International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2021.3734

E-ISSN : 2454-6135

Volume.7, No. 9
September -2021

Subject Review: Image Encryption Based on Multi Techniques

Zainab Mohammed Essa, Doaa Mohsin Abd Ali Afraji, Donia Fadhil Chalob,

Sahar Hasan Hashim, and Ziad M. Abood*

Department of Computer Science

Collage of Education, Mustansiyiah University

Iraq

ABSTRACT

The enormous advancements in communication network, particularly the internet networks, that employed to allow numerous individuals to exchange various forms of data, Security of data has become a big issue. As a result, the usage of cipherment and decipherment ways is becoming more popular. Sundry cipherment means have been created to ensure data security, the chaos encryption system being one of the most widely employed in recent years. In this research, a review of diverse image cipherment algorithms have been reviewed, which researchers can gain insight into the most efficient techniques to employ.

Keywords: Cryptography, Decryption, Encryption, Image Encryption, Key Space.

---

1. INTRODUCTION

Information security is a must-have for everyone nowadays. People need to protect their resources and information, especially their private photographs, from unauthorized access, which necessitates the use of image encryption in our daily lives. Image encryption can be defined as the process of transforming an original image into a cipher image via employing certain techniques or methods [1]. Image cipherment is employed to safeguard the content of an image, authenticate images and hide data. [2]. The Image cipherment employs standard encryption methods like DES, AES and RSA algorithms. However, when used these algorithms in a cryptosystem that ciphers a huge number of images or videos, the standard encryption technique is less efficient. In the field of information ciphering, the chaos system has better features. It is sensitive to initial conditions, unpredictable and has a complex bifurcation. Chaos has a number of unique qualities that aid in the development of more secure and reliable encryption schemes [3,4].

Henon map, Arnold Cat map, Logistic map, Lorenz system and extra chaotic models are examples. The features of various cipherment methods related to perfect cipher, like diffusion, assessment and avalanche, reflect the complicated nature of chaos mapping. [2, 3]

An growing variety of image cipherment techniques are proposed for use in cryptography applications in the previous two eras. Image encryption algorithms have been examined in depth in this study. The remainder of this work is prepared as follows: The literature review of some papers proposed in the last decade is presented in Section Two. The inferences are found in Section 3.

2. LITERATURE SURVEY

There are numerous image cryptography methods are investigated during the previous decade. Some of these studies are discussed in this section.

Taqi and Hameed [5] employed chaotic maps to check that the security cipher characteristics of confusion and diffusion are met. A mixture of 1-D logistic and Sine chaos map is employed to construct the key sequence for encrypting an image. Three chaotic sequences are constructed to generate a key sequence to encrypt an image. The binary representation of sx, sy and sz is created**.** The original image is divided into three bands. The resulting sequences are subjected to an XOR procedure. The collected outcomes are then translated to decimal form in order to create an encrypted image.

El-Latif and Xiau Niu [6] proposed a cyclic elliptic curve and a chaotic system, developing an effective hybrid image encryption approach. In a feedback approach, The suggested approach uses a chaos system and a 256-bit external secret key to generate an initial key stream. Key sequences obtained from cyclic elliptic curve points are then combined with the resulting

keystream. To begin, A binary data stream is created by converting an image. Via using a random keystream created from a mix of cyclical elliptic curve points and a chaos map to mask these data, the equivalent cipher image is shaped.

Bashir et al. [7] suggested a new image cryptography depended on the mixture of shifted picture blocks and original AES. The image is divided into blocks using the shifted technique. Each block is made up of a certain numeral of pixels, and the pixels are scrambled via a shift technique to make the shift image, the original image's rows and columns are shifted. The AES technique is then used to encrypt the pixels of the shift image via this shift image as an input image.

Younes and Jantan [8] presented an image ciphering method where the plain image was separated into blocks, then reorganized using a transformation method to create a converted image. The Blowfish technique was used to encrypt the altered image. The proposed technique greatly reduced the correlation between image elements, according to the results. The results also demonstrate that utilizing smaller block sizes to increase the number of blocks resulted in a lower correlation and increased entropy.

Saraireh et al. [9] encrypted image using filter bank encryption through one or two rounds. The cipher and decipher operations are based on a circular convolution method that is "linear". It is well-known for its superior diffusion. A lifting method with a nonlinear function is used to add the necessary nonlinearity, confusion, to the cipher.

Sakthidasan and Krishna [10] developed a strategy for image cryptography that shuffles the location of the image pixels via a dynamic chaos system (one of three: Lorenz, Chen or LU chaos system choiced depended on 16- byte key). It confuses the link between the cipher image and the plain image by using another of the same three chaotic maps (diffusion). This algorithm offers the advantages of a larger key space, shorter repetition time and a high level of key space analysis, for example, is a type of security analysis.

Mehdi and Kadhim [11] presented a new technique for chaos scheme placed on the Sudoku matrix, where there is a new 5D chaos strategy is devised in order to produce a random key for encrypting the colour image. Using the chaos sequence generated, the cryptosystem contains a shuffled image. Then, between the Sudoku Matrix and the scramble, execute an XOR operation, repeat the scrambling procedure. After the previous operations, conduct XOR to combine a chaotic key with the plain image. The histogram, correlation coefficient, NPCR (Number of Pixels Change Rate), entropy, UACI (Unified Average Changing Intensity) and PSNR (Peak Signal into Noise Ratio) have all been used to determine the encryption power.

Xu1 et al. [12] provided a new image cryptography technique rely on two hyper chaos systems and bit- plane matrix rotation. The technique splits the original image into 8- bit planes before constructing a 3D matrix. The 3D bit-plane sub-matrix is then rotated in several ways using PRNS created via a hyper chaos system. Lastly, another key stream is employed to replace the pixels of the intermediate image. The MD5 hash function of plain image produces the beginning values of diffusion and other parameters important for creating chaos sequence. It improves the correlation between the encryption and plain image processes. Simulation experiments are presented to investigate the encryption security in terms of key space, histogram, entropy, key sensitivity and adjacent pixels correlation index.

Li et al. [13] proposed a chaos-based image cryptosystem. It employs a jigsaw-like approach involving rotating and shifting methods. There are three encryption steps in this scheme: pretreatment, encryption, and postprocessing. The plain image is partitioned into 64 by 64 pixel blocks in preprocessing phase. Then, using control sequences, they were rotated and shifted at random produced via the hyper chaos Lorenz system, which initial conditions are determined using the keys and original image. As a result, the preprocessing phase is vulnerable to differential attack on plain image. In the encipherment phase, the image is splited into 32 by 32 pixel blocks, then aimlessly rotated and cipher using control sequences and key blocks created using the skew tent chaos map. The after encryption, image is split into 16 by 16 pixel blocks in postprocessing, and they are rotated and shifted at random under control sequences relating to cipher image and keys. The diffusion characteristics are improved even further after postprocessing. The experimental and security evaluations are also provided.

Al-Maadeed et al. [14] proposed a new image cryptosystem. The encryption and compression are included in the new approach. A wavelet transform was utilized to deconstruct and decorrelate the image's pixels into approximating and detailed ingredients in this technique. A chaotic cryptosystem is used to encrypt the more significant component (approximation component). The approach generates a test image cipher with excellent diffusion and confusion qualities. A wavelet transform is used to compress the remaining components (detailed components).

G. A. Sathishkumar et al. [15] introduces a new image cryptosystem. First, use multiple chaos-based circular mapping, using chaos logistic maps, a pair of sub keys is produced. Next, the image is ciphered with a logistic map sub key, which results in a diffusion process during transformation. Third, four distinct chaotic maps yield sub keys. Depending on the intial conditions, each map generates distinct random numbers from different orbits of the maps. A specific number and orbit from among those random numbers is chosen as a key for the cipher method. A binary sequence is created based on the key to control the cipherment. There are two different scanning patterns (raster and Zigzag) are used to convert the 2D input image into a 1D array,

DOI : 10.31695/IJERAT.2021.3734

which is then separated into several sub blocks. Next, using numerous chaotic maps, position and value permutation are implemented on every binary matrix. The receiver decrypts the cipher image via the similar sub keys.

Wang et al. [16] proposed a new spatiotemporal chaos model named as MCML via combining Logistic, Sine and Tent maps into a CML map to encrypt images by creating a new key distribution and binding rule, as well as an improved diffusion strategy. In different lattices, vary the structure of CML and the coupling technique. The chaos behavior of MCML system are measured by a bifurcation graph, Lyapunov exponent and NIST analysis. Moreover, the unique bit Z-scan scramble approach could employed to improve the encryption scheme's security. As a final point, a vast number of experiments demonstrate that our suggested technique is appropriate for image processing.

Yi He et al. [17] created a new image cryptosystem using Once Forward Long Short Term Memory Structure named as OF-LSTMS and the 2D Coupled Map Lattice known as (2DCML) fractionalorder chaos system. The original image is separated into many blocks each of which is entered as a sub-pixel sequence into the OF-LSTMS. The parameters of the input entrance, output entry of OF-LSTMS and memory unit are all initialized via the chaos sequences produced via the 2D CML fractional order chaos system. The pixel location is altered a similar time that the pixel value is changed. Accomplishing permutation and diffusion operation synchronization, which dramatically enhances image ciphering performance and decreases time depletion. Furthermore, the 2D CML fractional order chaos system has enhanced ergodicity than the typical chaos system and the values of chaos sequences are longer.

Ch et al. [18] proposed a new chaos image cryptosystem, a rapid cipherment method based on a substitution and permutation scheme with logistic and rectangular chaos map. Rectangular chaos map are key dependent and used for pixels permutation, while logistic maps create a substitution box. This technique is applicable to images of any size.

3. CONCLUSIONS

Many essential cryptosystems have been produced and explored in this paper in order to familiarize with the different cipherment algorithms used in ciphering images that have been transmitted over the network. The study results reveal that each method has strengths and weaknesses dependent on the approaches used to modify images. Following are some recommendations based on a careful examination of all of the above-mentioned researchs: Chaos-based algorithms should be used to secure multimedia assets. To give the cryptosystem a lot of speed and security, a more complicated and compressed algorithm should be implemented. To boost the security level, modified versions of several algorithms are employed.

REFERENCES

1. Arwa Benlashram et al., ”A novel approach of image encryption using pixel shuffling and 3D chaotic map”, 1447 (2020) 012009 IOP Publishing, doi:10.1088/1742-6596/1447/1/012009.

2. Shima Ramesh Maniyath and Thanikaiselvan, “Robust and Lightweight Image Encryption Approach Using Public Key Cryptosystem” Springer International Publishing AG, part of Springer Nature 2019, AISC 765, pp. 1–11, 2019.

3. Ziad M. Abood, Zainab M. Essa, “Increase Security of Image Encryption Depends on Change Pixel Location”, journal of the college of basic education, Vol. 23, Issue 98, 2017.

4. Dejian Fang and Shuliang SunID, “A new secure image encryption algorithm based on a 5D hyperchaotic map” Hua Wang, Victoria University, AUSTRALIA, November 12, 2020.

5. Ibtisam A.Taqi and Sarab M. Hameed, “A new Color image Encryption based on multi Chaotic Maps”, *Iraqi Journal of Science, 2018, Vol. 59, No.4B, DOI:10.24996/ijs.2018.59.4B.17.*

6. Ahmed A. Abd El-Latif and Xiamu Niua,” A hybrid chaotic system and cyclic elliptic curve for image encryption”, Int. J. Electron. Commun. (AE-) 67 (2013) 136– 143.

7. Ahmed Bashir et al.,” A New Image Encryption Approach using The Integration of A Shifting Technique and The Aes Algorithm” *International Journal of Computer Applications (0975 – 8887), Volume 42– No.9, March 2012.*

8. Mohammad Ali Bani Younes and Aman Jantan, ”Image Encryption Using Block-Based Transformation Algorithm”, IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03, 27 May 2014.

9. Saleh Saraireh et al.,”Image Encryption Scheme Based on Filter Bank and Lifting”, Int. J. Communications, Network and System Sciences, 2014, 7, 43-52.

10. K. Sakthidasan and B. V. Santhosh Krishna,” A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images”, International Journal of Information and Education Technology, Vol. 1, No. 2, June 2011.

DOI : 10.31695/IJERAT.2021.3734

11. Sadiq A. Mehdi and Ashwaq A. Kadhim,"Image Encryption Algorithm Based on a New Five Dimensional Hyperchaotic System and Sudoku Matrix", Fifth International Engineering Conference on Developments in Civil & Computer Engineering Applications 2019 - (IEC2019) - Erbil – IRAQ.

12. Cong Xu et al.,"A novel image encryption algorithm based on bit-plane matrix rotation and hyper chaotic systems", Springer Science+Business Media, LLC, part of Springer Nature 2019.

13. Zhen Li et al.,"An Effective Chaos-Based Image Encryption Scheme Using Imitating Jigsaw Method", Volume 2021, Article ID 8824915, 18 pages, https://doi.org/ 10.1155/2021/8824915.

14. Somaya Al-Maadeed et al., "A New Chaos-Based Image-Encryption and Compression Algorithm", Journal of Electrical and Computer Engineering, Volume 2012, Article ID 179693, 11 pages.

15. G. A.Sathishkumar et al.," Image Encryption Based On Diffusion And Multiple Chaotic Maps", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.

16. Xingyuan Wang et al.,"A new image encryption scheme based on coupling map lattices with mixed multi-chaos", (2020) 10:9784 | https://doi.org/10.1038/s41598-020-66486-9.

17. Yi He et al.,"A new image encryption algorithm based on the oF-LSTMS and chaotic sequences", (2021) 11:6398 | https://doi.org/10.1038/s41598-021-85377-1.

18. Anoosha.Ch et al.," image encryption using substitution-permutation chaotic map", www.joics.org, Volume 9, Issue 9, 2019.

* C. Author: dr.ziadmabood@uomustansiriyah.edu.iq

DOI : 10.31695/IJERAT.2021.3734