IRAQI Academic Scientific Journals

Samarra Journal of Pure and Applied Science

SJPAS

www.sjpas.com

ISSN:2663-7405

Chaotic Image Cryptography Systems: A Review

Amal H. Khaleel[1*], Iman Q. Abduljaleel[2]

1- Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Iraq (amal_albahrany@yahoo.com)
2- Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Iraq

Article Information

Received: 04/02/2021
Accepted: 24/03/2021

Keywords:

Image, Cryptography, Chaotic Map, *Encryption, and Scrambling.*

Abstract

In recent decades, image encryption has been a popular and important field of research. The image encryption techniques have been studied thoroughly to ensure the safety of digital images on transmission through the networks. A large range of algorithms for chaotic-based cryptographic systems has been suggested and submitted to enhance the efficiency of the encryption methods. The chaotic map is one technique to guarantee security. The benefits of chaotic image encryption include the fact that it is simple to implement; it has a faster encryption speed, and it is powerful against attacks. Due to their extreme sensitivity to initial conditions, unpredictability, and random-like behaviours, many image encryption systems using chaotic maps have been proposed. This study paper presents a scientific review of many types of researches over a decade (2010-2020) that has been used chaotic with its various types (one-dimensional, multi-dimensional, or hyper-chaotic) to process the digital images in the encryption stage or the scrambling phase. Furthermore, it presents a future reading of researches that has a wider role in developing the cryptography field by improving the efficiency of Algorithms where using a chaotic map with other methods gives better results than using chaotic alone in scrambling and encryption methods.

Introduction:

Image data security has become a major problem as a result of the enormous, rapid growth of information interchange through internet transmission [1]. Different encryption techniques have been developed and applied in recent years to protect confidential images from unauthorized users [2].

Cryptography is the art and science of data protection from undesirable people by converting it, while stored and transmitted, into a form not recognizable by its attackers [3]. Cryptographic algorithms are designed around assumptions of computational hardness, making it difficult for any opponent to break these algorithms in practice. Therefore, cryptography plays an important role in the safety of digital content [4]. Current encryption techniques are not suited to the encryption of image data due to the size and redundancy of the images and therefore cannot guarantee the confidentiality and security of the data [5].

Several methods for encrypting image data have been proposed over the last couple of decades, where chaotic-based cryptography is the most powerful and common due to its random and unpredictable nature [6].

In this article, the overview of the chaotic maps are presented in section 1, and the use of chaotic image encryption are presented in section 2. In section 3, a focus on various chaotic imaging techniques and related work for each of the methodologies studied. The pros and cons of each strategy are summarized in section 4. Finally, the conclusion display the main purpose of paper is to assist in the future development of new chaotic image encryption techniques by studying the behaviour of several existing chaotic image encryption algorithms.

1- Overview of Chaotic Map Theory

One-dimensional (1D) chaotic maps and multi-dimensional (MD) chaotic maps are used for chaotic-based image encryption. Due to its complex structure and the presence of several parameters, the use of (MD) chaotic maps improves the security of the image encryption, leading to increased difficulty in implementing the algorithm [7].

In the late 1980s, Matthews first used chaotic to encrypt information, while Habutsu et al. proposed the first chaotic block cipher algorithm in 1991. Baptista published an algorithm for chaotic encryption in 1998. Besides that, Friedrich suggested that it is necessary to repeat the image encryption system in two steps: diffusion and permutation to obtain a good level of security [8]. The stage of permutation is necessary to reduce the high correlation for both adjacent pixels. The permutation methods can be categorized into two main levels: pixel and bit level. To acquire an oscillatory behaviour and avoid the attack, the diffusion phase is responsible for changing pixel values. [9].

Two issues drive almost all suggestions for chaotic-based image encryption: (i) the possible reduction of computational effort compared to traditional encryption; and (ii) alleged security concerns when traditional ciphers are applied to images [10].

2- Chaotic Map Domain In Image Encryption

The image encryption method is one of the most common and useful methods for image data security. In the mid-1990s, most of the algorithms specifically intended to encrypt digital images were proposed. There are two main groups of algorithms for image encryption: (a) selective non-chaotic methods and (b) non-selective chaotic-based methods [11].

Presently, numerous methods are proposed for image encryption to reduce the redundancy of image content using chaotic-based ciphers. The chaotic system has several features, including high initial conditions sensitivity, determination, ergodicity, and complex pseudo-random sequences that are difficult to analyse [12]. Fig. 1 shows the relationship of chaotic map theory with cryptography.

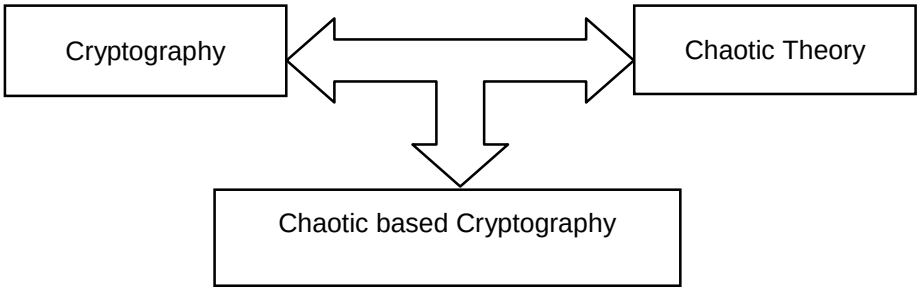

Fig. 1 *Chaotic based cryptography*

3- Different Chaotic-Based Encryption Techniques: Overview

Several methods of data cryptography have employed chaotic maps, so they are widely used and easily understood. In this section, the research work of some prominent authors in the same field is presented and the various chaotic-based techniques used to encrypt images are briefly described as shown in Fig. 2.

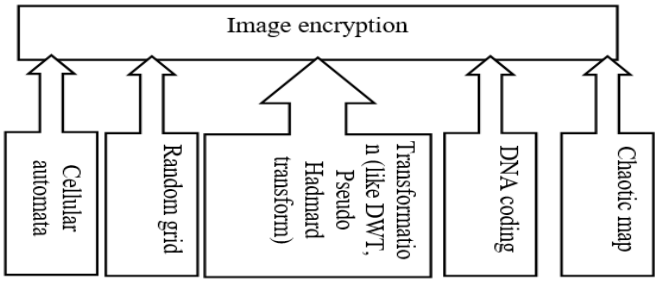

Fig. 2 *Most techniques using in the image encryption*.

3.1. Chaotic Image Cryptography Systems, 2010-2013

The chaotic map concept was the beginning of its use at the primitive of the year 2010, and most of the researches ideas during the 2010-2013 period are old ideas. In [13], presented an algorithm for encrypting images based on two types of chaotic, Arnold and Logistic maps, where logistic map is used to scramble the original image blocks, while Arnold cat map uses it to encrypt the resulting image after scrambling. In [14], an algorithm was proposed to encrypt colour images based on the (confusion-diffusion) architecture. Where the confusion is based on a chaotic 2D Standard Map, while the diffusion is based on 1D Logistic Map in two horizontal and vertical stages to ensure that the original image values are mixed. A combination of three types of one-dimensional chaotic maps were introduced in [15]. The random key sequence created by the chaotic map is selected depending on the logistic map to choose the type of chaotic use for it (Sine or Tent maps). In [16], an algorithm was introduced to scramble image values based on Arnold Cat Map and produce Pseudo-random number sequence based on Henon Map. This algorithm is suitable for various types of images and can be used to encrypt and securely transmit images over the Internet, as XOR operates between the key value and the values of the scrambled image.

3.2. Chaotic Image Cryptography Systems, 2014

A new approach to image encryption is proposed in [17] based on a 2-D Zaslavskii map and Pseudo Hadmard transformation. It contains two stages to the encryption process, i.e. permutation and diffusion. Scrambling rows and columns using chaotic values achieve permutation. The method is proposed to offer high security and high speed. In [18], a new technique is used to generate a secondary key that enhances the protection of the encrypted images. The different keys were used in the diffusion phase to be diffused in every round. Image pixel bits are hidden with randomly generated binary sequences in the diffusion phase. The combination of three chaotic maps is based on this encryption algorithm. A chaotic image encryption algorithm using the 3D Rossler system was suggested in [19]. Three significant steps were involved in the encryption process: first, the chaotic sequence generation using the Rossler system; next, the replacement of pixels and pixel shuffling is based on the chaotic sequences generated. The encryption algorithm presented can take any one-time password of 16 characters, and it is very safe.

3.3. Chaotic Image Cryptography Systems, 2015

In [20], a new image encryption method was proposed consisting of both phases of permutation and diffusion using the chaotic map with the cellular automata of Conway's game, and the equation of the Chebyshev map with Lorenz sequentially. [21] suggested a quick, and efficient cryptosystem-based chaotic structure. The encryption algorithm uses a diffusion layer followed by a bit-permutation layer to change the position of the image pixels. The new encryption algorithm includes an extensive and uniform chaotic pseudo-random generator for changing control value parameters.

3.4. Chaotic Image Cryptography Systems, 2016

The new scheme for image encryption is presented in [22]. To select a fractal key for encoding, the researchers used chaotic mappings. The Hennon map was also used to select pixels from the fractal key. The use of the fractal key leads to higher key space and greater safety and resistance. An image encryption algorithm on the basics of the formal DNA computing-splicing proposed system and the hyper-chaotic scheme is presented in [23]. Quaternary coding in the suggested technique is used to divide the image into four segmentations. This novel approach can be used to drastically alter the information of the plain image.

3.4. Chaotic Image Cryptography Systems, 2017

A special, lightweight encryption system for a protected transmission model was proposed in [24]. In this system, it used a pseudo-random number (PRN) sequence and Deoxyribose Nucleic Acid (DNA) computation. Furthermore, a Pseudo-Random Number Generator premised on a chaotic, cross-coupled chaotic map was used to generate two PRN sequences using two keys to increase security. A new hybrid encryption image approach is proposed in [25]. The proposed system uses a new scrambled triangular method by dividing the image into six interest matrices and then using the DNA sequence to improve the scrambled and encryption method. A new symmetrical image encryption system (SIES), suggested in [26], focuses on a recent class of quadratic chaotic maps. In the suggested scheme, the image is converted to a serial bit stream, which, with modulo-2 added to the binary chaotic sequence stream, was generated using a new quadratic chaotic map class. A new chaotic map based on

the Concave Chaotic Map, which performs two operations, was suggested in [27]; the first operation shifts the image pixel location while the second operation changes image pixel intensity value. Based on the Concave Chaotic Map, the proposed algorithm is created and used to encrypt images of grayscale and plain text.

3.5. Chaotic Image Cryptography Systems, 2018

The authors in [28] presented the new method of RGB image encryption using multi-chaotic maps. In the proposed system, the colour image component is reshaped by the hyper-chaotic map of Chen and converted into a binary form. The key was generated by using the Sine Chaotic Map and the 1D Logistic Chaotic Map. In [29], a new image encryption system has been suggested using pixel-level, bit-level scrambling, and DNA encryption. The proposed method used the 5-D hyper-chaotic system's original conditions to generate chaotic sequences. The authors in [30] present a new image encryption algorithm related to DNA coding and the 2D chaotic logistic map. The suggested encryption system consists of three steps (DNA coding, permutation, and diffusion). An improved encryption scheme has been suggested in [31] utilizing RT-enhanced chaotic tent maps. The SHA-3 hash value parameter of the plaintext image is shown as a private key parameter in the enhanced algorithm.

3.6. Chaotic Image Cryptography Systems, 2019

A novel colour imaging system that relies on the hyper-chaotic map and the permutation-diffusion architecture was suggested in [32]. The encryption scheme used a block permutation made by mixing the components R, G, B, and the key streams produced by the hyper-chaotic method. In [33], a current plaintext-related and high-speed chaotic image encryption model based on series is proposed, which includes two cycles of encryption operations. Block parity checking is held out during the first cycle of encryption, while repetitive coding is done in the second cycle. The authors in [34] proposed an efficient cryptosystem that integrates scattering-confusion systems and memory cellular automata image encryption. A new technique for image encryption is proposed in [35], which combines the pseudo-randomness of the hyper-chaotic method with the sensitivity of the initial values. A colour image encryption based on adaptive DNA and 4-D memristive hyper-chaotic is proposed in [36]. In [37], the 2D Logistic-Sine-Cosine map is presented, which is based on the classic 2D Logistic, Sine, and Cosine maps.

3.7. Chaotic Image Cryptography Systems, 2020

In [38], a new image encryption scheme was proposed that focuses on two-dimensional Lorenz and Logistic. In the encryption system, the classic chaotic method is used to produce two pairs of chaotic sequence data to encode the image. A new method of image encryption was suggested in [39], which focuses on a discrete chaotic map and S-Box using the Logistic-Sine system. A secure and rapidly chaotic image encryption algorithm is suggested in [40], with concurrent permutation-diffusion operation. This algorithm combines the procedures of permutation and diffusion. In [41], a new encrypted image method based on a chaotic system was described. The proposed method used the Schur decomposition method to obtain N orthogonal matrices and certain basic dynamic characteristics of the chaotic system. The authors in [42] present a novel image cryptographic algorithm integrating the (5-D) hyper-chaotic map with the DNA method. This system was designed for four sections: pixel-level diffusion, pixel-level permutation, DNA level diffusion, and the second permutation. An image

encryption technique depending on the framework of the hash table scrambling and DNA replacement is suggested in [43]. The algorithm uses the classic process of 'scrambling-diffusion', and the hyper-chaotic Chen. The system generates the pseudo-random series used for each phase. A new technique that conceals text inside an audio signal is presented in [44]. By scrambling using the Chaotic Map, then encrypting using the Zaslavsky map, and concealing by using K-means with the LSB technique.

4- Analysis of Chaotic Cryptography

In this section, the results of the research tests are reviewed to evaluate different practical experiments using the chaotic map. Moreover, we analyse the pros and cons of each technique. The researches [8], [19], [22], [26], [27], [28], [38], [40] and [45] use the standard chaotic map in their algorithms. These algorithms were characterized by their simplicity of work and speed of implementation, but the disadvantage is the ability to break the keys because they rely on the chaotic key only [32]. In this research, work was developed using hyper-chaotic. However, relying on the hypermarket alone is not sufficient to prevent all attacks if we compare it to other research that used additional methods. The only benefit of this method is that the execution time becomes less.

In recent years, the use of chaotic map with other techniques has been adopted as shown in Fig. 3. It has been observed that if combined with other technologies, chaotic map indicates better results.

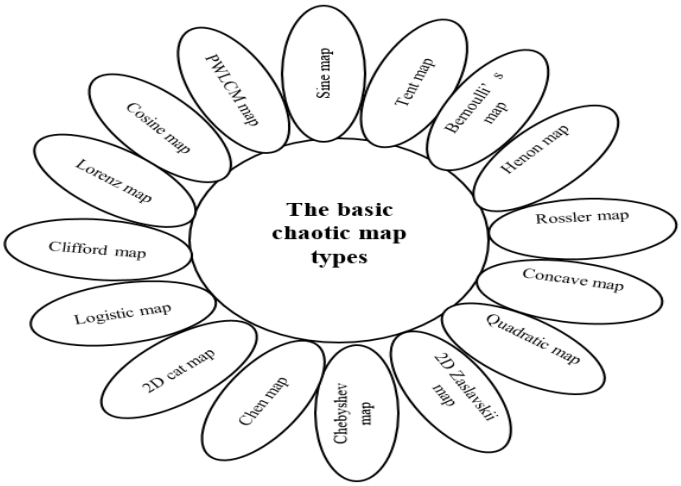

Fig. 3 *The basic chaotic map types*

Examples of these techniques are:

a. **DNA and Chaotic Map:** We note that these studies [22], [23], [25], [29], [30], [42], [43], and [46] merged the chaotic map and DNA. The combination measures were relatively better due to its dependence on the randomness of chaotic sequences and on the scrambling of values using DNA codes, which provided a suitable behaviour to isolate the values and change them in a simple way to strengthen its randomness.

b. **Dynamic DNA and Chaotic Map:** We note that the UACI values were small compared to the ideal value of 33 in these research studies [36] and [47]. It was either 28 or 30 in the two studies, although the rest of the parameters were close to the ideal values for the

measurements. Here, we conclude that it is better to use hyper-chaotic with DNA dynamic than traditional chaotic.

c. **Cellular Automata with Chaotic Map:** The use of CA provides randomness to generate an array of values to be used with chaotic keys. This improves the values of the various measures. Through the studies [20] and [36], we conclude here that the current trend is to use hyper chaotic with CA or double, triple or quadruple-directional chaotic to achieve the best results.

d. **Combining Chaotic Map with Transformations:** The advantage of these researches [17], [37], and [48] are that the values of the correlation, entropy, UACI, and PNCR parameters were good. The implementation time was largely due to the frequent need to analyse values using these transformations. Transformations save large key space to ensure keys are hard to break. Here we conclude that the DWT conversion can be used with hyper-chaotic to obtain high values.

e. **S-box with Chaotic Map:** Papers [39] and [49] have the advantage of using regular chaotic together with s-boxes that require space and time to store. We note that the correlation values were not good because they did not support the correlation between the original and the encoded image, and the key space values were relatively small compared to other studies. Here we conclude that this merger does not produce good results.

f. **Combining Chaotic Map with Hash Function:** This combination has the advantage of the difficulty of breaking the key due to its dependence on the hash function, whether it is SHA-3 or SHA-256. Here we conclude that this merging is internally used instead of being treated as two independent algorithms. This merging showed good results, as we note in these papers [31], [34], [35], and [38].

The stages in the development of the use of chaotic in encoding images during the previous years are shown in Table 1, in addition to the most important technologies that have been used and are still in use. While previous studies using chaotic maps in various encryption algorithms were compared using several measurements in Table 2.

Table 1. The summary of the important characteristics of the researches that use of chaotic in encryption images.

Years	Paper	The important characteristics of the papers
2010-2013	[13],[14],[15], [16]	During this period, papers focused on the variety of chaotic maps. The cause for this was the search for methods to generating random numbers which difficult to predict by adding the complexity resulting from mixing all these types.

2014	[17],[18],[19]	Interest in applying the basic types of chaotic map in its various forms, 1D, 2D or 3D. Furthermore, it work on making Hyper chaotic from the well-known types in a simple way.
2015	[20],[21]	The use of basic types of chaotic with the introduction of mathematical theories such as automata theory
2016	[22],[23]	The use of DNA coding technology, which constitutes a successful start and it continues to this day.
2017	[24],[25],[26],[27]	Experimenting with new chaotic types and starting to be interested in the scrambling phase.
2018	[28],[29],[30],[31]	The beginning of the interest in generating chaotic from the fourth dimension upwards, as well as making chaotic keys of the hyper chaotic type, in addition to the introduction of the HASH function technology in the generation of keys.
2019	[32],[33],[34],[35],[36],[37]	Development of work chaotic with dynamic DNA coding.
2020	[38],[39],[40],[41],[42],[43],[44]	Continuing work on creating new or hybrid chaotic keys and combining them with previously known or new technologies, and a great interest in generating the keys with the hash function technology.

Table 2. Comparing different chaotic map methods using the results of the encryption algorithms in review papers

Paper	Cipher-text Image entropy	Image name	NPCR %	UACI %	Key Space	Correlation of Encryption Image		
						H	V	D
[8]	7.9992	Lina	99.63	33.57	-	-0.0093	-0.0009	-0.0003
[9]	7.9969	Lina	99.61	33.45	10^{42}	-0.0008	-0.0025	0.0011
[17]	7.9976	Lina	99.6	33.4	2^{320}	-0.0027	-0.0111	0.0013
[18]	7.9998	Lina	99.61	33.36	2^{240}	-0.0094	-0.0003	0.0039
[19]	7.9970	Lina	99.60	28.45	-	0.0403	-0.0085	0.0052
[20]	7.9972	Lina	99.61	33.45	2^{498}	-0.0019	-0.0002	-0.0001
[21]	-	Lina	99.60	33.46	-	0.0013	0.0012	0.0012
[22]	7.9966	Lina	-	-	2^{128}	0.0066	-0.0103	0.0014
[23]	7.9971	Lina	99.57	33.51	2^{128}	0.0015	0.0018	0.0018
[24]	7.9992	Lina	2^{133}	39.12	2^{133}		0.0012	
[25]	7.9408	Lina	99.63	30.51	-	0.0012	-0.0056	0.0028
[26]	7.9993	Camer aman	2^{106}	-	2^{106}		0.0046	
[27]	7.988	Camer	-	-	2^{169}	0.0346	0.0269	0.0311

		aman						
[28]	7.9993	Lina	99.62	33.50	2^{276}	0.0004	0.0002	-0.0005
[29]	7.9967	Lina	99.61	33.46	2^{298}	0.0068	−0.0054	0.0010
[30]	7.9972	Lina	-	-	-	0.0015	-0.0037	0.0079
[31]	7.9990	Lina	100	33.44	$(5\times10^{102})\times 10^{15}$	-0.0014	0.0006	-0.0010
[32]	7.999	Lina	99.64	33.50	2^{260}	0.0064	0.0045	0.0057
[33]	-	Elain	99.60	33.51	2^{324}	-0.0014	-0.0007	0.0013
[34]	7.9992	Camer aman	99.61	33.46	2^{373}	-0.0033	0.0005	-0.0007
[35]	7.9979	Lina	99.56	33.44	$10^{40}\times2^{128}$	0.0015	-0.0014	-0.0028
[36]	7.9993	Lina	99.61	30.41	10^{112}	0.0011	-0.0013	-0.0019
[37]	7.9950	Camer aman	99.45	33.11	4.295×10^{71}	-0.0005	-0.0002	0.0013
[38]	7.9894	Lina	99.66	33.42	10^{112}	0.0044	0.0015	0.0019
[39]	7.9971	Lina	99.61	33.46	2^{124}	-0.0056	0.0006	0.0018
[40]	7.9972	Lina	99.62	33.50	2^{351}	0.0106	-0.0012	0.0009
[41]	7.9975	Lina	99.61	33.61	10^{135}	-0.0327	-0.0414	-0.0037
[42]	7.9976	Lina	99.63	33.45	2^{584}	0.0040	0.0033	0.0021
[43]	7.9171	Lina	99.65	33.46	10^{70}	0.0015	0.0021	-0.0005
[45]	-	Lina	99.60	33.47	$2\times10^{5}\times2^{6}$	-	-	-
[46]	7.9974	Lina	99.65	33.36	10^{154}	0.0013	-0.0009	0.0012
[47]	7.989	Lina	99.62	28.73	2^{512}	0.0039	-0.0314	0.0158
[48]	7.9972	Lina	99.71	33.45	$5\times(10^{2})^{6}\times(10^{15})^{6}$	-0.0002	0.00003	-0.00006
[49]	7.888	Lina	99.61	33.47	-	0.0674	0.0561	0.0286

Conclusion:

Chaotic image encryption is one of the most efficient methods of encrypting an image. In this study, various chaotic methods of image encryption are reviewed, discussed and evaluated.

This paper is based on providing an integrated study of the uses of the chaotic map in the field of encrypting over the past ten years in an integrated manner with other techniques that we have mentioned in our research according to the years and the techniques supporting chaotic map. We presented this study so that any researcher can develop this field by choosing the appropriate techniques used with the chaotic map. Thus we provided any academic researcher with a summary of the various researches that used chaotic map

Through our analysis of the studies that used chaotic technique, we noted the ongoing effort of the researchers to apply it to the encryption methods used due to its advantages of ease of generation and difficulty of penetration compared to traditional methods of encryption such as the AES algorithm.

In recent years, researchers have moved towards the production of hybrid algorithms through a collaboration between chaotic method and other methods that increase their

randomness, such as (S-box or DNA). In addition, we noted the use of data mining algorithms and statistical methods to create new types of chaotic. Through modern studies, we have also found the possibility of using chaotic in the scrambling phases and its role in improving encryption algorithms, and this leads to the inference that the rate of generation of chaotic will play a major role in the scrambling of values before used in the traditional encryption algorithms. The scrambling phases are characterized by provides excellent randomness that has the ability to scramble image values and show them in a way that is difficult for hackers to retrieve in addition to the speed it provides compared to other encryption algorithms.

The future proposal is to implement bioinformatics inputs, such as fingerprints or voice prints, to decide the chaotic parameters used, and make dynamically variable while a person uses the proposed algorithm to ensure that it is difficult to crack.

References:

1. Kabir, F., Kaur, J., Cse, M. T., Goyal, A. P., & Pradesh, H. (2017). Color Image Encryption for Secure Transfer over Internet : A survey. 860–863.

2. Rupa Rajoriya, Kailash Patidar, S. C. (2018). A survey and analysis on color image encryption algorithms. ACCENTS Transactions on Information Security, 3(9)(2455–7196), 1–5.

3. Solak, E., Rhouma, R., & Belghith, S. (2010). Cryptanalysis of a multi-chaotic systems based image cryptosystem. Optics Communications, 283(2), 232–236. https://doi.org/10.1016/j.optcom.2009.09.070

4. Sathishkumar, G. ., Bhoopathy bagan, K., & Sriraam, N. (2011). Image Encryption Based On Diffusion And Multiple Chaotic Maps. International Journal of Network Security & Its Applications, 3(2), 181–194. https://doi.org/10.5121/ijnsa.2011.3214

5. ALIREZA JOLFAEI, A. M. (2010). An image encryption approach using chaos and stream cipher. Journal of Theoretical and Applied Information Technology, 117–125.

6. Fadhel Hamood, S., Mohd Rahim, M. S., & Farook Mohammado, O. (2017). Chaos image encryption methods: A survey study. Bulletin of Electrical Engineering and Informatics, 6(1), 99–104. https://doi.org/10.11591/eei.v6i1.599

7. Arroyo, D., Diaz, J., & Rodriguez, F. B. (2012). Cryptanalysis of a one round chaos-based Substitution Permutation Network. Elsevier

8. Fathi-Vajargah, B. (2018). Image Encryption Based on Permutation and Substitution Using Clifford Chaotic System and Logistic Map. Journal of Computers, 13(3), 309–326. https://doi.org/10.17706/jcp.13.3.309-326

9. Ping, P., Fan, J., Mao, Y., Xu, F., & Gao, J. (2018). A chaos based image encryption scheme using digit-level permutation and block diffusion. IEEE Access, 6, 67581–67593. https://doi.org/10.1109/ACCESS.2018.2879565

10. Preishuber, M., Hutter, T., Katzenbeisser, S., & Uhl, A. (2018). Depreciating motivation

and empirical security analysis of chaos-based image and video encryption. IEEE Transactions on Information Forensics and Security, 13(9), 2137–2150.

11. Kumar, N., Wadhwa, D., Tomer, D., & Vijayalakshmi, S. (2014). Review on Different Chaotic Based Image Encryption Techniques. International Journal of Information and Computation Technology, 4(2), 197–206. http://www.irphouse.com/ijict.htm

12. Zhang, Q., Xue, X., & Wei, X. (2012). A novel image encryption algorithm based on DNA subsequence operation. The Scientific World Journal, 2012. https://doi.org/10.1100/2012/286741

13. Huang, M. Y., Huang, Y. M., & Wang, M. S. (2010). Image encryption algorithm based on chaotic maps. ICS 2010 - International Computer Symposium, 154–158. https://doi.org/10.1109/COMPSYM.2010.5685529

14. Mazloom, S., & Eftekhari-Moghadam, A. M. (2011). Color image cryptosystem using chaotic maps. IEEE SSCI 2011 - Symposium Series on Computational Intelligence - CIMSIVP 2011: 2011 IEEE Symposium on Computational Intelligence for Multimedia, Signal and Vision Processing, 142–147. https://doi.org/10.1109/CIMSIVP.2011.5949254

15. Long Baoa, Yicong Zhoub, C. L. Philip Chenb, H. L. (2012). A New Chaotic System for Image Encryption. 2012 International Conference on System Science and Engineering, 978-1–4673, 69–73.

16. Prusty, A. K., Pattanaik, A., & Mishra, S. (2013). An image encryption & decryption approach based on pixel shuffling using Arnold Cat Map & Henon Map. ICACCS 2013 - Proceedings of the 2013 International Conference on Advanced Computing and Communication Systems: Bringing to the Table, Futuristic Technologies from Around the Globe, 1–6.

17. Hanchinamani, G., & Kulakarni, L. (2014). Image Encryption Based on 2-D Zaslavskii Chaotic Map and Pseudo Hadmard Transform. International Journal of Hybrid Information Technology, 7(4), 185–200. https://doi.org/10.14257/ijhit.2014.7.4.16

18. R, R. Kumar & M, B.Kumar (2014). a New Chaotic Image Encryption Using Parametric Switching Based Permutation and Diffusion. ICTACT Journal on Image and Video Processing, 4(4), 795–804. https://doi.org/10.21917/ijivp.2014.0114

19. Mrinal K. Mandal, Madhumita Kar, S. K. S. and V. K. B. (2014). symmetric key image encryption using chaotic Rossler system. Security And Communication Networks, DOI: 10.1002/sec.927, 2145–2152.

20. Murugan, B., Nanjappa Gounder, A. G., & Manohar, S. (2016). A hybrid image encryption algorithm using chaos and Conway's game-of-life cellular automata. Security and Communication Networks, 9(7), 634–651. https://doi.org/10.1002/sec.1386

21. El Assad, S., & Farajallah, M. (2016). A new chaos-based image encryption system. Signal Processing: Image Communication, 41(March), 144–157. https://doi.org/10.1016/j.image.2015.10.004

22. Kashanian, H., Davoudi, M., & Hamed, K. (2016). Image Encryption using chaos functions and fractal key. IJCSNS International Journal of Computer Science and Network Security, 16(10), 87–92.

23. Niu, H., Zhou, C., Wang, B., Zheng, X., & Zhou, S. (2016). Splicing model and hyper-chaotic system for image encryption. Journal of Electrical Engineering, 67(2), 78–86. https://doi.org/10.1515/jee-2016-0012

24. Al-Mashhadi, H. M., & Abduljaleel, I. Q. (2017). Color image encryption using chaotic maps, triangular scrambling, with DNA sequences. International Conference on Current Research in Computer Science and Information Technology, ICCIT 2017, 93–98. https://doi.org/10.1109/CRCSIT.2017.7965540

25. Mondal, B., & Mandal, T. (2017). A light weight secure image encryption scheme based on chaos & DNA computing. Journal of King Saud University - Computer and Information Sciences, 29(4), 499–504. https://doi.org/10.1016/j.jksuci.2016.02.003

26. Falih, S. M. (2017). A Simple Chaotic Image Cryptography Algorithm Based on New Quadratic Chaotic Map. Journal of Babylon University/Engineering Sciences 4(25), 1221–1229.

27. Abu-amara, F., & Amro, A. M. S. (2017). Concave Chaotic-Based Image Encryption. International Journal of Electronics Communication and Computer Engineering 8(1), 13–17.

28. Taqi, I. A., & Hameed, S. M. (2018). A new Color image Encryption based on multi Chaotic Maps. Iraqi Journal of Science, 59(4B), 2117–2127. https://doi.org/10.24996/ijs.2018.59.4b.17

29. Sun, S. (2018). A Novel Hyperchaotic Image Encryption Scheme Based on DNA Encoding, Pixel-Level Scrambling and Bit-Level Scrambling. IEEE Photonics Journal, 10(2), 1–14. https://doi.org/10.1109/JPHOT.2018.2817550

30. Fayza Elamrawy, Maha Sharkas, Abdel Monem Nasser (2018). An image encryption based on DNA coding and 2DLogistic chaotic map. International Journal of Signal Processing, 3(2367–8984), 27–32.

31. Zhu, C., & Sun, K. (2018). Cryptanalyzing and Improving a Novel Color Image Encryption Algorithm Using RT-Enhanced Chaotic Tent Maps. IEEE Access, 6, 18759–18770. https://doi.org/10.1109/ACCESS.2018.2817600

32. Cheng, G., Wang, C., & Chen, H. (2019). A Novel Color Image Encryption Algorithm Based on Hyperchaotic System and Permutation-Diffusion Architecture. International Journal of Bifurcation and Chaos, 29(9).

33. Ma, S., Zhang, Y., Yang, Z., Hu, J., & Lei, X. (2019). A New Plaintext-Related Image Encryption Scheme Based on Chaotic Sequence. IEEE Access, 7, 30344–30360. https://doi.org/10.1109/ACCESS.2019.2901302

34. Li, A., Belazi, A., Kharbech, S., Talha, M., & Xiang, W. (2019). Fourth Order MCA and Chaos-Based Image Encryption Scheme. IEEE Access, 7, 66395–66409.

https://doi.org/10.1109/ACCESS.2019.2911559

35. Zhang, X., Wang, L., Zhou, Z., & Niu, Y. (2019). A Chaos-Based Image Encryption Technique Utilizing Hilbert Curves and H-Fractals. IEEE Access, 7, 74734–74746. https://doi.org/10.1109/ACCESS.2019.2921309

36. Liu, Z., Wu, C., Wang, J., & Hu, Y. (2019). A Color Image Encryption Using Dynamic DNA and 4-D Memristive Hyper-Chaos. IEEE Access, 7, 78367–78378. https://doi.org/10.1109/ACCESS.2019.2922376

37. Huang, H. (2019). Novel Scheme for Image Encryption Combining 2D Logistic-Sine-Cosine Map and Double Random-Phase Encoding. IEEE Access, 7, 177988–177996. https://doi.org/10.1109/ACCESS.2019.2958319

38. Li, T., Du, B., & Liang, X. (2020). Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz. IEEE Access, 8, 13792–13805. https://doi.org/10.1109/ACCESS.2020.2966264

39. Lu, Q., Zhu, C., & Deng, X. (2020). An Efficient Image Encryption Scheme Based on the LSS Chaotic Map and Single S-Box. IEEE Access, 8, 25664–25678. https://doi.org/10.1109/ACCESS.2020.2970806

40. Liu, L., Lei, Y., & Wang, D. (2020). A Fast Chaotic Image Encryption Scheme with Simultaneous Permutation-Diffusion Operation. IEEE Access, 8, 27361–27374. https://doi.org/10.1109/ACCESS.2020.2971759

41. Wang, T., Song, L., Wang, M., & Zhuang, Z. (2020). A novel image encryption algorithm based on parameter-control scroll chaotic attractors. IEEE Access, 8, 36281–36292. https://doi.org/10.1109/ACCESS.2020.2975376

42. Liu, L., Wang, D., & Lei, Y. (2020). An Image Encryption Scheme Based on Hyper Chaotic System and DNA with Fixed Secret Keys. IEEE Access, 8, 46400–46416. https://doi.org/10.1109/ACCESS.2020.2978492

43. Wang, X., & Liu, L. (2020). Image Encryption Based on Hash Table Scrambling and DNA Substitution. IEEE Access, 8, 68533–68547. https://doi.org/10.1109/ACCESS.2020.2986831

44. Abduljaleel, I. Q., & Khaleel, A. H. (2020). Hiding text in speech signal using K-means, LSB techniques and chaotic maps. International Journal of Electrical and Computer Engineering, 10(6), 5726–5735. https://doi.org/10.11591/ijece.v10i6.pp5726-5735

45. DHANALAXMI BANAVATH, S. T. (2017). A new image encryption algorithm based on logistic chaotic map. International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), 6(11), 1248–1260.

46. Wang, X., Hou, Y., Wang, S., & Li, R. (2018). A New Image Encryption Algorithm Based on CML and DNA Sequence. IEEE Access, 6, 62272–62285. https://doi.org/10.1109/ACCESS.2018.2875676

47. Zhang, X., Zhou, Z., & Niu, Y. (2018). An Image Encryption Method Based on the Feistel Network and Dynamic DNA Encoding. IEEE Photonics Journal, 10(4), 1–14. https://doi.org/10.1109/JPHOT.2018.2859257

48. Wu, X., Zhu, B., Hu, Y., & Ran, Y. (2017). A Novel Color Image Encryption Scheme Using Rectangular Transform-Enhanced Chaotic Tent Maps. IEEE Access, 5, 6429–6436. https://doi.org/10.1109/ACCESS.2017.2692043

49. Muhammad Asif Gondal, I. H. (2015). An Image Encryption Scheme based on Nonlinear Chaotic Algorithm and Substitution Box Transformation. Applied Mathematics & Information Sciences An International Journal, 9(http://dx.doi.org/10.12785/amis/090627), 2991–2995.

IRAQI Academic Scientific Journals

Samarra Journal of Pure and Applied Science

SJPAS

www.sjpas.com

ISSN:2663-7405

انظمة تشفير الصور الفوضوي: مراجعة

امل حميد خليل [1]*، ايمان قيس عبدالجليل[2]

1- قسم علوم الحاسوب، كلية علوم الحاسوب وتكنولوجيا المعلومات، جامعة البصرة (amal_albahrany@yahoo.com)

2- قسم علوم الحاسوب، كلية علوم الحاسوب وتكنولوجيا المعلومات، جامعة البصرة

معلومات البحث:

تأريخ الاستلام: 2021/02/04

تأريخ القبــول: 2021/03/24

الكلمات المفتاحية:

الصورة، التشفير، الخريطة الفوضوية، التشفير، البعثرة

الخلاصة:

في العقود الأخيرة، كان تشفير الصور مجالًا شائعًا وهامًا للبحث. تمت دراسة تقنيات تشفير الصور بدقة لضمان سلامة الصور الرقمية عند الإرسال عبر الشبكات. تم اقتراح مجموعة كبيرة من الخوارزميات لأنظمة التشفير القائمة على الفوضى وتقديمها لتعزيز كفاءة طرق التشفير. الخريطة الفوضوية هي إحدى تقنيات ضمان الأمن. تشمل فوائد تشفير الصور الفوضوي حقيقة أنه سهل التنفيذ؛ لديه سرعة تشفير أسرع، وهو قوي ضد الهجمات. ونظرًا لحساسيتها الشديدة للظروف الأولية، وعدم القدرة على التنبؤ، والسلوكيات العشوائية، تم اقتراح العديد من أنظمة تشفير الصور باستخدام الخرائط الفوضوية. تقدم هذه الدراسة مراجعة علمية لأنواع عديدة من الأبحاث على مدار عقد من الزمان (2010-2020) والتي استخدمت فيها الفوضى بأنواعها المختلفة (أحادي البعد أو متعدد الأبعاد أو هجينه) لمعالجة الصور الرقمية في مرحلة التشفير أو مرحلة البعثرة. علاوة على ذلك، يقدم قراءة مستقبلية للأبحاث التي لها دور كبير في تطوير مجال التشفير من خلال تحسين كفاءة الخوارزميات، حيث يؤدي استخدام الخريطة الفوضوية مع طرق أخرى إلى نتائج أفضل من استخدام الفوضى وحدها في البعثرة وطرق التشفير.