International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2019.3559

E-ISSN : 2454-6135

Volume.5, Issue 9
September -2019

Review: Image Encryption Techniques based on Chaotic Map

Amal Abdulbaqi Maryoosh[1] Raniah Ali Mustafa[2] & Zahraa Salah Dhaief[3]

[1-3]Computer Science Department

Collage of Education

Mustansiriyah University

Baghdad- Iraq

ABSTRACT

Due to the tremendous developments in communication networks especially in the Internet network, which used to exchange many types of data by many people. Data security has become a major concern. Therefore, there is an increasing interest in the use of encryption and decryption methods. Many encryption methods have been developed to maintain data security, one of these methods that commonly used in recent are chaotic encryption systems. Where many methods were suggested to encrypt images using a chaotic map because their features such as sensitivity to initial conditions and unpredictability of random behaviors etc... In this paper, we attempt to review and describe many methods used to encrypt images and make a comparison among these methods.

Key Words: *Image Encryption, Chaotic Schemes, Deoxyribonucleic acid series, Cryptography.*

1. INTRODUCTION

Given the need to exchange and store many types of data such as text, video, audio and image over the Internet, an environment in which it is easy to penetrate the information exchanged, cryptographic techniques have been used to protect the confidentiality of data from unauthorized access [1].

Image encryption is the most benefit way to preserve the confidentiality when storing or transferring images through a network. Image encryption applications can expand to include multimedia systems, military communications, online communications, medical science, etc. Images has some characteristics different from text such as less sensitive, huge data capacity, data redundancy and correlation between adjacent pixels. To get rid of these challenges that facing the image encryption, many encryption methods have emerged. Several conventional encryption algorithms such as RSA, DES, triple DES and AES have been used for many years, but are not convenient for image encryption these algorithms have some weakness in image encryption especially when the image size is large [2,3]

Recently, cryptography based on chaotic systems has been discovered and is becoming commonly used in image encryption methods. In fact, chaotic systems show pseudorandom behavior and have substantial features such as unpredictability of the orbital growth, high sensitivity to parameters and initial conditions, lead the simplicity of implementation of software and hardware to increase the encryption rate, etc... These characteristics and another make from chaotic based cryptography is related with most important properties of cryptography like confusion, diffusion [2,4].

In the latest two decades, an increasing number of image encryption schemes have been proposed for used in cryptographic applications. In this paper, we conduct a deep analysis of image encryption technique that based on chaotic schemes. The remaining of this paper arranged as follow: In Section 2 the literature survey of some schemes that proposed in the latest decade. In Section 3 comparative analysis of the schemes that discussed in section 2. Finally, the conclusions are shown in Section 4.

2. LITERATURE SURVEY

In the last decade, there are many methods that related to image encryption has been studied. In this section we discuss some of these research.

Kamlesh Gupta and Sanjay Silakari [5] used 3D standard map and 3D cat map to implement confusion and diffusion process on color images. They divided the plain color image to three bands and rotate the red band vertically, rotate green band horizontally and blue band stay without any change. Then permuted each band using 3D standard map and 3D cat map. Finally, they make XOR between confusion and diffusion steps.

In this paper, H. Liu and X. Wang [6] encrypted color image by using bit level and high dimension chaotic map. They convert the color image to gray scale (M x 3N) and then convert it to binary after that permute it by using piecewise linear chaotic map. Finally, they used chen system to confuse and diffuse the three bands.

Color image encryption based on chaotic map was proposed by Xingyuan Wang et al. [7] the main idea of this paper is divided the color image to three bands and make these bands effect each other. After that combine R, G and B bands vertically and permute its rows, then divided the resulting image to another three bands and combine R, G and B bands horizontally to permute the columns. Finally, make the three permuted bands diffuse mutually.

An image encryption algorithm proposed by Narendra K. Pareek et al. [8] to encrypt a gray image. In this scheme the encryption of an image is done in three steps, first step is diffused image by applied zigzag process to each image block. Second step is substitution operation, in this step they confused each block of image by applied XOR operation between the current pixel and one of the adjacent pixels. The third step is mixing process, in this step implement XOR operation among the current pixel, its pervious pixel and session key. The three steps were repeated sixteen times to achieve a high level of image security.

Dynamic substitution box constructed by XingyuanWang and QianWang [9] based on kent map and logistic map. The parameters and initial conditions of first s- box are generated by using the last bit of plain image and an external 256-bit key. The plain image divided to less than ten blocks each block encrypted with different s-box. After encrypting the previous block, the initial conditions of the next s-box are generated based on the pixels of encrypted block. To encrypt 256 gray image, they construct less than 50 s-box.

Yicong Zhou et al. [10] proposed a novel 1-D LTS (Logistic-Tent System) chaotic map and used it to encrypt color and grey images. The encryption algorithm contains five steps. First step is random pixel insertion; in this step they insert a random value in the beginning of each row in the image. The second step is a row separation step; in this step they separate image rows to prepare it to the next step. The third step is image substitution based on 1D LTS key. Fourth step is combination the rows that resulting from substitution step. The last step is rotation the resulting image 90°counterclockwise. Repeat these steps four time to generate encrypted image.

Atal Chaudhuri and P.Kr. Naskar [11] used tow logistic maps one for image encryption and another for image shuffling. In this work, they used three different key (k0 and k1) are two primary values of two chaotic functions and k2 is a two-byte random number, which is applied to exchange the two-chaotic values at every k2th reiteration.

The cycle shifts in bits of pixels and the chaotic system are employed by Xing-Yuan Wang et al. [12] for image encryption. They used a random integer numbers with the size equal to the plain image for cycle bit-level shift. Then they used chaotic map to generate a key which used to encrypt the scramble image.

In this paper, Xing-Yuan Wang et al. [13] proposed a scheme novel for image encryption based on chaotic system and DNA (Deoxyribonucleic acid) series operations. The encryption scheme contains three steps. First step is using the pseudorandom sequences for perform bitwise XOR operation on the pixels of the plain image produced by the spatiotemporal chaos system, i.e., coupled map lattice (CML). The second step is using a DNA matrix (using a kind of DNA encoding rule) to obtain by encoding the confused image. According to this DNA matrix and the previous initial conditions. They generated the new initial conditions of the CML, which can make the encryption result closely depend on every pixel of the plain image. The third step is permuted DNA matrix (the rows and columns) is confused once again. At last, they obtained the ciphered image after decoding the confused DNA matrix using a kind of DNA decoding rule.

A new schema sentient encryption to secure the digital images based on the Zaslavsky chaotic map was proposed by Faiza Titouna and Rafik Hamza [14]. The main idea of this paper they product the key encryption of the suggested image cryptosystem through the perform of the Zaslavsky chaotic map as a pseudo-random generator. They use permutation-diffusion processes for choose cipher structure, where they suppose the classical permutation substitution network, that assure together confusion and diffusion characteristics for the encrypted image.

In this paper, Sumangala Biradar and Prema T. Akkasaligar [15] proposed an approach novel by using DNA encoding and Chao's theories to make digital medical images security. the main idea for suggested method contains three steps. First step, the use is intensity levels for rehashes the input medical image into two DNA encoded matrices. The second step, they are produce the chaotic sequences separately through utilized two-pixel value (even pixel value based DNA encoded matrix Lorenz chaotic map and for odd pixel value based DNA encoded matrix Chen's hyper chaotic map). By using chaotic sequences, the pixel's positions

DOI : 10.31695/IJERAT.2019.3559

of both DNA encoded matrices are sophisticated. The last step, is utilized ADD operation for the addendum of sophisticated both DNA encoded matrices to acquire an encrypted image. By reverse process of encryption and image decrypted is acquired

Akram Belazi et al. [16] proposed an approach novel for image encryption based on chaotic systems and permutation-substitution (SP) network. The encryption scheme contains four cryptographic steps: substitution, diffusion, diffusion and permutation. First step, new chaotic map for proposed a diffusion step. The second step, strong S-boxes for proposed a substitution step and the third step chaotic logistic map are presented for proposed a diffusion step, which will, in turn, importantly accretion the encryption achievement. The last step, the increase the statistical achievement of the proposed encryption scheme through accomplished the block permutation step by a permutation function.

A new image encryption algorithm proposed by Xiuli Chai et al. [17] based on chaotic systems and DNA sequence operations. The encryption structural design of permutation and diffusion was adopted. The encryption algorithm contains five steps. First step is calculated the initial values and a new 1D chaotic system and scheme parameters of the 2D -LASM through obtain 256-bit for hash value of the plain image; therefore, the encryption system strongly relies on the original image. The second step is obtaining the DNA encoding and DNA decoding rule matrix, and the plain image was encoded into a DNA matrix through utilized the chaotic series of 2D Logistic-Adjusted-Sine map (2D-LASM). The third step is applied two level DNA (row and column permutation) on the DNA matrix of the original image, intra-DNA-plane permutation and inter-DNA-plane permutation can be acquired jointly, subsequently, DNA XOR operation was acquired on the permutated DNA matrix utilizing a DNA key matrix was product by the incorporation of two 1D chaotic schemes. The last step is obtained the cipher image, after decoding the confused DNA matrix.

In this paper, Z. Hua et al. [18] proposed a novel encryption approach of protecting medical images. The encryption approach contains two phase. First phase is using surroundings of the image for inserted some random data. The second phase is containing two rounds: the first round is high-rapidity jostle and pixel adjustment diffusion were implemented to randomly mixture neighbouring pixels, the second round propagation these integrated random data over the complete image. The present encryption approach can be immediately utilized to medical images with every representation format. In the work, they provided two types of operations to performance the pixel adjustment diffusion: modulo arithmetic and bitwise XOR.

In this paper, M. Ghebleh et al [19] presents a new image encryption algorithm based on least squares approximations and chaotic maps. The presented algorithm comprises of two major stages, which were perform respectively in some rounds, namely a shuffling stage and a masking stage. In this work, both stages were based on two tasks:1– D piecewise linear chaotic maps (LCM) and performance on the rows and columns of the input plain image. To enhance the security of the suggested algorithm by supplier a powerful mixture between the rows /columns of the image through the use of least squares approximations

In this article, S. Abdulnabi and M. Sabbih [20] presents a novel image encryption technique to beat the hurdles to prior image encryption techniques, their technique was applied Duffing map to mixed all image pixels, in this work they use cross Chaotic Map for perform the shuffling process after the generating image was separated into a set of blocks. lastly, they obtain to key image was generated through applying square number snails which will be applied to create numbers of polynomial equations by Lagrange interpolation to apply pixel diffusion.

In this article, Z. Hua et al. [21] used a two-dimensional Logistic-Sine-coupling map. In this work, achievement estimates demonstration that it had best ergodicity, huge chaotic range and more complex demeanor than various recently sophisticated two-dimensional chaotic maps. using the suggested 2DLSCM, also suggest a 2DLSCM- based on image encryption algorithm (LSCM-IEA), that espouses the classic confusion-diffusion framework. permutated image pixels to various columns / rows through designed a permutation algorithm and propagation little variations of plain-image to the entire encrypted produce through developed a diffusion algorithm.

A. Abdulbaqi [22] proposed a new image encryption scheme based on Lorenz system, logistic map and s-box. The proposed algorithm encrypts and decrypts 128-byte block. At first the plain image was confused then permuted the result by used permutation algorithm, after that input block by block to substitution by variable s-box and adding key stages. The resulted image XOR with another encrypted key that generated by logistic map, and then confused the resulted image again.

A color image crypto scheme based on chaos and effective DNA encryption was presented by Xiuli Chai et al. [23]. Firstly, resolve color plain image into red, green and blue ingredients and use a jointly inter-intra-ingredient permutation technique, which rely on the plaintext SCPMDP was presented to mix them. next, through using a DNA encoding rule, convert the recycled permutated ingredients into a DNA matrix, and then various from the classical DNA series operations approbate to the aw of binary computation, a diffusion technique relies on random numbers regarding to plaintext (DMRNRP) was offered to prevalent it. Moreover, according to a DNA decoding rule will transform the diffused DNA matrix into a decimal one, and split it into three equal images. lastly, they used second confusion scheme for respectively scramble images, to reinforce security of the image cryptosystem, and subsequently the color cipher image was obtained. In this paper, used a four-wing hyper chaotic scheme to provide for each: SHA 384 hash function of the plain image, pseudo-random chaotic sequences and exterior parameters were compiled to computation its primary values and one-time-pad encryption politics creates the suggested encryption efficiently resistant plaintext attacks.

Joshua C. Dagadu et al. [24] proposed an encryption scheme based on multiple chaos and DNA coding for gray scale medical images. The chaotic tent map was utilized to generate chaotic key stream and the logistic map was utilized to randomly select DNA encoding and decoding rules. The chaotic key and the plain medical image were first encoded into DNA sequences. A selected DNA algebraic operation (addition/subtraction/XOR) was carried out between the plain image DNA sequence and the key DNA sequence; the outcome was then decoded to get the cipher image. The process is carried out both on row and column bases to achieve a robust cipher.

3. COMPARATIVE ANALYSIS OF THE SCHEMES

Table 1 will explain the comparison among previous systems.

Table1.1. Comparative analysis of the schemes for Lena image

Ref.	Key space	Histogram distribution	Entropy	Correlation Coefficient			UACI	NPCR	SPNR	MAE
				Vertical	Horizontal	Diagonal				
[5]	2^{148}	Fairly Uniform	7.9991	0.006	0.001	0.091	27.37	99.62	-	77.54
[6]	2^{563}	Fairly Uniform	7.9878	-0.0035	-0.0574	0.0578	33.63	99.66	-	-
[7]	2^{179}	Fairly Uniform	-	-0.0126	-0.0077	-0.0463	33.47	99.65	-	-
[8]	2^{128}	Fairly Uniform	7.9952	−0.0016	0.0031	0.0067	31.79	-	-	-
[9]	2^{256}	Fairly Uniform	7.9971	0.0136	0.0097	0.0178	33.42	99.61	-	-
[11]	2^{142}	Fairly Uniform	7.991	–0.0007	0.0024	–0.0030	22.67	99.61	24.436	-
[12]	$>2^{100}$	Fairly Uniform	7.9984	0.0342	0.0096	0.0205	33.33	99.82	-	-
[13]	2^{172}	Fairly Uniform	7.9970	-0.0007	0.0020	-0.0014	33.48	99.65	-	-
[14]	2^{711}	Fairly Uniform	7.9978	0.0049	0.0023	0.0054	33.54	99.63	-	-
[16]	$>2^{624}$	Fairly Uniform	7.9963	-0.0112	-0.0048	-0.0045	33.70	99.62	-	-
[17]	$>2^{100}$	Fairly Uniform	7.9993	0.0177	−0.0139	6.7947e−04	33.43	99.58	-	-
[20]	$>2^{100}$	Fairly Uniform	7.9992	0.0242	-0.0091	-0.0137	33.14	99.69	9.7896	-
[23]	$>2^{100}$	Fairly Uniform	7.9971	-0.0012	-0.0007	-0.0017	33.50	99.60	-	77.87

4. CONCLUSION

In this paper, we reviewed different technique for image encryption based on chaotic systems within the period (2011-2019). Digital image security become very significant specially when the transmitting will have done thought open network. These encryption schemes are studied and analyses fully to boost the efficiency of the encryption methods and to guarantee the security performance. the summary of this study, all these the techniques are beneficial for real-time image encryption. every scheme is unrivaled in its own method, which may be appropriate for various applications. The new encryption technology is evolving every day, so the fast and secure traditional encryption technology will always achieve a high security rate. Recently, suggested image encryption techniques also increase the level of security by providing more than a chaotic system for image encryption algorithms. All technologies have some benefits and drawbacks and therefore new technologies have been developed.

REFERENCES

1. Priya R Sankpal and P. A. Vijaya, “Image Encryption Using Chaotic Maps: A Survey”, *2014 Fifth International Conference on Signals and Image Processing, IEEE*, DOI 10.1109/ICSIP.2014.80.
2. J.S. Armand Eyebe Fouda et al., “A fast chaotic block cipher for image encryption”, *Commun Nonlinear Sci Numer Simulat 19* (2014) 578–588, doi: http://dx.doi.org/10.1016/j.cnsns. 2013.07.016.
3. Ali Shakir Mahmood and Mohd Shafry Mohd Rahim, “State of the Art of Image Ciphering: A Review”, *International Journal of Computer Science Issues*, Vol. 11, Issue 2, No 1, March 2014.
4. Chunhu Li, Guangchun Luo, Ke Qin and Chunbao Li, “chaotic image encryption schemes: a review”, *2nd Internatio nal Conference on Electrical, Automation, and Mechanical Engineering, Advance in Engineering Research*, volume 86, 2017.
5. Kamlesh Gupta and Sanjay Silakari, “New Approach for Fast Color Image Encryption Using Chaotic Map”, *Journal of Information Security*, 2011, 2, 139-150 doi:10.4236/jis.2011.24014.
6. Hongjun Liu and Xingyuan Wang, “Color image encryption using spatial bit-level permutation and high-dimension chaotic system”, *Optics Communications 284* (2011) 3895–3903, doi:10.1016/j.optcom.2011.04.001.
7. Xingyuan Wang, LinTeng and XueQin, “A novel colour image encryption algorithm based on chaos”, *Signal Processing 92* (2012) 1101–1108, doi:10.1016/j.sigpro.2011.10.023.
8. Narendra K. Pareek, Vinod Patidar and Krishan K. Sud, “Diffusion–substitution based gray image encryption scheme”, *Digital Signal Processing*, 2013, http://dx.doi.org/10.1016/j.dsp.2013.01.005
9. XingyuanWang and QianWang, “A novel image encryption algorithm based on dynamic S-boxes constructed by chaos”, *Nonlinear Dyn* (2014); 75:567–576, doi: 10.1007/s11071-013-1086-2.
10. Yicong Zhou, LongBao and C.L.Philip Chen, “A new 1D chaotic system for image encryption”, *Signal Processing 97*(2014)172–182, DOI:org/10.1016/j.sigpro.2013.10.034.
11. Prabir Kr. Naskar and Atal Chaudhuri, “A robust image encryption technique using dual chaotic map”, *Int. J. Electronic Security and Digital Forensics* (2015); 7(4): pp.358–380.
12. Xing-YuanWang, Sheng-XianGu and Ying-QianZhang, “Novel image encryption algorithm based on cycle shift and chaotic system”, *Optics and Lasers in Engineering 68(*2015)126–134, DOI: org/10.1016/j.optlaseng.2014.12.025.
13. Xing-YuanWang, Ying-QianZhang and Xue-MeiBao, “A novel chaotic image encryption scheme using DNA sequence operations”, *Optics and Lasers in Engineering 73*(2015)53–61, DOI: 10.1016/j.optlaseng.2015.03.022.
14. Rafik Hamza and Faiza Titouna, “A novel sensitive image encryption algorithm based on the Zaslavsky chaotic Map”, *INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE*, 2016, doi: 10.1080/19393555.2016.1212954.
15. Prema T. Akkasaligar and Sumangala Biradar, “Secure Medical Image Encryption based on Intensity level using Chao’s theory and DNA Cryptography”, *IEEE International Conference on Computational Intelligence and Computing Research*, 2016.
16. Akram Belazi, Ahmed A. Abd El-Latif and Safya Belghith, “A novel image encryption scheme based on substitution-permutation network and chaos”, *Signal Processing*, 2016, doi: 10.1016/j.sigpro.2016.03.021.
17. Xiuli Chai et al., “A novel image encryption scheme based on DNA sequence operations and chaotic systems”, *Neural Comput & Applic*, 2017, DOI: 10.1007/s00521-017-2993-9.
18. Zhongyun Hua, Shuang Yi and Yicong Zhou, “Medical image encryption using high-speed scrambling and pixel adaptive Diffusion”, *Signal Processing*, 2017, doi: 10.1016/j.sigpro.2017.10.004.
19. M. Ghebleh, A. Kanso and D. Stevanovi´c, “A novel image encryption algorithm based on piecewise linear chaotic maps and least squares approximation”, *Multimed Tools Appl*, 2017, doi: 10.1007/s11042-017-4634-9.
20. Salam Abdulnabi Thajeel and Mohammed Sabbih Hamoud Al- Tamimi, “An Improve Image Encryption Algorithm Based on Multi-level of Chaotic Maps and Lagrange Interpolation”, *Iraqi Journal of Science*, 2018, Vol. 59, No.1A, pp: 179-188 DOI: 10.24996/ijs.2018.59.1A.19.
21. Zhongyun Hua et al., “2D Logistic-Sine-Coupling Map for Image Encryption”, *Signal Processing*, 2018, doi: 10.1016/j.sigpro.2018.03.010.
22. Amal Abdulbaqi maryoosh, “A new block cipher algorithm for image encryption based on chaotic nap and S-box”, *International Journal of Civil Engineering and Technology*, Volume 9, Issue 13, 2018, PP. 318–327.
23. Xiuli Chai et al., “A color image cryptosystem based on dynamic DNA encryption and Chaos”, *Signal Processing*, 2018, doi: 10.1016/j.sigpro.2018.09.029.
24. Joshua C. Dagadu et al., “Medical Image Encryption Scheme Based on Multiple Chaos and DNA Coding”, *International Journal of Network Security*, Vol.21, No.1, PP.83-90, Jan. 2019, DOI: 10.6633/IJNS.201901 21(1).10.

DOI : 10.31695/IJERAT.2019.3559