ISSN: 0974-5823 Vol. 7 No. 2 February, 2022

International Journal of Mechanical Engineering

A New Encryption Algorithm Based on Controlling The Seed of The Logistic Map: Spline-Logistic Algorithm

Heba Abdul-Jaleel Al-Asady[1,3*], Saad Saffah Hreshee[2], Osama Qasim Jumah Al-Thahab[2]

[1,2]University of Babylon, College of Engineering, Dept. of Electrical Engineering, Babylon-Iraq

[3] The Islamic University, Computer Technical Engineering Department, College of Technical Engineering, Najaf, Iraq.

ABSTRACT:

chaos map and its ability to generate a random sequence with nonlinear properties are widely used in applications, especially those requiring high security. The generation of chaos sequence depends on some control determinant and initial value where to be assumed. This paper proposed a method that combines another polynomial with a chaotic map to control the input value of a chaotic map and not take it. This method states on use the cubic spline function as input to the logistic map with determinant to keep the nonlinear characteristic of chaos to generate a new map called spline-logistic map. The simulation of this function are made in matlab2018 to generate the random values. Theoretically and the simulation analysis confirms that spline-logistic map possesses a high performance and uniquely randomness value.

Keywords: logistic, cubic, spline, chaotic, map, steganography.

1. Introduction

Steganography is a practice that enables secrecy – and deception – in the same way, that cryptography is a science that mainly allows privacy[1]. Within a cover file, steganography hides many forms of data. Images, texts, videos, and other types of messages can use as input[2]. Although it is nearly identical to the cover file, the generated stego file contains secret information[3]. Steganography exploits human perception; human senses are not trained to hunt for files with information concealed inside them, even though algorithms can perform what is known as Steganalysis (Detecting the use of steganography)[4]. In the last century, and since the discovery of chaotic waves as one of the mathematics branches. Chaotic is still in development and takes a vast field in applications such as encryption[5], the science of robotics[6], biology[7], Chemistry[8], Astronomy mechanics[9], etc. The concept is that algorithms used under chaos are specified exclusively on real numbers, while systems used in cryptography are defined on a limited number of integers. This significant distinction between the two fields of study made chaos theory prominent in the cryptographic system. In the encryption field, the main requirement was to search for a chaotic wave and use it uniquely and separately to give coding that differs somewhat from the studies dealt with. The use of a chaos map in cryptography gives us a perfect algorithm that has highly robust to any attacks [10]. As the definition, Chaos disorders the state and disrupts it in nonlinear ways with specific determinants. It is susceptible to these determinants and naturally behaves similar to pseudo-random sequence but in the decimal values[11]. Notes that just the change of initial roots of the map (which is dependent on the researcher) and use any function if need or not as a second step can give a new algorithm for encryption with the perfect result, but this could behold a similarity in how the map was applied, regardless the change of the root which is imposed value, so this point was stopped in to reach a new method for generating the initial values for the map since all the researcher still depends on changing the value of the initial points and not search for the function to control this initial point and make the choice of it not easy to increase the security of the system. This paper produces a new method for generating the logistic from another generating function to generate the roots of the logistic map with specific determinants, which is a cubic spline interpolation function[12]. Combining the logistic map with cubic spline generates a new chart with chaotic characteristics. This chart gave a Spline-logistic name. In the following sections, Literature Review, the mathematical model and the diagrams, the proposed system followed by the results and discussion, and finally, the conclusion and references in the last sections of the paper.

2- Literature Review

Researchers have utilized the logistic map in their cryptographic algorithms to encrypt the information gathered from various sources (image, audio, and text). There was an example of them. How to be very cautious while determining the capacity seed in the creation of chaotic-steganography is discussed. The dependence on the strength range alone is not sufficient to decide on the phantom characteristics of the steganography generated from the logistic map, which must be considered. The experiments were presented to demonstrate that, although this technique provides an effective and powerful watermarking process, it falls short if the client makes an irrational decision about the capacity required for the logistic map. In recent years, a slew of new methods to hybrid digital image steganography has emerged. For increased resilience, ability, and security, it attempts to conceal information while maintaining the visual quality of the copyrighted picture. In the article[13], a new digital picture steganography technique is presented, and a novel three-dimensional chaotic map is utilized to improve the method's security. The suggested chaotic map's irregular outputs are used to identify the coordinates of pixels employed in the embedding and extraction procedures. Because the

integer coefficients are used in the embedding and extraction procedures, integer wavelet transformations are used on cover and stego pictures. Another article[14] proposes a CHHCS and LBP-based picture encryption method. CHHCS "combines two hyper-chaotic systems" randomly and dynamically, with each pixel diffused with a distinct LBP operation. Because LBP-based diffusion is dynamic, it achieves a better diffusion effect than other chaotic algorithms. Article[15] suggested approach uses two robust mathematical transformations; DWT and SVD. The watermark data is also encrypted before being inserted into the DWT-SVD domain. It also enables blind extraction of the embedded watermark signature. In article[16], a new stego-key directed LSB replacement method for secret message delivery over public networks was proposed. "Large keyspace for stego-key" is required to defeat public domain brute force attacks. They addressed the high embedding capacity issue using Cuckoo Search, a state-of-the-art evolutionary optimization. A new copyright protection method using both secrecy and authentication is presented in the paper[17]. To safeguard our digital media from theft, we included an encrypted watermark on a hosted picture. Many researchers suggest other applications and technologies that use chaotic systems to encrypt images or audio with different scenarios [18-24].

3-The Proposed Method

The new method consists of two main parts: cubic spline transform and logistic transform; this part explained the mathematical model for these functions and their combination to get the new map.

3.1 CUBIC SPLINE TRANSFORM

Cubic spline function is a third-order polynomial that has a characteristic in its derivatives: a smooth curve in the 1'st and continuous in the 2'nd derivative, sometimes called natural line when the second derivatives put out to zero[8]. The cubic spline function f(x) are illustrate in equation (1)[25].

$$y_i = f(x_i), \quad 0 < i < n \tag{1}$$

the coordinates points is (x_0, y_0),…,(x_n, y_n), and the first iteration of these points are (x_i, x_{i+1}), so the 2'nd derivatives of these points are $(f''(x_i))$ and$(f''(x_{i+1}))$ respectively [26]. The cubic-polynomial and its parameters are shown in equations(2,3,4,5,6,):

$$f(x) = A_1 f(x_i) + A_2 f'(x_{i+1}) + A_3 f''(x_i) + A_4 f'''(x_{i+1}) \tag{2}$$

where $x \in (x_i, x_{i+1})$

$$A_1 = \frac{(x_{i+1} - x)}{(x_{i+1} - x_i)} \tag{3}$$

$$A_2 = \frac{(x - x_i)}{(x_{i+1} - x_i)} \tag{4}$$

$$A_3 = \frac{(A^3 - A)}{6}(x_{i+1} - x_i)^2 \tag{5}$$

$$A_4 = \frac{(B^3 - B)}{6}(x_{i+1} - x_i)^2 \tag{6}$$

The continuity of the second derivative means that the radius of the arc is defined at each point so:

$$f_0''(x_0) = f_{n-1}''(x_n) = 0 \tag{7}$$

finally, you can rewrite the mathematical cubic spline equation as (8)[25], and the graphical model of it is shown in figure (1).

$$f(x) = a_1 + a_2.x + a_3.x^2 + a_4.x^3 \tag{8}$$

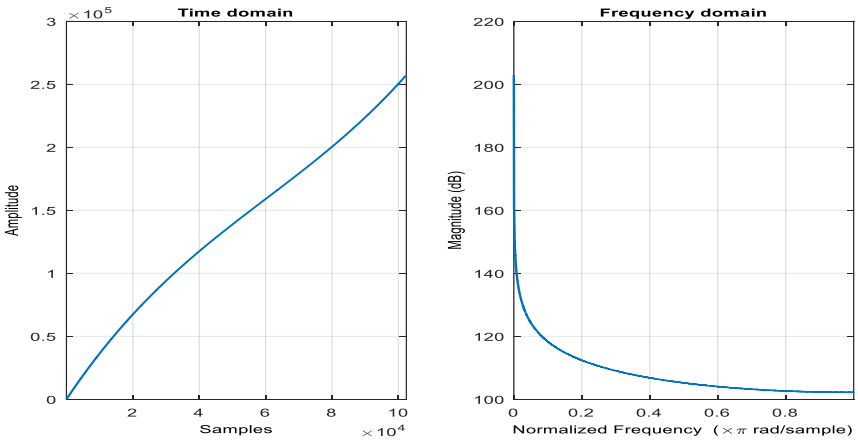


Figure 1: the mathematical graph of the cubic spline function

3.2 LOGISTIC MAP

The logistic map is a discrete system in the dynamical state, defined by equation(9)[27]:

$$x_{i+1} = \propto . x_i(1 - x_i) \quad (9)$$

This formula consists of many parts defined as x_i is the initial point which is also called the seed or the root (x_0) of the logistic map lies in $0 \leq x_i \leq 1$. The index (i) is the role of the discrete state. In addition to the root, the parameter ($\propto$) plays the primary role in the behavior of the logistic map, which is mentioned as follows[16].

1- For $\propto < 1$, x_i is approached to 0 exponentially

2- For $0 \leq \propto \leq 3$, x_i is an attractive fixed point.

3- For $3 < \propto < 4$, The behavior of the logistic map will be a recurring period

4- For $\propto = 4$, the logistic map is a chaotic situation.

The schematic representation of a logistic map is shown in figure(2), and when this diagram focuses on seeing the inside bifurcation, figure (3) appears.

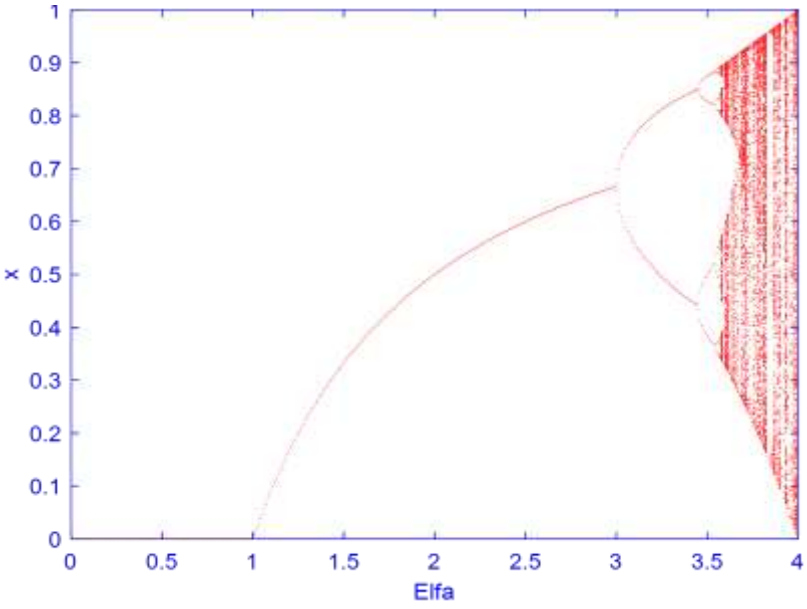


Figure (2) the line drawing of the logistic map

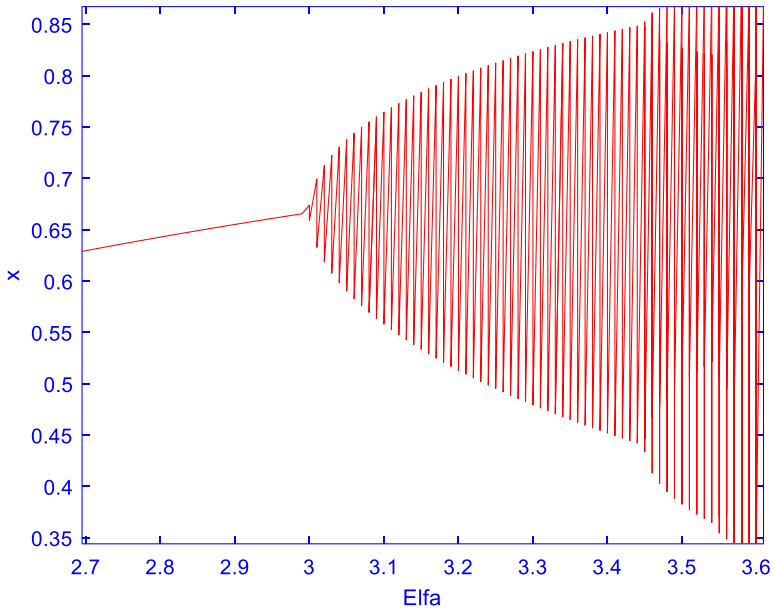


Figure (3) focusing on the bifurcation of the logistic map

3.3 The Combination of The Two Equations(Spline-logistic Function)

Still, the final result is to generate the logistic sequence to use in any application. As explained in section (3.1), the generation of the logistic function depends on the initial value that differs from one researcher to another. To control this virtual value, the input variable is assumed as cubic spline function, which is a linear function but use determinant to convert the work to a nonlinear operation which is chaotic work by combined equation(8) and equation (9) as depicted in the following equations:

We have already from the previous sections:

$$f(x) = a_1 + a_2.x + a_3.x^2 + a_4.x^3 \quad (8)$$

$$x_{i+1} = \propto . x_i(1 - x_i) \quad (9)$$

Then the combination is:

$$x_i = Ħ.f(x) \quad (10)$$

where: Ħ the determinant of the Spline-logistic function lie in the threshold values which are $0 < Ħ < 0.5$

So the Spline-logistic *function is:*

$$\begin{cases} x_i = Ħ\,(a + b.x + c.x^2 + d.x^3) \\ x_{i+1} = \alpha.x_i\,(1 - x_i) \end{cases} \quad (11)$$

The line drawing diagram of Spline-logistic function generally is the same as the logistic map as in figure (4)

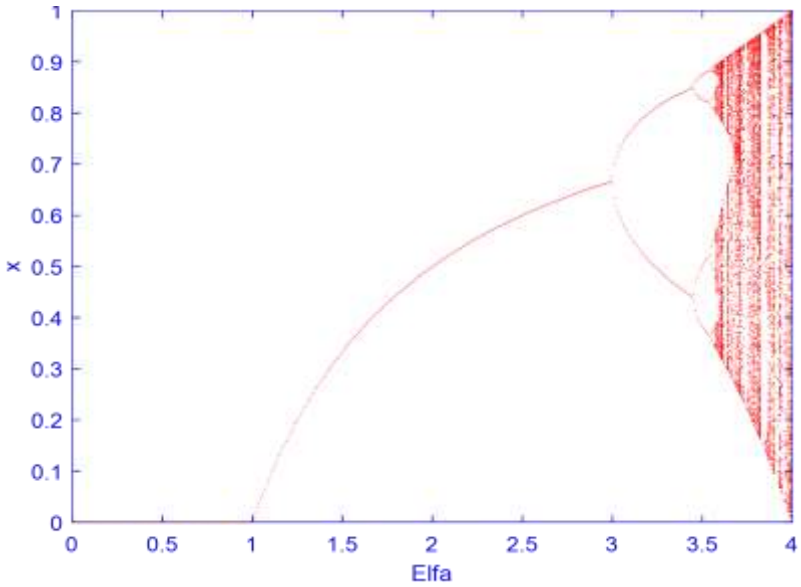
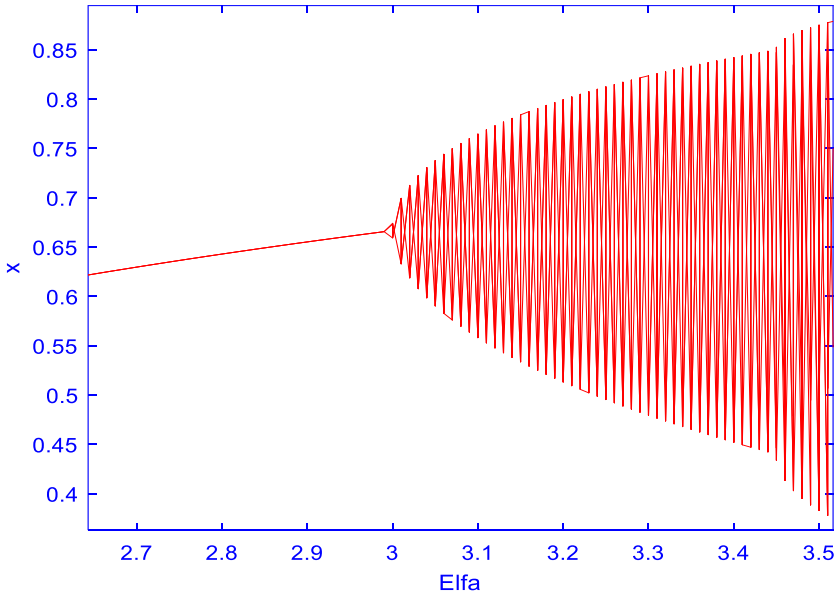
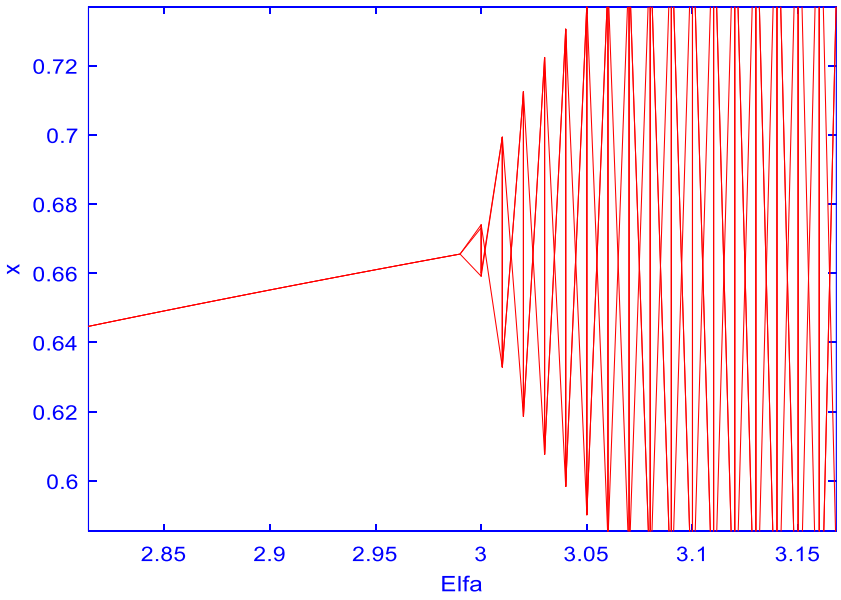


Figure (4) the line drawing diagram of Spline-logistic map

The highlighted Split-logistic diagram is shown in figures (5a,b)



(a)

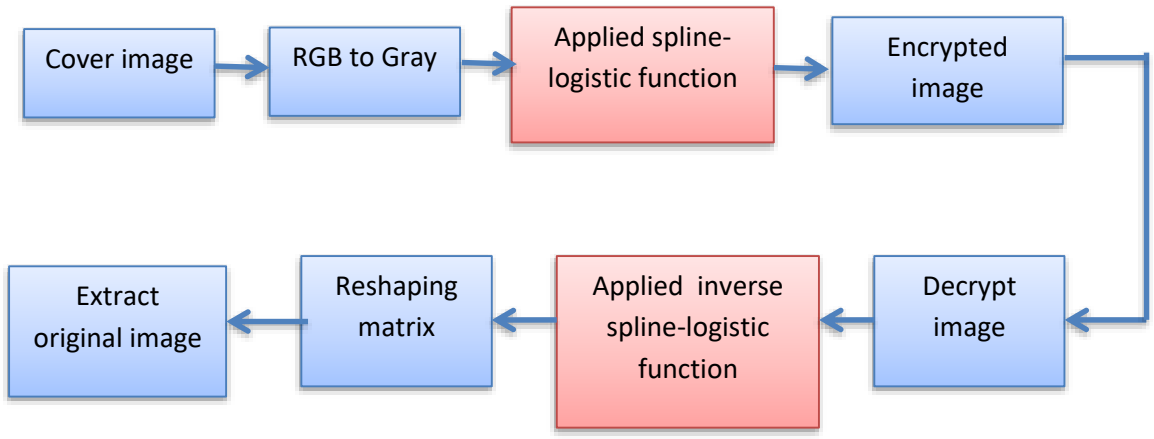


(b)

Figure(5): Zooming in the Spline-logistic diagram (a): The highlighted on Spline-logistic diagram (b): Highlighted at the beginning of Spline-logistic diagram

4- The Proposed Algorithm

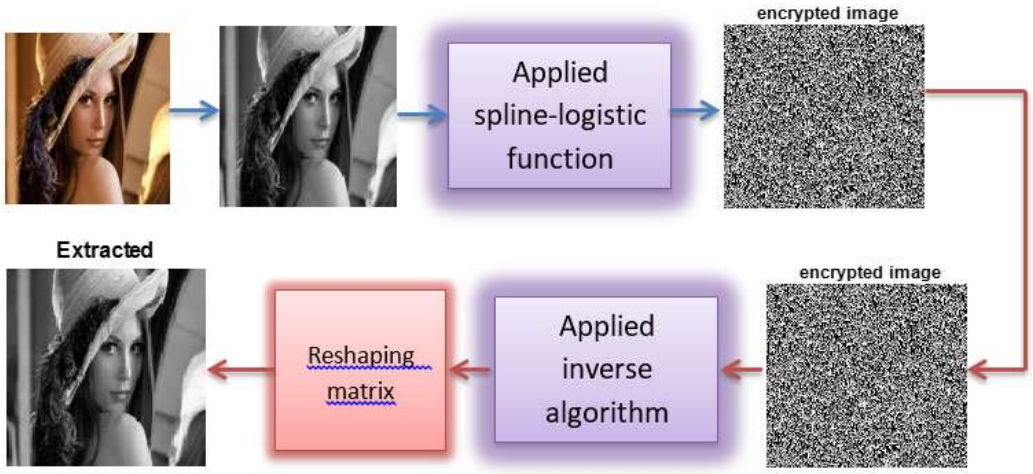
To study the effectiveness of the proposed function, a gray image is taking as a case study. The proposed algorithm is using to encrypt the jpg gray image (Lena as a case study) shown in figure(6). The block diagram consists of two main parts: the encryption part and the decryption part.



Figure(6): the proposed encryption algorithm

4.1 Encryption proce...

1- Reading the RGB (Lena) image and converting it to the grayscale image
2- Resize the gray image to the 128*128 pixels and the converting it to the binary values
3- Generating the cubic spline-logistic sequence with five parameters A=0.3, B=0.9, C=0.2, D=0.8 randomly, and H=0.2 in the range mentioned above and the converting to the binary series.
4- Encrypting the image using the generating sequence from number 3 and finally transmit it throw the channel. Figure(7) show the applied image in the steganographic system.



Figure(7) show the applied image in the steganographic system

4.2 Extraction Process

1- after reaching the information throw the channel; it is converting to the binary values

2- generating the cubic spline logistic sequence with the same parameters in the encryption part to applying inversely to extract the information of image hiding.

3- reshaping the extracting data and converting to the decimal value to show the image

4-Histogram of the cover image and extracted are measure and plotting as in figure(8) to see the underlying distribution's form**.**

Figure (3): Histogram of the embedded and extract images

5. DISCUSSION OF THE RESULTS

As seen when comparing figure5(a, b) with the original shape of the logistic map depicted in figure(3), the difference appears at the beginning of the wave noticed in the logistic wave just one beam rippled up and down to make the shape while in the Spline-logistic wave the beam is separated into two crosses beams overlapped with each other's up and down to construct the final form of it, this was the reason behind calling it Spline-logistic map. The Spline-logistic wave contained large numbers of dark and bright points, meaning large contrast values that change the properties of the map and its determinant. All these differences happen due to merging the main equations of the logistic and cubic spline methods as in equation (11). This combination gives the possibility to generate a robustness map that may be used in some fields where the chaotic maps are the main rule in its applications.

6. Similar Techniques Comparison

Many studies suggested the generation of the encryption system through the logistic map, whether using the logistic map alone to generate the key or by using other functions such as the wavelet function or the discrete cosine function or other functions in addition to the logistic map to generate a high-strength encrypted system. Still, none of them addressed using a process others in developing stem points and roots for the logistic map, as we did in this research, which gave excellent results and high strength, as we noted in the presented case.

4. CONCLUSION

Chaos map has been widely used in the last century because of its properties which give high robustness in any application. Using a unique map leads to searching about adding or changing any parts or details to the chaotic map. This paper produces a unique method by combining the cubic spline and logistic map in one map and called it a Spline-logistic map. The generation of the chaotic sequence without needing to think about the initial value is more flexible when depending on the input equation, which is here a cubic spline equation and involves its limitation. The spline-logistic map can produce a specific sequence that differs from the logistic sequence with length depends on the user's need. Simple implementation and high accuracy of the cubic spline function damage with chaos characteristic produce distinctive properties observed in the Spline-logistic map.

5. REFERENCES

[1] M. Zamani, H. Taherdoost, A. a Manaf, R. B. Ahmad, and A. M. Zeki, "A Genetic-Algorithm-Based Approach for Audio Steganography," *Int. J. Comput. Electr. Autom. Control Inf. Eng.*, vol. 3, no. 6, pp. 64–68, 2009.

[2] M. M. Hashim, M. S. Mohd Rahim, and A. A. Alwan, "A review and open issues of multifarious image steganography techniques in spatial domain," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 4, pp. 956–977, 2018.

[3] A. Jalali and H. Farsi, "A new steganography algorithm based on video sparse representation," *Multimed. Tools Appl.*, vol. 79, no. 3–4, pp. 1821–1846, 2020, doi: 10.1007/s11042-019-08233-5.

[4] "VIDEO STEGANOGRAPHY FOR SECURE COMMUNICATION BASED ON ADJOIN PREDICTION AND VECTOR," no. 1, 2018.

[5] C. Rajpreetha, C. Haripriya, and V. L. M, "A Secured Video Steganography by Linear Feedback Shift Register Method," vol. 1, no. 4, pp. 56–59, 2015.

[6] V. L. Narayana, A. P. Gopi, and N. A. Kumar, "Different techniques for hiding the text information using text steganography techniques: A survey," *Ing. des Syst. d'Information*, vol. 23, no. 6, pp. 115–125, 2018, doi: 10.3166/ISI.23.6.115-125.

[7] S. K. Dubey and V. Chandra, "Steganography Cryptography and Watermarking: A Review," *Int. J. Innov. Res. Sci. Eng. Technol.*, vol. 6, no. 2, pp. 2595–2599, 2017, doi: 10.15680/IJIRSET.2017.0602076.

[8] S. Kingslin and R. S. Dhanalakshmi, "Design of a Security Based Technique for Handling Secure SMS in Mobile Phones using Text Steganography," no. February, pp. 139–147, 2018.

[9] F. I. Practice and C. Platform, "RESEARCH ARTICLE A Steganography based Framework to Forbid Insecure Practice in Cloud Platform," vol. 7, pp. 1113–1116, 2018.

[10] Al-Asady, Heba Abdul-Jaleel, Osama Qasim Jumah Al-Thahab, and Saad S. Hreshee. "Robust encryption system based watermarking theory by using chaotic algorithms: A reviewer paper." *Journal of Physics: Conference Series*. Vol. 1818. No. 1. IOP Publishing, 2021.

[11] Akhavan, A., A. Samsudin, and A. Akhshani, A symmetric image encryption scheme based on combination of nonlinear chaotic maps. Journal of the Franklin Institute, 2011. **348**(8): p. 1797-1813.

[12] Behnia, S., et al., A novel algorithm for image encryption based on mixture of chaotic maps. Chaos, Solitons & Fractals, 2008. **35**(2): p. 408-419.

[13] M. Y. Valandar, P. Ayubi, and M. J. Barani, "A new transform domain steganography based on modified logistic chaotic map for color images," *J. Inf. Secur. Appl.*, vol. 34, pp. 142–151, 2017, doi: 10.1016/j.jisa.2017.04.004.

[14] H. Zhu, X. Zhang, H. Yu, C. Zhao, and Z. Zhu, "An image encryption algorithm based on compound homogeneous hyper-chaotic system," *Nonlinear Dyn.*, vol. 89, no. 1, pp. 61–79, 2017, doi: 10.1007/s11071-017-3436-y.

[15] Nehmzow, U. and K. Walker, Quantitative description of robot–environment interaction using chaos theory. Robotics and Autonomous Systems, 2005. **53**(3-4): p. 177-193.

[16] Liz, E. and A. Ruiz-Herrera, Chaos in discrete structured population models. SIAM Journal on Applied Dynamical Systems, 2012. **11**(4): p. 1200-1214.

[17] Li, M., et al., Prediction of gas solubility in polymers by back propagation artificial neural network based on self-adaptive particle swarm optimization algorithm and chaos theory. Fluid Phase Equilibria, 2013. **356**: p. 11-17.

[18] Froeschlé, C., E. Lega, and M. Guzzo, Analysis of the chaotic behaviour of orbits diffusing along the Arnold web, in Periodic, quasi-periodic and chaotic motions in celestial mechanics: Theory and applications. 2006, Springer. p. 141-153.

[19]S. S. Hreshee, H. N. Abdullah, and A. K. Jawad, "A high-security communication system based on chaotic scrambling and chaotic masking," International Journal on Communications Antenna and Propagation (I.Re.C.A.P.), vol. 8, no. 3, pp. 257–264, 2018. doi:10.15866/recap.v8i3.13541

[20] H. A. Ismael, and S. B. Sadkhan, "Security enhancement of speech scrambling using triple Chaotic Maps," In 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), pp. 132-137. IEEE, 2017.

[21] Rajendran, S. and M. Doraipandian, Chaotic Map Based Random Image Steganography Using LSB Technique. IJ Network Security, 2017. **19**(4): p. 593-598.

[22] Wang, Y., M. Angelova, and A. Ali, Fuzzy clustering of time series gene expression data with cubic-spline. Journal of Biosciences and Medicines, 2013. **1**(3): p. 16-21.

[23] Ahmad, N. and K.F. Deeba, The study of new approaches in cubic spline interpolation for auto mobile data. Journal of Science and Arts, 2017. **17**(3): p. 401-406.

[24] Dunfield, L.G. and J.F. Read, Determination of reaction rates by the use of cubic spline interpolation. The Journal of Chemical Physics, 1972. **57**(5): p. 2178-2183.

[25] Phatak, S. and S.S. Rao, Logistic map: A possible random-number generator. Physical review E, 1995. **51**(4): p. 3670.

[26] Wu, G.-C. and D. Baleanu, Discrete fractional logistic map and its chaos. Nonlinear Dynamics, 2014. **75**(1-2): p. 283-287.