Kufa Journal of Engineering
Vol. 15, No. 4, October 2024, P.P. 55-64
Article history: Received 17 February 2024, last revised 10 April 2024, accepted 14 May 2024

AN IMAGE ENCRYPTION METHOD BASED ON LOGISTICAL CHAOTIC MAPS TO ENCRYPT COMMUNICATION DATA

Heba Abdul-Jaleel Al-Asady[1,3], Hassan Falah Fakhruldeen[1,2], and Yousif Mudhafar[3]

[1] Department of Electrical Engineering, College of Engineering, University of Kufa, Kufa, Iraq, Email: hebaa.alasady@uokufa.edu.iq.

[2] Department of Computer Techniques Engineering, Faculty of Information Technology, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq , Email: hassan.falah@sadiq.edu.iq.

[3] Department of Computer Technical Engineering, College of Technical Engineering, The Islamic University, Najaf, Iraq, Email: yousif.mudhafar@iunajaf.edu.iq.

https://doi.org/10.30572/2018/KJE/150405

ABSTRACT

Encryption is crucial because of how integral to daily life things like smartphones, computers, and the internet have become. It's almost inconceivable to think about getting by without it. Everything from paying bills and buying goods to email and social networking is done online nowadays. Participating in measures that can prevent illegal access to our accounts, data, and devices is more crucial than ever. In this study, we combined a 256-by-256-pixel cover picture with a 128-by-128-pixel inner image using the logistic map (the chaotic function), where both images were in the PNG format. where the encrypted image is converted to a grayscale image and then encrypted through the logistic function. the output of this process is chaotic data that has been converted into binary data to be encrypted again through the colors of the cover image (red, green and blue) each separately and measuring the standard factors to know the strength of the system. The bit error rate was calculated after measuring the signal-to-noise ratio (SNR), system similarity(SSIM), and Peak Signal to Noise Ratio(PSNR) for these three hues. Using the logistic map, all three colors were found to be equally secure during encryption in the chaotic signal and due to unpredictability.

KEYWORDS

Encryption, Image, Binary vector, Chaotic signal, Logistic map.

1. INTRODUCTION

Encryption is the act of preserving sensitive data by employing mathematical algorithms to encode it in a manner that restricts access solely to individuals possessing the decryption key. The complexity of this procedure can vary greatly, and mathematicians and computer scientists have devised distinct cryptographic techniques to safeguard the information and data that consumers and businesses depend on daily basis (Dhawan, S., 2011).

The process of depicting encryption plays a vital role in ensuring the security of information by preserving the confidentiality and integrity of digital images. This is achieved by converting the visual data contained within an image into a format that is both unreadable and incomprehensible (Bindu, K., and etc.2012).

In recent years, chaotic signals have emerged as a promising tool for encrypting digital data. The use of chaotic signals in encryption schemes provides a high degree of security and complexity, making it difficult for attackers to decipher the encrypted data (Odeh, A., 2023).

Chaotic signals are non-periodic signals that exhibit high levels of unpredictability and complexity. These signals have been used in various applications, including communications, cryptography, and data security (Al-Thahab, 2020). The use of chaotic signals in encryption schemes involves generating a chaotic signal and using it to modify the data before transmission. With the characteristics of sensitivity to initial conditions and control parameters, pseudo-randomness and rest, chaos maps have been widely used in data encryption recently in comparison to traditional encryption systems It is easy to achieve chaos, which makes it more suitable for encrypting large-scale data such as photos, videos, or audio data. However, there is still no security analysis model suitable for most chaos-based cryptographic systems which makes for messy cryptographic systems that are rarely accompanied by a detailed security analysis (Alasadi, 2017).

Encryption using chaotic signals has gained significant attention in recent years due to its high degree of security and robustness. The basic idea behind this approach is to use a chaotic signal to modify the original data, thereby making it difficult for attackers to decipher the encrypted data. Various encryption schemes have been proposed using chaotic signals, including chaotic stream ciphers and chaos-based block ciphers. Encryption using chaotic signals offers several benefits over traditional encryption methods. First, it provides a high degree of security and robustness against attacks. Second, it is resistant to statistical attacks due to the random nature of the chaotic signals. Third, it is computationally efficient, making it suitable for real-time applications (Bindu, K., and etc.2012).

However, there are also some drawbacks to encryption using chaotic signals. One of the major drawbacks is the difficulty in generating truly chaotic signals. Additionally, the sensitivity of the chaotic signals to initial conditions can make them vulnerable to attacks if the initial conditions are known. Furthermore, the security of the encryption scheme is highly dependent on the quality of the chaotic signal generator (Al-Kaabi, 2023).

In conclusion, encryption using chaotic signals has emerged as a promising approach for securing digital data. Despite some of the drawbacks associated with this approach, the benefits it offers in terms of security and efficiency make it a popular research topic. Future research should focus on improving the quality of chaotic signal generators and developing more robust encryption schemes based on chaotic signal (Fadhil, 2022).

2. LOGISTIC MAP

In recent years, secure picture encryption approaches have been greatly aided by suggestions made by chaos-based cryptography algorithms (Ahmad, S., 2021). In order to fulfill the needs of the safe picture transfer, they offer a new method for image encryption based on chaotic logistic maps in the message (Shen, 2017). In the proposed picture encryption approach, the external secret key is used to derive the beginning conditions for both logistic maps by assigning distinct weights to each of its bits (Setyono, 2018). Furthermore, in the proposed encryption method, eight distinct operations are employed to encrypt the pixels of a picture, with the conclusion of the logistic map determining which operation will be used for a given pixel (Shah, 2020). After encrypting each block of sixteen pixels, the secret key is changed to make the cipher more secure against any assault. Multiple experimental, statistical, and key sensitivity tests validate the efficiency and security of the proposed picture encryption technique for real-time image transmission and dencryption (Muhammad, 2019).

In a fascinating and influential review article (linked below), Robert May (1976) emphasize that even simple nonlinear maps could have very complicated dynamics (Abd, 2022) May illustrated his point with the logistic map given by: (Pourasad, 2021)

$$X_{n+1=}\ \ RX_n(1-X_n) \tag{1}$$

A discrete-time analog of the logistic equation for population growth, where xn is the dimensionless measure of the population in the nth generation and r is the intrinsic growth rate(Al-Asady, 2021). As shown in Fig. 1, the graph of map (1) is a parabola with a maximum value of r/4 at x = 1/2 (Zamani, 2015). We restrict the control parameter r to the range (−2 or) $0 \leq r \leq 4$ so that Eq. (1) maps the interval $0 \leq x \leq 1$ into itself.

Numerous fields, including cryptography, secure communications, engineering, physics, economics, robotics, and control, have found use for the principles of chaos theory (Doğan, 2016). Due to their great sensitivity to changes in initial conditions and parameters, chaotic systems provide a robust foundation for modeling intricate natural events and enhancing the complexity of security-related applications (Jalali, 2020). Novel chaotic systems are always in high demand. This is typically done by taking into account an already chaotic system and modifying it in some way, such as by changing a term in the system's differential/difference equations, by adding more nonlinear components, or by shifting the system to a higher dimension and introducing new variables (Emad, 2018). One of the most well-known and heavily changed chaotic systems is the logistic map, which operates in one dimension and discrete time. The map's one parameter and straightforward design make it useful in a wide variety of contexts (Narayana, 2018), (Dubey, 2017).

3. THE PROPOSED SYSTEM

The fundamental structure of an information encryption system comprises two fundamental components: the encryption component and the decryption component, irrespective of the specific technique employed by the system for data encryption. The proposed system relies on the encryption of data (images) using a chaotic function (logistic function) through a cover image. This process involves reading the image data and generating a logistic function based on the collected data. Subsequently, the encrypted data is concealed within the cover image after converting the two images into separate images. Decimals shown in Fig.1 which is depicts a block diagram shows the process of hiding and extraction an encrypted image using a chaotic map into the cover image.

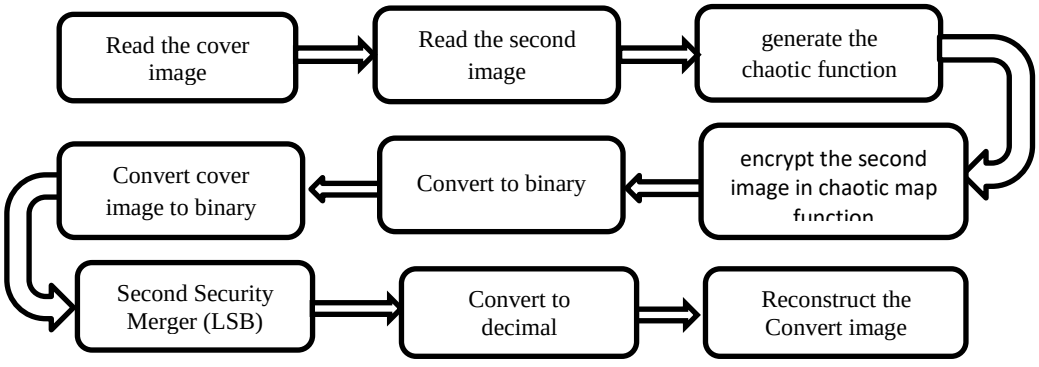


Fig.1a: The block diagram shows the process of hiding an encrypted image using a chaotic map into the cover image.

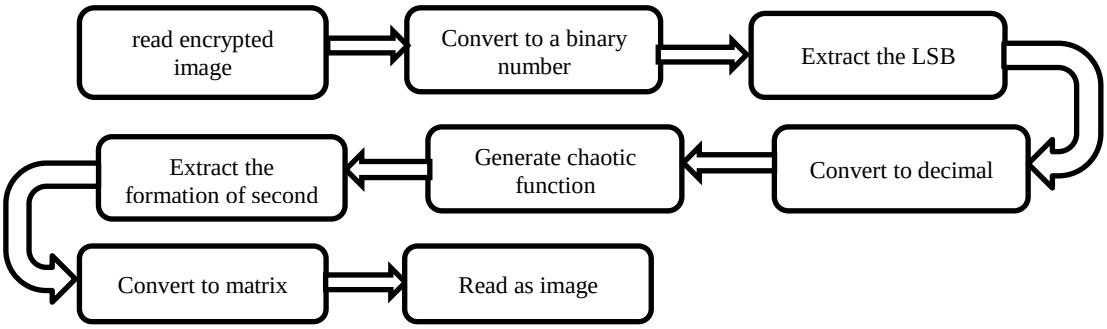


Fig.1b: The block diagram shows the process of extracting an encrypted image using a chaotic map into the cover image

3.1. Methods And Tools Of Encryption System

1. The cover image was called in Matlab by imread, with an image size of 256 * 256 and with a (PNG) extension. this extension was lossless data compression, so you can encrypt, print, and send without any loss of information.

2. A second image was called in Matlab by the same command, with an image size of 128 * 128 and a PNG extension.

3. Generating a chaotic logistic function that depends in length on the length of the second internal image, and because its characteristics are chaotic, it results in complete concealment of the small image data, which becomes random and unguessable.

-The encryption is designed using the chaotic logistic function to encrypt images inside other images, where the encrypted image is converted to a grayscale image and then encrypted through the logistic function.

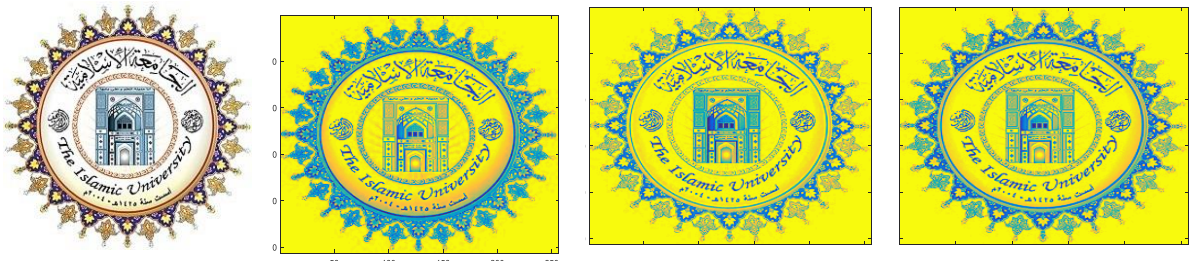
4. the output of this process is chaotic data that has been converted into binary data to be encrypted again through the colors of the cover image (red, green and blue) each separately and measuring the standard factors to know the strength of the system and the extent of the effect of the chaotic function on encrypting the colors of the images.

5. After the process of hiding the information (second encryption) through the cover image, the image is returned and sent

6.On the other side (the recipient side), the cover image is received and the operations are returned in reverse depending on the key used, which is the root and length of the logistic map, which represents the length of the internal image, where the colors of the cover image are separated and data is extracted from it, which is chaotic, and then the chaotic logistic function is generated to extract internal image data.

4. RESULTS

Chaos theory shows an unstable periodic behavior in the form of a nonlinear dynamical system defined by a mathematical equation. one of the characteristics of chaotic systems is that it has an unexpected behavior, as model of the system may appear completely different from the one that appeared previously as a result of a simple change in one of the system variables. The results of each step of encryption on cover image and hiding image are shown in figures from Fig. 2 to Fig 7.



(a) cover (b) blue (c) red (d) green

Fig.2 the cover image and its colors

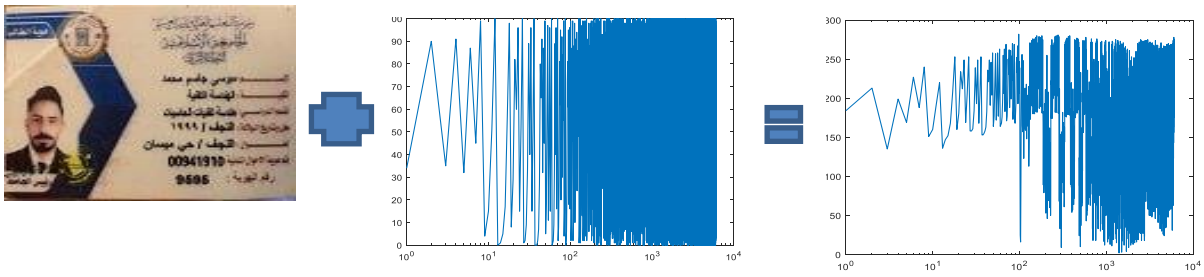
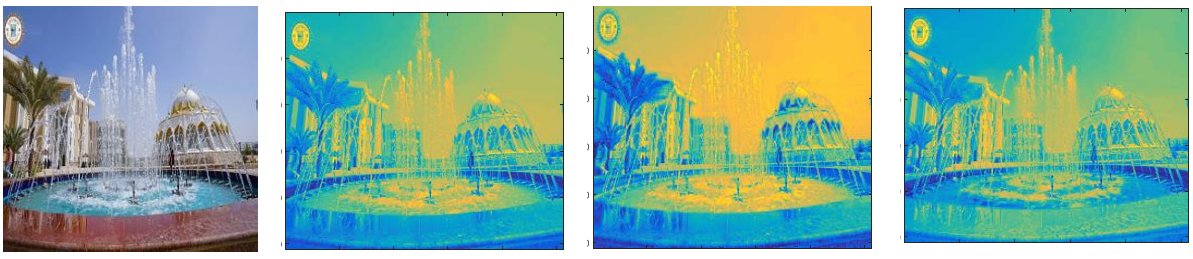


Fig.3 the hidden image with logistic map

The second cover image and its colors with second security image are shown in Fig.4



(a) cover (b) blue (c) red (d) green

Fig.4 the cover image and its colors

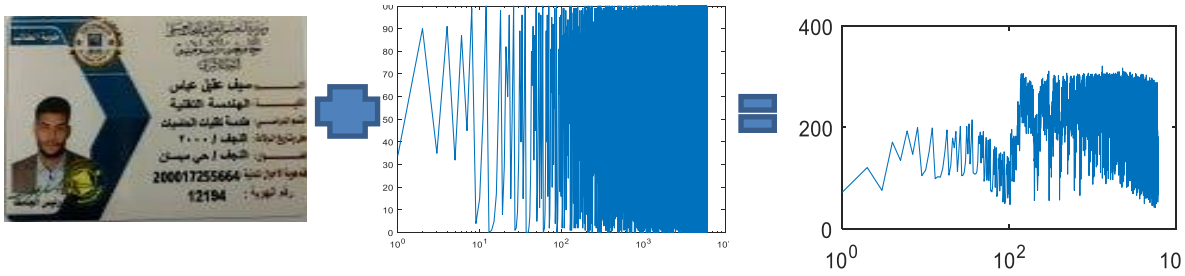
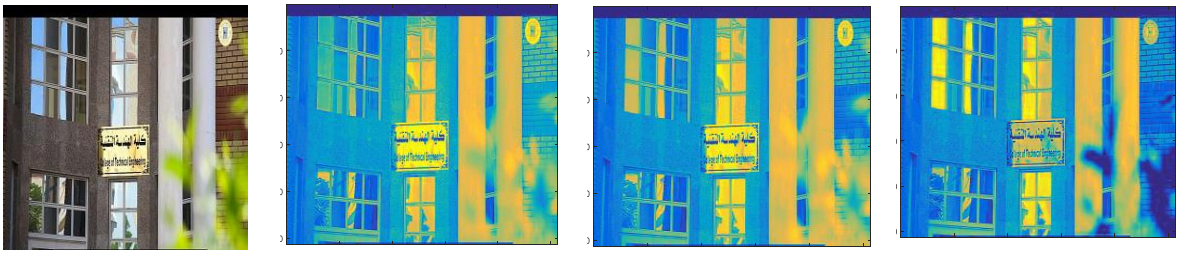


Fig.5 the hidden image with logistic map

The third cover image and its colors with second security image are shown in Fig.6.



(a) cover (b) blue (c) red (d) green

Fig.6 the cover image and its colors

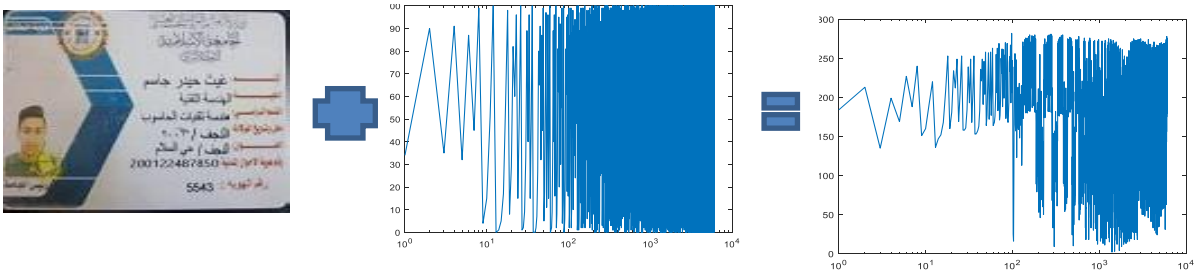


fig.7 the hidden image with logistic map

The performance parameters that measured the robustness of the system are shown in the Table 1 below

Table 1: The performance parameters of the three-encryption image

	Red	**Green**	**blue**
parameter	**Value**	**Value**	value
SSIM	0.9994	0.9994	0.9994
SNR(dB)	31.8397	31.8397	31.9020
MSE	0.0279	0.0279	0.0274
PSNR(dB)	73.3126	73.3126	73.3935
BER	0.0172	0.0172	0.0171
RMS	0.1670	0.1670	0.1656

	Red	Green	blue
parameter	**Value**	**Value**	value
	Second image		
SSIM	0.9999	0.9999	0.9999
SNR(dB)	31.8533	31.8077	31.7976
MSE	0.0237	0.0241	0.0238
PSNR(dB)	74.1315	74.0448	74.1061
BER	0.0171	0.0171	0.0173
SSIM	0.9999	0.9999	0.9999
	Thrid image		
SSIM	0.9994	0.9997	0.9994
SNR(dB)	31.5301	31.5175	31.5199
MSE	0.0223	0.0221	0.0220
PSNR(dB)	74.4357	74.4774	74.4966
BER	0.0171	0.0171	0.0171
SSIM	0.1492	0.1486	0.1483

From reviewing the way in which the encryption system was implemented, we see that the encryption process took place in two stages. The first was encrypting the basic data to be protected in the chaotic logistical function, which made the data completely chaotic, and then encrypting this data through another image, which serves as a cover image in order to protect the data, the results of which were displayed within Table 1, where we note that the encryption process was carried out in the three colors of the image to test its robustness in the data hiding process. The data that was measured, such as the PSNR that reached 74.4db in green with a slight fluctuation rate of approximately 0.07 with other colors, and the error rate that ranges indicate the strength of the proposed system and the robustness of this method of hiding data, in addition to measuring the percentage of similarity between the cover image. The original image and the cover image, after the encryption process, we see that the ratio is approximately equal to 0.999, which means that it is not possible to notice the difference between the two images, and this gives high durability and good efficiency in encrypting the data by not affecting the original image.

5. CONCLUSIONS

Security and dependability issues are major obstacles to internet data transmission. In this study, we present a new image coding method based on logistical chaotic maps to address the need for encrypted data communication during image acquisition. The suggested picture encryption strategy is an effective and secure method for real-time image encryption and transmission. We run the security program on images with three different colors and find that it encrypts and decrypts data with a high degree of efficiency in comparison with the systems that were presented in this research and the results that were obtained (Al-Asady, H.A.J., 2021). There is

an inherent security risk in using the same key for both encryption and decryption. Logistic chaotic maps were used to investigate the process of digital picture encryption (which involves transforming the source images into a format that is difficult to decipher). The outcomes demonstrated that this approach provides a higher level of security.

6. REFERENCES

Abd, A.S. and Hussein, E.A., 2022. Design secure multi-level communication system based on duffing chaotic map and steganography. Indonesian Journal of Electrical Engineering and Computer Science, 25(1), pp.238-246.

Ahmad, I. and Shin, S., 2021. A novel hybrid image encryption–compression scheme by combining chaos theory and number theory. Signal Processing: Image Communication, 98, p.116418.

Alasadi, A.L.H.A.J., 2017. Watermarking Algorithm Based On Discrete Wavelet Transform Using Two Types Of Images. International Journal of Science, Engineering and Technology Research (IJSETR), 6(05).

Al-Asady, H.A.J., Al-Thahab, O.Q.J. and Hreshee, S.S., 2021, March. Robust encryption system based watermarking theory by using chaotic algorithms: A reviewer paper. In Journal of Physics: Conference Series (Vol. 1818, No. 1, p. 012086). IOP Publishing.

Al-Kaabi, R.A., Fakhruldeen, H.F. and Al-Asady, H.A.J., 2023, March. An overview of the status, challenges, and trends of the advanced crypto algorithms to enhance the security of wireless networks. In AIP Conference Proceedings (Vol. 2591, No. 1). AIP Publishing.

Al-Thahab, O.Q. and Hussein, A.A., 2020, July. Implementation of stego-watermarking technique by encryption image based on turbo code for copyright application. In 2020 1st. Information Technology To Enhance e-learning and Other Application (IT-ELA (pp. 148-153). IEEE.

Bindu, K., Ganpati, A. and Sharma, A.K., 2012. A comparative study of image compression algorithms. International Journal of Research in Computer Science, 2(5), p.37.

Dhawan, S., 2011. A review of image compression and comparison of its algorithms. International Journal of electronics & Communication technology, 2(1), pp.22-26.

Doğan, Ş., 2016. A new data hiding method based on chaos embedded genetic algorithm for color image. Artificial Intelligence Review, 46, pp.129-143.

Dubey, S.K. and Chandra, V., 2017. Steganography Cryptography and Watermarking: A Review. International Journal of Innovative Research in Science, Engineering and Technology, 6(2), pp.2595-2599.

Emad, E., Safey, A., Refaat, A., Osama, Z., Sayed, E. and Mohamed, E., 2018. A secure image steganography algorithm based on least significant bit and integer wavelet transform. Journal of Systems Engineering and Electronics, 29(3), pp.639-649.

Fadhil, S.A. and K Farhan, A., 2022. Color visual cryptography based on three dimensional chaotic map. Iraqi Journal of Computers, Communications, Control and Systems Engineering, 22(2), pp.1-12.

Jalali, A. and Farsi, H., 2020. A new steganography algorithm based on video sparse representation. Multimedia Tools and Applications, 79(3-4), pp.1821-1846.

Muhammad, Z.M.Z. and Özkaynak, F., 2019. Security problems of chaotic image encryption algorithms based on cryptanalysis driven design technique. IEEE Access, 7, pp.99945-99953.

Narayana, V.L. and Kumar, N.A., 2018. Different techniques for hiding the text information using text steganography techniques: A survey. Ingénierie des Systèmes d'Information, 23(6).

Odeh, A. and Al-Haija, Q.A., 2023. Medical image encryption techniques: a technical survey and potential challenges. no. January, pp.3170-3177.

Pourasad, Y., Ranjbarzadeh, R. and Mardani, A., 2021. A new algorithm for digital image encryption based on chaos theory. Entropy, 23(3), p.341.

Setyono, A. and Muljono, M., 2018. Dual encryption techniques for secure image transmission. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 10(3-2), pp.41-46.

Shah, A.A., Parah, S.A., Rashid, M. and Elhoseny, M., 2020. Efficient image encryption scheme based on generalized logistic map for real time image processing. Journal of Real-Time Image Processing, 17(6), pp.2139-2151.

Shen, J., Zuo, X., Li, J., Yang, W. and Ling, H., 2017. A novel pixel neighborhood differential statistic feature for pedestrian and face detection. Pattern Recognition, 63, pp.127-138.

Zamani, M. and Manaf, A.B.A., 2015. Genetic algorithm for fragile audio watermarking. Telecommunication Systems, 59, pp.291-304.