ISSN 2712-0562
Sustainable Engineering and Innovation
Vol. 5, No. 1, June 2023, pp.99-106
https://doi.org/10.37868/sei.v5i1.id187
Review Article

A review of enhanced image techniques using chaos encryption

Nazar Jabbar Alhyani[1], Oday Kamil Hamid[2*], Riyadh Bassil Abduljabbar[3]
[1,2,3] Department of Computer Techniques Engineering, Dijlah University College, Iraq

*Corresponding author e-mail: oday.kamil@duc.edu.iq

Received Oct. 3, 2021
Revised Jan. 29, 2021
Accepted Feb. 16, 2021

Abstract

Secured multimedia data has grown in importance over the last few decades to safeguard multimedia content from unwanted users. Generally speaking, a number of methods have been employed to hide important visual data from eavesdroppers, one of which is chaotic encryption. This review article will examine chaotic encryption methods currently in use, highlighting their benefits and drawbacks in terms of their applicability for picture security.

Keywords: Security, LFSR, AES, Sine, Chebyshev, Arnold's cat, Block cipher

1. Introduction

Different image/video encryption methods have been developed over time to satisfy a variety of requirements for compression ratio, image/frame quality, and bandwidth. While data encryption has a long history, image/video encryption is more recent and calls for specific considerations because of the data's amount and spatial and temporal redundancy. We review the literature on current data chaotic encryption in this article.
Throughout the ages, a wide variety of data encryption techniques have been created and used to safeguard transmitted and stored data and information. A growing variety of ciphers have been created during the past century to protect digital data and communications. Depending on the domain, signal format, and desired level of security, many approaches have been implemented for picture encryption. The security and complexity of these techniques vary. The DES (Data Encryption Standard), AES (Advanced Encryption Standard), RSA (Rivest–Shamir–Adleman), and 3DES ciphers are some of the most well-known and tried ciphers. For real-time video encryption, these block ciphers' high computational cost is a significant barrier. There are several limitations on the kinds of ciphers and/or encryption keys that can be used to encrypt internet video broadcasts that have no set length. As a result, stream ciphers, such as LFSRs and chaotic map ciphers, are preferable to block ciphers for the encryption of GSM signals and video/image streams [1].

2. Cipher streams

A random key generator is such ciphers' primary and most crucial component. The easiest way to create a random key stream of arbitrary length is via a linear feedback shift register (LFSR), which outputs one bit at a time and uses a basic polynomial, a fixed-length starting secret register, and an iterative process. The resulting bit stream was used to XOR encrypt the key portions of the image/video bit stream.

2.1. Linear-feedback shift register (LFSR)

The linear-feedback shift register (LFSR) has clocked storage components (also referred to as flip flops) and feedback paths. The LFSR is successively connected in a flip flop configuration with feedback from contents

of some flip flops output (taps) that XOR together and the result is feedback into a register input as shown in Figure 1 [2]:

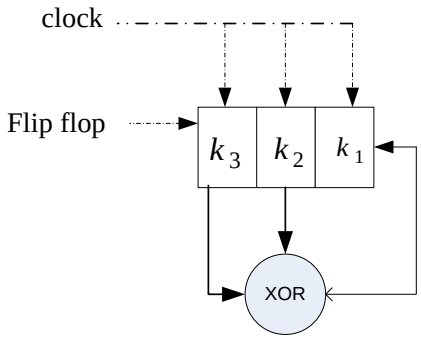

Figure 1. LFSR of degree 3

A so-called basic polynomial determines the register's length and the locations of the taps. For example, if the basic polynomial was x^3+x^2+1, the register would be made up of 3 flip flops (the largest exponential of the original polynomial), and the tap positions would be 3 and 2 in the register sequence, as illustrated in the above diagram. Until the start set (also known as the seed of LFSR), where *n* is the length of LFSR, repeats, there are typically (2*n*-1) potential binary states that may be generated from LFSR. Each bit in an LFSR sequence is linearly connected to the beginning state, which makes it susceptible to correlation and algebraic attacks. This is the major vulnerability of LFSR. Chaos in the creation of random numbers solves this issue [3].

3. Logistic map

A degree two recursive polynomial function called the logistic map has the following definition:

$$x_{n+1} = rx_n(1 - x_n) \tag{1}$$

The control parameter is r, and $n \in \mathbb{Z}^+$, if $n = 0$, x_0 is known as initial condition. As shown in Figure 2, the logistic map's continuous dynamic system is a mapping $f: x \to x$ from the state space to itself, as follows [4, 5]: $x_{n+1} = f(x_n)$

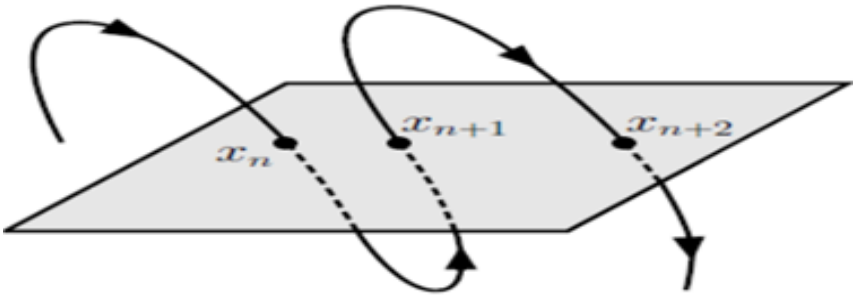

Figure 2. Shows the orbital map's curvature

The cobweb diagram is a visual representational technique that may be used to depict the logistic map. The chaotic logistic map's control parameter (r) and starting condition value (x_0) iterations are displayed in a cobweb diagram. The web of a logistic map is seen in Figure 3 under various beginning conditions and control parameters.

To get around LFSR's linearity flaw, a number of different strategies have been devised. Another method for generating random numbers is the chaos theory. In reality, image/video encryption has frequently employed chaotic maps. The Chaotic Video Encryption Scheme (CVES) [6], developed by Li and Yu, is a method of video encryption based on several digital chaotic systems. This method generates pseudorandom signals to mask the video using a number of chaotic maps, and then the masked video is permuted based on the chaotic map.

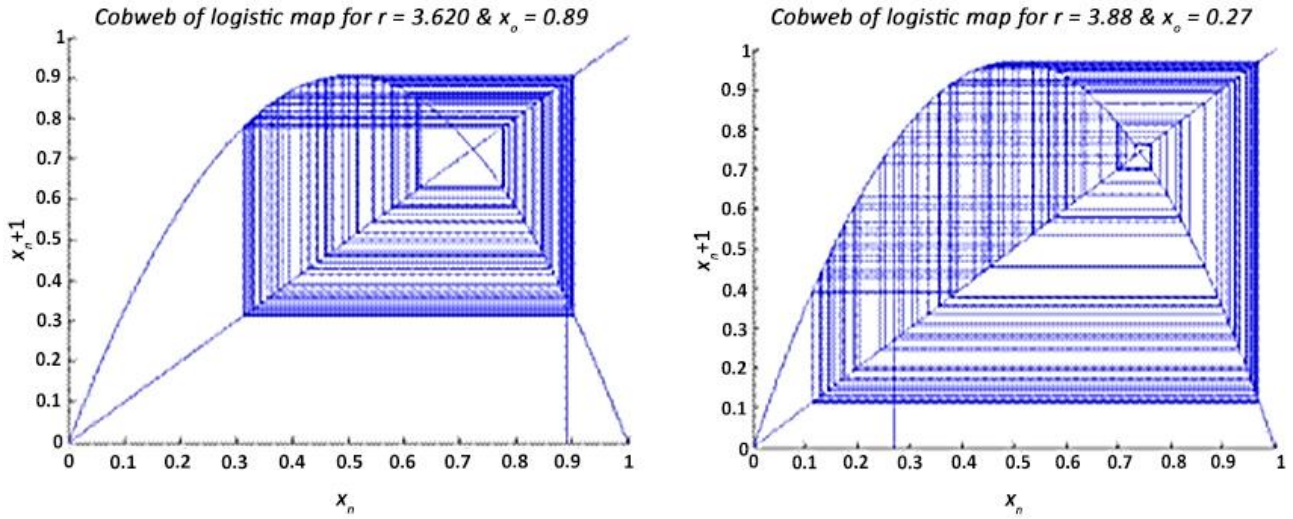

Figure 3. Logistic map's cobweb diagram, which depicts chaotic behavior over a range of initial condition (x_0) and control parameter (r) values; *n* indicates the number of iterations

The chaotic logistic map's key space is not sufficiently vast to prevent brute-force attacks from being successful. Chen and Zhang [7] suggested a new picture encryption based on fusing a chaotic logistic map with a sine map in order to expand key space and the security level of chaotic logistic maps. Two grayscale pictures are created by employing two separate logistic maps in Liansheng and Wang's proposed encryption system, which is based on chaotic logistic maps. First, an original picture is converted into a random grayscale image using a one-dimensional chaotic map. The randomized picture is then split into two random grayscale images using a two-dimensional logistic map. Finally, the original picture [8] is blended with these randomly generated images.

The S-box method of block cipher encryption with logistic maps is used for picture encryption [9]. The four basic operations of the encryption system are first, the plain picture is fed into the permutation stage. Next, the permuted image is divided into 4x4 blocks and entered into *n* iterations of replacement with the addition of the Lorenz key. The final graphic will be XORed with a logistic map key to heighten uncertainty after revisions. Implementing the last step, adds more confusion by deducting each pixel value from 255, to complete the process.

Rabinovich-Fabrikant equations for color picture encryption were proposed by H. J. Yakubu to increase the effectiveness and security of image encryption [10]. The suggested technique uses the system's rich chaotic qualities to adopt the traditional permutation-substitution network in cryptography, ensuring both confusion and diffusion properties for a safe cipher. The approach consists of two stages: the confusion stage, which is accomplished using the complex chaotic characteristics of the Rabinovich-Fabrikant equations, and the diffusion stage, which is accomplished using bit XOR and MOD operations as well as the chaotic map sequence on the confused picture. Dhanalaxmi and Tadisetty [11] present a self-adaptive medical picture encryption technique to increase the encryption robustness of medical images. The pixel grayscale value of the top left corner under Chebyshev mapping produced a comparable size matrix in the top right corner. The matrix previously constructed has replaced the grayscale value of the block in the upper right corner. Up until the top left corner block, the other blocks were encrypted in the same way, clockwise.

An encryption system with high security and great sensitivity was suggested by Benyamin and Seyed [12] and is based on the hyper chaos-based picture encryption approach. Three major components make up the algorithm. First, a row-column technique was used to encrypt the image's rows and columns rather than individual pixels to achieve greater sensitivity, complexity, and security. In addition, a masking procedure is used, applied to each encrypted quarter of the picture (i.e., sub-image), utilizing the data from that sub-image, one of the other sub-images, and the average data from other quarters of the image. The four most important bit planes will finally be encrypted.

Lossless picture encryption was suggested by Shouvik and Arindrajit [13] by combining the DNA application and chaotic logistic map technique. This proposal converts the incoming picture pixels into 8-bit binary and flips them. Following the construction of four pairs of pixels, each pair is reversed, converted to decimal, and put through an XOR operation using bits produced by a chaotic pseudorandom sequence as the key. Using the Dho-Encryption (DE) method, the secret information may be transferred over public networks while being concealed under a cover picture. There are two distinct stages that make up the DE process. Using the Reverse Matrix (RM) encoding technique, the original secret information is concealed under a cover picture in the first procedure. The encoded cover image pixels are moved around inside the picture itself during the second step. Following the shuffle operation, the picture pixels are encrypted using a lookup table and the Alpha-Encryption (AE) procedure. This method's sole foundation is substitution. The encrypted data is transferred to the opposite party for reconstruction when the operations are complete [14].

Duffing maps, also known as Holmes maps at times, are essentially one of the types of chaotic maps that exhibit chaotic behavior. They are discrete in time and give off a dynamic impression. Essentially, if you take any specific pixel coordinates, like (x_m, y_m), and feed them as an input to the Duffing map, this will result in the generation of new pixel coordinates, like(x_{m+1}, y_{m+1}). This is accomplished by the following equations [15]:

$$x_{m+1} = y_m \tag{2}$$

$$y_{m+1} = -ax_m + by_m - {y_m}^3 \tag{3}$$

The variables *a* and *b*, which determine how the map behaves, are often set to 0.2 and 2.75, respectively, to give the map a chaotic behavior. Cross-chaotic maps are a novel sort of chaotic map that Wang and Tian developed. By combining two different chaotic map types that were originally created for one-dimensional, non-linear dynamic systems (Logistic and Chebyshev), the resulting map in two dimensions provided a higher level of security. The following equations define the cross-chaotic map formula that has been created.

$$x_{i+1} = 1 - u{y_i}^2 \tag{4}$$

$$y_{i+1} = \csc\left(K.cos^{-1}x_i\right) \tag{5}$$

The cross-chaotic map system gives off a strong and diverse sense of dynamism where *u* and *K* denote the control parameters, when $K = 6$ and $u = 2$, while *x* and *y* stand in for the original, randomly chosen pixel [16]. Salam and Mohammed [17] introduced the Duffing map in 1996 as a way to randomly shuffle every pixel in a picture. The generated image was then separated into blocks and randomly shuffled using the cross-chaotic map. The final picture, dubbed "key image," was produced using quadratic number spirals, and it will be utilized to accomplish pixel diffusion by generating a number of polynomial equations through Lagrange interpolation.

Chaotic is a method that is frequently used to produce random numbers, and it is distinguished by its effectiveness in the diffusion and permutation processes. Chaos is highly well-suited for picture encryption methods. There are a number of dynamic properties that make this the case, including fundamental conditions, natural dissimulation, and little movement disorders, as it is highly sensitive. The level of rounding between the signal and the random numbers produced by the secret key generator determines how secure this system is. Arnold's cat map is one of the chaotic map types; it is used to move pixels around in a picture without erasing any data or altering their values. Arnold's cat map two-dimensional equation appears as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \ mod\ n \tag{6}$$

Where *p* and *q* are positive integers, *n* is the size of the picture, and *x* and *y* are the positions of the pixels [18, 19]. According to Kamel Faraoun [20], combining basic chaotic maps can result in a very complicated behavior

that suggests a good pseudorandom sequence, increases security, and uses less key space. The method for creating an image encryption technique is based on the hierarchical combination of three chaotic maps. Three chaotic maps are used to create a pseudorandom keystream generator for the system's stream-cipher architecture, which is used for both stream creation and random mixing. The findings demonstrate that even when implemented with finite accuracy, such a design may increase unpredictability and sensitivity to beginning circumstances. The intersecting planes technique within a cube and the color picture encryption algorithm are based on several chaotic maps (Logistic map, Sine map, and Chebyshev map) [21]. The three channels of the color picture are represented by these faces (red, green, and blue). The first step of the method is removing every pixel from the original image and searching for the values of each pixel on the cube's three faces. Next, a circular rotation procedure depending on each pixel's location was employed (row, column). Two similar pixels cannot have the same encrypted value because of this rotation. The proposal then encrypted the pixels using the intersecting planes approach with the associated face. Arnold's cat map, a 2D transformation, was used to shuffle and move every pixel in the original image in accordance with parameters that were obtained from every pixel.

Nonlinear differential equations define and characterize strange attractors. When given enough repetitions, they form fractal patterns that resemble butterfly patterns. Since they are more responsive to the beginning circumstances, they are classified as continuous chaos. This means that even a minor change in the input seed might result in significant changes in the output. Attractors' characteristics can be helpful in the encryption process. Different weird attractors have been developed and used in picture encryption schemes [22, 23], depending on the system equations, beginning circumstances, and system patterns. An image encryption method using Chen attractor and FPGA-generated synthetic images was described by Kumar and Yuvaraja. A synthetic picture was produced using an Altera Cyclone II FPGA, utilizing 438 logic components and 34.03 mW of power consumption [24].

Cloud computing is a modern technology that offers a vast pool of virtualized computer resources. In cloud computing, the user may access these resources from anywhere, at any time, on-demand, and based on the pay-per-usage model. Customers that use cloud computing may share resources, information, and services while online. In order to ensure privacy, encryption systems are therefore largely created to safeguard sensitive data in storage. Amal developed a revolutionary data security system for cloud computing architecture based on a modified version of the AES algorithm using a mix of chaotic maps. Arnold's cat map, on the other hand, was utilized to build a new chaotic mask to replace mix column transformations and increase the key sensitivity by implementing some circular shift on the S-box based on the round keys [25, 26].

One of the popular techniques is the one-dimensional logistic map, which is represented by the following equation.

$$N_{q+1} = z.N_q(1 - N_q) \tag{7}$$

Where $z \in [0, 4]$, $Nq \in (0, 1)$, q=0, 1, 2 ... The approach would be in a decent chaotic state under condition [27] $3.56994 \leq z \leq 4$.

In a two-dimensional approach, Vladimir Arnold proposed a cat map for ergodic theory study. Assume that the image's pixel location coordinates are:
H = {(i, j) | i, j = 1, 2, 3, m}, two control parameters are used in the 2D cat map as follows [28]:

$$i1 = (i+ p*j) \bmod (m) \tag{8}$$

$$j1 = (q*i+ (p*q+1) j) \bmod (m) \tag{9}$$

Where (i, j) original pixel position, (i1, j1) is the new position, (p, q) are positive integers representing control parameters, and m x m plain-image when 2D cat map is carried out one time to the original.

In order to encrypt the color image, Salah and May [29] suggested a novel image encryption method based on fusing 1D logistic maps with 2D cat mapping. The initial part of this method involves making three keys, one for each color (R, G, and B), and using 1D logistic maps to generate random integers to encrypt the image's data. Using 2D cat mapping and random numbers, the pixels in the image that were produced from the first step were shifted about in the second stage. Compressive sensing (CS) theory's fundamental idea is to represent the original signal on a practical basis. It then uses a non-adaptive linear projection onto the observation matrix ϕ, which maintains the signal's structure and is unrelated to the transform basis Ψ, and after that, the signal may be precisely recreated by using a small number of measured values to solve the convex optimization problem or greedy pursuit algorithm [30]. CS is based on two tenets: scarcity and incoherence. Scarcity refers to the indications of interest, and it reflects the concept that a signal's information rate may be significantly lower than what its bandwidth would imply. Incoherence relates to the modality of sensation. The principle behind incoherence is that signals with sparse representation in the representation basis must be dispersed in the sensing basis ϕ [31]. Two key components of the CS framework are sampling (encoding) and recovery (decoding). An image encryption system based on compressive sensing and chaos was presented by Maher and Jinan [32]. CS, which is employed because of a variety of characteristics, significantly lowers the signal sampling rate, power consumption, storage space, and computational complexity. In addition to the aforementioned benefits, CS also combines compression and encryption in one step. Since CS-based encryption is not resistant to the chosen-plaintext attack, the approach alone is ineffective. As a result, the CS output was once more encrypted using a multi-chaotic method. This is utilized to improve security. In addition, using multiple chaotic variables as the key will expand the available key space. This is because the multi-chaotic system has a more complex structure than low-dimensional chaotic systems, making it more challenging to predict since there are multiple initial conditions and parameters. The findings demonstrate that the cipher picture has a significant key space, minimal storage and transmission requirements, excellent security, and little need for encryption time, incoherence, key sensitivity, and strong statistical properties. Additionally, the recovered image is of high quality (to human vision) and retains its properties and ability to be understood.

4. Conclusions

Securing their contents from hackers and eavesdroppers has become a crucial step in protecting their knowledge assets for many organizations that rely on the transmission of digital media objects over open network channels. The most effective method for safeguarding data from security breaches during storage and transmission is to utilize encryption methods. Numerous systems suggested using cryptographic techniques to preserve data security. The easiest way to create a random key stream of arbitrary length is via a linear-feedback shift register (LFSR), which outputs one bit at a time and uses a basic polynomial, a fixed-length starting secret register, and an iterative process. Traditional LFSR generation employs fixed-length primitive polynomials over finite field feedback registers that are randomly initialized. Because the length of the first register determines how long the produced stream is before repeating, chaotic random number generation solves this issue. This review paper includes a thorough investigation of chaotic encryption technology as well as a thorough description of how this technology applies to picture encryption.

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

References

[1] A. Uhl, “Image and video encryption: From Digital Rights Management to secured personal communication,” *Google Books*, 04-Nov-2004. [Online]. Available:

https://books.google.com/books/about/Image_and_Video_Encryption.html?id=CTsJuJBZg7UC. [Accessed: 20-Dec-2022].

[2] C. Paar and J. Pelzl, Understanding cryptography: a textbook for students and practitioners, Springer Science \& Business Media, 2009.

[3] J. L. Imana, "LFSR-based bit-serial $GF(2^m)$ multipliers using irreducible trinomials," *IEEE Transactions on Computers*, pp. 1–1, 2020.

[4] Kocarev and Lian, *Chaos-based cryptography*. Berlin: Springer-Verlag Berlin and Heidelberg GmbH & Co. K, 2011.

[5] Y. Mao and G. Chen, "Chaos-based Image Encryption," *Handbook of Geometric Computing*, pp. 231–265.

[6] A. Pande and J. Zambreno, "A chaotic encryption scheme for real-time embedded systems: Design and implementation," *Telecommunication Systems*, 2011.

[7] C. L. P. Chen, T. Zhang, and Y. Zhou, "Image encryption algorithm based on a new combined chaotic system," *2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2012.

[8] S. Liansheng, W. Wengang, D. Kuaikuai, and Z. Zhiqiang, "A novel grayscale image encryption algorithm based on logistic map," *2014 International Conference on Information Science, Electronics and Electrical Engineering*, 2014.

[9] D. F. Chalob, A. A. Maryoosh, Z. M. Esa, and E. N. Abbud, "A new block cipher for image encryption based on Multi Chaotic Systems," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 6, p. 2983, 2020.

[10] H. Yakubu, E. Dada, S. Joseph and A. Anukem, "A new chaotic image encryption algorithm for digital colour images using rabinovich-fabrikant equations," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 17, no. 1, 2019.

[11] D. Banavath and T. Srinivasulu, "A New Self-Adaptive Approach For Medical Image Security," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 16, no. 6, 2018.

[12] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki and M. R. Mosavi, "A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos," *Multimedia Tools and Applications*, vol. 74, no. 3, pp. 781-811, 2015.

[13] S. Chakraborty, A. Seal, M. Roy, and K. Mali, "A novel lossless image encryption method using DNA substitution and chaotic logistic map," *International Journal of Security and Its Applications*, vol. 10, no. 2, pp. 205–216, 2016.

[14] S. Al-Mutairi and S. Manimurugan, "An efficient secret image transmission scheme using Dho-encryption technique," *International Journal of Computer Science and Information Security*, vol. 14, no. 10, p. 446, 2016.

[15] P. NagaSrinivasu and C. Seshadri Rao, "A multilevel image encryption based on Duffing map and modified DNA hybridization for transfer over an unsecured channel," *International Journal of Computer Applications*, vol. 120, no. 4, pp. 1–4, 2015.

[16] X. Wang, B. Tian, C. Liang, and D. Shi, "Blind image quality assessment for Measuring Image Blur," *2008 Congress on Image and Signal Processing*, 2008.

[17] "An improve image encryption algorithm based on multi-level of chaotic maps and Lagrange interpolation," *IRAQI JOURNAL OF SCIENCE*, vol. 59, no. 1A, 2018.

[18] T.-gong Pan and D.-yong Li, "A novel image encryption using Arnold cat," *International Journal of Security and Its Applications*, vol. 7, no. 5, pp. 377–386, 2013.

[19] E. Hariyanto and R. Rahim, "Arnold's cat map algorithm in digital image encryption," *International Journal of Science and Research (IJSR)*, vol. 5, no. 10, pp. 1363-1365, 2016.

[20] K. Faraoun, "Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption.," *Int. Arab J. Inf. Technol.*, vol. 7, no. 3, pp. 231-240, 2010.

[21] M. Es-Sabry, N. El Akkad, M. Merras, A. Saaidi, and K. Satori, "A new color image encryption algorithm using multiple chaotic maps with the intersecting planes method," *Scientific African*, vol. 16, 2022.

[22] L. Wang, H. Song, and P. Liu, "A novel hybrid color image encryption algorithm using two complex chaotic systems," *Optics and Lasers in Engineering*, vol. 77, pp. 118–125, 2016.

[23] H. M. Al-Najjar and A. M. AL-Najjar, “Multi-chaotic image encryption algorithm based on one time pads scheme,” *International Journal of Computer Theory and Engineering*, pp. 350–353, 2012.

[24] S. Arumugham, S. Rajagopalan, S. Rethinam, S. Janakiraman, C. Lakshmi, and A. Rengarajan, “Synthetic Image and Strange Attractor: Two folded encryption approach for secure image communication,” *Advances in Intelligent Systems and Computing*, pp. 467–478, 2020.

[25] D. Mukhopadhyay, G. Sonawane, P. S. Gupta, S. Bhavsar and V. Mittal, "Enhanced security for cloud storage using file encryption," arXiv preprint arXiv:1303.7075, 2013.

[26] M. R. Bin Emdad and M. S. Khan, “A standard data security model using AES algorithm in cloud computing,” *International Journal of Software & Hardware Research in Engineering*, vol. 7, no. 5, 2019.

[27] M. Xu, “Cryptanalysis of an image encryption algorithm based on DNA sequence operation and hyper-chaotic system,” *3D Research*, vol. 8, no. 2, 2017.

[28] M. Ahmad and M. S. Alam, "A new algorithm of encryption and decryption of images using chaotic mapping," *International Journal on computer science and engineering*, vol. 2, no. 1, pp. 46-50, 2009.

[29] S. T. Allawi, M. M. Abbas and R. H. Mahdi, "New Method for Using Chaotic Maps to Image Encryption," *International Journal of Civil Engineering and Technology (IJCIET)*, vol. 9, no. 13, 2018.

[30] V. Athira, S. N. George, and P. P. Deepthi, “A novel encryption method based on compressive sensing,” *2013 International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s)*, 2013.

[31] R. Baraniuk, “Compressive sensing [lecture notes],” *IEEE Signal Processing Magazine*, vol. 24, no. 4, pp. 118–121, 2007.

[32] M. K. Mahmood, J. N. Shehab and others, "Image encryption and compression based on compressive sensing and chaos," *International Journal of Computer Engineering and Technology*, vol. 5, no. 1, 2014.