Journal of The Gujarat Research Society

ISSN: 0374-8588
Volume 21 Issue 8, August 2019

IMAGE ENCRYPTION TECHNIQUES: A COMPREHENSIVE REVIEW

Hari Krishna Moorthy
Faculty of Engineering and Technology
Jain (Deemed-to-be University), Ramnagar District, Karnataka - 562112
Email Id- hari.moorthy@jainuniversity.ac.in

Abstract

A complex chaotic system that combines two or more discrete chaotic systems is the composite discrete chaotic system (CDCS). In a random way, this system retains the chaotic features of various chaotic systems and has chaotic behaviors that are more complex. We intend to provide a novel image encryption algorithm based on a new two-dimensional (2D) CDCS in this paper. The suggested method consists of two parts: first, we propose a new 2D CDCS and analyze the chaotic behaviors, and then, with the new CDCS, we implement the bit-level permutation and pixel-level diffusion encryption architecture to form the entire proposed algorithm. To improve the security of the proposed algorithm, random values and the total information of the plain image are applied to the diffusion process. The theoretical analysis and simulations both confirm the security of the algorithm proposed.

Keywords: *Communication Channel, Image Encryption, Data Secrecy, Image Encryption, Encryption Algorithm.*

I. INTRODUCTION

The image encryption techniques are highly demanded to ensure the secrecy of the image data during transmission over insecure networks around the globe [1]. Due to the growth of multimedia applications worldwide, various studies on pragmatic image encryption techniques have been investigated from the confidentiality perspective of images. Color image encryption techniques

are highly demanded to ensure the secrecy of the image data during transmission over insecure networks around the globe [2].

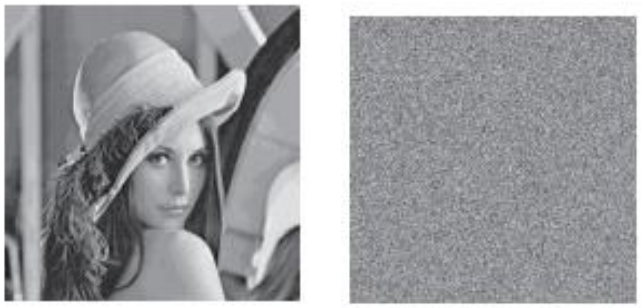

Fig. 1 Illustrates the real and encrypted picture

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2$$

$$cov\,(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))\;(y_i - E(y))$$

$$r_{xy} = \frac{cov\,(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$\sqrt{D(x)}\; \neq 0, \sqrt{D(y)} \neq 0$$

In order to lose the image data during the transmission through the communication channel, there are some parameters that ensure the vulnerability of the different image formats against the strikers' various attacks [3][4]. The Pixel Change Rate Number (NPCR) and Unified Average Shifting of Power (UACI). The formulas for calculating the NPCR and UACI for an image is given below [5].

$$NPCR = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\ \%$$

$$UACI = \left[\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C1(i,j) - C2(i,j)|}{255}\right] \times \frac{100\%}{M \times N}$$

II. LITERATURE REVIEW

Ziad et al. reviewed another paper on DES, AES and Blowfish for image encryption and decryption. The most critical aspect of information security is Network Security, since it is responsible for protecting all data passed through networked computers. We answer and survey DES, AES and Blowfish for Image Encryption and Decryption in this document. It is a key concern in today's world that when transmitting images over the internet from one network to another network. For this authors offered a survey related researches and done some problem identification and suggest some future suggestion which can be useful for image encryption [6].

Somaya et al. explored another paper on the topic of a survey of steganography and steganalysis technique in image, text, audio and video as cover carrier. The steady growth in communication technologies and the use of public domain (i.e. the Internet) networks has greatly facilitated data transmission. Such open communication networks, however, have a greater susceptibility to security threats that cause unauthorized access to information. Encryption is traditionally used to understand the confidentiality of communication. This paper provides a critical overview of steganography and analyses the features of different cover media, namely image, text, audio and video, in relation to the fundamental concepts, the advancement of steganographic methods and the creation of the corresponding steganalysis schemes.

III. DISCUSSION

Another critical constraint is the correlation coefficient to ensure that the encryption algorithm is very accurate. The expression is given below. To guarantee confidential transmission and image capability over the network, image encryption plays a paramount role [7]. Then again, due to the large amount of details used, real-time image encryption faces a more noteworthy test.

$$r_{x,y} = \frac{C(x,y)}{\sqrt{D(x)}.\sqrt{D(y)}}$$

Where $C(x,y), D(x)$ and $D(y)$ may be evaluated by utilizing the following equations.

$$C(x,y) = \frac{\sum_{i=1}^{K}(x_i - E(x))(y_i - E(y))}{K}$$

$$D(x) = \frac{1}{K}\sum_{i=1}^{K}(x_i - E(x))^2$$

$$D(y) = \frac{1}{K}\sum_{i=1}^{K}(y_i - E(y))^2$$

IV. CONCLUSION

A new two-dimensional composite discrete chaotic system-based image encryption scheme is introduced in this paper and we use the new CDCS to achieve bit-level permutation and pixel-level diffusion. The results of the simulation demonstrate the safety and legitimacy of the proposed system with many characters: (1) The CDCS has outstanding chaotic behaviors because it spontaneously combines two single chaotic systems. (2) It has an architecture of bit-level permutation and pixel-level diffusion in which the image is encrypted with a single-permutation and double-diffusion effect, scanning the plain image only once. (3) The value of the ciphered pixel has affected the permutation and diffusion effect of the next pixel, and any location can be allowed for a pixel in the plain picture, and a minor shift can spread overall pixels in the cypher image. In the future, the excellent chaotic actions of the map of high-dimensional chaos and hyper chaos will be considered. With the good structure of the composite discrete chaotic system, composite discrete high-dimensional chaotic system and composite hyper-chaotic dynamic system can be designed to enhance the chaotic system complex and obtain excellent chaos, but when using these systems in image encryption, we should consider the time consuming and convenience.

V. REFERENCES

[1] M. Khan and T. Shah, “A Literature Review on Image Encryption Techniques,” *Autoimmunity Highlights*. 2014, doi: 10.1007/s13319-014-0029-0.

[2] S. Liu, C. Guo, and J. T. Sheridan, “A review of optical image encryption techniques,” *Opt. Laser Technol.*, 2014, doi: 10.1016/j.optlastec.2013.05.023.

[3] F. Walter, G. Li, C. Meier, S. Zhang, and T. Zentgraf, “Ultrathin Nonlinear Metasurface for

Optical Image Encoding," *Nano Lett.*, 2017, doi: 10.1021/acs.nanolett.7b00676.

[4] E. Setyaningsih and R. Wardoyo, "Review of Image Compression and Encryption Techniques," *Int. J. Adv. Comput. Sci. Appl.*, 2017, doi: 10.14569/ijacsa.2017.080212.

[5] S. Al-Maadeed, A. Al-Ali, and T. Abdalla, "A new chaos-based image-encryption and compression algorithm," *J. Electr. Comput. Eng.*, 2012, doi: 10.1155/2012/179693.

[6] Z. E. Dawahdeh, S. N. Yaakob, and R. Razif bin Othman, "A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher," *J. King Saud Univ. - Comput. Inf. Sci.*, 2018, doi: 10.1016/j.jksuci.2017.06.004.

[7] Sanjeev Kumar, "Triple Frequency S-Shaped Circularly Polarized Microstrip Antenna with Small Frequency-Ratio," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 4, no. 8, 2016, [Online]. Available: http://www.ijircce.com/upload/2016/august/24_Triple_new.pdf.