Image Encryption Based on Chaotic Logistic Map

Mahmoud H. S. Hasan [1] and Adel Ali Eluheshi [2]

[1] College of Information Technology, Alasmarya Islamic University, Zliten – Libya
[2] Department of Electrical Engineering and Computer, Libyan Academy, Tripoli, Libya
tea_mhs@asmarya.edu.ly

DOI: https://doi.org/10.5281/zenodo.17172262

Abstract. One of the most efficient methods for ensuring privacy in the digital world is image encryption. We should facilitate and secure the transfer of private images from one location to another when sent over a public network, such as when sending them to be stored on a cloud drive. This paper proposed an algorithm to encrypt and decrypt the images. The approach uses a chaotic logistic map to generate a keystream and then applies an XOR operation for the encryption and decryption of images. The findings indicate that the proposed technique is an effective method for image encryption and decryption. We evaluate the metrics for encryption performance analysis: information entropy, histogram analysis, correlation coefficients between plain and cipher images, energy, contrast, and homogeneity, and the analysis of the key's sensitivity. The results indicate that the proposed technique demonstrates efficacy.

Keywords: Image encryption, Chaotic Logistic Map, XOR operation.

1 Introduction.

Chaotic denotes aperiodic, long-term behavior shown in a deterministic system. Chaosbased systems demonstrate considerable sensitivity to initial conditions, commonly known as the "butterfly effect." Nonlinear dynamical discrete-time systems that display chaotic behavior are termed "chaotic maps." The advantage of a chaotic map resides in its deterministic characteristics. Many researchers leverage the benefits of chaotic systems, incorporating them with the advantageous features of cryptographic codes, such as confusion and diffusion, to improve security. The chaotic system is relevant to security-dependent systems, such as image encryption techniques, block cyphers, and stream cyphers [1].

Researchers utilize this map to examine population dynamics, chaos theory, and various other disciplines because of its intriguing behavior, which encompasses bifurcations and chaotic regimes.

The logistic map is a nonlinear difference equation capable of demonstrating chaotic behavior. The logistic map is characterized by the underlying equation:

$$x_n = \alpha x_{n-1}(1 - x_{n-1}) \quad (1)$$

Where x_n is the population at time $x \in (0, 1)$, and $\alpha \in (0, 4)$ is a parameter that determines the behavior of the map [2]. The Logistic map is chaotic when $3.57 < \alpha \leq 4$ [3].

Fig. 1 presents the bifurcation figure for the one-dimensional logistic map. This map creates a chaotic map with an initial value x equal to 0.3 and $1 < \alpha < 4$. When α exceeds 3.5, a captivating phenomenon known as bifurcation emerges, unveiling a complicated and intriguing diagram [4].

Fig. 2 illustrates the graph of x_n against n for $x_0 = 0.6543$ and $\alpha = 3.9$ during 100 iterations.

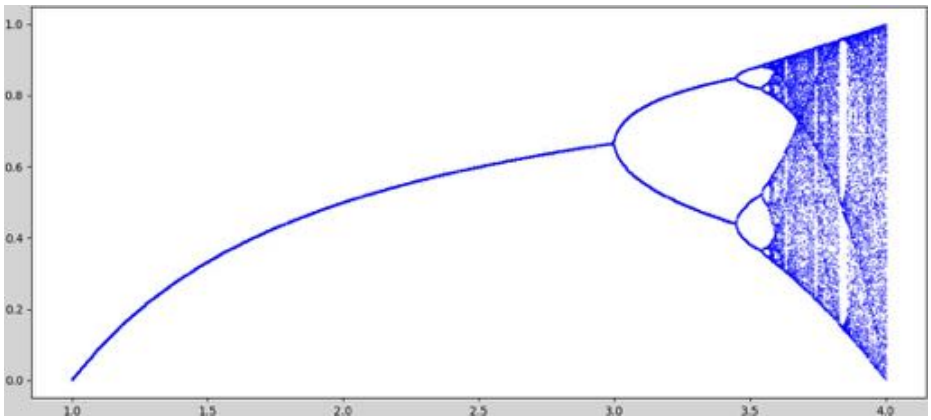


Fig. 1. Bifurcation diagram of the logistic map equation.

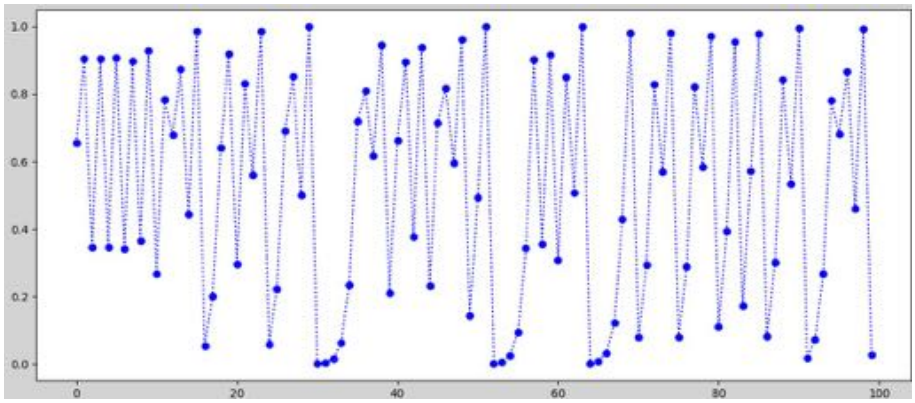


Fig. 2. Chaotic function of the one-dimensional logistic map with $x_0 = 0.5$ and $\alpha = 3.9$.

The logistic map is one of the simplest chaotic systems, where small changes in starting conditions can produce very different results. Chaos systems exhibit a high sensitivity to initial conditions. This is linked to fractals and the idea of strange attractors in dynamic systems. As R goes up, these fixed points may become unstable, which can lead to loops that get longer over time. Researchers in the fields of chaos theory and nonlinear dynamics extensively study the logistic map. The number of individuals of a species

at time $x + 1$ depends on the number of individuals in that species at time x. It's also used to show how chaos, fractals, and bifurcation theory work. The one-dimensional logistic map demonstrates how simple nonlinear equations can result in complex behavior. As the parameter r is changed, it goes from safe fixed points to periodic cycles and, for larger values of r, to chaotic behavior. It is one of the most important models for understanding how fixed systems can act in unpredictable ways, which is a central idea in chaos theory.

The remainder of this paper follows this structure: Section 2 describes the literature reviews related to my proposed method. Section 3 presents the constructor-proposed image encryption using the logistic map. In Section 4, we look at the experimental results of the suggested method for encrypting images and compare them to results from other studies. Section VI concludes the research paper.

2 Literature Review.

In [5], the author introduces a modified RC4 stream cipher technique for image encryption that rearranges image pixels before applying the XOR encryption function, yielding results that surpass the standard RC4 approach in terms of resistance to statistical attacks. Reference [1] presents a color image encryption method aimed at securing color images, utilizing an s-box based on the one-dimensional logistic map. The proposed color image encryption method is based on the newly generated S-box. The new S-box met the criteria for balance, completeness, avalanche, and strict avalanche in testing. In [4], the authors propose a novel image encryption scheme utilizing chaotic maps and fuzzy numbers for secure information transmission. The encryption method integrates logistic and sine maps to create the logistic sine map, alongside the fuzzy concept and the Hénon map to develop the fuzzy Hénon map. These maps are utilized to generate secure secret keys, respectively. A fuzzy triangular membership function is employed to adjust the initial conditions of the maps throughout the diffusion process. The encryption process entails the scrambling of image pixels, the summation of adjacent row values, and the application of XOR with randomly generated numbers derived from chaotic maps. The proposed method undergoes testing against multiple attacks, such as statistical attack analysis, local entropy analysis, differential attack analysis, signal-to-noise ratio, signal-to-noise distortion ratio, mean square error, brute force attack analysis, and information entropy analysis. Additionally, the randomness number is assessed using the NIST test. The authors in [6] proposed encrypting images through the use of chaotic signals. This employs the simultaneous manipulation of pixel movement and the adjustment of grey level quantity. approach. The movement of pixels depends on a sequence derived from the logistic map, while the adjustment of grey levels involves altering the arrangement of bits corresponding to the pixel's grey level using a chaotic signal.

3 Proposed Image Encryption Utilizing Logistic Map.

This section outlines the procedure for the image encryption algorithm, which employs a logistic map equation to generate a sequence of keys. The encrypting process uses XOR operations, enabling the encryption and decryption of images. This approach allows for the successful encryption and decryption of images. the full steps to produce an encryption image are as following steps:

Step1: Generate G number has 256 bits.

Step2: Create a Karr array that has 8 values by splitting the G number into 8 chunks; each chunk contains 4 bytes.

Step3: To reduce values in the Karr array between 0 and 1, we apply the following equation:

$$Karr_i = Karr_i \times 2^{-32} \quad (2)$$

Where $i = 0, 1, \dots, 7$.

Step4: To generate the initial value x_0 for the logistic map equation, we apply the following equation:

$$x_0 = (\sum_{i=0}^{7} Karr_i) \; mod \; 1 \quad (3)$$

Step5: Convert the image $H \times W$ to greyscale after reading it. Whereas the width represents W and the height represents H, and create a one-dimensional array of $M_i = [M_1, M_2, \dots, M_N]$ where $i = 1, 2, 3, \dots, N$ and N equals $H \times L$ from the image of size $H \times W$ pixels.

Step6: We apply equation (1) to generate the sequence of keys corresponding to N, using x_0 as the **initial** value for the logistic map equation.

Step7: We use Eq. (1) to generate the $K = [K_1, K_2, \dots, K_N]$ array, which contains the sequence of **numbers** corresponding to N and contains the values between $[0, 1]$. She sets the parameter α to 3.999 and uses x_0 as the initial value for the logistic map equation. Subsequently, modify the K array to include N elements between 0 and 255 using the following equation:

$$K_i = (K_i \times 10^{16}) \; mod \; 256 \quad (4)$$

Step8: To encrypt **the** image M, we apply the following equation:

$$C_i = K_i \oplus M_i \quad (5)$$

Where $\oplus$ denotes the XOR operation.

Step9: We can construct the encrypted image using the values in the C array. We can do the same **steps** as the encryption process to decrypt the image.

4 Results and Analysis.

This section demonstrates the efficacy of the image encryption algorithm utilizing a logistic map function initiated with x_0 from equation 3 and $\alpha = 3.999$. It employs

standard test images measuring 256 × 256 pixels, including Lena, Mandrill, Peppers, and Cameraman. Figure 3 demonstrates the efficacy of the image's encryption algorithm by presenting the encryption results for various image types: Lena, Mandrill, Peppers, and Cameraman images. The initial column illustrates the unencrypted images. The second column illustrates the encrypted images. The third column exhibits the decrypted images.

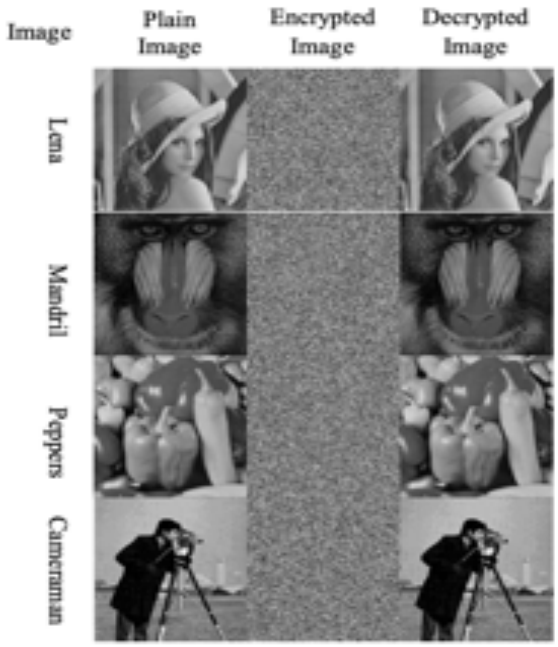


Fig. 3. Results of the encryption and decryption process.

4.1 The Analysis of Statistical Characteristics.

Examining statistical attributes for image encryption often involves assessing the impact of encryption methods on the data's statistical properties. Utilizing information entropy, correlation coefficient between plaintext and cipher image, and image histogram analysis to evaluate the security of an encryption technique allows us to ascertain the efficacy of the encryption process in concealing the statistical properties of the original image.

- The Analysis of Histograms

Image histograms disclose compelling insights regarding the distribution of pixels within the image. Cypher resistance statistical analysis is more effective when the histogram distribution of the encrypted image is more uniform. An alternative method to quantify the distribution characteristics is to utilized the variance of the histogram [3].

To statistically elucidate the distribution characteristics of a histogram, one may calculate its variance utilizing the subsequent equation:

$$V(P) = \frac{1}{R^2}\sum_{x=0}^{R-1}\sum_{y=0}^{R-1}\frac{1}{2}\left(U_x - U_y\right)^2 \quad (6)$$

Here, R is the image's greyscale value. For an 8-bit greyscale image, R equals 256. The vector V, defined as $[P_0, P_1, \ldots, P_{R-1}]$, expresses the numbers of pixels U_x and U_y, which are grey values of x and y, respectively.

The histogram becomes thinner and the distribution of greyscale pixels in an image becomes more uniform as the variance of the histogram diminishes. The pixel values in the image are becoming more uniformly distributed. Image processing employs a histogram as a graphical representation to depict the distribution of pixel intensities within an image. Smoothing the histogram distributes the range of pixel intensities more uniformly throughout the entire spectrum of intensities.

In a uniformly distributed greyscale image, each intensity level (ranging from 0 to 255 in an 8-bit format) occurs approximately with equal frequency. This degree of homogeneity might enhance an image's appearance and safeguard it from statistical assaults. The variance of a histogram quantifies the extent to which the values in the matrix (or the pixel intensities in the image represented by the histogram) differ from one another, offering a measure of the dispersion or variation in the pixels of the underlying image.

A thinner histogram signifies a growing uniformity across pixel values, as evidenced by a reduction in variance. Since 0 is the ideal value of $V(P)$, we can write $U_x = U_y$ for all x and y.

We produced the histograms of the four test photographs and the cypher images utilising our technique, as illustrated in Fig. 4. Each unencrypted image displays a distinctly varied histogram distribution, while the histogram distribution of each encrypted image is notably consistent. Table 1 displays the variances of the histograms for the analyzed plain images (256 × 256) and their corresponding cipher images. The mean variance of the cipher images encrypted using our algorithm approach is 258.73827, significantly lower than that of unencrypted images. Table 2 shows a comparison of the histogram variance for Mandrill and Cameraman images between this study and previous studies. As a result, our improved methodology is impervious to statistical attacks.

Table 1. Histogram variance: Comparison of Encrypted versus Unencrypted Images

Image	Plain Image	Encrypted Image
Lena	39547.15625	305.44531
Mandril	73050.21875	270.33593
Peppers	30972.07031	246.17968

Cameraman	98249.78125	212.99218
Mean	60454.80664	258.73827

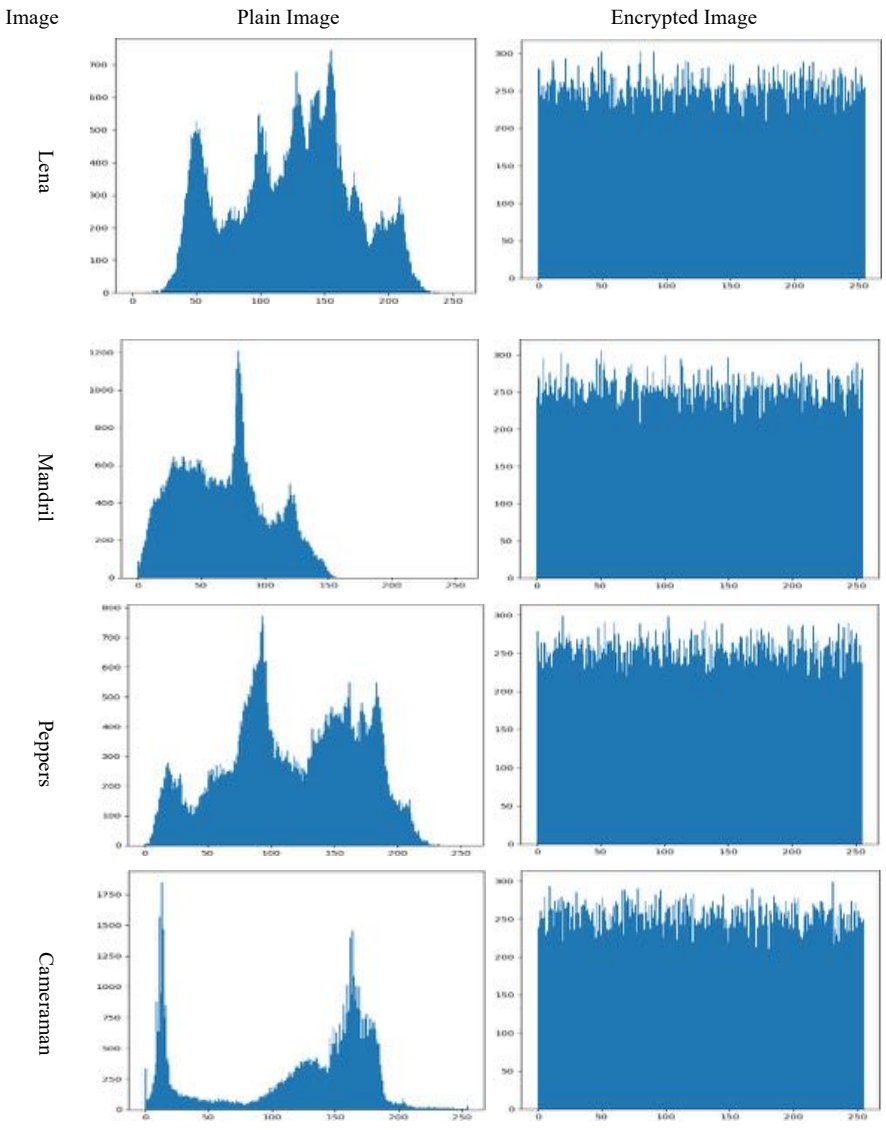


Fig. 4. Histogram of both unencrypted and encrypted images.

Table 2. Comparison of histogram variance between this research and other research.

Research	Encrypted Image	Value
This Research	Mandril	270.33593
	Cameraman	212.99218
[7]	Mandril	272.9219
	Cameraman	339.5938
[8]	Mandril	405.9375
	Cameraman	1074.2000

- The Analysis of Information Entropy

In 1948, Claude Shannon developed the statistical metric known as information entropy [9]. In the context of image encryption, the entropy of a cipher image is a measure of the extent to which its pixel distribution is random. A higher entropy number indicates a well-covered plaintext devoid of discernible patterns. To evaluate the randomness and unpredictability of an encryption technique, we can use entropy measures such as global entropy or Shannon entropy, which calculate pixel information across the entire image [10]. To calculate the Shannon entropy, we can employ the subsequent equation:

$$H(R) = -\sum_{i=0}^{2^n-1} \mathrm{R}_i \ \log_2(\mathrm{R}_i) \qquad (7)$$

In this equation, n is the total number of bits used to represent the pixels, while R_i denotes the probability associated with each pixel value.

To successfully resist brute force attacks, an encryption method has to tightly match the entropy of a cypher image with the ideal entropy value of 8 [10].

Table 3 illustrates an evaluation of the entropy of the plaintext in comparison to the encrypted image for our methodology. Table 4 presents a comparison between this study and previous studies on the entropy of the Lena image. As a result, our improved methodology is close to value 8, which is the optimal value and better than the results of other researches, as shown in Table 4.

Table 3. Comparative Analysis of Information Entropy in Plain and Encrypted Images.

Image	Plain Image	Encrypted Image
Lena	7.36352	7.99664
Mandril	7.05805	7.99702
Peppers	7.58018	7.99728
Cameraman	7.12996	7.99766

Table 4. Comparison of entropy between this research and other research.

Research	Encrypted Image
This Research	7.99664
[5]	7.9846
[6]	7.9949
[11]	7.9943
[12]	7.9953

- The Analysis of Correlation Coefficient Between Plaintext and Cipher Images

The correlation coefficient between plaintext and cipher images is a statistical measure that quantifies the correlation between the pixel intensity values of the original and encrypted images. It quantifies the extent to which the encryption technique disrupted the correlation and patterns of plaintext images. The correlation coefficient between the plaintext and cipher images is determined by the following equation:

$$R = \frac{cov(X,Y)}{\sqrt{Var(X)}\sqrt{Var(Y)}} \quad (8)$$

Where $cov(X, Y)$ is the covariance between the plaintext and cipher images and computed as the following equation:

$$cov(X,\ Y) = \frac{1}{N}\sum_{i=1}^{N}(X_i - \mu X)(Y_i - \mu Y) \quad (9)$$

Where μX and μY are the mean intensity values of the plaintext and cipher images, respectively, and N is the total number of pixels in the image.

The $Var(X)$ is the variance of the plaintext image and computed as the following equation:

$$Var(X) = \frac{1}{N}\sum_{i=1}^{N}(X_i - \mu X)^2 \quad (10)$$

The $Var(Y)$ is the variance of the cipher image and computed as the following equation:

$$Var(Y) = \frac{1}{N}\sum_{i=1}^{N}(Y_i - \mu Y)^2 \quad (11)$$

The correlation coefficient between the plaintext and cypher images should approximate 0, indicating that there is no association, in order to ensure a robust encryption algorithm. The correlation coefficient between normal text and encrypted images for four images is summarized in Table 3. We chose 3000 pixels randomly to calculate The correlation coefficient between plain and cipher images for the four tested images (Peppers, Cameraman, Lena, and Mandrill) is illustrated in Fig. 5. The correlation between the plain image and the cipher is feeble. This has the potential to enhance the resilience of our algorithm to statistical attacks.

Table 5. The outcomes for the correlation coefficient between plaintext and cipher images.

Image	Correlation Value
Lena	0.00444
Mandril	-0.00153
Peppers	-0.00055
Cameraman	-0.00223

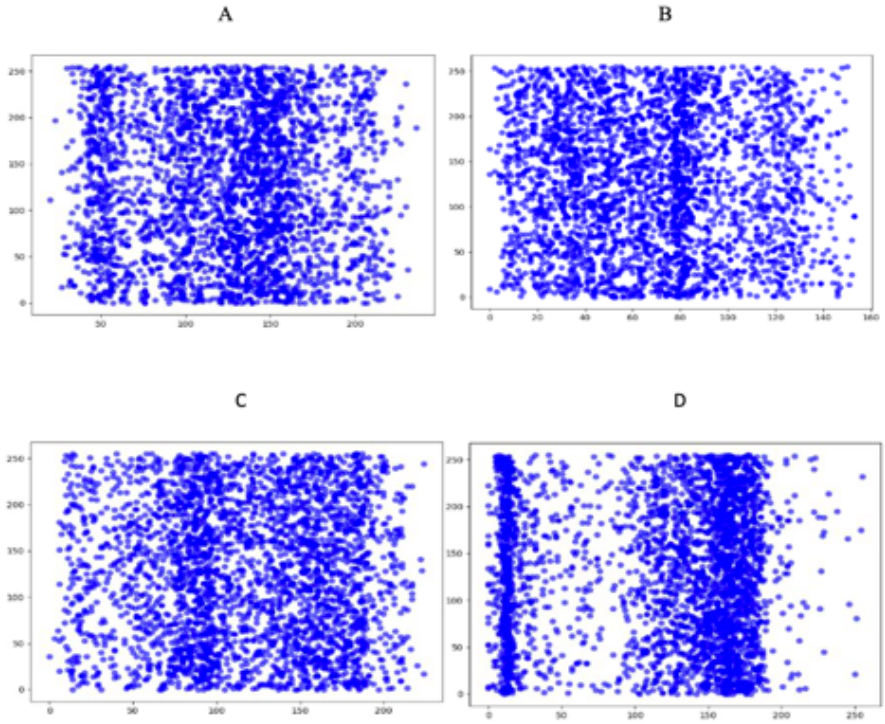


Fig. 5. The correlation coefficient between plaintext and cipher images: (A) is the correlation for Lena's image, (B) is the correlation for Mandril's image, (C) is the correlation for Peppers's image, and (D) is the correlation for Cameraman's image.

4.2 Analysis of Mean Square Error and Peak Signal-to-Noise Ratio.

The mean square error (MSE) and peak signal-to-noise ratio (PSNR) are often utilised metrics for assessing image quality. The Mean Squared Error (MSE) measures the similarity of unencrypted images and their encrypted versions; a lower MSE signifies su-

perior image quality, whereas a greater MSE denotes inferior quality [4]. The calculation of MSE, as illustrated in Equation (12), entails contrasting the unencrypted image with the encrypted image. Conversely, we employ PSNR to assess the effectiveness of image encryption algorithm, where reduced PSNR values indicate enhanced encryption performance. Equation (13) delineates the formula for computing PSNR in this scenario.

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(T_{ij} - E_{ij}\right)^2 \quad (12)$$

$$PSNR = 20\ log_{10} \frac{[255]}{\sqrt{MSE}} \quad (13)$$

Here, T_{ij} and E_{ij} represent the pixels of the plain and encrypted images, respectively. Table 6 summarizes the experimental results for encrypted images, showing both PSNR and MSE values. The high MSE value and low PSNR value suggest that the encryption technique is effective.

For our method, Table 6 shows an analysis of the MSE and PSNR between the plaintext and the encrypted image, as well as between the plain image and the decrypted image. Table 7 compares the PSNR for the Mandrill image between this study and previous studies. As relayed in the results shown in Table 7, our improved methodology is better than the previous studies.

Table 6. Comparative Analysis of MSE and PSNR.

Image	Measures	Encrypted Image	Decrypted Image
Lena	MSE	7753.57287	0
	PSNR	9.23578	Inf
Mandril	MSE	10350.20935	0
	PSNR	7.98131	Inf
Peppers	MSE	8326.03906	0
	PSNR	8.92641	Inf
Cameraman	MSE	9458.21838	0
	PSNR	8.37271	Inf

Table 7. Comparative Analysis of PSNR.

Research	PSNR value
This Research	7.98131
Case 1 In [13]	9.8015
Case 2 In [13]	9.7765
[14]	9.7208
[15]	9.8015

4.3 Analysis of Gray-Level Co-Occurrence Matrix (GLCM)

The Grey-Level Co-Occurrence Matrix (GLCM) is a technique employed in image processing and cryptography to extract texture information from images. The Grey Level

Co-occurrence Matrix (GLCM) analyses the spatial relationships between pixel intensities to discover co-occurrence patterns in an image.

Energy: The statistical measure called energy is usually based on the GLCM. It measures the consistency or concentration of an encrypted image's pixel intensity distribution. The degree to which an encryption technique has altered the image's original spatial and intensity patterns can be determined by its energy. The following equation provides the mathematical definition of energy, which is the sum of the squared elements in the GLCM:

$$E = \sum_{y=0}^{R-1} \sum_{x=0}^{R-1} G(x,y)^2 \quad (14)$$

Where $G(x,y)$ is the value at position (x, y) in the GLCM and R is the number of intensity levels in the image.

The encrypted image must have minimal energy, or be closest to zero value, for an image encryption algorithm to be considered secure[16]. This suggests that the image needs to have a well-disrupted spatial structure and a high degree of unpredictability. Because of this, hacking and statistical analysis will be challenging.

Contrast: The contrast measure is derived from the GLCM. It measures the difference in intensity between adjacent pixels in the encrypted picture. We can assess how successfully the encryption technique has changed the intensity patterns of the original image by looking at contrast. The following equation provides the mathematical definition of contrast:

$$C = \sum_{x=0}^{R-1} \sum_{y=0}^{R-1} G(x,y) \times (x-y)^2 \quad (15)$$

Where $G(x, y)$ is the value at position (x, y) in the GLCM, R is the number of intensity levels in the image, and $|x - y|$ represents the difference in intensity be- tween pixel pairs.

The encrypted image should exhibit high contrast, reflecting significant disruption of intensity patterns.

High contrast in the image indicates a major disturbance of intensity patterns. This increases the encrypted image's resilience to assaults and statistical analysis by ensuring that it lacks observable structures or regularities [16].

Homogeneity: The GLCM yields a number called homogeneity, which indicates how evenly the intensity values of the pixels in an encrypted image are distributed. The degree to which the pixel intensities in the encrypted image are comparable to those of their neighbors is known as homogeneity.

The following formula provides the mathematical definition of homogeneity:

$$H = \sum_{x=0}^{R-1} \sum_{y=0}^{R-1} \frac{G(x,y)}{1+|x-y|} \quad (16)$$

Where $G(x, y)$ is the value at position (x, y) in the GLCM, R is the number of intensity levels in the image, and $|x - y|$ represents the difference in intensity between pixel pairs. Low homogeneity implies a more erratic distribution of pixel intensity and shows that the texture and patterns of the original image have been successfully hidden by the encryption process [16].

The results demonstrate that the encryption of the images is robust against statistical analysis. Table 8 displays the energy, contrast, and homogeneity values for four encrypted images. The energy values are close to zero, the contrast values are high, and the homogeneity values are low. Based on these results, our methodology has excellent results and successfully hides the patterns of the original image by the encryption process. Table 9 shows the comparison of energy and homogeneity to the Lena image between this study and another study, and based on these results, our methodology has excellent value in energy and homogeneity.

Table 8. Energy, contrast, and homogeneity of encrypted images.

Image	Energy	Contrast	Homogeneity
Lena	0.00550	10939.36853	0.01238
Mandril	0.00554	10917.25500	0.01176
Peppers	0.00554	10932.88655	0.01218
Cameraman	0.00552	10865.81237	0.01247

Table 9. Comparison of energy and homogeneity between this research and another research.

Research	Measures	Average Value
This Research	Energy	0.00550
	Homogeneity	0.01238
[16]	Energy	0.01563
	Homogeneity	0.38929

4.4 Analysis of Key Sensitivity.

The key sensitivity analysis procedure assesses the encryption algorithm's sensitivity to key changes. This examination looks at how changes to the encryption key affect the picture encryption scheme's efficacy and security. When evaluating an encryption algorithm's resilience to key changes, key sensitivity analysis is essential.

A unique encrypted image can be produced with a small change in the key combinations. It has been demonstrated that the suggested technique is extremely sensitive to modifications in the encryption key. The four incorrect keys ($k1$, $k2$, $k3$, and $k4$) are chosen. The technique used to decipher the Cameraman's encrypted image is sensitive to even the smallest bit changes, as illustrated in Fig. 5. The least significant bit's final four bits were altered, one bit at a time, from 0 to 1 or the other way around. Therefore, the decryption method will not be able to properly decrypt the image if the decryption key is slightly changed.

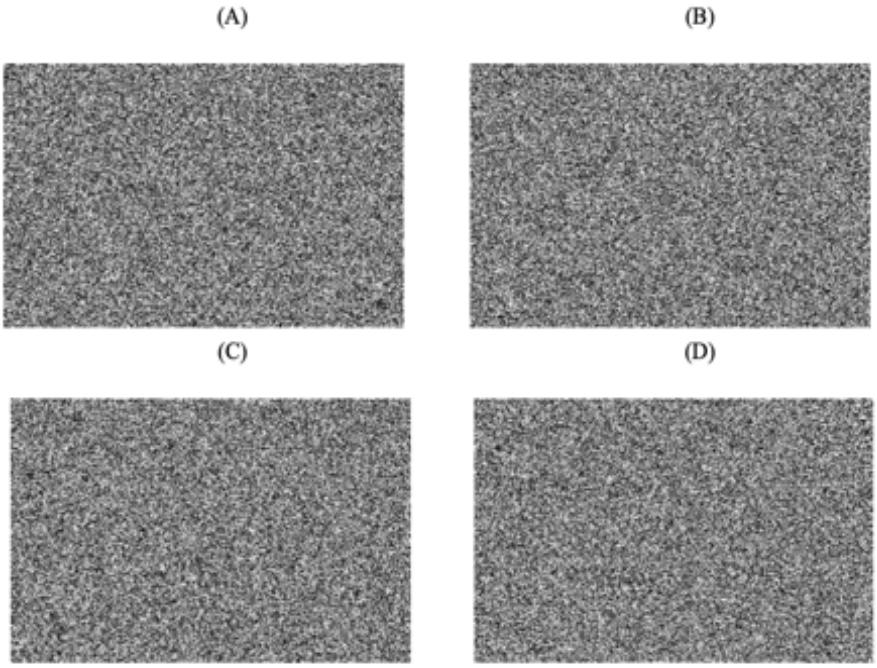


Fig. 6. The cameraman's cipher image decrypted by the change of one bit in the key. (A) the decrypted cameraman's cipher image with k1. (B) the decrypted cameraman's cipher image with k2. (C) the decrypted cameraman's cipher image with k3. (D) the decrypted cameraman's cipher image with k4.

5 Conclusion and Future Work.

In this paper, we proposed an image encryption algorithm using a chaotic map to generate a series of encryption keys and apply an XOR operation to encrypt image pixels. The obtained results demonstrated the efficiency of the encryption algorithm for encrypting various kinds of images. We also analyzed the information entropy, histogram analysis, correlation coefficients between plain and cipher images, energy, contrast, and homogeneity, and the analysis of the key sensitivity of the key. The study results show that the logistic map equation can be used to encrypt images. The suggested encryption method has a high level of security, works better than some others, and is satisfactory all around. That indicates the effectiveness and resistance against attacks.

In the future, researchers may look into how this encryption method can be used in different areas, such as to protect multimedia data stored in the cloud or to send images in real time. It would also be helpful to test this idea on different images of different sizes and see if the results are the same each time. Furthermore, we could focus on applying this algorithm to colored images. We are developing algorithms to safeguard images from attacks and encrypt them, thereby enhancing the security of all private images stored on cloud computing.

References

1. R. S. Salman, A. K. Farhan, and A. Shakir, 'Creation of S-Box based One-Dimensional Chaotic Logistic Map: Colour Image Encryption Approach', *Int. J. Intell. Eng. Syst.*, vol. 15, no. 5, 2022, doi: 10.22266/ijies2022.1031.33.
2. B. Yang and X. Liao, 'A new color image encryption scheme based on logistic map over the finite field ZN', *Multimed. Tools Appl.*, vol. 77, no. 16, 2018, doi: 10.1007/s11042-0175590-0.
3. Q. Lu, C. Zhu, and X. Deng, 'An Efficient Image Encryption Scheme Based on the LSS Chaotic Map and Single S-Box', *IEEE Access*, vol.8, 2020, doi: 10.1109/ACCESS.2020.2970806.
4. D. E. Mfungo, X. Fu, Y. Xian, and X. Wang, 'A Novel Image Encryption Scheme Using Chaotic Maps and Fuzzy Numbers for Secure Transmission of Information', *Appl. Sci.*, vol. 13, no. 12, 2023, doi: 10.3390/app13127113.
5. M. H. S. Hasan, 'Image Encryption using Modified RC4 Algorithm', in *Proceeding - 2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering, MI-STA 2023*, 2023. doi: 10.1109/MISTA57575.2023.10169339.
6. K. Jadidy Aval, M. Sabery Kamarposhty, and M. Damrudi, 'A Simple Method for Image Encryption Using Chaotic Logistic Map', *J. Comput. Sci. Comput. Math.*, 2013, doi: 10.20967/jcscm.2013.03.007.
7. X. Wang *et al.*, 'S-box based image encryption application using a chaotic system without equilibrium', *Appl. Sci.*, vol. 9, no. 4, 2019, doi: 10.3390/app9040781.
8. Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, 'Secure image encryption algorithm design using a novel chaos based S-Box', *Chaos, Solitons and Fractals*, vol. 95, 2017, doi: 10.1016/j.chaos.2016.12.018.
9. C. E. Shannon, 'A Mathematical Theory of Communication', *Bell Syst. Tech. J.*, vol. 27, no. 3, 1948, doi: 10.1002/j.1538-7305.1948.tb01338.x.
10. Y. Alghamdi and A. Munir, 'Image Encryption Algorithms: A Survey of Design and Evaluation Metrics', 2024. doi: 10.3390/jcp4010007.
11. J. Thiyagarajan, B. Murugan, and A. G. N. Gounder, 'A chaotic image encryption scheme with complex diffusion matrix for plain image sensitivity', *Serbian J. Electr. Eng.*, vol. 16, no. 2, 2019, doi: 10.2298/SJEE1902247T.
12. M. M. Hazzazi, S. Attuluri, Z. Bassfar, and K. Joshi, 'A Novel Cipher-Based Data Encryption with Galois Field Theory', *Sensors*, vol. 23, no. 6, 2023, doi: 10.3390/s23063287.
13. Z. K. Obaidand and N. F. H. Al Saffar, 'Image encryption based on elliptic curve cryptosystem', *Int. J. Electr. Comput. Eng.*, vol. 11, no. 2, pp. 1293–1302, 2021, doi: 10.11591/ijece.v11i2.pp1293-1302.
14. Z. E. Dawahdeh, S. N. Yaakob, and R. Razif bin Othman, 'A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher', *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 30, no. 3, pp. 349–355, Jul. 2018, doi: 10.1016/j.jksuci.2017.06.004.
15. L. Chen, H. Yin, T. Huang, L. Yuan, S. Zheng, and L. Yin, 'Chaos in fractional-order discrete neural networks with application to image encryption', *Neural Networks*, vol. 125, 2020, doi: 10.1016/j.neunet.2020.02.008.
16. R. Flores-Carapia, V. M. Silva-García, and M. A. Cardona-López, 'A Dynamic Hybrid Cryptosystem Using Chaos and Diffie–Hellman Protocol: An Image Encryption Application', *Appl. Sci.*, vol. 13, no. 12, 2023, doi: 10.3390/app13127168.

تشفير الصور بالاعتماد على الخريطة الفوضوية

محمود حسن سعيد حسن [1] ، عادل علي الوحيشي [2]

[1] كلية تقنية المعلومات ، الجامعة الاسمرية الإسمرية ، زليتن – ليبيا
[2] قسم الهندسة الكهربائية والحاسوب ، الأكاديمية الليبية ، طرابلس – ليبيا
tea_mhs@asmarya.edu.ly

الملخص: تعد عملية تشفير الصور من أكثر الطرق فعالية لضمان الخصوصية في العالم الرقمي . يجب علينا تسهيل وتأمين نقل الصور التي لها خصوصية للأشخاص من مكان إلى آخر عند إرسالها عبر شبكات الانترنت، مثل إرسالها لتخزينها على السحابة. اقترحت هذه الورقة خوارزمية لتشفير وفك تشفير الصور. يستخدم النهج خريطة لوجستية فوضوية لتوليد مفتاح ثم تطبيق عملية XOR لتشفير وفك تشفير الصور. تشير النتائج إلى أن التقنية المقترحة هي طريقة فعالة لتشفير وفك تشفير الصور. نقوم بتقييم مقاييس تحليل أداء التشفير: إنتروبيا المعلومات، وتحليل الهيستوجرام، ومعاملات الارتباط بين الصور العادية والمشفرة، والطاقة، والتباين، والتجانس، وتحليل حساسية المفتاح. تشير النتائج إلى أن التقنية المقترحة قد أثبتت فعاليتها.

الكلمات المفتاحية: تشفير الصور ، الخريطة اللوجستية الفوضوية ، عملية XOR.