IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 17, Issue 5, Ser. I (Sep. – Oct. 2022), PP 38-43
www.iosrjournals.org

A Review of Secure Image Technique with Chaotic Encryption

Nazar Jabbar Alhyani[1], Oday Kamil Hamid[2],Riyadh Bassil Abduljabbar[3]
[1](Department of computer techniques engineering/ Dijlah Universitycollege, Iraq)
[2](Department of computer techniques engineering/ Dijlah University college, Iraq)
[3](Department of computer techniques engineering/ Dijlah University college, Iraq)

Abstract: *At the last decades, the secured multimedia data has become essential to protect the multimedia contents from unauthorized persons. Generally, various techniques have been used to disguise significant image data from intruders, one of them the chaotic encryption to prevent the vulnerable to eavesdropping. In this review article, a review of existing chaotic encryption techniques will be conducted highlighting the advantages and shortcomings in relation to suitability for image security.*

Key Word: *Image encryption Security, Logistic map, Sine map, Chebyshev map Arnold cat map, LFSR,AES and block cipher.*

Date of Submission: 14-09-2022 Date of Acceptance: 29-09-2022

I. Introduction

Over the years, variant image/video encryption techniques have been developed to meet a number of conditions on compression ratio, image/frame quality and bandwidth. Data Encryption, on the other hand, has a long history but image/video encryptions are more recent and requires special considerations due to the large size of image/video data and the presence of spatial as well as temporal redundancies. In this paper, we deal with the literature review on existing data chaotic encryption.

Many data encryption algorithms have been developed and deployed throughout the centuries to protect transmitted/stored data and information. Over the last century, an increasing number of ciphers have been developed to meet for the protection of digital data and communications. There are different methods that have been adopted for image encryption depending on the domain, format of signal and the expected level of security. These methods vary in their complexity and security. Among the most widely available and tested ciphers are the DES, AES, RSA and 3DES. High computational cost of such block ciphers is a major obstacle for real-time video encryption. Encrypting online video streams, of no fixed duration, imposes some restrictions on type of ciphers and/or encryption keys. Stream ciphers (e.g. LFSR’s and chaotic map ciphers) - rather than block ciphers are, therefore, more appropriate for encrypting video/image streams and GSM signals[1]

II. Stream Ciphers

The main and most important component of such ciphers is a random key generator. Linear Feedback Shift Register (LFSR) is the simplest method of generating a random key stream of any length using an initial fixed length initial secret register, a primitive polynomial and an iterative procedure that outputs one bit at a time. The generated bit stream used to encrypt the significant parts of images/video bit stream by XORing.

III. Linear Feedback Shift Register (LFSR)

The Linear Feedback Shift Register consists of clocked storage elements (known as flip flop) and feedback paths, The LFSR is successively connected in a flip flop configuration with feedback from contents some flip flops output (taps) that XOR together and the result is feedback into a register input as shown in Figure 1.[2]

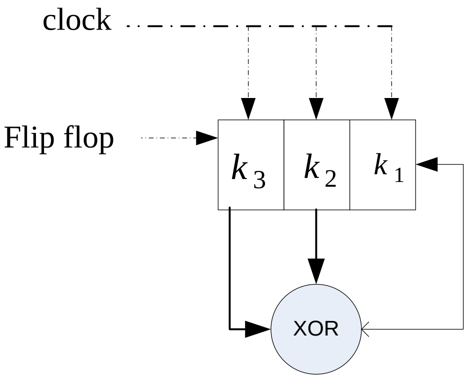

Figure 1:LFSR of degree 3

The length of register and positions of taps depend on a so-called primitive polynomial. For instance, if the primitive polynomial was $x^3 + x^2 + 1$, then the register would be composition from 3 (the highest exponential of primitive polynomial) flip flops and the positions of taps would be 3 and 2 in register sequence as shown in figure above. Usually, there are$(2^n - 1)$ possible binary states that are produced from LFSR until the start set (called the seed of LFSR) repeats, where n is the length of LFSR.The main drawback of LFSR is its linearity weakness that the each bit in a LFSR sequence is linearly related to the initial state and is thus vulnerable to algebraic and correlation attacks. Chaotic random number generation overcomes this problem[3]

IV. The Logistic map

The logistic map is a recursive polynomial function of degree 2 defined as follows $x_{n+1} = rx_n(1 - x_n)$ Where r is the control parameter and $n \in \mathbb{Z}^+$, if $n = 0$, x_0 is known as initial condition. The continuous dynamic system of the logistic map is a mapping $f: x \to x$ from the state space to itself; see Figure 2, defined as follows[4,5]: $x_{n+1} = f(x_n)$

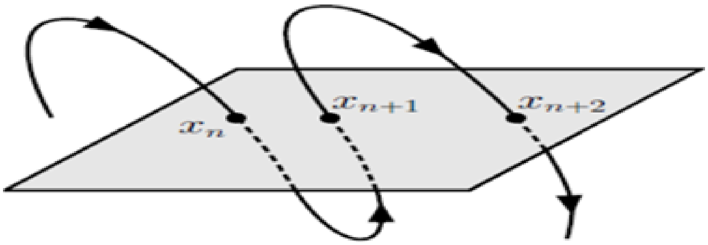

Figure 2:Represents the curve of the orbit map

The logistic map can be represented by using a graphical method called a cobweb diagram. The cobweb diagram shows the iterations of control parameter (r) and initial condition value (x_0) of chaotic logistic map. Figure 3 shows the cobweb of logistic map at different initial condition and control parameters.

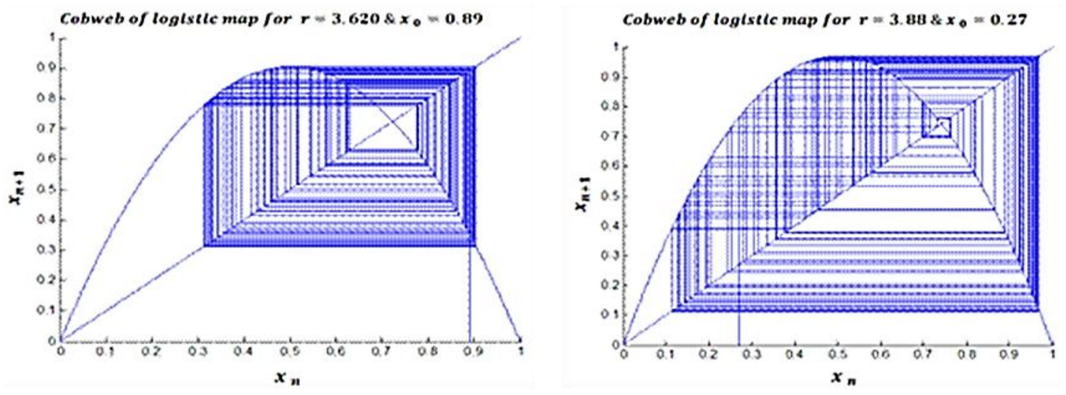

Figure 3: A cobweb diagram of the logistic map, showing chaotic behaviour for various values of initial condition (x_0) and control parameters (r), n is the number of iterations.

Several other approaches have been developed to overcome the linearity weakness of LFSR. Chaos theory is another source of random number generation. In fact, chaotic maps have been widely used in image/video encryption. Li and Yu is described a video encryption technique based on multiple digital chaotic systems, called the Chaotic Video Encryption Scheme (CVES)[6]. In this approach, a number of chaotic maps are used to generate pseudo-random signals to mask the video, and then the masked video is permuted based on the chaotic map. The key space of chaotic logistic map is not large enough to make brute-force attack infeasible. In order to increase key space and the security level of chaotic logistic map Chen and Zhang[7]proposed a new image encryption based on combining a chaotic logistic map with a sine map. Liansheng and Wang proposed an encryption scheme based on chaotic logistic map, where two grayscale images are formed by using two different logistic maps. Firstly, a one-dimensional chaotic map is used to constitute a random grayscale image from original image. Next, a two-dimensional logistic map is used to convert the randomized image into two random grayscale images. Finally, these randomized images are combined with the original image [8].

The block cipher encryption S-box technique with logistic maps for image encryption proposed in[9] .The encryption scheme contain four main operations Firstly, the plain image will input to permutation step, then the permuted image will divided to 4x4 blocks to enter to n iterations of substitution and add Lorenz key. After the end of iterations the resulting image will XO Red with Logistic map key to increase the confusion. Finally, implement the complement step which provide extra confusion process and it’s done by subtract each pixel value from 255.

To improve efficiency and security of image encryption, H. J. Yakubu suggested Rabinovich-Fabrikant Equations for colour images encryption[10]. The proposed scheme adopts the classic framework of the permutation-substitution network in cryptography using the rich chaotic properties of the system and this ensures both confusion and diffusion properties for a secure cipher. The proposal has two stages: confusion stage achieved using the rich chaotic properties of the Rabinovich-Fabrikant equations and the diffusion stage achieved using the MOD and bit XOR operations as well as the chaotic sequence of the map on the confused image.In order to improve encryption robustness of medical image,self-adaptive medical image encryption algorithm is proposed byDhanalaxmi and Tadisetty[11],A corresponding size of matrix in the top right corner was created by the pixel grayscale value of the top left corner under Chebyshev mapping. The grayscale value of the top right corner block replaced by the matrix created before. The remaining blocks encrypted in the same manner in clockwise until the top left corner block encrypted. Benyamin and Seyed[12] proposed an encryption scheme based on hyper chaos based image encryption method with high security and high sensitivity.The algorithm consists of three main sections. Firstly, instead of encrypting each pixel, the rows and columns of the image encrypted using a row-column algorithm. In order to reach higher sensitivity, higher complexity and higher security. Secondly, employs masking process, which applied to each quarter of the image (i.e. sub-images) that is encrypted, using that sub-image data itself and one of the other sub-images and the average data of other quarters of image. Finally, the four most significant bit planes will be encrypted.

Shouvik and Arindrajit[13] proposed combine the DNA application and chaotic logistic map algorithm to lossless image encryption. In this proposal, the input image pixels are convert into 8 bit binary and reversed. Thenfour pairs of pixels are constructed, reverse each pair and convert it into decimal and XOR with bits generated by a chaotic pseudorandom sequence as key.TheDho-Encryption (DE) technique used for hiding secret information within a cover image that can be transmitted over public networks. The DE process can be classified into two processes. In the first process, the original secret information is hidden inside of a cover image using Reveres Matrix (RM) encoding process.In the second process, the encoded cover image pixels are shuffled inside the image itself. After the shuffle process, the shuffled image pixels are encrypted using the Alpha-Encryption (AE) process using a lookup table. This technique is purely based on substitution. Once the processes are over, the encrypted information is sent to the other party for the reconstruction process[14].

Essentially, Duffing map (which are as well is called sometimes as Holmes Map is a one of the kinds of chaotic map which show chaotic demeanour ,and across time domain it is discrete and has a dynamic impression[15].Essentially, when take any certain pixel coordinates such as $(x_m, y_m)$and then has been passed it as an input to the Duffing map, so this will lead to generates a new pixel coordinates (x_{m+1}, y_{m+1})this is perform by the following equations

$x_{m+1} = y_m$ and $y_{m+1} = -ax_m + by_m - {y_m}^3$

Where a and b are constant and on which the map depends, these constants are normally set to 0.2 and 2.75 respectively in order to make the map have a chaotic behaviour.Wang and Tian are invented new variant of chaotic maps called cross chaotic map,where two types of chaotic maps used which one dimensional and non-linear dynamic systems (Logistic, and Chebyshev) has been merged this lead to fulfilled superior level of security via utilizing the eventual map which was in two dimensions. The formula of Cross chaotic map that has been constructed is defined by the following equations

$x_{i+1} = 1 - u{y_i}^2$ and $y_{i+1} = \csc(K.cos^{-1} x_i)$

Where *u and K* indicate to the control parameters of the Cross Chaotic Map system, the system give a great and diversity of the dynamics attitude When *u*=2 and *K*=6 . While *x* and yrepresent the initial pixel that has been selected randomly[16].

In 1996 Salam and Mohammed[17] proposed Duffing map to shuffled all image pixels ,after that the resulting image will be divided into a group of blocks for perform the shuffling process via Cross Chaotic Map. Finally, an image called key image created by using Quadratic number spirals, which will used to generate numbers of polynomial equations via Lagrange interpolation to perform pixel diffusion.

Chaotic is a technique widely used to generate the random number, it characterized by efficiency in the processes of diffusion and permutation. Chaos is very suitable for image encryption method, there is a set of dynamic characteristics that make it suitable for chaos image encryption like: It has a high sensitivity for primary condition, natural dissimulation, and tiny movement disorder. This system's security based on the degree of rounding between signal and random numbers that generated by secret key generator. Arnold cat map is one of chaotic map types, it used to change the pixel location in the image without deleting any information from the image or change its value . Two-dimensional equation of Arnold's Cat Map can be written as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ qpq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} modn$$

Where x and y are pixel's locations, p and q are positive integers and n is a size of image[18,19].

Kamel Faraoun[20]has shown that the combination of simple chaotic maps, can lead to a very complex behaviour that implies good pseudo random sequence and improve level of security and small key space. The approach based on hierarchical combination of three chaotic maps toimage encryption scheme. The system is in a stream-cipher architecture, where the pseudo-random keystream generator is constructed using three chaotic maps, serving the purpose of stream generation and random mixing, respectively. The results show that such a design can enhance the randomness and sensitivity to initial conditions even under finite precision implementation. The colour image encryption algorithm based on multi- ple chaotic maps (Logistic map, Sine map, and Chebyshev map) and the intersecting planes method inside a cube is described in[21], these faces represent the three channels of the color image (red, green, and blue). The first phase of approach begins with extracting all the pixels from the original image and looking for the corresponding values of each pixel on the three faces of the cube. Then, used a circular rotation operation based on the position of each pixel (row, column). This rotation prevents two identical pixels to have the same encrypted value. Afterward, the proposal used the intersecting planes method with the corresponding face to encrypt the pixels. The 2D transformation Arnold Cat Map used to shuffle all the pixels and change their positions according to the parameters calculated from all the pixels of the original image.

Strange attractors defined and described by nonlinear differential equations. They produce butterfly pattern when subjected to number of iterations and these patterns are fractal in nature. They are defined as continuous chaos as they are more responsive to initial conditions that means even though for a small alteration in input seed can produce drastic changes in output. This property of attractors can be useful in encryption approach. Depending on the system equations, initial conditions and system patterns, different strange attractors have been proposed and employed in image encryption schemes[22, 23].Kumar and Yuvaraja described an image encryption technique employing Chen attractor and FPGA generated synthetic image has been discussed. Altera Cyclone II FPGA was used to generate synthetic image that consumed 438 logic elements and 34.03 mW of power consumption[24].

Cloud computing is era technology that provide virtualized significant pool of computing resources. The consumer in cloud computing can use these resources everywhere, anywhere, on-demand and depend on the principle of pay per use In cloud computing the consumers can share resources, information and services during use of internet. Therefore, encryption schemes designed primarily to protect sensitive information in storage for privacy protection[25]. Amal introduced a novel data security in cloud computing architecture based on modified AES, by combination of chaotic map and AES algorithm. Whereas Arnold Cat map used to construct new chaotic mask to replace mix columns transformations and improve the key sensitivity by implement some circular shift on the S-box based on the round keys[26].

The one dimension (1D) logistic map is one of the widely using methods, described in following equation

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

Where $z \in [0, 4]$, $N_q \in (0, 1)$, q=0, 1, 2, ... After conducting research it emerged that the method would be in a good chaotic under condition[27] $3.56994 \leq z \leq 4$.

Method two dimensions 2D Cat map submitted by V.I. Arnold in the research of ergodic theory. Suppose the coordinates of pixels position in the image are
H = {(i, j) | i, j = 1, 2, 3, m}, two control parameters are used in 2D Cat map is as follows[28]:
i1 = (i+ p*j) mod (m)
j1 = (q*i+ (p*q+1) j) mod (m)

Where (i, j) original pixel position, (i1, j1) is the new position, (p, q) are positive integers represent control parameters and m x m plain-image when 2D Cat map is carried out one time to the original.
Salah and May[29]proposed a new image encryption based on combining a 1D-Logistic maps and 2D Cat Mapping to encrypt the colour image. This method depends upon using 1D-Logistic maps to generate random numbers to encrypt the information of image through generating three keys (Rk, Gk, Bk) one for each colour (R, G, B) in the first stage. In the second stage using the 2D Cat Mapping
to generate random numbers to change the position of the pixels in the image that got from previous step.
The basic concept of Compressive Sensing (CS) theory is to represent the original signal in a convenient basis Ψ. Then itemploys a non-adaptive linear projection onto observation matrix ϕ that preserves the structure of the signal and uncorrelated with the transform basis Ψ , and then the signal can be accurately reconstructed by solving the convex optimization problem or greedy pursuit algorithm with a small amount of measured values[30]. CS relies on two principles 1) sparsity: - which pertains to the signals of interest, Sparsity expresses the idea that the information rate of signals can be much smaller than suggested by its bandwidth. and 2) incoherence: - which pertains to the sensing modality, Incoherence expresses idea that signals having sparse representation in representation basis Ψ must be spread out in the sensing basis ϕ[31]. CS framework that mainly consists of two crucial parts: - sampling (encoding) and recovery (decoding).Maher and Jinan[32] proposed an image encryption scheme based on compressive sensing and chaos. CS, which is used due to many properties; greatly reduces the signal sampling rate, power consumption, storage volume and computational complexity, in additional to above; CS combined compression and encryption in the same step. Since CS-based encryption, method alone fails to resist against the chosen-plaintext attack. Hence, the output of CS again encrypted based on multi-chaotic system. This is use to enhance the security. In addition, multi- chaotic used, as key will increase key space, since multi-initial conditions and multi-parameters make it very difficult to decrypt without knowing all those values, the structure of this system is more complex than the low-dimensional chaotic systems and it is more difficult to forecast such chaotic. The results show that the cipher image has large key space, low storage and transmitted requirement, high security and low encryption time requirement, incoherence, key sensitivity and good statistical property. In addition, the recovered image has good quality (to human perception) and preserves both the intelligibility and the characteristics of the image.

V. Conclusion

For many organisations that rely on their work on the transmission of digital media objects over open network channels, protecting their contents from hackers and eavesdroppers have become an essential step in protecting their knowledge asset. The encryption techniques are the natural scheme to use to protect data against security violations in storage and in transmission. Many systems proposed to maintain the security of data by applying cryptographic algorithms. Linear Feedback Shift Register (LFSR) is the simplest method of generating a random key stream of any length using an initial fixed length initial secret register, a primitive polynomial and an iterative procedure that outputs one bit at a time. Traditional LFSR generation use fixed length randomly initialised feedback register using primitive polynomials over finite fields. The generated stream has relatively short length, before repeating itself, which is determined by the length of the initial register, chaotic random number generation overcomes this problem. In this review paper, a comprehensive study conducted on the chaotic encryption technology and a detailed explanation of the concept of this technology to image encryption.

References

[1]. A. Uhl and A. Pommer, Image and video encryption: from digital rights management to secured personal communication, vol. 15, Springer, 2005.

[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) $ G F (2 m) Multipliers Using Irreducible Trinomials," *IEEE Transactions on Computers*, vol. 70, no. 1, pp. 156-162, 2020.

[4]. L. Kocarev and S. Lian, Chaos-based cryptography, Springer, 2011.

[5]. Y. Mao and G. Chen, "Chaos-based image encryption," in *Handbook of Geometric Computing*, Springer, 2005, pp. 231-265.

[6]. S. Li, X. Zheng, X. Mou and Y. Cai, "Chaotic encryption scheme for real-time digital video," in *International Society for Optics and Photonics*, 2002.

[7]. C. Chen, T. Zhang and Y. Zhou, "Image encryption algorithm based on a new combined chaotic system," in *IEEE*, 2012.

[8]. S. Liansheng, W. Wengang, D. Kuaikuai and Z. Zhiqiang, "A novel grayscale image encryption algorithm based on logistic map," 2014.

[9]. D. F. Chalob, a. A. Maryoosh, z. M. Essa and e. N. Abbud, "a new block cipher for image encryption based on multi chaotic systems," *telkomnika,* vol. 18, no. 6, pp. 2983-2991, 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. N. Srinivasu and S. 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, 2015.

[16]. X. Wang, B. Tian, C. Liang and D. Shi, "Blind image quality assessment for measuring image blur," in *IEEE,* 2008.

[17]. S. A. Thajeel and M. S. Hamoud, "An improve image encryption algorithm based on multi-level of chaotic maps and lagrange interpolation," Iraqi Journal of Science, vol. 59, no. 1A, pp. 179-188, 2018.

[18]. P. Tian-gong and L. Da-yong, "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. E. 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, p. e01217, 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, vol. 4, no. 3, p. 350, 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," in Advanced Computing and Intelligent Engineering, Springer, 2020, pp. 467-478.

[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]. A. L. Amal, "Data Security in Cloud Computing Architecture Based on Modified AES".

[27]. A. Y. Niyat, R. M. Hei and M. V. Jahan, "A RGB image encryption algorithm based on DNA sequence operation and hyper-chaotic system," 2015.

[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. Deepthi, "A novel encryption method based on compressive sensing," in IEEE, 2013.

[31]. R. G. 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.

Nazar Jabbar Alhyani, et. al. "A Review of Secure Image Technique with Chaotic Encryption." *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)* 17(5), (2022): pp 38-43.