ρ = 28 and β = 8/3, considering these original values, Eq. (1) produces the four- wing attractor depicted in Fig. 1.

$$\begin{cases} \dot{x_1} = \delta\,(y_1 - x_1), \\ \dot{y_1} = \rho x_1 - y_1 - x_1 z_1 + k_1(x_2 - y_2), \\ \dot{z_1} = x_1 y_1 - \beta z_1, \\ \dot{x_2} = \delta\,(y_2 - x_2), \\ \dot{y_2} = \rho x_2 - y_2 - x_2 z_2 + k_2(x_1 - y_1), \\ \dot{z_2} = x_2 y_2 - \beta z_2, \end{cases} \tag{1}$$

whereas k_1 $(x_2\text{-}y_2)$ and k_2 $(x_1\text{-}y_1)$ scaled by the parameters $k_1>0$ and $k_2>0$ are two linear coupling terms. The control parameters and initial values of the 6D chaotic system are: x_1=2.543210007543721, y_1=3.674515623875401,z_1=1.235685120036054,x_2= 1.6758174322200155643, y_2 = 4.785400011325467, z_2 = 2.3576335564327899543 [26].



(a)

(b)

Figure. 1 Four-wing attractor when k_1 =0.1, k_2 =0.01: (a) (x_1,x_2, z_1) plane and (b) (x_1,y_2, z_2) plane

Received: April 28, 2024. Revised: June 12, 2024.

2.2 Fibonacci Q - matrix

Fibonacci sequence is a sequence where each number is the sum of the two prior ones after the first two [27]. It is a list of numbers associated with the golden ratio well. Specifically, the sequence Fn of Fibonacci numbers is distinct as follows.

$$F_n = F_{n-1} + F_{n-2} \quad (2)$$

In Eq. (2), $F_1 = F_2 = 1$. Given a (2 × 2) square matrix, the Fibonacci number can be denoted as follows:

$Q = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, the Fibonacci number can be denoted as the *n*th power of Q in Eq. (3):

$$\begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} = Q^n = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \quad (3)$$

Implementing the determinant of both left and right sides of Eq. (3) earnings Eq. (4), which is identified as Cassini’s identity.

$$F_{n+1}.F_{n-1} = F_n^2 = Det(Q^n) = (-1)^n \quad (4)$$

3. Proposed algorithm

The proposed cryptography algorithm composes of three parts:

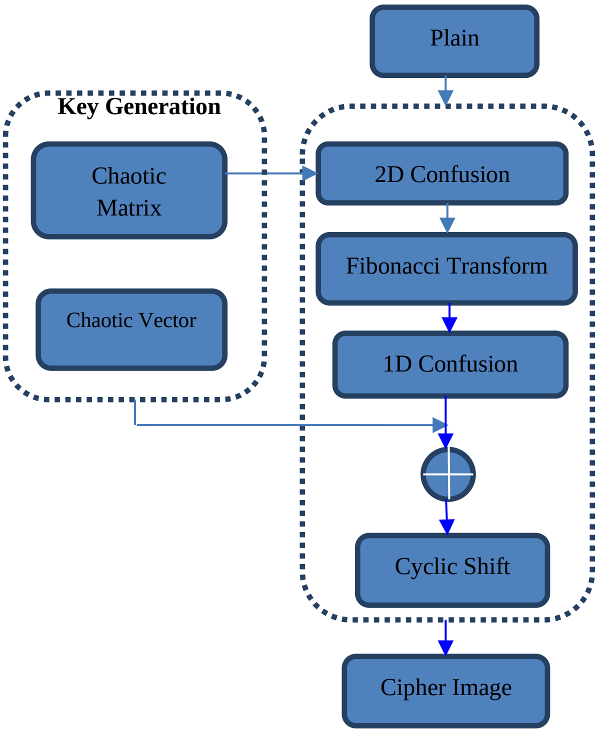


Figure. 2 General diagram of proposed cipher algorithm

- Key generation part, where the key is derived from the 6D hyper chaotic system clarified in previous section.
- The confusion stage shuffles the pixel locations via chaotic index.
- The diffusion stage is implementing to alter the pixels values, applying Fibonacci transformation, XOR operation and cyclic shift are applied. The general diagram of the proposed mechanism is shown in Fig. 2. The encryption method is demonstrated in Algorithm 1. Each phase is explained in the next subsections.

3.1 Key generation

In the current cryptography technique, the cipher key is resultant from the 6D chaotic system. The generation of chaotic vectors begins by considering the initial conditions and parameters belong to 6D hyper chaotic system, then applying the systems a certain number of iterations in order to generate the chaotic sequences. Six chaotic vectors are generated in this step, each vector is the same size as image dimensions. These keys are utilized in confusion and diffusion phases of an image.

3.2 Confusion phase

In 2D Confusion Phase, the 6D hyper chaotic system is utilized to achieve the confusion of image pixels via the six hyper chaotic sequences made from the system. Each one of the six chaotic vectors will be sorted in ascending order. Different two vectors is specified to confuse a certain level of image, the first and second new index vectors are used as row & column index of red level of a color image, the third and fourth new index vectors are used as row & column index of green level of a color image, and the fifth and sixth new index vectors are used as row & column index of blue level of a color image. To pass on all the matrix pixels there will be two indicators, one indicator for the rows and the other for the columns. The row indicator is set to the current row until the column indicator passes through all columns

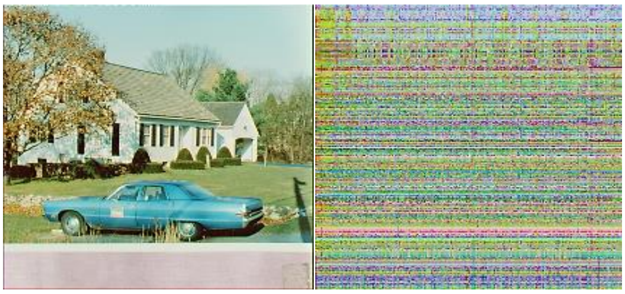


Figure. 3 (2D) Confusion Phase

of the same row. The same mechanism is repeated until the last value of the two indicators is reached. Fig. 3 depicts the House image after 2D confusion phase. In 1D Confusion Phase, the same chaotic system is applied to perform confusion but, this time a vector is obtained of size N*N, then confusing (R, G, B) planes according to vector indices after sorting.

3.3 Diffusion phase

An attacker may be use the information obtained from the histogram outline of the confused image. To resolve this problem, we need to alter the pixels intensity to ensure that nothing can be expected about the original image. Two operations have been accomplished in this phase to reach the goal. First, the confused image is XORed with the key'; second, the pixels values of the resultant image are modified using cyclic shift by 4 positions. The XOR operation and cyclic shift are applied very fast.

Algorithm 1. Image Encryption (*Img*$_{N*N}$,$\delta, \rho, \beta, k_1, k_2,$ *Img*$_{enc}$)

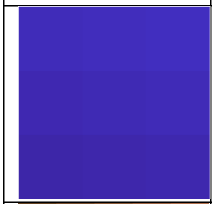
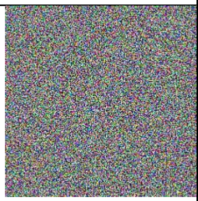
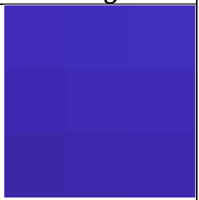
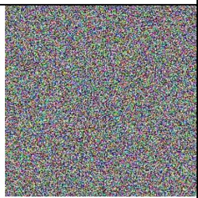
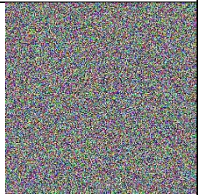
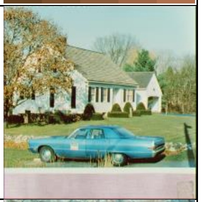
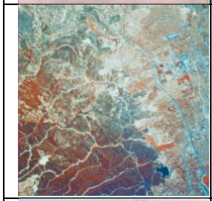
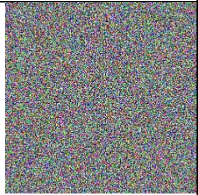
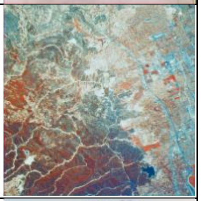
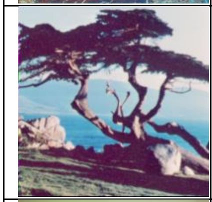
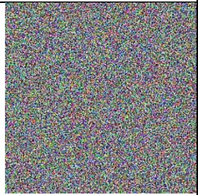
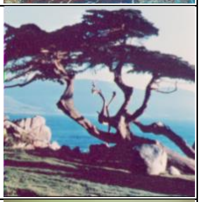
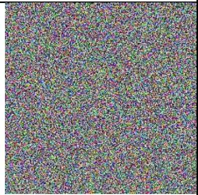
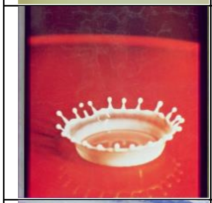
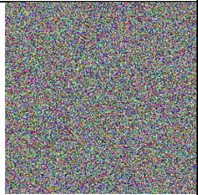
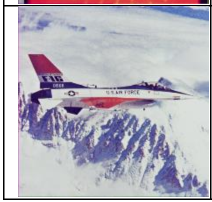
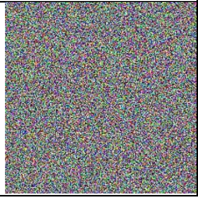
```
Input: Plain Image Img,$\delta, \rho, \beta, k_1, k_2$.
Output: Encrypted Image Img_enc.

Step1. Key Generation
    I. $key$, iterating system 1, to generate random sequences:
        $x_1 = \{x_1, x_2, x_3, \dots, x_{NN}\},\ y_1 = \{y_1, y_2, y_3, \dots, y_{NN}\},\ z_1 = \{z_1, z_2, z_3, \dots, z_{NN}\}$,
        $x_2 = \{x_{2.1}, x_{2.2}, x_{2.3}, \dots, x_{NN}\},\ y_2 = \{y_{2.1}, y_{2.2}, y_{2.3}, \dots, y_{NN}\},\ z_2 = \{z_{2.1}, z_{2.2}, z_{2.3}, \dots, z_{NN}\}$.
    II. $key'$, converting each sequence of $x_1$, $y_1$, $z_1$, $x_2$, $y_2$, and $z_2$ into integers as:
        $key' = floor(key) * 10^{15}\ mod$ N * N.
Step2. 2D Confusion Phase
    I. Key_Index $(x'_1, y'_1, z'_1, x'_2, y'_2, z'_2)$= sort $(x_1, y_1, z_1, x_2, y_2, z_2)$
    II. For row = 1 to N
            For column = 1 to N
                Img_R (row, column) = Img_R $(x'_1$(row), $y'_1$(column))
                Img_G (row, column) = Img_G $(z'_1$(row), $x'_2$(column))
                Img_B (row, column) = Img_B $(y'_2$(row), $z'_2$(column))
            End
        End
    III. Img_1 = Combine (Img_R, Img_G, Img_B)
Step3. Fibonacci $Q$-matrix
    I. Divide Img_1 into (2×2) sub blocks
    II. Multiply every block in Img_1 D, by Fibonacci $Q$-matrix ($Q$10):
        $\begin{bmatrix} F_{i,j} & F_{i,j+1} \\ F_{i+1,j} & F_{i+1,j+1} \end{bmatrix} = \begin{bmatrix} D_{i,j} & D_{i,j+1} \\ D_{i+1,j} & D_{i+1,j+1} \end{bmatrix} \begin{bmatrix} 89 & 55 \\ 55 & 34 \end{bmatrix} mod\ 256,\ i = 1:3:..N,\ j = 1:3:..N.$
Step4. 1D Confusion Phase
    I. For vector = 1 to $N * N$
            Img_1R (vector) = Img_1R (Key_index(vector))
            Img_1G (vector) = Img_1G (Key_index(vector))
            Img_1B (vector) = Img_1B (Key_index(vector))
        End
    II. Img_2 = Combine (Img_1R, Img_1G, Img_1B)
Step5. For $i$ = 1 to N*N
        Img_3 $(i)$ = Img_2 $(i) \oplus key'(i)$
    End
Step6. For $i$ = 1 to N*N
        Img_enc $(i)$ = Cyclic shift (Img_3$(i)$) by 4 position
    End
Step7. Return (Img_enc).
```

4. Test and discussion

The robust of proposed algorithm is tested via blue add monochrome images and different standard colour images of dimension 256 × 256, six of them are selected from SIPI datasets. The tests are accomplished to evaluate the proposed cryptography algorithm utilizing visible scene, key space, entropy, correlation coefficients, differential attack and histograms.

Table 1. Visible scene of experiment images

Original Image	Cipher Image	Decipher Image
		
		
		
		
		
		
		
		

4.1 Visible scene

The visible scene is a vital and simple measurement for assessing the security of the cipher images. The test relies on the scene of the cipher image. The optimal state for the experiment happens when the scene of the encrypted image has no facts about the plain image. From Table 1, one can notice that the cipher images are contrast completely from their corresponding plain form and there is no perceptual similarity between plain images and their cipher counterparts no information can be inferred from the cipher image so as draw no conclusion about the appearance of original image.

4.2 Key space analysis

The key space is vital in cryptography. If the key space >2^{100} , then the cryptography algorithm is robust towards brute force attacks [28]. The proposed algorithm has dissimilar security keys: $x_1, x_2, x_3, x_4, x_5, x_6, a_1, a_2, a_3, r_1\ and\ r_2$. assuming the accuracy of the initial value equivalents to 10^{16}, then the whole key space is greater than $d_0 \times 10^{176}$, which displays heftiness to brute force attack.

4.3 Key sensitivity analysis

The value of one initial condition of chaotic system is slightly altered from y(0) = 2.543210007543721 into y(0) = 2.5432100075437210000000000001 in decryption. Fig. 4 shows that even with a minor variation of 10^{-14}, the decipher image with minor altered key is completely changed from the plain image. It implies that the proposed algorithm is tremendously sensitive to any potential changes of the key.

4.4 Information entropy analysis

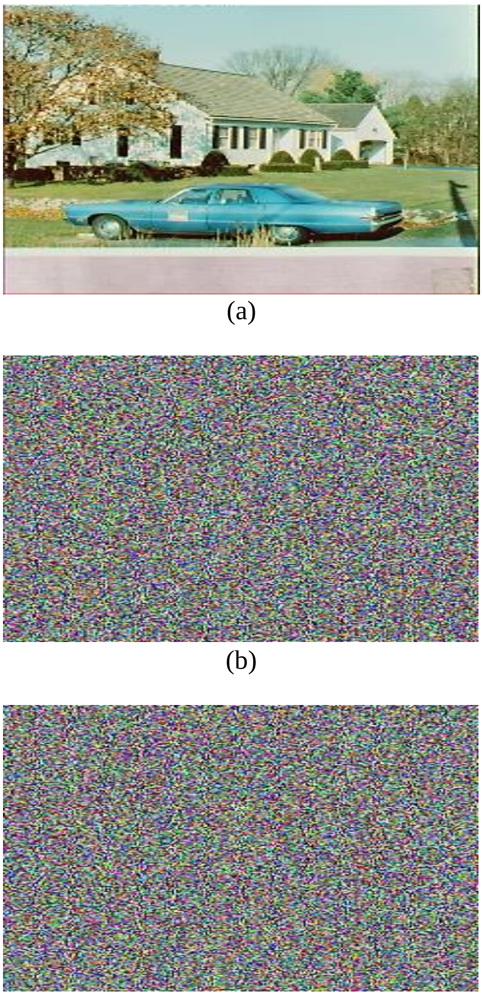
Information entropy assesses indecision of a random variable as follows [28, 29]:

$$E = -\sum_{i=0}^{255} p(i) log_2\big(p(i)\big) \tag{5}$$

where P(i) is the possibility incidence of pixel i. When the entropy value near to the optimal value of (8) is considered protected from the brute force attack.

Table 2. Information entropy of plain and cipher images

Images	Entropy	
	Plain image	Cipher image
Blue Color	4.4249	7.9990
Monochrome	4.1325	7.9990
House	7.4788	7.9989
Woodland Hills	7.3380	7.9992
Tree	7.5371	7.9990
Jelly Beans	6.5835	7.9992
Splash	7.2413	7.9991
Airplane (F-16)	6.6787	7.9991



(a)

(b)

(c)

Figure. 4 Key Sensitivity Test: (a) House image, (b) Cipher image when y(0)= 2.543210007543721 and (c) Decipher image when y(0)= 2.5432100075437210000000000001

The values of information entropy that acquired from proposed algorithm are nearer to 8, these indications that the proposed scheme has high randomization. Table 2 displays the information entropy of different plain images and corresponding cipher images.

4.5 Correlation analysis

Correlation expresses the association between two random variables to establish the relationship concerning two contiguous pixels. There is a huge association between the pixels of original image and its nearby pixels. Consequently, it is susceptible to statistical attacks. To defend this attack, the correlation between adjacent pixels in the cipher image should be minimized, via confusion concept that shuffle the pixels of the original image and diffusion concept that altered pixels values [24]. The pixel correlation is computed as demarcated in Eqs. (6)-(8). Tables 3 lists the correlation among pixels.

$$d_{xy} = (cov(x,y))/(\sqrt{D_x * D_y}) \quad (6)$$

$$cov(x,y) = E[(x - E(x))(y - E(y))] \quad (7)$$

$$E(x) = \frac{1}{L}\sum_{i=1}^{L} x_i \, ; \, D(x) = \frac{1}{L}\sum_{i=1}^{L}(x_i - E(x))^2 \quad (8)$$

Table 3. Correlation of encrypted and original images

Image	Direction	Original Image	Cipher Image
Blue	Horizontal Vertical Diagonal	0.4988 0.8193 0.0104	0.0027 -0.0008 -0.0003
Monochro -me	Horizontal Vertical Diagonal	0.9969 1 0.9969	-0.0005 -0.0009 0.0036
House	Horizontal Vertical Diagonal	0.9536 0.9579 0.9224	0.0014 0.0022 -0.0024
Woodland Hills	Horizontal Vertical Diagonal	0.9153 0.8938 0.8452	-0.0048 0.0032 0.0071
Tree	Horizontal Vertical Diagonal	0.9590 0.9361 0.9159	-0.0032 0.0022 -0.0006
Jelly Beans	Horizontal Vertical Diagonal	0.9745 0.9763 0.9537	0.0068 0.0063 -0.0037
Splash	Horizontal Vertical Diagonal	0.9936 0.9951 0.9894	-0.0004 0.0036 0.0030
Airplane (F-16)	Horizontal Vertical Diagonal	0.9389 0.9253 0.8753	0.0043 0.0003 0.0003

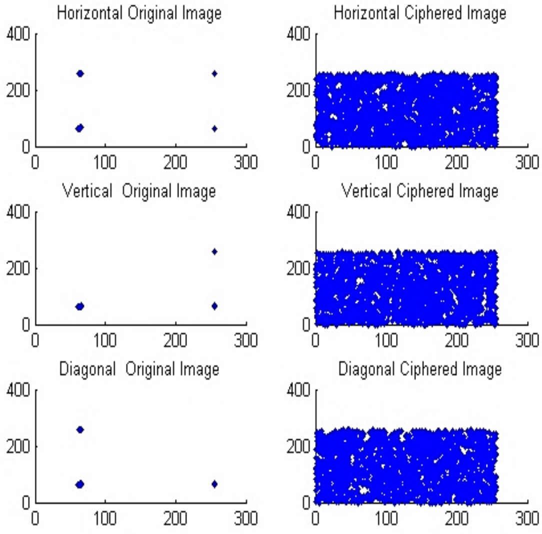


Figure. 5 Correlation of neighbouring pixels in original and cipher blue image

Received: April 28, 2024. Revised: June 12, 2024.

As shown in Table 3, the correlation coefficient of original image is close to 1, while the correlation coefficient of the encrypted image in average is fewer than 0.001. Thus, the correlation of the cipher image is significantly concentrated and the proposed scheme has a great defense toward statistical attacks. Fig. 5 illustrates the horizontal, vertical and diagonal correlation for pairs of original and cipher images of contiguous pixels.

4.6 Study of differential attack

The differential attack means that an attacker discovers the association concerning the plain image and the cipher image via linking the variances amid the equivalent cipher previous and after a minor altering the plain text. Two indicators: number of pixels change rate (NPCR) and unified average change intensity (UACI) are utilized to evaluate the capability of algorithm to withstand differential attacks, calculated using Eq. (9) [30]. A pixel from the plain image is randomly chosen and its value is enlarged by one. The cryptography experimentations are executed 1000 times, and diverse pixels are selected every time. The average NPCR and UACI values are computed and the analysis results are displayed in Table 4. Our algorithm has faintly advanced NPCR and UACI values demonstrating the effective resistance towards differential attacks.

$$\begin{cases} D(i,j) = \begin{cases} 0 \; if \; P_1(i.j) = P_2(i,j) \\ 1 \; if \; P_1(i.j) \neq P_2(i,j), \end{cases} \\ NPCR = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} D(i,j)}{M\times N} \times 100\%, \\ UACI = \frac{1}{M\times N}\left[\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|P_1(i,j)-P_2(i,j)|}{L-1}\right]\times 100\% \end{cases} \quad (9)$$

Table 4. UACI and NPCR indication of encrypted images

Images	NPCR	UACI
Blue Colour	99.6063	32.5991
Monochrome	99.6343	29.1687
House	99.6089	30.7258
Woodland Hills	99.6120	28.3824
Tree	99.5972	31.9905
Jelly Beans	99.5956	30.4157
Splash	99.6134	33.8871
Airplane (F-16)	99.6104	32.4720

4.7 Histogram indicator

Image Histogram is the visual depiction of image pixels distribution, which is used to estimate image cryptography algorithms. A powerful image encryption algorithm must produce a flat histogram for the cipher image [31]. The histogram of the plain and cipher image demonstrated in Fig. 6. The cipher image has very identical and uniform histograms, the histograms of ciphered image using the suggested algorithm has identical spreading. These outcomes confirm the competence of algorithm.

Table 5. Image Cryptography Technique of SoA and proposed algorithm

Method	Image Cryptography Technique
[27]	4D Chen hyper chaotic system produces random values to shuffle pixel locations. Splitting the shuffled image into 2×2 blocks where the Fibonacci Q-matrix diffused each.
[32]	Mutual diffusion is utilized to shuffle two binary components via Logistic, Sine, Tent, Chebyshev maps, XOR and cyclical shift. Binary component confusion is achieved via a chaos map and converted into binary bit levels.
[33]	Three individual chaotic maps, including 2D Henon map, Logistic map and Tent map. For adding another level of security, DNA encoding has been utilized.
[34]	2D hyper chaotic logistic- sine map and two way Josephus traverse are used for confusion process.
[35]	4D Chaotic Laser System, Zig-Zag confusing Method. In diffusion, DNA encoding scheme.
[36]	4D hyper chaotic dynamical system and DNA layer diffusion is implemented to extra rise the uncertainty in an image.
[37]	6D hyper chaotic map and enhanced logistic map, mixture of various inserted patterns, including Zigzag, Hilbert, and Morton patterns to thwart the confusion and diffusion characteristics.
[38]	6D memristive hyper chaotic system and a 2D sinusoidal feedback Sine ICMIC modulation map (SF-SIMM) discrete hyper chaotic map are utilized as the double entropy foundation construction.
Our Proposed	Six-dimensions hyper chaotic is implemented in confusion phases. In diffusion phases, Fibonacci transformation, XOR operation and cyclic shift are applied.

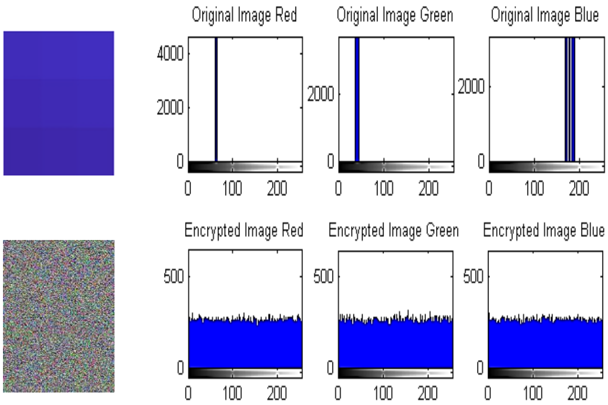


Figure. 6 Histogram analysis of blue image

5. Complexity order (O)

The computational complexity of the algorithm is estimated via the phases required to achieve the encryption operation. The time complexity of the confusion stage is O (N×N). Concerning the diffusion phase, the complexity order is O ((N×N) divided by Bs), Bs stands for the number of image blocks. Thus, the entire complexity order of the suggested cryptography algorithm is O (N×N).

6. Comparison of performance

The performance of suggested algorithm is compared with the state of the art (SoA) approaches. The proposed method is tested on 24-bit colour images generally used in the following different studies: [27, 32-35, 37]. All images are resized to have dimensions of 256 × 256, unless another dimension is mentioned.

Table 6. The comparative result of entropy with SoA methods

Image	Method	Red	Green	Blue
Mandrill	[32] [33] Proposed	7.9973 7.9972 7.9974	7.9974 7.9970 7.9966	7.9975 7.9973 7.9969
House 4.1.05	[34] [35] Proposed	7.9970 7.9973 7.9970	7.9974 7.9972 7.9968	7.9972 7.9973 7.9976
Jelly Beans	[34] Proposed	7.9972 7.9974	7.9972 7.9975	7.9977 7.9972
Tree	[27] [34] [35] Proposed	7.9971 7.9976 7.9973 7.9971	7.9972 7.9971 7.9974 7.9975	7.9971 7.9971 7.9976 7.9970
Female 4.1.01	[35]	7.9971	7.9972	7.9967
	Proposed	7.9967	7.9973	7.9971

Table 7. The comparative result of Correlation coefficient with SoA

Image	Method	Direction	R	G	B
Man-drill	[27] 512*512	H V D	0.0064 0.0191 0.0132	0.0110 -0.0070 0.0056	0.0056 0.0064 0.0190
	[33]	H V D	-0.0027 -0.0174 0.0022	0.00023 0.0105 -0.0017	-0.0008 -0.0732 -0.0029
	Proposed	H V D	0.0033 0.0016 -0.0079	-0.0012 0.0051 0.0029	0.0031 -0.0019 -0.0019
House 4.1.05	[35]	H V D	0.0103 -0.0167 -0.0127	-0.0113 0.0106 0.0052	0.0073 0.0124 0.0018
	Proposed	H V D	0.0029 0.0071 0.0059	0.0061 -0.0053 0.0008	0.0005 0.0036 0.0016
Tree	[27]	H V D	-0.0124 0.0161 0.0058	0.0081 -0.0307 0.0039	0.0278 0.0110 0.0035
	[35]	H V D	0.0077 -0.0177 0.0049	-0.0069 0.0035 -0.0024	0.0032 0.0025 -0.0200
	Proposed	H V D	-0.0032 0.0022 -0.0005	-0.0011 0.0053 -0.0021	0.0021 0.0018 0.0088
Female 4.1.01	[35]	H	-0.0285	-0.0008	0.0003
		V	-0.0050	0.0169	-0.0254
		D	-0.0147	-0.0062	0.0069
	Proposed	H	0.0052	0.0014	-0.0023
		V	0.0024	0.0025	-0.0009
		D	0.0002	-0.0068	-0.0015

Table 5 reports the comparative technique of the proposed method with the SoA techniques employed. From this table, we observe that the performance of the proposed method is comparable with SoA methods. The information entropy outcomes confirm that the suggested method has effectively changed the value of to nearly 8, which is even superior to the preceding technique in some levels as demonstrated in Table 6. Furthermore, if the performance is compared due to correlation depicted in Table 7, mixed observations are obtained. For example, the performance of our method for Mandrill is superior for horizontal, vertical and diagonal orientations in all planes than SoA. Again, for diagonal correlation, the performance of our proposed is superior to [27, 33] but inferior to [27, 33] in diagonal correlation of red plane. Regarding House image, our proposed method is superior to [37] concerning all correlation orientations and planes.

Table 8. NPCR, UACI comparison with SoA methods

Image	Method	Channel	NPCR	UACI
Mandrill	[27] 512*512	R	99.6048	33.4024
		G	99.6162	33.4443
		B	99.5937	33.4964
	[32]	R	99.5900	33.3700
		G	99.5800	33.3900
		B	99.5700	33.5600
	[37]	R	99.6105	33.4350
		G	99.6058	33.5029
		B	99.5887	33.4972
	Proposed	R	99.6109	29.4515
		G	99.6124	27.9861
		B	99.5743	30.5252
House 4.1.05	[34]	R	99.6048	33.5047
		G	99.6216	33.3756
		B	99.6414	33.5031
	[35]	R	99.6094	33.5724
		G	99.5895	33.4664
		B	99.6155	33.3415
	[36]	R	99.6297	33.4144
		G	99.6297	33.6090
		B	99.6267	33.4248
	[37]	R	99.6080	33.4523
		G	99.6034	33.4533
		B	99.5903	33.4830
	Proposed	R	99.6414	27.2729
		G	99.5865	30.0408
		B	99.5850	31.5073
Jelly Beans	[34]	R	99.6567	33.4501
		G	99.5865	33.4492
		B	99.6292	33.5508
	[36]	R	99.6143	33.4069
		G	99.6302	33.6900
		B	99.6140	33.4726
	[37]	R	99.5888	33.3949
		G	99.5972	33.4595
		B	99.5891	33.4865
	Proposed	R	99.5621	30.8366
		G	99.5895	32.4497
		B	99.6353	27.9609
Tree	[27]	R	99.6490	33.4965
		G	99.6231	33.4607
		B	99.6155	33.4270
	[34]	R	99.6292	33.4070
		G	99.6033	33.4116
		B	99.6292	334639
	[35]	R	99.646	33.1465
		G	99.6185	33.3823
		B	99.6048	33.389
	[36]	R	99.6185	33.6858
		G	99.6238	33.6383
		B	99.6395	33.5260
	[37]	R	99.6099	33.4442
		G	99.5920	33.4818
		B	99.6074	33.4131
	Proposed	R	99.5728	30.1176
		G	99.6033	34.1170
		B	99.6155	31.7367
Female 4.1.01	[35]	R	99.617	33.5234
		G	99.5956	33.2569
		B	99.5941	33.343
	Proposed	R	99.5758	32.1182
		G	99.6201	36.5677
		B	99.6109	37.3596

Table 9. The comparative result of key space

Method	Key Space
Ref. [32]	4.2×10^{122}
Ref. [33]	2^{436}
Ref. [35]	2^{239}
Ref. [37]	$2^{512\,+}7*10^{16}$
Ref. [38]	2^{315}
Our proposed	$>d_0 \times 2^{556}$

Whereas our proposed technique is superior to [27, 35] concerning Tree image in all correlation orientations and planes except the vertical orientation of green plane. As observed, the correlation coefficient comparative result of the proposed method is superior to SoA methods in most ways, indicating that our proposed method has better cryptography accomplishment. A comparable type of mix explanations is there when comparing the result for diverse images from proposed technique with SoA approaches via NPCR and UACI metrics depicted in Table 8. While Table 9 compares with SoA researches in key space analysis. Obviously, the proposed algorithm has larger key space than all SoA techniques.

7. Conclusion

The optimal cryptosystem is comprised of two core operations which are confusion and diffusion as proposed by Shannon (1949). The proposed research demonstrates that the novel processes of confusion and diffusion can achieve the perfect secrecy system in cryptography. The proposed implementation yields nearly optimal results for the cipher image's histogram and information entropy. Additionally, the remaining statistical features, such the correlation between nearby pixels, experience a remarkable improvement. The proposed method enhances the key secrecy via increase key space by utilizing 6D Hyper chaotic system. The proposed method contains of multi confusion and diffusion phases, with new methods instead of one conservative image encryption process. The 6D hyper chaotic system is utilizes in both confusion and diffusion phases. The diffused image is partitioned into blocks of dimension 2 × 2, then the Fibonacci Q- matrix with n= 10 is utilized in altering the pixel values for every block besides XOR and cyclic shift operations. Eliminating the strong correlations between nearby pixels is due to the proposed confusion mechanism. The proposed diffusion approach also eliminates the statistical characteristics of the encrypted image while increasing resistance to differential attack. The results of proposed algorithm in concrete data recorded a key space larger than 10176. The proposed technique accomplishes 7.99% of average entropy. Furthermore, the average NPCR and UACI are 99.61% and 31.21, respectively. Moreover, the proposed technique records average correlation coefficient values equal to 0.0030, 0.0024, and 0.0026 in horizontal, vertical, and diagonal orientations.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualization, Donia Fadil Chalob, and Rusul Hussein Hasan; methodology, Donia Fadil Chalob, Rusul Hussein Hasan; software, Donia Fadil Chalob and Rusul Hussein Hasan; validation, Donia Fadil Chalob, Rusul Hussein Hasan; formal analysis, Donia Fadil Chalob; resources, Donia Fadil Chalob; writing—original draft preparation, Donia Fadil Chalob; writing—review and editing, Donia Fadil Chalob, Rusul Hussein Hasan and Rusul Fadhil Yaser; visualization, Rusul Hussein Hasan; supervision, Donia Fadil Chalob, Rusul Hussein Hasan; prepared the figures, Donia Fadil Chalob, Rusul Hussein Hasan. Rusul Fadhil Yaser.

Acknowledgments

We would like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad - Iraq for its support in the present work.

References

[1] C. Sun, E. Wang, and B. Zhao, “Image encryption scheme with compressed sensing based on a new six-dimensional non-degenerate discrete hyperchaotic system and plaintext-related scrambling”, *Entropy*, Vol. 23, No. 3, pp. 1-26, 2021, doi: 10.3390/e23030291.

[2] M. K. Khairullah, A. A. Alkahtani, M. Z. Bin Baharuddin, and A. Al-Jubari, “Designing 1d chaotic maps for fast chaotic image encryption”, *Electron*, Vol. 10, No. 17, 2021, doi: 10.3390/electronics10172116.

[3] Z. Hua, S. Yi, and Y. Zhou, “Medical image encryption using high-speed scrambling and pixel adaptive diffusion”, *Signal Processing*, Vol. 144, pp. 134-144, 2018, doi: 10.1016/j.sigpro.2017.10.004.

[4] J. Chen, Z. liang Zhu, L. bo Zhang, Y. Zhang, and B. qiang Yang, “Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption”, *Signal Processing*, Vol. 142, pp. 340-353, 2018, doi: 10.1016/j.sigpro.2017.07.034.

[5] Z. Hua, Y. Zhou, and H. Huang, “Cosine-transform-based chaotic system for image encryption”, *Inf. Sci. (Ny)*, Vol. 480, pp. 403-419, 2019, doi: 10.1016/j.ins.2018.12.048.

[6] N. N. Jasem and S. A. Mehdi, “Multiple Random Keys for Image Encryption Based on Sensitivity of a New 6D Chaotic System”, *Int. J. Intell. Eng. Syst.*, Vol. 16, No. 5, pp. 576-585, 2023, doi: 10.22266/ijies2023.1031.49.

[7] Q. Zhang and J. Han, “A novel color image encryption algorithm based on image hashing, 6D hyperchaotic and DNA coding”, *Multimed. Tools Appl.*, Vol. 80, No. 9, pp. 13841-13864, 2021, doi: 10.1007/s11042-020-10437-z.

[8] A. A. Rashid and K. A. Hussein, “Image encryption algorithm based on the density and 6D logistic map”, *Int. J. Electr. Comput. Eng.*, Vol. 13, No. 2, pp. 1903-1913, 2023, doi: 10.11591/ijece.v13i2.pp1903-1913.

[9] S. Sun, “A New Image Encryption Scheme Based on 6D Hyperchaotic System and Random Signal Insertion”, *IEEE Access*, Vol. 11, No. June, pp. 66009-66016, 2023, doi: 10.1109/ACCESS.2023.3290915.

[10] S. A. Mehdi and Z. latif Ali, “Image Encryption Algorithm Based on a Novel Six-Dimensional Hyper- Chaotic System”, *Al-Mustansiriyah J. Sci.*, Vol. 31, No. 1, pp. 54-63, 2020, doi: 10.23851/mjs.v31i1.739.

[11] X. Wu, D. Wang, J. Kurths, and H. Kan, “A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system”, *Inf. Sci. (Ny).*, Vol. 349-350, pp. 137-153, 2016, doi: 10.1016/j.ins.2016.02.041.

[12] H. MONDAL, A. PATHAK, S. PAL, A. K. DAS, and S. CHOUDHURY, “Sparse Based Image Encryption Using 6D-Chaotic System and Rc6”, *Sci. Cult.*, Vol. 89, No. November-December, pp. 400-405, 2023, doi: 10.36094/sc.v89.2023.sparse_based_image_encryption.choudhury.400.

[13] S. A. Yassir and H. R. Shakir, “Hybrid Image Encryption Technique for Securing Color Images Transmitted Over Cloud Networks”, *Int. J. Intell. Eng. Syst.*, Vol. 16, No. 6, pp. 850-862,

2023, doi: 10.22266/ijies2023.1231.70.

[14] S. Sun, "A New Image Encryption Scheme Based on 6D Hyperchaotic System and Random Signal Insertion", *IEEE Access*, Vol. 11, No. June, pp. 66009-66016, 2023, doi: 10.1109/ACCESS.2023.3290915.

[15] F. Yu *et al.*, "A 6D Fractional-Order Memristive Hopfield Neural Network and its Application in Image Encryption", *Front. Phys.*, Vol. 10, No. March, pp. 1-14, 2022, doi: 10.3389/fphy.2022.847385.

[16] M. Naim and A. A. Pacha, "A Novel Image Encryption Algorithm Based on Advanced Hill Cipher and 6D Hyperchaotic System", *International Journal of Network Security*, Vol. 25, No. 5, 2023, doi: 10.6633/IJNS.202309.

[17] S. John and S. N. Kumar, "6D Hyperchaotic Encryption Model for Ensuring Security to 3D Printed Models and Medical Images", *J. Image Graph.*, Vol. 12, No. 2, pp. 117-126, 2024, doi: 10.18178/joig.12.2.117-126.

[18] O. Dişkaya, E. Avaroğlu, H. Menken, and A. Emsal, "A New Encryption Algorithm Based on Fibonacci Polynomials and Matrices", *Trait. du Signal*, Vol. 39, No. 5, pp. 1453-1462, 2022, doi: 10.18280/ts.390501.

[19] A. M. Cyriac and B. M. K. Sheeja, "A hybrid encryption scheme based on optical scanning cryptography and Fibonacci-Lucas transformation", *AIP Adv.*, Vol. 11, No. 1, 2021, doi: 10.1063/5.0030619.

[20] C. Maiti, B. C. Dhara, S. Umer, and V. Asari, "An Efficient and Secure Method of Plaintext-Based Image Encryption Using Fibonacci and Tribonacci Transformations", *IEEE Access*, Vol. 11, No. April, pp. 48421-48440, 2023, doi: 10.1109/ACCESS.2023.3276723.

[21] X. Hu, L. Wei, W. Chen, Q. Chen, and Y. Guo, "Color Image Encryption Algorithm Based on Dynamic Chaos and Matrix Convolution", *IEEE Access*, Vol. 8, pp. 12452-12466, 2020, doi: 10.1109/ACCESS.2020.2965740.

[22] Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen, "Image encryption using P-Fibonacci transform and decomposition", *Opt. Commun.*, Vol. 285, No. 5, pp. 594-608, 2012, doi: 10.1016/j.optcom.2011.11.044.

[23] H. Weng et al., "A Quantum Chaotic Image Cryptosystem and Its Application in IoT Secure Communication", *IEEE Access*, Vol. 9, pp. 20481-20492, 2021, doi: 10.1109/ACCESS.2021.3054952.

[24] Z. Tang, Y. Yang, S. Xu, C. Yu, and X. Zhang, "Image Encryption with Double Spiral Scans and Chaotic Maps", *Secur. Commun. Networks*, Vol. 2019, 2019, doi: 10.1155/2019/8694678.

[25] G. Grassi, F. L. Severance, and D. A. Miller, "Multi-wing hyperchaotic attractors from coupled Lorenz systems", *Chaos, Solitons and Fractals*, Vol. 41, No. 1, pp. 284-291, 2009, doi: 10.1016/j.chaos.2007.12.003.

[26] D. Kumar et al., "6D-Chaotic System and 2D Fractional Discrete Cosine Transform Based Encryption of Biometric Templates", *IEEE Access*, Vol. 9, pp. 103056-103074, 2021, doi: 10.1109/ACCESS.2021.3097881.

[27] K. M. Hosny, S. T. Kamal, and M. M. Darwish, "Novel encryption for color images using fractional-order hyperchaotic system", *J. Ambient Intell. Humaniz. Comput.*, Vol. 13, No. 2, pp. 973-988, 2022, doi: 10.1007/s12652-021-03675-y.

[28] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation-substitution-based encryption", *Nonlinear Dyn.*, Vol. 87, No. 1, pp. 337-361, 2017, doi: 10.1007/s11071-016-3046-0.

[29] Y. Xian, X. Wang, X. Yan, Q. Li, and X. Wang, "Image Encryption Based on Chaotic Sub-Block Scrambling and Chaotic Digit Selection Diffusion", *Opt. Lasers Eng.*, Vol. 134, No. May, 2020, doi: 10.1016/j.optlaseng.2020.106202.

[30] N. Khalil, A. Sarhan, and M. A. M. Alshewimy, "An efficient color/grayscale image encryption scheme based on hybrid chaotic maps", *Opt. Laser Technol.*, Vol. 143, No. April, p. 107326, 2021, doi: 10.1016/j.optlastec.2021.107326.

[31] M. Jiang and H. Yang, "Image Encryption Using a New Hybrid Chaotic Map and Spiral Transformation", *Entropy*, Vol. 25, No. 11, 2023, doi: 10.3390/e25111516.

[32] S. M. Basha, P. Mathivanan, and A. B. Ganesh, "Bit level color image encryption using logistic-sine-tent-chebyshev (LSTC) map", *Optik*, Vol. 259, No. 168956, 2022, doi: 10.1016/j.ijleo.2022.168956.

[33] S. Mansoor, P. Sarosh, S. A. Parah, H. Ullah, M. Hijji, and K. Muhammad, "Adaptive Color Image Encryption Scheme Based on Multiple Distinct Chaotic Maps and DNA Computing", *Mathematics*, Vol. 2022, No. 10, 2004. https://doi.org/10.3390/ math10122004.

[34] M. Wang, X. Wang, C. Wang, S. Zhou, Z. Xia, and Q. Li, "Color image encryption based on 2D enhanced hyperchaotic logistic-sine map and twoway Josephus traversing", *Digit. Signal Process.*, Vol. 132, No. 103818, 2023, doi:

10.1016/j.dsp.2022.103818.

[35] F. Meng, and Z. Gu, “A Color Image-Encryption Algorithm Using Extended DNA Coding and Zig-Zag Transform Based on a Fractional-Order Laser System”, *Fractal Fract*, Vol. 7, No. 795, 2023, doi: 10.3390/fractalfract7110795.

[36] M. G. A. Malik, Z. Bashir, N. Iqbal, and Md. A. Imtiaz, “Color image encryption algorithm based on hyper-chaos and DNA computing”, *IEEE Access*, Vol. 8, pp. 88093-88107, 2020, doi: 10.1109/ACCESS.2020.2990170.

[37] E. D. Y. Winarno, K. Nugroho, P. W. Adi, D. E. R. Ignatius, and M. Setiadi, “Combined Interleaved Pattern to Improve Confusion-Diffusion Image Encryption Based on Hyperchaotic System”, *IEEE Access*, Vol. 11, No. July, pp. 69005-69021, 2023, doi: 10.1109/ACCESS.2023.3285481.

[38] F. Yu *et al.*, “Chaos-Based Engineering Applications with a 6D Memristive Multistable Hyperchaotic System and a 2D SF-SIMM Hyperchaotic Map”, *Complexity*, Vol. 2021, 2021, doi: 10.1155/2021/6683284.