Journal of Basrah Researches (Sciences) **48**(2), 77 (2022)
DOI: https://doi.org/10.56714/bjrs.48.2.8

Chaotic-Based Color Image Encryption Algorithms: A Review

Ghofran K. Shraida*, Hameed A. Younis

Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq.

ARTICLE INFO

Received 23 July 2022
Accepted 19 August 2022
Published 30 December 2022

Keywords:

Chaotic Map, Color image, Decryption Encryption, Image Encryption

Citation: G.K. Shraida, H.H. Younis, J. Basrah Res. (Sci.) **48**(2), 77 (2022). DOI:https://doi.org/10.56714/bjrs.48.2.8

ABSTRACT

The protection of multimedia information is becoming very essential due to the significant advancements in communication networks, particularly the Internet network, which is utilized by many individuals to transmit various kinds of data. The safety of this multimedia information may be performed with encryption and decryption methods. There are such a lot of special strategies need to be used to guard personal image from unauthorized access, chaotic encryption systems are one of these technologies that have recently become popular. Many ways for encrypting images using a chaotic map have been proposed due to various advantages, such as, ease of implementation, better encryption speed, and resistance to assaults. Many image encryption techniques based on chaotic maps have been proposed due to their great sensitivity to beginning circumstances, unpredictability, and random-like behavior. This paper reviews various image encryption algorithms based on chaos theory that give good security.

1. Introduction

In view to the necessity to communicating and storing multiple kinds of data over the Internet, including text, audio, image, and video, in an environment where the information shared is easily penetrated, cryptographic approaches have been utilized to preserve data confidentiality from unwanted access [1].

When exchanging or storing images over a network, the most beneficial technique to maintain secrecy is image encryption. Its applications have the potential to grow into military communications, multimedia systems, medical science, online communications, and other fields. Images vary from text in several ways, including their lower sensitivity, correlation between neighboring pixels, data redundancy, and massive storage capacity. Many encryption approaches have evolved to address the issues that image encryption faces. Several traditional encryption techniques, such as AES, DES, 3DES, and RSA, have been employed for many years, it is not appropriate in terms of image encryption. Several shortcomings exist in these techniques when images are large in size [2].

Chaos-based cryptography was recently developed and is now widely employed in image encryption techniques. These chaotic systems have a number of intriguing qualities. These systems generate iterative values that are completely random yet limited within boundaries. The convergence of the repeating numbers

*Corresponding author email : itpg.ghofran.khaled@uobasrah.edu.iq

ISSN: 1817-2695 (Print); 2411-524X (Online)
Online at: https://bjrs.uobasrah.edu.iq

can never be visible after any number of repetitions. Chaotic systems are the most sensitive to initial circumstances. A nonlinear feature of a physical system is connected with chaotic behavior. It occurs for a certain set of parameters. Chaos is built and evolved utilizing one-dimensional or high-dimensional systems, i.e., chaotic maps. Chaotic maps can be built with a discrete or continuous time parameter. The power of cryptography resides on the proper selection of keys for data encryption. This decryption key is kept private and protected from the opponent. In cryptography, chaotic cryptosystems can be built using a pseudorandom bit stream generator.

Some reviews are specifically focused on the image encryption that uses chaotic systems. N. R. Deepa and N. M. Sivamangai [3] claimed that a wrongfully altered medical image allows diagnosing an actual disease more difficult. This highlights the critical importance of clinical image confidentiality.

K. Yadav and T. Chaware [4] believed that, copyrights violated and information can be stolen despite current encryption and information concealment strategies. They began by reviewing cutting-edge image encryption algorithms. They concentrated on joint encoding encryption techniques in particular. Then, with the help of the AES and Substitution boxes (S-boxes), they suggested algorithm based on chaotic maps and Low-Density Parity-Check (LDPC).

A comparative approach is used in some existing reviews. For instance, the benefits and drawbacks of current chaotic image encryption techniques were weighed. in [5]. Another pertinent survey was published in [6], where the authors evaluated and discussed some 1D chaotic maps to some hyper-dimensional ones in terms of image encryption applications. As another example, the authors of [7] mentioned chaotic encryption as an effective alternative for encoding images and videos with highly correlated neighboring pixels. They presented a review of the current chaotic techniques for image encryption in order to find the best chaotic map. They investigated tent maps, logistic maps, sine maps, and so on, and concluded that Arnold's cat map was the most promising chaotic map for this goal.

The purpose of this review paper is to discuss and analyze chaotic-based image encryption schemes to verify their efficacy, and their performance against different types of attacks. The rest of this paper is organized as follows: Section 2 contains a simple overview to chaotic system based image encryption. Performance metrics shows in Section 3. Section 4 includes a review of the literature on several ideas suggested in the last decade. Section 5 compares the strategies outlined in Section 4. Section 6 displays the conclusions.

2. Chaotic System based Image Encryption

There are two types of image encryption: chaos-based specific or non-specific tactics and non-chaos specific approaches. In chaos-based approaches, initial circumstances are extremely sensitive. If we modify something in the starting circumstance, the entire outcome will change [8], [9]. The advantages of image encryption algorithms based on chaotic systems are ease of use, higher encryption speed, and resistance to attacks [10].

The chaotic-based encryption approach has various types of functions in a variety of fields, including Internet communication, health care, military, medical images, multimedia systems, security, and government documents, and so on [10].

Permutation and diffusion are the two phases of chaos-based image encryption approaches. The chaos-based image encryption technique is depicted in block diagram form in Fig. 1. The whole permutation-diffusion (i, j respectively) round repeats for number of times to achieve security of satisfactory level. During the permutation phase, chaotic sequences or matrix transformations are used to modify the positions of the pixels. Although, this permutation approach improves encryption, it is unable to change the pixel value. Because pixels are not modified, the encrypted image's histogram and the original image's histogram are identical. As a result, the statistical analysis could threat its security. During the diffusion phase, chaotic sequences modify the pixel values of the plain image. In comparison to permutation, diffusion may provide more security. As a result, several researchers have coupled permutation and diffusion to increase the level of secrecy. Thus, the use of discrete chaotic maps not only helps to build a good encryption system but, also, makes it a good candidate for efficiency. To ensure the security of digital image information, the effective protective measure is image encryption.

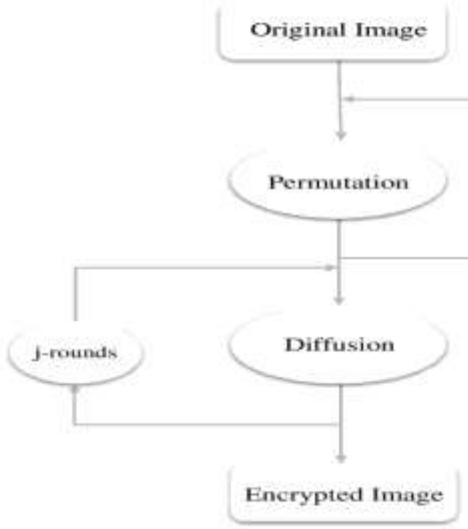

Fig. 1. Approach of Chaotic Image Encryption.

3. Performance Metrics

3.1. Key Security Evaluation

In a good encryption technique, we should concentrate on the encryption keys throughout both the encrypting and decrypting processes. The amount of different keys that may be used in encryption and decryption procedures is referred to as the key space. The ciphertext images are sent over the public channel, while the security key is sent over the private channel. As a result, the security key should be of legal size and resistant to brute force attacks. In terms of cryptography, a key space higher than 2^{100} may give an extra layer of protection. [11].

3.2. Key Sensitivity Analysis

A protected algorithm must provide a wide key space to increase the resistance to brute force attacks on a cryptosystem. Furthermore, be fully sensitive to the key, which indicates that the image cannot be decrypted by minor changes in the key. This means that even a minor variation in the secret key will result in an entirely different encrypted image; in other hand, a secret key that is slightly different from the correct one will never decrypt the image and will generate a completely wrong image.

3.3. Histogram Analysis

An image histogram represents the pixels values intensity distribution in an image, so to resist any statistical attack and to ensure a secure encryption system, the histogram of the encrypted image must be uniform [12]. From a mathematical standpoint, the histogram is a discrete function with gray level values ranging from 0 to L – 1 as in the following equation [13]:

$$hist(rk) = \frac{nk}{M \times N} \qquad (1),$$

The k^{th} gray level is represented by rk, and the number of pixels in the image with that gray level value is represented by nk. $M \times N$ represents the total number of pixels in the image, and rk = 0, 1,..., L - 1.

3.4. Correlation Coefficient Evaluation

A good cipher image should have a restricted link between the pixel values. The best way to determine the efficacy of the suggested picture cryptosystem is to use correlation coefficient analysis to uncover the relationship between the cipher's pixel values. An original image's pixels always have a strong link with their neighboring pixels, whether in a vertical, horizontal, or diagonal orientation. As a result, a good image encryption computation should eliminate significant relationships between nearby pixels. the following equation can be used to determine the horizontal, vertical, and diagonal correlation of two neighboring pixels [14]:

$$\begin{cases} \bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \\ \sigma_x = \frac{1}{N}\sum_{i=1}^{n}(x_i - \bar{x})^2 \\ cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y}) \\ corr_{xy} = \frac{cov(x,y)}{\sqrt{\sigma_x}\sqrt{\sigma_y}} \end{cases}, \qquad (2)$$

where x and y are two neighbouring grayscale values and N is the total number of pixels in the image, $\bar{x}$ and $\bar{y}$ denote the mean value depicted in the following equation:

$$\bar{x} = \frac{1}{M\times N}\sum_{i=1}^{M\times N} x_i \qquad (3)$$

3.5. Information Entropy

Shannon developed the notion of information entropy for the first time in 1949. It is one of the mathematical axioms that represents an information source's unpredictability and randomness. It is a crucial notion in information theory since it describes the degree of disorder in a system. The entropy $H(d)$ of data d is calculated using the following equation [15]:

$$H(d) = \sum_{i=1}^{2^l-1} p(d_i)log_2(\frac{1}{p(d_i)}), \qquad (4)$$

where l represents the number of digits in the gray value of the image pixels, and $p(d_i)$ signifies the likelihood of a pixel with value d_i occurring.

3.6. Differential Attack Evaluation

The difference attack is one of the most often used and effective security attacks. The number of pixel change rate (NPCR) and formally unified average change intensity (UACI) are two measurements that may be used to determine if image computation encoding can withstand differential attack. The following equations can be used to calculate NPCR, and UACI [16]:

$$NPCR = \frac{\sum_{i,j} D(i.j)}{L} \times 100\% \qquad (5)$$

$$UACI = \frac{1}{L}\left[\sum_{i,j}\frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\%\ , \qquad (6)$$

$C_1(i,j)$ and $C_2(i,j)$ represent two encrypted images with only one pixel value change from the corresponding plain images, $D(i.j)$= 0 when it is the same value in C_1 and C_2, while, it is 1 when it is different.

3.7. MSE and PSNR

The MSE and PSNR are used to assess the similarity between the plain image and the encrypted image for the encryption method. MSE is written as the following equation [17].

$$MSE = \frac{1}{M\times N}\sum_{a=0}^{M-1}\sum_{b=0}^{N-1}[\lfloor F(a,b) - F_0(a,b)\rfloor^2] \qquad (7)$$

A lower MSE value indicates that the algorithm is more accurate in describing experimental data. PSNR is written as the following equation [17].

$$PSNR = 10.log_{10}(\frac{peakval^2}{MSE}) \qquad (8)$$

$Peakval$ denotes the maximum number of image pixels; for an 8-bit integer-based image, $peakval$ = 255.

4. Literature Review

This section includes some major authors' research work in the relevant domain of image cryptosystems during the previous decade, as well as, a brief discussion of several versions of chaos-based algorithms utilized for image cryptosystems.

J. Wu *et al.* [18] introduced a safe color image encryption method using the modified 4D cat map and the elliptic curve ElGamal cryptosystem. They first reduced the size of the plain image, then separated it into blocks and linked each of them to make a final block whose pixel values were stretched as far as feasible into the full EC finite field to form a preprocessed image. The revised 4D cat map was then used to equalize the histogram of the preprocessed image. Third, they embed the second encryption image inside EC and encrypted the embedded data with the enhanced ElGamal encryption algorithm. Finally, the encrypted image was universally diffused to generate the final encrypted image. This method has a large key space and is indicated to take less time to execute.

M. Essaid *et al.* [19] presented a system based on three maps: the Pseudorandomly Enhanced Sine Map (PESM), the Pseudorandomly Enhanced Logistics Map (PELM), and the Pseudorandomly Enhanced Skew Tent Map (PESTM). The original image's red channel was blended with the ELM, the green channel with the ESM, and the blue channel with the ESTM. Finally, the three mixed channels were subjected to a powerful avalanche effect in order to generate an encrypted color image. It is shown by simulative means that the encryption algorithm is robust against statistical, differential and exhaustive attacks with a higher order of security.

Color image encryption based on combination of a chaotic map and block cipher was presented by E. A. Albahrani, and T. K. Alshekly [20]. This paper's major point is to encrypt and decrypt image of different size based on permutation and substitution. Each block was permuted by using 3D Cat map and 3D Hénon map, and then the result was substituted using 1D Bernoulli map. Finally, the resulted block was XORed with the key block. Key streams are produced during both the diffusion and permutation stages, resulting in a large key space that is less vulnerable to multiple attacks.

An image encryption method was suggested by Xiaolin Wu *et al.* [21] to encrypt a grey and color image. In this paper, an improved algorithm based on a rectangular transform (RT)-enhanced chaotic tent map (CTM) system was presented. It encrypted the three RGB channels at the same time and these channel encryptions associate with each other. Analyses and experiments have demonstrated that the proposed algorithm is both secure and effective.

C. Zhu, and K. Sun [22] enhanced the color image encrypting method. The updated algorithm incorporated the three significant enhancements listed below. First, a novel combined chaotic system called *Logistic-tent map* (LTM) was suggested, which outperforms tent map in terms of chaotic performance. Second, the enhanced encryption algorithm was applied to the new chaotic system. Third, the key generation process and encryption approach were enhanced. The reliability and performance of the method against the many known attacks are confirmed by security analysis using MATLAB simulations.

Josephus traversing and mixed chaotic map were employed by X. Wang *et al.* [23] to present a new image encryption. The scheme consists of three processes: In the first process, the mathematical model used for the key stream generator. The starting settings and parameters are sensitive to both the new scheme's secret keys and original images. The second process used Josephus traversing in shuffling, after which the columns and rows of pixels were switched. The third process adjusted the pixel gray values and removed the associations between neighboring pixels. Various tests, experiments, and analyses were carried out to demonstrate that the suggested encryption algorithm provides suitable security.

C. Zhu *et al.* [24] suggested a novel color image encryption technique based on the Sine-Sine system that was more secure and efficient. The novel encryption approach generates diffusion arrays based on the image's content and the permutation position array. Two effects, ciphertext feedback and pixel scrambling, were also applied concurrently in the diffusion process. The algorithm has small key space, therefore the transmission of ciphered image will be threatened by brute force attack.

R. A. Aboughalia, and O. A. S. Alkishriwo [25] used logistic map and duffing map for color image encryption. First, the original image was separated into equal-sized pieces. Then, two chaotic maps were employed to produce two key streams, which were then permuted to form a single key steam. Following that, a portion of the key stream was used to shuffle the image blocks. Finally, the encrypted image was XORed with the scrambled image. The experimental results demonstrate that the proposed method offers sufficient security. Using logistic map and XOR gates, the algorithm achieves a multi-chaos encryption impact.

An efficient color image encryption was proposed by A. Firdous, and M. M. Saad Missen [26] based on chaotic map and linear transformation. Each channel of a color image was permuted using chaotic sequences through rows and columns using cyclic shift. Pseudorandom numbers were created using chaotic maps and then built into pseudo-random matrices using linear transformations. Under the XOR process, these random matrices were coupled with permuted colored channels. Following several tests, it was determined that the algorithm is resistant to various attacks, has a larger key space, faster encryption speed, and high complexity, all of which lead to higher security.

A color image encryption using hyperchaotic system and block permutation was proposed by G. Cheng *et al.* [27]. By combining R, G, and B components, a block permutation was created. The pixels of the color components were then dispersed, and the three components began to interact again. The G component was diffused in reverse order throughout the diffusion process. Because the components are handled separately, it has been experimentally verified that this process takes less time to execute. As a result, when decrypted, it can produce a higher quality image.

The Logistic-Fraction Hybrid Chaotic Map (LFHCM) and a 4D hyperchaotic system were employed by L.-L. Huang *et al.* [28] for RGB image encryption. The LFHCM worked in conjunction with a 4D hyperchaotic system to create the key streams that rotated and relocated the columns and rows of each Red, Green, and Blue component for the color image. Furthermore, the key stream that was updated by the plain images was used for diffusion and scrambling at the bit level. This paper demonstrated bit-level image encryption and illustrated its effectiveness.

Permutation-diffusion simultaneous operation (PDSO) was used by L. Huang *et al.* [29] to develop a color image encryption system. During the encryption process, the initial encrypted pixel's position in the cipher image was picked at random, and its value was decided by all the pixels in the original image as well as all the elements in three one-dimensional chaotic maps. The current encrypting pixel's value was then assigned to the preceding encrypted pixel. The method presented here is highly secure and efficient.

A color image encryption was proposed by X. Hu *et al.* [30] based on a cloud model Fibonacci chaotic system. The matrix convolution operation was used to permute the pixel points after scrambling image pixel points sliced by RGB components using hybrid chaotic sequences and then combining matrix convolution processes in convolutional neural networks. Finally, the XOR had been applied between the chaotic sequence and pixel values. This encryption method has been demonstrated to defend against a variety of assaults and thus provide enough security.

In this paper, a novel color image encryption was developed by T. S. Ali, and R. Ali [11] based on chaotic maps. The encrypted image was constructed in three stages. The first stage comprises permuting an original image with a chaotic map. In the second stage, the chaotic substitution box was used for pixel substitution, and in the third stage, a Boolean operator XOR was used to mix chaotic logistic-based random sequences. After several simulations, the algorithm is resistant to differential, statistical, and entropy attacks and takes less time to execute.

The benefits of structured random perception matrix and chaos were combined in this research to provide a structured sensing matrix measurement image. X. Wang, and Y. Su [31] presented a compression-based and 2D fractional Fourier image encryption method. This work compresses and encrypts using Chebyshev (CS), then re-encrypts using 2D FrFT (Fractional Fourier Transform). The CS chaotic sequence generates the inverse scrambling matrix, the chaotic cyclic matrix, the sampling subset, and the double random phase mask, implying that the chaotic system controls the encryption process. This technique ensures security because it has a large key space, close to optimum entropy, and a high encryption efficiency.

Z. Li *et al.* [32] presented a skew tent map and Rucklidge method for efficient and secure color image encryption. The suggested cryptosystem was divided into two components: bit-level permutation and diffusion. There are three elements to the bit-level permutation algorithm: a plain-image related rows and columns replacement, a pixel-level roll shift portion, and a bit-level cyclic shift part. Various experiments and tests have demonstrated that this algorithm is effective against a variety of attacks.

A novel color image encryption was proposed by X. Qian *et al.* [33] used of the 3D chaotic maps and some data reconstruction techniques. The 3D chaotic Logistic map was employed in the encryption diffusion process to modify the pixel value of the plain image. Meanwhile, the 3D chaotic Cat map was used to cope with the location of the image pixels during the confusion phase. Experiments revealed that the encryption method has a large key space, is more sensitive, and has a higher level of security.

A color image encryption technique based on the Fisher-Yates scrambling algorithm and chaos theory was suggested by K. Ma *et al.* [34]. To begin, the key was generated using the SHA-384 by merging the plaintext image and the encrypted. Then, three groups of chaotic sequences were created by iterating the 3D Chen chaotic system, and three groups of pseudo-random sequences were obtained by processing with the key. For image pixel location scrambling, the batch of pseudo-random sequences was merged using Fisher's technique. To get the final encrypted image, the last group formed the matrix after pixel replacement was employed for diffusion transformation. Because of the relationship between the original image and the keys, this cryptosystem has a high key and plaintext sensitivity, and it effectively resists chosen/known plaintext attacks or differential attacks. The algorithm has been subjected to numerous tests and has proven to be resistant to a wide range of attacks.

This paper was presented by G. Kaur *et al.* [35] to propose a strong color image encryption method based on a real fractional Hartley transform with chaotic transformation orders. To obtain an encrypted image, the multilayer scheme employs a PWLCM (piecewise linear chaotic map) based circular blending of color components, PWNCA (piecewise nonlinear chaotic map) based nonlinear processing in the spatial domain, and a multiple chaotic order fractional Hartley transform. The results of various tests and analyses have revealed that the suggested technique is extremely secure.

T. S. Ali and R. Ali [36] proposed a new method for the encryption of color images based on the S-box and chaotic system. During the encryption phase, the generated S-box by PWLCM substitutes image pixel values, causing confusion and diffusion in the image. For the generation of random chaotic sequences, the tent logistic system is used as a PRNG. Finally, for stable noise-like effects in the encrypted image, a self-mixing operation on the image components is used. The algorithm has been developed resistance to statistical, differential, and plain image attacks.

A color image encryption method based on a chaotic and bit-plane was proposed by J. Xu *et al.* [15]. First, three RGB image channels were extracted. A logistic chaotic sequence was then used to scramble the position of the transformed image. The Chen chaos sequence was then applied to the permuted image's gray pixel values. Finally, the encrypted image's gray value was converted to a decimal number to create a single-channel encrypted image, and the three-channel encrypted image was synthesized into an encrypted color image. Analyses and experiments have demonstrated that the suggested scheme is both secure and effective.

A modified image encryption process was proposed by S. Kanwal *et al.* [37] used chaotic maps and orthogonal matrix in Hill cipher. Image encryption involves three phases. In the first phase, a chaotic Hénon map was used for permuting the digital image. In the second phase, a Hill cipher was used whose encryption key was generated by an orthogonal matrix which further was produced from the equation of the plane. Finally, a sequence was generated by a chaotic tent map which was later XORed. Various experiments and tests have demonstrated that this algorithm is effective against a variety of attacks.

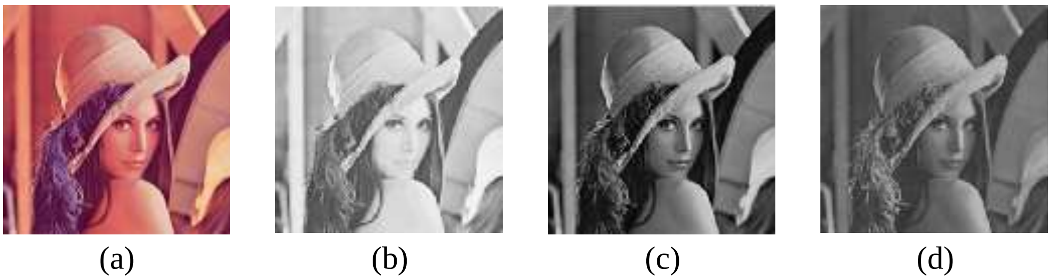

Fig. 2. Lena image including (a) Color plain image, (b) Red component, (c) Green component, and (d) Blue component.

Table 1. A comparison of the approaches for the Lena image.

Ref.	**Year**	**Key Space**	**Correlation Coefficients**			**Entropy (bit)**	**NPCR (%)**	**UACI (%)**
			H.	**V.**	**D.**			
[18]	2017	10^{117}	-0.0001	0.0089	0.0091	7.9912	1.0000	0.3347
[19]	2017	2^{252}	0.0027	-0.0033	0.0048	7.9997	0.9961	0.3347
[20]	2017	2^{213}	-0.0002	0.0008	0.0087	7.9988	0.9949	0.3339
[21]	2017	5×10^{102}	0.0005	-0.0070	0.0005	7.9972	0.9971	0.3345
[22]	2018	2^{390}	-0.0020	0.0008	-0.0029	7.9990	1.0000	0.3344
[23]	2018	4.5×10^{114}	-0.0029	-0.0017	0.0004	7.9971	0.9959	0.3345
[24]	2018	2^{128}	0.0006	-0.0005	-0.0001	7.9973	0.9991	0.3350
[25]	2018	2^{265}	-0.0470	-0.0475	0.0015	7.9992	0.9962	0.3346
[26]	2019	10^{189}	0.0015	-0.0200	-0.0070	7.9993	0.9962	0.3348
[27]	2019	2^{260}	0.0064	0.0045	0.0057	7.9992	0.9964	0.3349
[28]	2019	2^{335}	-0.0009	0.0008	0.0021	7.9993	0.9960	0.3347
[29]	2019	2^{170}	-0.0031	0.0010	-0.0008	7.9992	0.9960	0.3346
[30]	2020	2^{219}	0.0012	0.0034	0.0017	7.9941	0.9962	0.3361
[11]	2020	2^{299}	-0.0024	0.0052	-0.0003	7.9984	0.9960	0.3346
[31]	2020	10^{144}	-0.0000	-0.0032	0.0026	7.9959	0.9960	0.3345
[32]	2020	2^{261}	-0.0022	0.0009	0.0013	7.9992	0.9961	0.3345
[33]	2021	2^{600}	-0.0012	-0.0015	-0.0012	7.9996	0.9962	0.3352
[34]	2021	10^{126}	-0.0075	0.0004	0.0062	7.9970	0.9960	0.3345

[35]	2021	10^{247}	0.0019	0.0026	0.0025	7.9952	0.9963	0.3356
[36]	2022	10^{120}	0.0019	0.0035	0.0008	7.9959	0.9962	0.3346
[15]	2022	10^{150}	0.0040	-0.0012	0.0113	7.9993	0.9961	0.3347
[37]	2022	2^{240}	0.0004	-0.0028	-0.0048	7.9992	0.9961	0.3346

5. Comparative Analysis of the Schemes

Throughout all of these algorithms experiments, for verifying the encryption approach in relation to the current security analysis criteria, Lena was used. The plain image of Lena has a size of $M \times N$, with M and N being respectively the width and height of the image. Each pixel's value is made up of R, G, and B (red, green, and blue, respectively) color components. Thus, depending on the color planes, the color image can be translated into three gray images, with the size of the matrix for each color (R, G, or B) being $M \times N$. As it is illustrated in Fig. 2 , the color Lena image (Fig. 2 (a)) with a size of 256 × 256 is the color original image with red, green, and blue components shown in Fig. 2 (b) − (d), respectively. The value of each gray pixel ranges from 0 to 255. The most prevalent security measures were those designed to withstand statistical, exhaustive search, and differential attacks, as well as, to quantify image uncertainty [49]. The comparison of previous algorithms is shown in Table1.

6. Conclusion

In this paper, we have reviewed a number of contemporary methods of image encryption techniques involving chaos theory. The image encryption techniques covered in this paper perform well. However, there is scope for improvement in a few algorithms in terms of time complexity, speed, and computational cost, among other things. However, due to the increasing number of image decryption methods, proposing a completely secure method may be difficult. As a result, we can conclude that when suggesting a chaos-based encryption technique, one should keep cryptanalysis in mind so that the suggested algorithm does not leak. Moreover, recently proposed image encryption approaches enhance security by offering more than one chaotic system or by utilizing hyper-chaotic systems for encryption methods.

References

[1] L.A. Shihab, Int. Trans. J. Eng. Manag. Appl. Sci. Technol. **11**(9), 1 (2020).

[2] H.A. Younis, T.Y. Abdalla, A.Y. Abdalla, Iraqi Journal of Intelligent Computing and Informatics **1**, 56 (2007).

[3] N.R. Deepa, and N.M. Sivamangai, 2022 6th International Conference on Devices, Circuits and Systems (ICDCS), 190 (2022).

[4] K. Yadav, T. Chaware, 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 111 (2021).

[5] K. Suneja, S. Dua, M. Dua, 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), 693(2019).

[6] Y. Bu, 2021 2nd International Conference on Computing and Data Science (CDS) **100** (2021).

[7] J. Ayad, F.S. Hasan, A.H. Ali, Z.K. Hussein, H.J. Abdulkareem, M.A. Jalil, G. Ahmed, A. Sadiq, 2021 International Conference in Advances in Power, Signal, and Information Technology (APSIT), 1 (2021).

[8] H.M. Al-Mashhadi, I.Q. Abduljaleel, 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT) **93** (2017).

[9] Abdul-Basset A. Al-Hussein, Iraqi Journal for Electrical & Electronic Engineering **17**, 2 (2021).

[10] J. Shah, J. Dhobi, Int. J. Eng. Technol. Manag. Res **5**(1), 81 (2020).

[11] T.S. Ali, R. Ali, Multimedia Tools and Applications **79**(27), 19853 (2020).

[12] M. Jarjar, S. Hraoui, S. Najah, K. Zenkouar, Multimedia Tools and Applications **81**, 1 (2022).

[13] I. Yasser, F. Khalifa, M.A. Mohamed, A.S. Samrah, Complexity **2020**, (2020).

[14] G.K. Shraida, H.A. Younis, Iraqi Journal for Electrical and Electronic Engineering **18**(2), (2022).

[15] J. Xu, B. Zhao, Z. Wu, Entropy, **24**(2), 186 (2022).

[16] B.D. Parameshachari, 2021 National Computing Colleges Conference (NCCC) **1,** (2021).

[17] M. Khan, S.S. Jamal, M.M. Hazzazi, K.M. Ali, I. Hussain, M. Asif, Integration **81**, 108 (2021).

[18] J. Wu, X. Liao, B. Yang, in Signal Processing **141**, 109 (2017).

[19] M. Essaid, I. Akharraz, A. Saaidi, A. Mouhib, E. Mohamed, A. Ismail, S. Abderrahim, M. Ali, Advances in Science, Technology and Engineering System Journal **2**(5), 94 (2017).

[20] E.A. Albahrani, T.K. Alshekly, International Journal of Applied Information Systems **12**(4), 34 (2017).

[21] X. Wu, B. Zhu, Y. Hu, IEEE Access **5**, 6429 (2017).

[22] C. Zhu, K. Sun, IEEE Access **6**, 18759 (2018).

[23] X. Wang, X. Zhu, Y. Zhang, IEEE Access **6**, 23733 (2018).

[24] C. Zhu, G. Wang, K. Sun, Entropy **20**(11), 843 (2018).

[25] R.A. Aboughalia, O.A.S. Alkishriwo, Libyan International Conference on Electrical Engineering and Technologies (LICEET2018), (2018).

[26] A. Firdous, M.M. Saad Missen, Multimedia Tools and Applications **78** (17), 24809 (2019).

[27] G. Cheng, C. Wang, H. Chen, International Journal of Bifurcation and Chaos **29**(09), 1950115 (2019).

[28] L.L. Huang, S.M. Wang, J.H. Xiang, Applied Sciences **9**(22), 4854 (2019).

[29] L. Huang, S. Cai, X. Xiong, M. Xiao, Optics and Lasers in Engineering **115**, 7 (2019).

[30] X. Hu, L. Wei, W. Chen, Q. Chen, Y. Guo, IEEE Access **8**, 12452 (2020).

[31] X. Wang, Y. Su, Scientific Reports **10**(1), 1 (2020).

[32] Z. Li, C. Peng, W. Tan, L. Li, Symmetry **12**(9), 1497 (2020).

[33] X. Qian, Q. Yang, Q. Li, Q. Liu, Y. Wu, W. Wang, IEEE Access **9**, 61334 (2021).

[34] K. Ma, L. Teng, X. Wang, J. Meng, Multimedia Tools and Applications **80**(16), 24737 (2021).

[35] G. Kaur, R. Agarwal, P. Vinod, Journal of King Saud University-Computer and Information Sciences **34**(8), 5883 (2021).

[36] T.S. Ali, R. Ali, Multimedia Tools and Applications **81**, 20585 (2022).

[37] S. Kanwal, S.S. Inam, M.T.B. Othman, A. Waqar, M. Ibrahim, F. Nawaz, Z. Nawaz, H. Hamam, Sensors **22**(12), 4359 (2022).

Journal of Basrah Researches (Sciences) **48**(2), 77 (2022)
DOI: https://doi.org/10.56714/bjrs.48.2.8

مراجعة: خوارزميات تشفير الصور الملونة القائمة على الفوضى

غفران خالد شريدة * ، حميد عبد الكريم يونس

قسم علوم الحاسوب، كلية علوم الحاسوب وتكنولوجيا المعلومات، جامعة البصرة، البصرة، العراق.

معلومات البحث

الاستلام	23 تموز 2022
القبول	19 أب 2022
النشر	30 كانون الاول 2022

الكلمات المفتاحية

خريطة عشوائية، صورة ملونة
فك التشفير، تشفير، تشفير الصور

Citation: G.K. Shraida, H.H. Younis, J. Basrah Res. (Sci.) **48**(2), 77 (2022). DOI:https://doi.org/10.56714/bjrs.48.2.8

الملخص

أصبحت حماية معلومات الوسائط المتعددة ضرورية للغاية بسبب التقدم الكبير في شبكات الاتصال، وخاصة شبكة الإنترنت، التي يستخدمها العديد من الأفراد لنقل أنواع مختلفة من البيانات. يمكن تنفيذ سلامة معلومات الوسائط المتعددة هذه باستخدام طرق التشفير وفك التشفير. هناك الكثير من الاستراتيجيات الخاصة التي يجب استخدامها لحماية الصورة الشخصية من الوصول غير المصرح به، وتعد أنظمة التشفير الفوضوية واحدة من هذه التقنيات التي أصبحت شائعة مؤخرًا. تم اقتراح العديد من الطرق لتشفير الصور باستخدام الخرائط الفوضوية بسبب مزاياه المختلفة، مثل سهولة التنفيذ وسرعة تشفير أفضل ومقاومة الهجمات. تم اقتراح العديد من تقنيات تشفير الصور القائمة على الخرائط الفوضوية نظرًا لحساسيتها الكبيرة لظروف البداية وعدم القدرة على التنبؤ والسلوك العشوائي. تستعرض هذه الورقة العديد من خوارزميات تشفير الصور بناءً على نظرية الفوضى التي توفر أمانًا جيدًا.

[*] **Corresponding author email : itpg.ghofran.khaled@uobasrah.edu.iq**

ISSN: 1817-2695 (Print); 2411-524X (Online)
Online at: https://bjrs.uobasrah.edu.iq