Dynamic DNA Rule-Based Fib-Cipher Technique for Securing Medical Images

K. Sudha Kumari[1], C. Nagaraju[2]

[1]Research Scholar, YSR Engineering College of Yogivemana University, Proddatur.
[2]Professor, YSR Engineering College of Yogivemana University, Proddatur.
Email: Sudhakumari.kanchegara@gmail.com

Medical Images are the most important carrier of human information. sending sensitive information of medical Images over the public channels may be critical. One of the ways to secure the reactive to data of the medical Image is applying the cryptographic method for sharing sensitive data over the Internet, it should be sent in encrypted form to prevent the access by wrong person. This paper presents Fib-cypher technique which amalgamate chaotic maps, Q-matric and DNA dynamic rules for achieving fast encryption and decryption along with privacy of images. Fib-cypher techniques provides inverse matrix for every scaling factor in the Image so that decryption is accurate. The strength of the Fib-cypher technique is assessed against plain text and differential attacks and verified that the Fib-cypher technique is faster, stronger and resilient to those attacks.

Keywords: Logistic map, Fibonacci Q-Matrix, DNA rules, Bit shifting operator.

1. Introduction

As digital content got more and more ingrained in our daily lives, people began sharing it online. Nevertheless, the images could also be easily obtained by unauthorized individuals, which presents a significant risk to the sharing of image data [1]. These reasons have made it imperative to preserve the data contained in images. The risk of unauthorized cryptanalysis also extends to the security of the real images. More significantly, certain images may violate people's right to privacy and include issues of national security. For example, satellite tracking and biometric identification fall within this category. Consequently, there has been a global interest from academics and corporate executives on the secure transmission of digital images [2]. For the purpose of concealing image content and safeguarding image material during transmission, digital image security Image encryption is not the same as normal text

encryption, despite the close correlation between image pixels. The starting parameters expressed in terms of persistent values and differentiating parameters have a substantial impact on the sensitivity and dependence of the chaotic system via the Internet on a PC or mobile device. Consequently, a multitude of unique chaos-based image security methods have been developed one after the other [3]. To keep image security at a high level, a strong encryption method is needed. Moreover, images include a large amount of bulk capacity and pixel redundancy, making them vulnerable to cryptanalysis methods to bolster Internet security The many cryptographic advantages of chaos-based image processing, such as its ergodicity, not predictable nature, pseudo-randomness, and great accuracy to beginning conditions and variables, Encryption has become more popular recently. The foundation of using a disordered diffusion paradigm is chaos theory. Beyond chaos, there are further methods such as the DNA rule, bit level scaling, block scrambling, matrix handling, and tensor theory [4], [5], [6], and [7]. The semi-tensor product matrix approach [6] was developed by using double scrambling for images and dual scaling at the bit level to provide increased security throughout the permutation process. Forecasting or deciphering the key that converts a color image into a noisy image is impossible with picture encryption algorithms. Without the key, no one can decrypt the image and recover it. Data concealing is one strategy for image security. A concealed message can be made invisible with the use of a cover image [7], watermarking [8], [9], [10], [11], and encryption [12], [13], [14], [15], [16]. However, recently, researchers have employed chaotic systems to encrypt high-security images [12], [13], [14], and [15]. Since chaotic systems are sensitive, erratic, and unexpected, they are the ideal option for image encryption [6]. Two categories of chaotic systems exist.: 1D and HD [17]. Due of its simplicity, some researchers have encrypted images using 1D chaotic systems [18]. The two stages of diffusion and scrambling, commonly referred to as confusion, are the foundation of the majority of image cryptography techniques. Pixels that are scrambled have different arrangements but the same values. Consequently, the correlation coefficient among adjacent pixels is lowered by the scrambling step. Using the diffusion process on the jumbled picture results in increased security. Diffusion modifies the values of pixels by mathematical procedures. The relationship between the image and its encrypted one is hidden by this method [19], [20]. The limitations of the previous methods will not apply to our proposed picture encryption methodology, which encrypts images using Chaotic map (Logistic map) and integration of FQM with DNA dynamic rules. The approved method successfully got the aforementioned drawbacks and defects to securely and adequately preserve the color image. The analysis identifies flaws in the encryption procedure that the chosen plaintext attack might take advantage of. Therefore, in order to harden the security and resilience of practical cryptographic applications, we propose an encryption technique. The primary contributions of this study are:

1. Using a straight forward logistic map as a starting point, a secret key is generated to jumble the image and later Circular bit shifting was applied.

2. The diffusion step is based on Fib-QM.

3. To encode the scattered pixels, DNA dynamic rules are applied.

4. To guarantee strong security and the capacity to resist different kinds of attacks, the Fib-QM and DNA dynamic rules are incorporated.

2. Preliminaries

2.1 Logistic map

Since LM has a straightforward concept but complex behavior, it can be viewed as an illustration of a chaotic system. Being a one-dimensional map, LM produces a single value—referred to as an iterate—for every iteration of the map. There is only one parameter used in the LM computations.

$$x_{n+1} = \mu * x_n(1 - x_n) \qquad (1)$$

where n = 0, 1, 2, ... and $\mu \in [0, 4]$. According to the study's findings, the system is in a random state when $3.5699 < \mu \leq 4$.

2.2 Circular Bit Shifting

A unique kind of cyclic rotation from one initial location to the next is called a circular shift. Execute either row-wise or column-wise in a circular shift. While switching rows two options for the procedure Circular bit shift refers to bit by bit shifting that can be done either left or right. Occasionally, it functions as a key-based rotation in accordance with our needs.

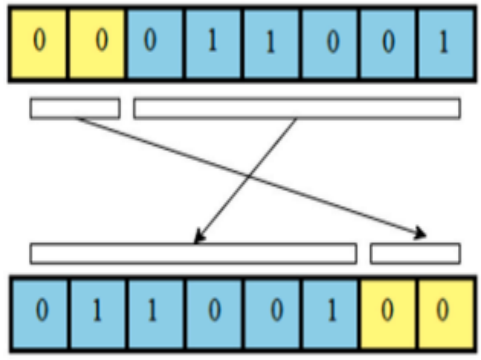

Fig 1:Two bits are shifted in a right circular manner.

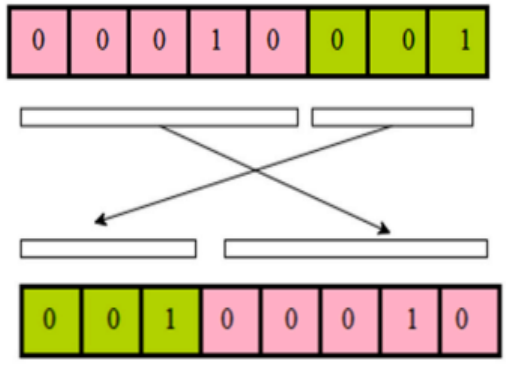

Fig 2:Three-bit circular shift to the left.

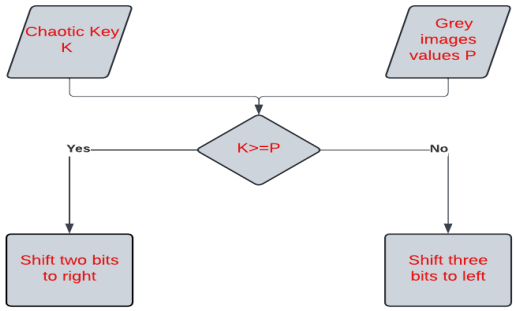

Fig 3: Flowchart for circular shifting.

2.3 Generalized Fibonacci Q-Matrix

The recurrence relation for Fibonacci numbers is as follows.

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

Where $F_0 = 0, F_1 = 1, n = 0, \pm1, \pm2, \ldots$

Using the Fibonacci matrix, these values can be calculated.

$$Q = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

The power matrix is $Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}, n = 0, \pm1, \pm2, \ldots$ (3)

The so-called "Cassini formula" is satisfied by the determinant of the power matrix above. The Q-matrices immediately give a number of important Fibonacci identities, including

$$|Q^n| = |Q|^n \quad (4)$$

Which gives,

$$F_{n-1}F_{n+1} - F_n^2 = (-1)^n \quad (5)$$

$$Q^{n+1}Q^n = Q^{2n+1} \quad (6)$$

Now let's show the matrix in the format that follows:

$$Q^n = \begin{pmatrix} F_n + F_{n-1} & F_{n-1} + F_{n-2} \\ F_{n-1} + F_{n-2} & F_{n-2} + F_{n-3} \end{pmatrix} = \begin{pmatrix} F_n & F_{n-1} \\ F_{n-1} & F_{n-2} \end{pmatrix} + \begin{pmatrix} F_{n-1} & F_{n-2} \\ F_{n-2} & F_{n-3} \end{pmatrix}$$

$$Q^n = Q^{n-1} - Q^{n-2}$$

By rewriting the above equation in the below form:

$$Q^{n-2} = Q^n - Q^{n-1} \quad (7)$$

The inverse matrix Q^{-n} has the following form:

$$Q^{-n} = \begin{pmatrix} F_{n-1} & -F_n \\ -F_n & F_{n+1} \end{pmatrix} \quad (8)$$

In order to invert matrix Q^{-n} from matrix Q^n, the diagonal elements F_{n+1} and F_{n-1} in equation x must be rearranged and taken with the opposite sign, that is

$$Q^{-n} = \begin{pmatrix} -F_{n-1} & F_n \\ F_n & -F_{n+1} \end{pmatrix} \quad (9)$$

The picture pixels are diffused using the Fibonacci Q matrix in the manner described below.

$$E = M * Q_p^n \quad (10)$$

Building upon the basic Fibonacci Q-matrix, new coding theory based on Q matrices is being developed. This is a coding approach that we will examine. Let's use 2*2 matrices to symbolize the first message:

$$M = \begin{bmatrix} m1 & m2 \\ m3 & m4 \end{bmatrix}$$

Where m1,m2,m3,m4 are greater than zero

2.4 Dynamic DNA Rules:

(A)Adenine, (G)guanine, (C)cytosine, and (T)thymine are the four nucleic bases that make up DNA. As per DNA base pairing rules, a doublestranded DNA molecule forms when the complementary chemical nitrogenous bases of the two components are bonded together, matching A with T and C with G. The binary coding rules for DNA sequences created by applying matching sequence rules and corresponding binary system rules are shown in below table.

Table 1: DNA Dynamic Rules

	A	C	T	G
Rule 0	00	11	10	01
Rule 1	00	11	01	10
Rule 2	11	00	10	01
Rule 3	11	00	01	10
Rule 4	10	01	00	11
Rule 5	01	10	00	11
Rule 6	10	01	11	00
Rule 7	01	10	11	00

The rule is selected based on the given formula

Rule number = Grey value mod 8

Table 2: XOR Operation

XOR	A	T	C	G
A	A	T	C	G
T	T	A	G	C
C	C	G	A	T
G	G	C	T	A

3. Existing Method

3.1 Hill cipher methodology

Since the Hill cipher relies on dimension-independent linear algebraic principles, it can be applied to blocks of any size. Brute force assaults can be made against the Hill Cipher, particularly if the key is weak and the block size is tiny. Because an attacker can access both plaintext and ciphertext in a known plaintext assault, Hill Cipher is susceptible to such attacks. Attackers can use cryptanalysis techniques to break the ciphertext and get to know the encryption key matrix, which can be applied to the Hill Cipher. The following operation forms the basis of the encryption process of the Hill cipher:

$$E(K,P) = (K * P) mod 26 \qquad (11)$$

where P is the vector form of the plaintext and K is our key matrix. The encrypted ciphertext is obtained by multiplying these two terms by a matrix.

The following process is the foundation of decrypting using the Hill cipher:

$$D(K,C) = (K^{-1} * C)\ mod\ 26 \qquad (12)$$

where K is our key matrix and C is the ciphertext's vector representation. Multiplying the ciphertext by the inverse of the key matrix yields the decrypted plaintext.

3.2 Drawback:

Understanding the general usage of Hill Ciphers requires an understanding of both encryption and decryption. It's critical to realize that no potential matrix within the system corresponds to a key matrix. Conversely, an inverted key matrix is needed for cipher decryption. The existence of the inverse can be ascertained using the determinant approach. There is no inverse for the matrix if the determinant has a value of 0 or shares a factor other than 1. Consequently, in order to decrypt, one will need to locate or select an alternative key matrix. For recovering results from the cipher, a useful or key matrix with non-zero determinants has to have a coprime component that is perfectly corresponding to the length of the alphabet.

4. Proposed Algorithm

Encryption Algorithm

1. Extract the content from the source image and store it in a two-dimensional array, or message matrix, of size m^n

$$M = \begin{bmatrix} m1 & m2 \\ m3 & m4 \end{bmatrix}$$

2. Generate the unique random values by logistic map as index values according to these indexes the grey level values in the image are shuffled.

$$x_{n+1} = \mu * x_n(1 - x_n)$$

3. To transform old grey level values into new grey level values, circular bit shifting technique is applied on binary values of each grey level in shuffled image such that

If K>=P then

two-bit right shift is applied

else

three-bit left shift is applied

where K, P represents chaotic random value and grey level value

4. Generate Fibonacci series as per the values of p and n.

$$F_{n+1} = F_n + F_{n-1}$$

Where $F_0 = 0$, $F_1 = 1, n = 0, \pm 1, \pm 2, \ldots$

5. Using the values of p and n from Fibonacci series 1 and neg_1, or the positive and negative series, respectively, create the Q_p^n matrix.

$$Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}, n = 0, \pm 1, \pm 2, \ldots$$

6. Convolution product of Q_p^n and M matrix to obtain the final value, after which these contents are stored in an encrypted image representation.

$$E = M * Q_p^n$$

7. Generate Dynamic DNA encrypted rules on encrypted image E such that to strengthen the security by providing confidentiality.

Decryption Algorithm

1. Read the contents of the encoded file

2. Using DNA encrypted rules decode the file into binary format

3. Bit shifting is applied on the binary format n*n matrix.

4. Reshuffling is done using the key generated by using logistic map on the above matrix.

5. Fibonacci series is generated as per the values p and n.
6. And Q_p^{-n} inverse matrix was generated using Fibonacci series.
7. Message Matrix is decoded by convolution of Q_p^{-n} and E.

Working example

Grey image = $\begin{bmatrix} 2 & 3 & 8 \\ 4 & 6 & 7 \\ 1 & 5 & 20 \end{bmatrix}$

Chaotic random values K = $(8,4,3,7,5,2,6,1,0)$

Shuffle the grey image indexes using the chaotic random values P= $(20,6,4,5,7,8,1,3,2)$

Circular Bit shifting:

Condition If $(K \geq P)$ then shift two bits right else shift three bits left

$(8 \geq 20) \rightarrow$ N then apply three bit left, now 20 becomes 130

Final transformed grey image after bit shifting = $\begin{bmatrix} 130 & 192 & 128 \\ 20 & 56 & 32 \\ 4 & 12 & 8 \end{bmatrix}$

Now apply Fib-Q matrix to encrypt the above shuffled grey image $E = M * Q_p^n$

$$E = \begin{bmatrix} 130 & 192 & 128 \\ 20 & 56 & 32 \\ 4 & 12 & 8 \end{bmatrix} * \begin{bmatrix} 8 & 5 & 3 \\ 5 & 3 & 2 \\ 3 & 2 & 1 \end{bmatrix}$$

Normalize the encrypted values, we get $E = \begin{bmatrix} 100 & 61 & 37 \\ 21 & 12 & 7 \\ 3 & 2 & 0 \end{bmatrix}$

Now apply the DNA dynamic rules on the encrypted values

Final Encrypted values using Dynamic DNA values

[GCTAATTCGATTAGGGAATAGGTCTTTAAAAGAAAG]

5. Experimental Analysis

Securing medical images is very challenging task transmitting over internet due to the most dangerous attacks like brute force, Plain text, differential attacks damage the useful information in medical images. In the paper Fib-cypher technique is proposed to provide robust security for medical images and tested the security with the following eleven statistical parameters and produced table of values. Most of the parameter's values are less than 50 such that all gray values are randomized their location more than 50%. this randomization strengthens the security against attacks. This method is compared with hill cypher method and found that it provides better security and time complexity than hill cypher.

5.1 Properties of the parameters

To determine the similarity between original image and encrypted eleven parameters are applied. higher values of parameter represent high similarity and lower values represents lower similarity. According to security lower values produce high security with high randomness in encrypted image and vice versa. the table values represent our method provides better security.

$$\text{jaccard} = \frac{a}{a+b+c} \quad (13)$$

a = quantity of variables that both object I and object J have one of them

b = quantity of variables in which item I is 1 and object J is 0

c = quantity of variables in which object i is equal to 0 and object j to 1

d = quantity of variables in which i and j are both zero

The number of variables is p, which is equal to a+b+c+d.

$$\text{Kulczynski1} = \frac{a}{b+c} \quad (14)$$

$$\text{Kulczynski2} = 0.5 * (\frac{a}{a+b} + \frac{a}{a+c}) \quad (15)$$

Braun = If $(a + b) > (a + c)$then

$$\text{Braun} - \text{Blanquet} := \frac{a}{a+b} \quad (16)$$

else

$$\text{Braun} - \text{Blanquet} := \frac{a}{a + c}$$

$$\text{Dice} = 2 * \frac{a}{(2*a+b+c)} \quad (17)$$

$$\text{Ochiai} = \frac{a}{\sqrt{(a + b) * (a + c)}}$$

$$\text{Sokmich} = \frac{a+d}{a+b+c+d} \quad (18)$$

Simpson= If $(a + b) < (a + c)$ then

$$\text{Simpson} := \frac{a}{a + b}$$

else

$$\text{Simpson} := \frac{a}{a+c} \quad (19)$$

$$\text{Rogers \& Tanimoto} = \frac{(a+d)}{(a+2*(b+c)+d)} \quad (20)$$

$$\text{Soksneath1} = \frac{a}{(a+2*(b+c))} \quad (21)$$

$$\text{Soksneath2} = 0.25 * (\frac{a}{(a+b)} + \frac{a}{(a+c)} + \frac{d}{(b+d)} + \frac{d}{(c+d)}) \quad (22)$$

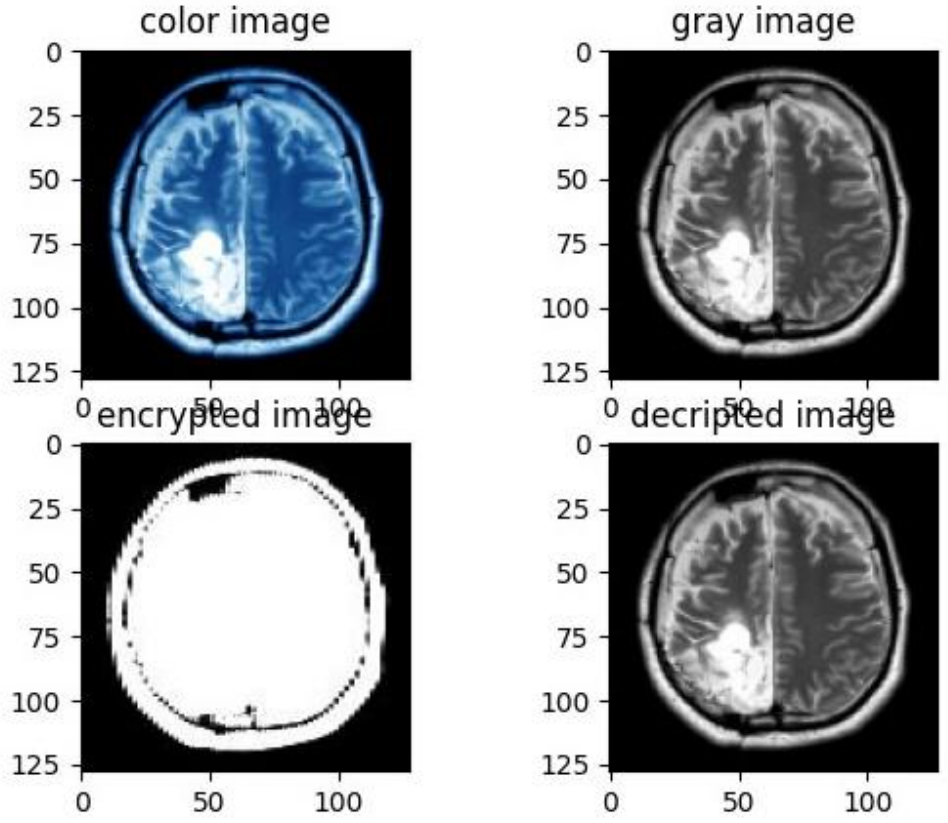

Fig 4: Transformation of the Medical Image

Table 3: Evaluated parameters

Parameters	Hill cypher	Fib-cypher
Jaccord	37.59	24.76
kulczynski1	60.23	32.91
kulczynski2	54.64	61.98
dice	54.64	39.69

ochiai	54.64	49.6
sokmich	52.17	57.31
rogers	35	40
soksneath1	69	73
soksneath2	23	14

Table 4: Comparison of time complexity

Size of image	hill cypher total time	Fib cipher time
255X255	89.96	62.83

6. Conclusion

A dynamic mechanism is introduced by the suggested Fib-cipher with dynamic DNA rules to increase the data's level of secrecy. During encryption, a first-level of secrecy is created by a chaotic map with circular bit shifting. The message is encrypted using the Fibonacci Q matrix, providing as second level of secrecy. The last degree of secrecy was achieved by employing dynamic encryption rules. eleven factors were used to evaluate the performance. It was shown to be sufficiently robust against differential and plain text attacks, but susceptible to brute force attacks such as the trial-and-error approach.

References

1. Hala I. Mohamed, Sarah M. Alhammad, Doaa Sami Khafaga, Osama El komy, and Kalid M. Hosny “A new image encryption scheme based on the hybridization of Lorenz Chaotic map and Fibonacci Q-matrix” IEEE Access Volume 12, 12 pages, 2023.
2. Balasaheb S Tarle, Dr.G.L. Prajapati “On the information security using Fibonacci series” Proceedings of the ICWET '11 International Conference & Workshop on Emerging Trends in Technology, 7 pages, 2011.
3. Sultan Almakdi, Iqra Ishaque, Majid Khan, Mohammed S. Alshehri, Noor Munir “Key dependent information confidentiality scheme based on deoxyribonucleic acid (DNA) and circular shifting” Heliyon(10), 13 pages,2024.
4. Hasan Ghanbari, Rasul Enayatifar , Homayun Motameni “A Fast Image Encryption based on Linear Feedback Shift Register and Deoxyribonucleic acid” Research Square, 14 pages, 2022.
5. Vineet Kumar Singh, Piyush Kumar Singh, K.N. Rai “Image Encryption Algorithm based on Circular Shift in Pixel Bit Value by Group Modulo Operation for Medical Images” 4th International Conference on Computing Communication and Automation (ICCCA), 7 pages, 2018.
6. A. Alghafis, F. Firdousi, M. Khan, S.I. Batool, M. Amin, An efficient image encryption scheme based on chaotic and deoxyribonucleic acid sequencing, Math. Comput. Simulat. 177 (2020) 441–466.
7. R. Lin and S. Li, "An image encryption scheme based on Lorenz hyperchaotic system and RSA algorithm", Secur. Commun. Netw., vol. 2021, pp. 1-18, Apr. 2021.
8. N. Munir, M. Khan, Z. Wei, A. Akgul, M. Amin, I. Hussain, Circuit Implementation of 3D Chaotic Self-Exciting Single-Disk Homopolar Dynamo and its Application in Digital Image Confidentiality, Wireless Networks, 2020, pp. 1–18.
9. M. Khan, N. Munir, A novel image encryption technique based on generalized advanced encryption standard based on field of any characteristic, Wireless Pers. Commun. 109 2 (2019)

849–867.
10. A. Alghafis, N. Munir, M. Khan, An encryption scheme based on chaotic Rabinovich-Fabrikant system and S 8 confusion component, Multimed. Tool. Appl. 80 5 (2021) 7967–7985.
11. M. Jun, F. Yang, R. Chu, Y. Cao, Image Compression and Encryption Algorithm Based on Hyper-Chaotic Map, Mobile Networks and Applications, 2019, pp. 1–13.
12. K.Sudha Kumari, C.Nagaraju "DNA Encrypting rules with Chaotic Maps for Medical Image Encryption" Proceedings of the Fifth International Conference on Intelligent Computing and Control Systems (ICICCS 2021) IEEE Xplore, 2021.
13. J. Karmakar, A. Pathak, N. Debashi, M.K. Mandal, Sparse representation based compressive video encryption using hyper-chaos and DNA coding, Digit. Signal Process. (2021), 103143.
14. K.Sudha Kumari, C.Nagaraju " Encryption of Medical Images Using Chaotic Maps and DNARuleswith Genetic Algorithm" International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 9, Issue 12, December 2022
15. A.A.K. Javan, M. Jafari, A. Zare, M. Khodatars, N. Ghassemi, R. Alizadehsani, J.M. Gorriz, Medical images encryption based on adaptive-robust multi-mode synchronization of chen hyper-chaotic systems, Sensors 21 11 (2021) 3925.
16. K. M. Hosny, S. T. Kamal, M. M. Darwish and G. A. Papakostas, "New image encryption algorithm using hyperchaotic system and Fibonacci Q-matrix", Electronics, vol. 10, no. 9, pp. 1066, Apr. 2021.
17. K. M. Hosny, S. T. Kamal and M. M. Darwish, "A novel color image encryption based on fractional shifted Gegenbauer moments and 2D logistic-sine map", Vis. Comput., vol. 39, no. 3, pp. 1027-1044, Mar. 2023.
18. V. Kumar and A. Girdhar, "A 2D logistic map and lorenz-rossler chaotic system based RGB image encryption approach", Multimedia Tools Appl., vol. 80, no. 3, pp. 3749-3773, Jan. 2021.
19. A.A.K. Javan, M. Jafari, A. Zare, M. Khodatars, N. Ghassemi, R. Alizadehsani, J.M. Gorriz, Medical images encryption based on adaptive-robust multi-mode synchronization of chen hyper-chaotic systems, Sensors 21 11 (2021) 3925.
20. J. Karmakar, A. Pathak, N. Debashi, M.K. Mandal, Sparse representation based compressive video encryption using hyper-chaos and DNA coding, Digit. Signal Process. (2021), 103143