www.ijaceeonline.com ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume: 8 Issue: 2, February 2023, pp. 1 – 8

A Review of Enhanced Image Techniques Using Chaos Encryption

Nazar Jabbar Alhyani
Lecturer, Department of computer techniques engineering,
Dijlah University college, Iraq, Baghdad
Email: nazar.alhayani@duc.edu.iq

Oday Kamil Hamid
Lecturer, Department of computer techniques engineering,
Dijlah University college, Iraq, Baghdad
Email: oday.kamil@duc.edu.iq

Riyadh Bassil Abduljabbar
Assistant Professor, Department of computer techniques engineering,
Dijlah University college, Iraq, Baghdad
Email: riyadh.bassil@duc.edu.iq

Abstract: *Over the past several decades, the need for secured multimedia data has increased as a means of protecting multimedia materials from unauthorized users. In general, a variety of techniques have been used to conceal crucial visual data from prying eyes, one of which is chaotic encryption. The chaotic encryption techniques now in use will be examined in this review article, with an emphasis on the advantages and disadvantages of each approach as it relates to photo security.*

Keyword: *LFSR; AES; Chebyshev; Arnold Cat; Block Cipher; Image Encryption.*

1. INTRODUCTION

Over time, various aspects of conversion efficiency, photo resolution, and limited bandwidth have been satisfied by possible result cryptographic algorithms. In contrast to data encryption, which has a longstanding tradition, image/video cryptography is relatively modern and necessitates special considerations due to the volume of data and the presence both of temporal and spatial duplication. We review the literature on current data chaos and encryption in this essay.

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 fulfill the needs of protecting 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, AES, RSA, 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].

1.1 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 employs simple polynomials and produces bits at a moment. 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 or video bit stream.

1.1.1 Linear Feedback Shift Register

Cranked amounts of the data, often known as flip flops, and feedback routes are features of such Linear Feedback Shift Register (LFSR). These elements of a few flip-flop outputs (presses) that XOR together can be consecutively linked to the LFSR plus feedback, and the result is communication into a register input as depicted in Figure 1. [2]:

Cite this paper:

Nazar Jabbar Alhyani, Oday Kamil Hamid, Riyadh Basssil Abduljabbar, "A Review of Enhanced Image Techniques Using Chaos Encryption", International Journal of Advances in Computer and Electronics Engineering, Vol. 8, No. 2, pp. 1-8, February 2023.

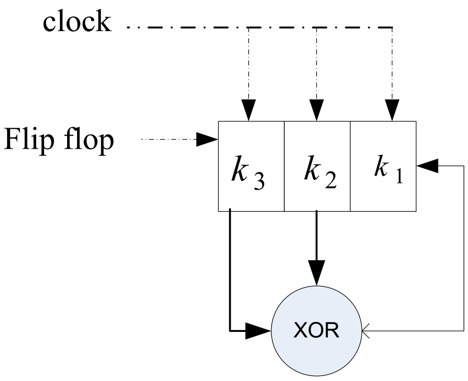


Figure 1 LFSR of degree 3

A so-called “basic polynomial” The duration of the register and the position of the entries are determined by this function. For example, if the underlying polynomials were x3+x2+1, the registers would've been made up of three flip flops (the biggest exponential of the original polynomial), as well as the tapping locations in the register succession would indeed be 3 and 2, as shown in the picture above. There are normally (2n-1) possible binary phases that may be formed from LFSR until the beginning setting (usually referred to as the grain of LFSR), where n is the width of LFSR, repetitions. In an LFSR sequence, each bit is linear with respect to the starting 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 [2, 3].

2. The Logistic Map

The logistic map is a recursive polynomial function of degree 2, defined as follows:

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

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: $x_{n+1} = f(x_n)$

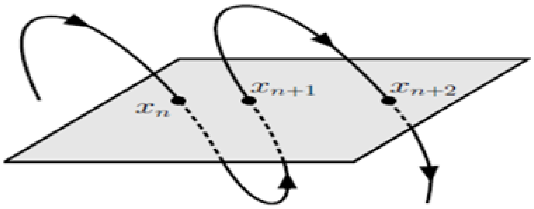


Figure 2 shows the orbital map's curvature [4, 5]

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.

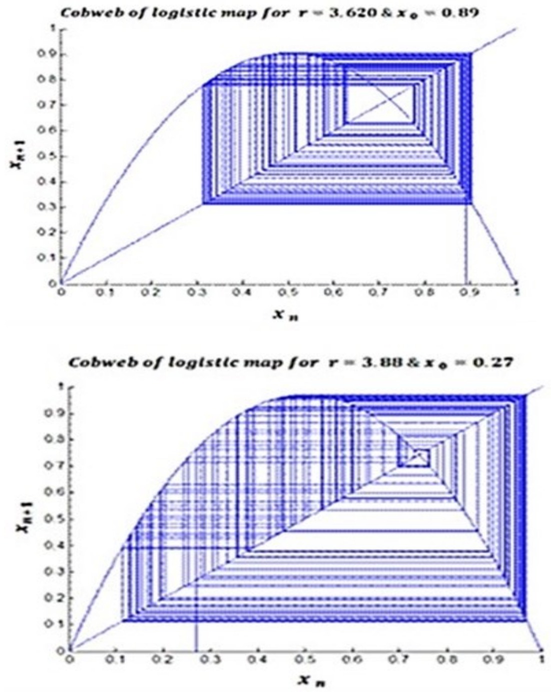


Figure 3 Shows a logistic map's cobweb diagram, which depicts chaotic behaviour over a range of initial condition (x_0 and control parameter (r) values. n indicates the number of iterations [6, 7]

To get around the LFSR's linearity flaw, a number of different strategies have been devised. The chaos theory is another method for generating random numbers. In reality, image/video encryption has frequently employed chaotic maps. Li and Yu's Chaotic Video Encryption Scheme (CVES) [6] is a video encryption scheme based on numerous digital chaotic systems. Using a variety of chaotic maps, this approach creates pseudo-random signals to mask the video, and then the masked video is permuted depending on the chaotic map. The chaotic logistic map's key space is insufficiently large to avoid effective brute-force assaults. Chen and Zhang [7] suggested a new image encryption method that combines a chaotic logistic maps with a sine chart to increase the secret region and safety performance of chaotic logistic maps. In Liansheng and Wang's suggested cryptosystem, which would be founded on chaotic logistic maps, two monochrome images are formed by deploying two different logistical 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.

According to the S-box method of block cipher encryption with logistic maps for picture encryption, as presented in [9], the four basic operations of the encryption system are as follows: 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. Implement the complement step, which 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]. This proposed approach takes advantage of the system's rich chaotic features to implement the classic pseudorandom networks in security, ensuring the confusion and dispersion characteristics needed for secure encryption. The method is divided into two stages: the confusion stage, which is achieved by utilizing the complicated chaotic properties of the Rabinovich-Fabrikant solutions, and the spread 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-sized 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, more complexity, and greater security. In addition, a masking procedure performed on every encrypting quadrant of the frame (i.e., sub-image), employing the information from the sub-image, another of the comment thread, and the averaged information from other quarters of the image. Lastly, the four largest data aircraft would be encoded.

Lossless picture encryption was suggested by Shouvik and Arindrajit [13] by combining the DNA application with the 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, 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 Reveres 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 other 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 adjusted to 0.2 and 2.75, correspondingly, to provide a chaotic behaviour for the map. 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.

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

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

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 the "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 to picture encryption methods; there are a number of dynamic properties that make this the case, including: For fundamental conditions, natural dissimulation, and a few movement disorders, 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 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. The Arnold's Cat Map's 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 very complicated behavior that suggests a good pseudorandom sequence, increases security, and uses a smaller 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 based on several chaotic maps (the logistic map, the Sine map, and the Chebyshev map) are explained in [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 (row, column) was employed. Two similar pixels cannot have the same encrypted value because of this rotation. The pixels were then encrypted using the intersecting planes approach and the associated face, according to the proposal. Arnold 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. They form fractal patterns that resemble butterfly patterns when repeated enough times. They are classified as "continuous chaos" because they are more responsive to the initial circumstances. 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 attracters' 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 and utilized 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 a pay-per-use 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 has 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. The Arnold 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 (1D) 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 decently chaotic state under condition [27] $3.56994 \leq z \leq 4$.

A two-dimensional approach 2D V.I. Arnold proposed a cat map for ergodic theory study. Assume that the image's pixel location coordinates are.

$H = \{(i, j) \mid i, j = 1, 2, 3, m\}$, two control parameters are used in 2D Cat map is 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) is the original pixel location, (i1, j1) is the starting position, (p, q) are positive integers indicating system parameters, and (m x m) is the plain-image after applying a 2D Cat map once to the official version. Salah and May [29] proposed an unique picture encoding approach on merging 1D-Logistic maps with 2D cat patterning to encrypt the color image. The first step in this approach is to produce three keys, one for each color (R, G, and B), and then use 1D-Logistic maps to generate random integers to encrypt the image's contents. In the second phase, the pixels in the picture created in the first phase were pushed around using 2D cat mapping and random integers. 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. 1) Scarcity: This refers to the indications of interest; sparsity reflects the concept that a signal's information rate may be significantly lower than what its bandwidth would imply. And 2) incoherence, which relates to the modality of sensation, the principle behind which 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 again encrypted using a multi-chaotic method. This is used 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 it has multiple initial conditions and parameters.

The findings demonstrate that the cipher picture has significant key space, minimal storage and transmission requirements, excellent security, 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 the image's properties as well as its ability to be understood. One of the main building blocks of symmetric key algorithms that implement substitution is the substitution box (S-box). The building blocks of symmetric cryptosystems are substitution boxes. For encryption methods to achieve the notion of complete security, substitution tables, or S-boxes, are essential.

The chaotic Lorenz system represents a major advancement in the investigation of system dynamics. Which proposes using chaotic maps to define the chaotic dynamics. E. Lorenz [33, 34] was the first to give a mathematical model of air movement in the atmosphere. The chaotic differential equation system is stated as follows:

$$\frac{dx}{dt} = a(y - x) \tag{10}$$

$$\frac{dx}{dt} = bx - y - xz \tag{11}$$

$$\frac{dx}{dt} = xy - cz \tag{12}$$

Where the intervals for variables *x, y* and z are given $-60 \le x \le 60$, $-60 \le y \le 60$, $-60 \le z \le 60$. For chaotic behaviours, the values for parameters *a, b*, and *c* are $a = 10$, $b = 28$ and $c = 8/3$ respectively.

For the picture encryption technique, it is suggested that S-boxes and chaotic maps be combined. The picture encryption technique is based on Temadher and Iqtadar's [35] combination of suggested S-boxes and the Lorenz chaotic system. There are two stages to the proposal. Multiple S-boxes are used in place of a single S-box to perform substitution. 16 different S-boxes are based on a projective general linear group and 16 primitive irreducible polynomials of the Galois field of order 256. These S-boxes are then combined with a chaotic map as part of an image encryption scheme. The disturbed Lorenz chaotic system may generate three chaotic sequences, which correspond to the variables x, y, and z. Based on x, y, and z, a new pseudo-random chaotic sequence called ki is created. The chaotic sequence ki and the XOR operation are used to encrypt the plain picture for image encryption.

Pixel position and information on the gray scale can be used to define a digital picture in the spatial realm. The combination of the two elements is the foundation for digital picture encryption. The two main components of a traditional picture encryption technique are pixel scrambling and gray diffusion. Scrambling an image merely modifies the positions of the individual pixels; it has no effect on pixel values or statistical properties. It is impossible for a single cipher text pixel to have an impact on all the other cipher text pixels when utilizing simply gray diffusion. In order to integrate scrambling and gray diffusion into the picture encryption technique, Lei and Shoulin [36] suggested chaotic mapping and the discrete wavelet transform. First, in order to improve the properties of picture confusion and diffusion, image encryption algorithms frequently combine grayscale diffusion and scrambling. The wavelet transform is then used to process the picture.

Finally, the Arnold mapping expression maps the picture. Another picture encryption method based on chaotic block permutation and XOR operation was presented by Raneem and Osamain [37]. It divides the original color image into blocks of millimeters. Key streams are generated using chaotic maps with a starting state of (x, y, v, w). The separated picture blocks are permuted using the resulting key stream. To create a single image, the rearranged image blocks are combined as shown in Figure 4.

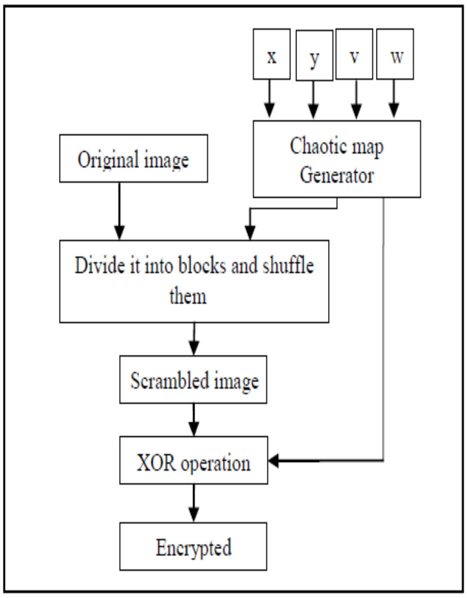


Figure 4 shows the block diagram of the encryption method [37].

The original image is first separated into equal-sized chunks. Then, one key stream is created by permuting two key streams that were first created using two chaotic maps. Then, a portion of the key stream is used to shuffle the picture blocks. To obtain the encrypted picture, the scrambled image is finally XORed with the key stream. Compressive sensing concept is an entirely different strategy to signal sampled reduction. Assume the message f of size N*1 may be described as a sparse basis Ψ:

$$f = \Psi_s \tag{13}$$

Ψ is a N×N sparse orthogonal basis, where s is a sparse coefficient. If the component s contains k << N nonzero coefficients, after which is thought to represent the signal's sparse basis. Then Ψ is said to be the sparse basis of the signal f.

$$y = \emptyset f = \emptyset \Psi_s = As \tag{14}$$

where Ψ is a projection matrix of size m × N. y is a linear measure of size m × 1 (m < N). Furthermore, the detecting array A must meet the RIP conditions as in Equation [15].

$$(1 - \delta_k)\|x\|_2^2 \leq \|Ax\|_2^2 \leq (1 + \delta_k)\ \|x\|_2^2 \tag{15}$$

In the equal distances constant $\delta_k \in (0, 1)$, k is the number of nonzero factors s.

The relation to this matter f measured using ϕ can be reconstructed through y.

$$\min\|s\|_0 s.t. y = As \tag{16}$$

Numerous reconstruction strategies, including the orthogonal tracking algorithm, have been developed to address the aforementioned non-convex difficulties (OMP), smooth norm SL_0 and so on.

The mathematical definition of the Chebyshev chaotic map is as follows:

$$r_{i+1} = \tau(r_j) = \cos\left(\alpha.arcos(r_j)\right) \tag{17}$$

α is a positive integer, $r_j \in [-1, 1]$, when $r_0 \in [-1, 1]$ is the initial value, $R_j = \{r_j = \tau^{\,j}(r_0)\}$, j = 0, 1, 2, ..., r_0 is a chaotic sequence. α, r_0 as the key of the cryptosystem. Sensation matrices and randomized bands are built using Chebyshev chaotic sequences. Many techniques for picture compression and encryption have been suggested during the past ten years that are based on combined compression and encryption. An image compression and encryption technique based on a structurally chaotic measurement was presented by Xingyuan and Yining in [38].

Mask with arbitrary phase and matrix the algorithm uses the Chebyshev chaotic sequence to produce the flip permutations matrix, sample selection, chaotic cyclical labyrinth, and stochastic mask for constructing the sensory structure. Compressed sensing simultaneously compresses and encrypts the original picture, which is then re-encrypted using a two-dimensional fractional Fourier transform.

Binary information is communicated by chaotic signals derived from distinct bits in binary chaotic shift keying (CSK) modulation. Encoding an information signal is accomplished by sending one chaotic signal at a time. So, if the information signal binary bit is "1," the chaos signal will be communicated; otherwise, it will not be transferred. Figure 5 depicts CSK modulation and demodulation. The two chaotic signals can be obtained by utilizing either the same chaos system with different parameters or two distinct systems. The transmitted signal may be characterized using the following formula [39]:

$$s(t) = \begin{cases} x_1(t) & ,1 \text{ is transmitted} \\ x_0(t) & ,0 \text{ is transmitted} \end{cases} \tag{18}$$

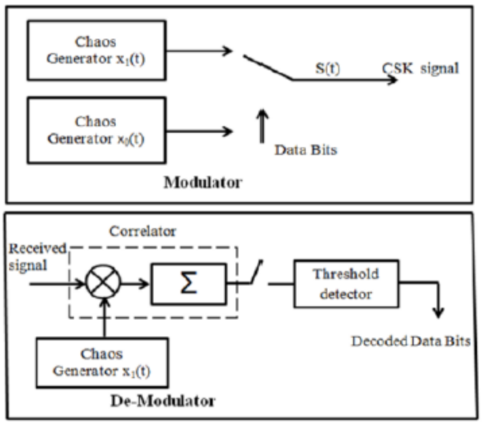


Figure 5 Block diagram of the CSK for modulator and demodulator [40]

In [9], Ashwaq and Bahaa introduced another combined compression and encryption approach based on compression and hyper-chaotic map techniques in which the RGB picture is divided into R, G, and B subbands and then compressed using a lossless technique for each band. The produced chaotic sequences from the 3D chaotic system are used to code the compressed results by encoding the three bands using the chaotic shift encoding (CSK) modulation concept.

3. CONCLUSION

Since many enterprises which relies on the delivery of digital multimedia through public network links, shielding the values from attackers and listening devices has evolved into a critical step in preserving their intellectual resource. 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's 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.

REFERENCES

[1] Uhl, Andreas, and Andreas Pommer, (2005). "Image and Video Encryption from Digital Rights Management to Secured Personal Communication", *Springer*. Part of the book series: Advances in Information Security ADIS, vol. 15. pp.10-12.

[2] Christof Paar, and Jan Pelzl, Understanding cryptography: a textbook for students and practitioners, retrieved date:[September, 2009], online available at:

[3] http://swarm.cs.pub.ro/~mbarbulescu/cripto/Understanding%20Cryptography%20by%20Christof%20Paar%20.pdf

[4] Imana, Pascual, and Josh Luis, (2021). "LFSR-based bit-serial $GF(2^m)$ multipliers using irreducible trinomials," *IEEE Transactions on Computers*, vol. 70, Issue. 1, pp.156–162.

[5] Kocarev, Ljupco and Lian Shiguo, (2001). "Chaos-Based Cryptography: A Brief Overview." *IEEE Circuits and Systems Magazine*, vol. 1, Issue. 3, pp. 6–21.

[6] Mao, Yaobin, and Guanrong Chen, (2005). "Chaos-Based Image Encryption." *Handbook of Geometric Computing*, pp. 231–265.

[7] Pande, Amit, and Joseph Zambreno, (2013). "A Chaotic Encryption Scheme for Real-Time Embedded Systems: Design and Implementation." *Telecommunication Systems*. vol. 52, pp. 551–561.

[8] Philip, Chen, Zang, Tong and Zhou Yicong, (2012). "Image encryption algorithm based on a new combined chaotic system."*IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 2500-2504

[9] Liansheng, Sui, et al. (2014). "A Novel Grayscale Image Encryption Algorithm Based on Logistic Map." *International Conference on Information Science, Electronics and Electrical Engineering*", pp. 222-225.

[10] Chalob, Donia Fadhil, et al. (2020). "A New Block Cipher for Image Encryption Based on Multi Chaotic Systems." *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, Issue. 6, p. 2983

[11] Yakubu, Dada, Emmanuel and Joseph Stephen, (2019). "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, Issue. 1. pp. 15-23

[12] Banavath, Dhanalaxmi and Srinivasulu Tadisetty, (2018). "A New Self-Adaptive Approach For Medical Image Security," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 16, Issue. 6.

[13] Norouzi, Benyamin, et al. (2013) "A Novel Image Encryption Based on Row-Column, Masking and Main Diffusion Processes with Hyper Chaos." *Multimedia Tools and Applications*, vol. 74, Issue. 3, pp. 781–811.

[14] Chakraborty, Shouvik, et al. (2016). "A Novel Lossless Image Encryption Method Using DNA Substitution and Chaotic Logistic Map." *International Journal of Security and Its Applications*, vol. 10, Issue. 2, pp. 205–216.

[15] Al-Mutairi, Saad, and Manimurugan Shanmuganathan, (2016). "An efficient secret image transmission scheme using Dho-encryption technique," *International Journal of Computer Science and Information Security*, vol. 14, Issue. 10, pp. 446-460.

[16] Naga, Srinivasu, and Seshadri Rao. (2015). "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, Issue. 4, pp. 1–4.

[17] Wang, Xin, et al. (2008). "Blind Image Quality Assessment for Measuring Image Blur." *2008 Congress on Image and Signal Processing*. vol.1. pp. 467-470.

[18] Abdulnabi, Salam and Sabbih Mohammed, (2018). "An Improve Image Encryption Algorithm Based on Multi-Level of Chaotic Maps and Lagrange Interpolation." *Iraqi Journal of Science*, vol. 59, Issue. 1A. pp. 179-188.

[19] Pan, Tian-gong, and Da-yong Li. (2013). "A Novel Image Encryption Using Arnold Cat." *International Journal of Security and Its Applications*, vol. 7, Issue. 5, pp. 377–386.

[20] Hariyanto, Eko and Rahim Robbi, (2016). "Arnold's cat map algorithm in digital image encryption." *International Journal of Science and Research (IJSR)*, vol. 5, Issue. 10, pp. 1363-1365.

[21] Faraoun, Kamel. (2010). "Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption." *Int. Arab J. Inf. Technol.,* vol. 7, Issue. 3, pp. 231-240.

[22] Sabry, Mohammed, et al. (2022). "A New Color Image Encryption Algorithm Using Multiple Chaotic Maps with the Intersecting Planes Method." *Scientific African*, vol. 16.

[23] Wang, Leyuan, et al. (2016). "A Novel Hybrid Color Image Encryption Algorithm Using Two Complex Chaotic Systems." *Optics and Lasers in Engineering*, vol. 77, pp. 118–125.

[24] Al-Najjar, Hazem Mohammad, and Asem Mohammad AL-Najjar. (2012). "Multi-Chaotic Image Encryption Algorithm Based on One Time Pads Scheme." *International Journal of*

Computer Theory and Engineering, vol. 4, Issue 3, pp. 350–353.

[25] Arumugham, Sridevi, et al. (2020). "Synthetic Image and Strange Attractor: Two Folded Encryption Approach for Secure Image Communication." *Advances in Intelligent Systems and Computing, Part of the Advances in Intelligent Systems and Computing book series (AISC)*, vol. 1082, pp. 467–478.

[26] Mukhopadhyay, Debajyoti, et al. (2014). "Enhanced security for cloud storage using file encryption," *arXiv preprint arXiv: 1303.7075*.

[27] Bin Emdad, et al. (2019) "A Standard Data Security Model Using AES Algorithm in Cloud Computing." *International Journal of Software & Hardware Research in Engineering*, vol. 7, Issue. 5, pp. 49-53.

[28] Xu, Ming. (2017). "Cryptanalysis of an Image Encryption Algorithm Based on DNA Sequence Operation and Hyper-Chaotic System." *3D Research*, vol. 8, Issue. 15, pp-1-9.

[29] Mishra, Mayank, et al. (2014). "A new algorithm of encryption and decryption of images using chaotic mapping," *International Journal on computer science and engineering*, vol. 4, Issue 7, pp. 741-746.

[30] Allawi, Salah, et al. (2018). "New Method for Using Chaotic Maps to Image Encryption," *International Journal of Civil Engineering and Technology (IJCIET)*, vol. 9, Issue. 13,pp. 242-231.

[31] Athira, V., et al. (2013). "A Novel Encryption Method Based on Compressive Sensing." *2013 International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s)*, pp. 271-275.

[32] Baraniuk, Richard. (2007). "Compressive Sensing [Lecture Notes]." *IEEE Signal Processing Magazine*, vol. 24, Issue. 4, pp. 118–121.

[33] Mahmood, Maher, and Shehab Jinan. (2014). "Image encryption and compression based on compressive sensing and chaos," *International Journal of Computer Engineering and Technology*, vol. 5, Issue. 1, pp.68-84.

[34] Aboughalia, Raneem and Osama Alkishriwo. (2018). "Color image encryption based on chaotic block permutation and XOR operation." arXiv preprint arXiv:1808.10198.

[35] Al-Maadeed, Temadher Alassiry, et al. (2021). "A image encryption algorithm based on chaotic Lorenz system and novel primitive polynomial S-boxes." *Multimed Tools and Applications*, *spriger*, vol. 80, pp. 24801-24822.

[36] Chen, Guanrong, Yaobin Mao and Charles K Chui. (2004). "A symmetric image encryption scheme based on 3D chaotic cat maps." *Chaos, Solitons \& Fractals*.vol. 21, Issue 3, pp. 749-761.

[37] Liu, Hongjun, Abdurahman Kadir and Yujun Niu. (2014). "Chaos-based color image block encryption scheme using S-box." *AEU-international Journal of Electronics and Communications*. vol. 68, Issue 7, pp. 676-686.

[38] Meng, Lei, et al. (2020). "An Improved Image Encryption Algorithm Based on Chaotic Mapping and Discrete Wavelet Transform Domain.' *Int. J. Netw. Secur.* Vol. 22, Issue 1, pp. 155-160.

[39] Wang, Xingyuan, and Yining Su. (2020). "Color image encryption based on chaotic compressed sensing and two-dimensional fractional Fourier transform." *Scientific Reports (Nature Publishing Group)*. vol. 10, Issue 1, pp. 1-19.

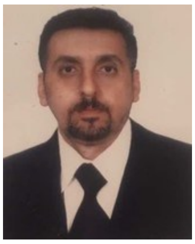
[40] Lau, Yuu Seng, (2006). "Techniques in secure chaos communication." PhD Thesis, RMIT University, Australia, pp.14-35.

[41] Lau, Yuu Seng, Zahir M Hussain .(2005). "A new approach in chaos shift keying for secure communication." *Third International Conference on Information Technology and Applications (ICITA'05)*, Sydney, NSW, Australia, vol.2, pp. 630-633

[42] Hashim, Ashwaq T and Bahaa D Jalil. (2020). "Color image encryption based on chaotic shit keying with lossless compression.," *International Journal of Electrical and Computer Engineering*, vol. 10, Issue 6, pp. 2088-8708.

Authors Biography

Nazar Jabbar Alhyani received his PhD of Science in Electronic Engineering from University of Buckingham - UK in 2015. Currently, he is a university staff at Dijlah University College Iraq (DUC). His research interests include secure transmission, video encryption and compression, cloud security and data encryption



Oday Kamil Hamid received his Bsc. in Electrical Engineering and Msc. Degree in Communication Engineering from University of Technology Iraq in 2000 and 2003 respectively. Currently, he is a senior lecturer in the Faculty of Computer Engineering Techniques at Dijlah University College Iraq (DUC). His research interest, communication, security, digital signal processing, speech recognition, neural network.

Assistant Professor **Riyadh Bassil AbdulJabbar,** born in 1978, holds a Bachelor's degree in Electrical Engineering, University of Baghdad in 2000, and a Master's degree in Control and Computer Engineering, University of Baghdad in 2003. I have worked as a lecturer at Dijlah university College since 2010, rapporteur of the of Computer Engineering Techniques Department for the period from 2011 to 2019, responsible for the university statistics unit during the year 2022, rapporteur of the department of business administration at Dijlah University College. Currently Head of medical instruments techniques engineering at Dijlah University College. I have a number of researches published within the international containers (SCOPUS). My research interests are in the areas of data security, artificial intelligence, and embedded systems**.**

Cite this paper:
Nazar Jabbar Alhyani, Oday Kamil Hamid, Riyadh Basssil Abduljabbar, "A Review of Enhanced Image Techniques Using Chaos Encryption", International Journal of Advances in Computer and Electronics Engineering, Vol. 8, No. 2, pp. 1-8, February 2023.