Journal of The Gujarat Research Society

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

DIFFERENT IMAGE ENCRYPTION METHODS: A SURVEY AND OVERVIEW

Sukumar R
Faculty of Engineering and Technology
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id- r.sukumar@jainuniversity.ac.in

Abstract

The rapid development of digital communication and multimedia applications increases the need for protection and becomes an important problem for multimedia communication and storage. One of the methods used to guarantee high security is Image Encryption. Several areas, such as military medical research, in which picture encryption can be used. Modern cryptography offers important methods for information security and multimedia data safety. In recent years, encryption technology has been rapidly developed and many methods of image encryption have been used to protect confidential image data from unauthorized access. In this paper survey, researchers have discussed various image encryption techniques from which they can get an idea of using effective techniques.

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

I. INTRODUCTION

Color image encryption techniques are highly demanded to ensure the secrecy of the image data during transmission over insecure networks around the globe. Due to the growth of multimedia applications worldwide, various studies on pragmatic image encryption techniques have been investigated from the confidentiality perspective of color photos[1]. Color image encryption techniques play a key role in preserving the privacy of the sensitive image data of the strikers globally through the internet[2]. There are several methods that are used to maintain the consistency of the images during decryption in order to retain the quality of the colored images.

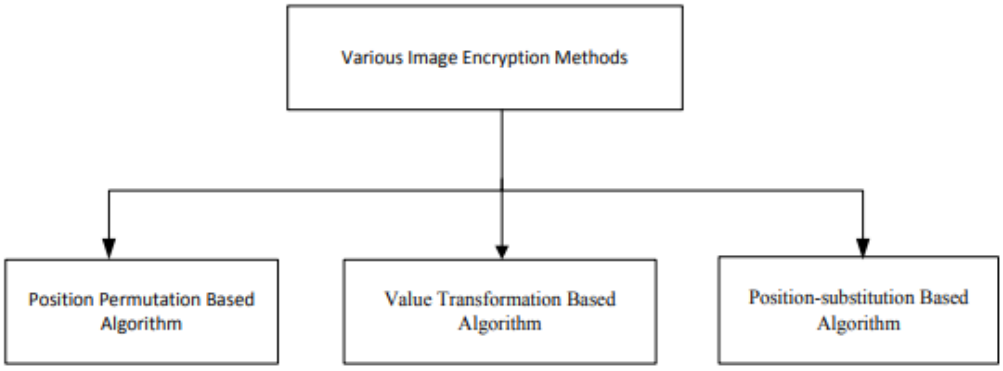

Fig.1 Illustrates various image encryption methods[3].

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

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

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

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

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

In order to lose the picture data through the communication channel during the transmission, there are some parameters that ensure the vulnerability of the various color image formats against the different attacks from the strikers. The Amount of Pixel Change Rate (NPCR) and the Strength Shifting Unified Average (UACI). The formulas for the NPCR and UACI calculation for a colored picture are given in below[4].

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

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

Another critical constraint is the correlation coefficient to ensure that the encryption algorithm is very accurate. The expression is given below[5].

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

Where $C(x,y), D(x)$ and $D(y)$ may be evaluated by utilizing the following equations[6].

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

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

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

II. LITERATURE REVIEW

Another novel image encryption algorithm based on chaos and a line map was investigated by Gao et al. In the age of big data, data protection boundaries have become increasingly blurred. Our privacy defense is undergoing a new round of research. In particular, multimedia images of big data often contain some privacy secrets or data. How to ensure security and authorize access to sensitive data becomes a hot issue of urgency when processing and transmitting image information. In this article, we propose a new algorithm based on the skew tent map for symmetrical image encryption. For encryption of any image size using a new chaos-based line map, the proposed algorithm is ideal[7].

A color imaging cryptosystem based on dynamic DNA encryption and chaos was investigated by Xu et al. This paper presents a color picture cryptosystem based on complicated DNA encryption and confusion. First, the plain color image is decomposed into elements of red, green and blue, and then a simultaneous intra-inter-component permutation mechanism (SCPMDP) based on plain text is applied to shuffle them. Secondly, the recombined permutable components are transformed into a DNA matrix by a DNA encoding law[8].

III. DISCUSSION AND CONCLUSION

After reviewing multifarious research papers, we conclude that there is a problem in the previous algorithms of image encryption and decryption. First of all, the majority of encryption algorithms are rooted on algorithms of scrambling in which pixel exchange occurred. This scheme encrypts the image, but the histogram of an image cannot be changed. So, their performance may not be

good for protection. Some of the approaches are algorithms focused on value transformation. This shifts the pixel value, rendering the image meaningless, but the relationship between pixels still remains after transformation. There is also no encryption algorithm that can pay attention to the principle of both the pixel exchange and the grey level exchange. There are several other problems besides these, such as the total size of keys and the calculation used in the previous algorithm is very high. So the complexity of time is high. The following recommendations can be taken on the basis of the analysis of all the above-mentioned research papers: To secure multimedia content, pixel permutation-based algorithms should be implemented or used. In order to provide the device with high speed and security, more complex and compressed algorithms should be used. Modified versions of different algorithms are used to increase the degree of security.

IV. REFERENCES

[1] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, 2004, doi: 10.1016/j.chaos.2003.12.022.

[2] Y. Wang, K. W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Appl. Soft Comput. J.*, 2011, doi: 10.1016/j.asoc.2009.12.011.

[3] Z. H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Phys. Lett. Sect. A Gen. At. Solid State Phys.*, 2005, doi: 10.1016/j.physleta.2005.08.006.

[4] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, 2012, doi: 10.1016/j.sigpro.2011.10.023.

[5] "A Modified AES Based Algorithm for Image Encryption," *Int. J. Comput. Inf. Eng.*, 2007, doi: 10.5281/zenodo.1334059.

[6] 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.

[7] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Phys. Lett. Sect. A Gen. At. Solid State Phys.*, 2008, doi: 10.1016/j.physleta.2007.07.040.

[8] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.*, 2016, doi: 10.1016/j.optlaseng.2015.09.007.