Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 9, September 2019

A REVIEW PAPER ON MULTIPLE-PICTURE ENCRYPTION ALGORITHMS

Shilpa K S
Faculty of Engineering and Technology,
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: shilpa@jainuniversity.ac.in

Abstract

This paper presents a new multiple-image encryption (MIE) algorithm based on the mixed image element and permutation, which can simultaneously encrypt any number of images, to enhance encryption efficiency and facilitate the secure transmission of multiple digital images by defining the pure image element and mixed image element. First, segment the original images into pure image elements; second, scramble all the pure image elements with the permutation produced by the piecewise linear chaotic map (PWLCM) system; third, combine mixed image elements into scrambled images; last, diffuse the content of mixed image elements by performing the exclusive OR (XOR) operation between scrambled images and the chaotic image g There is a comparison of two related algorithms. Experimental results and algorithm analyses show that the proposed MIE algorithm is very simple and efficient, which is suitable for practical image encryption.

Keywords: *Camera, Encryption, Image, Internet, Picture, Data Protection, Guidelines, Digital images.*

I. INTRODUCTION

In many fields, a large number of images are produced, such as military detection, monitoring of natural disasters, traffic monitoring, weather forecasting, electronic government, and personal affairs [1]. Meanwhile, over the past decade, the appearance of all sorts of shooting instruments has accelerated the age of big data [2]. A common single lens reflex camera, for instance, can shoot multiple images per second, and a traffic camera can at least shoot thousands of images per day. Digital images also hold many secrets or a lot of knowledge about privacy in the era of big data.

With the rapid development of computers and the Internet, multimedia security is becoming a challenge for both academic research and industry, especially for image security [3].

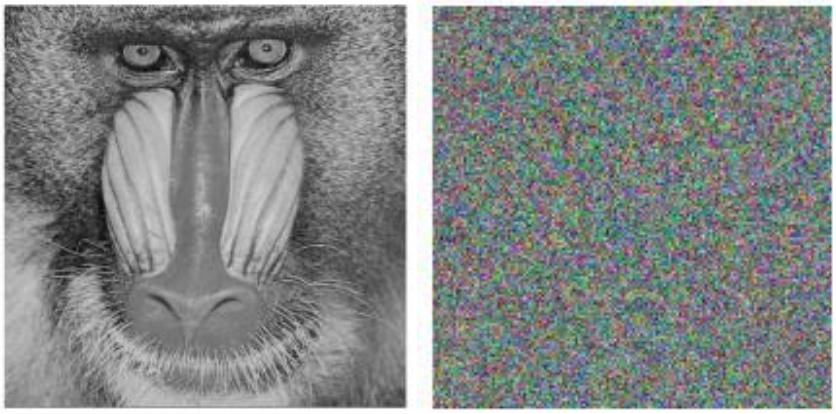

Fig. 1: Illustrates the Original Images and Encrypted Image

ENCRYPTION ALGORITHMS

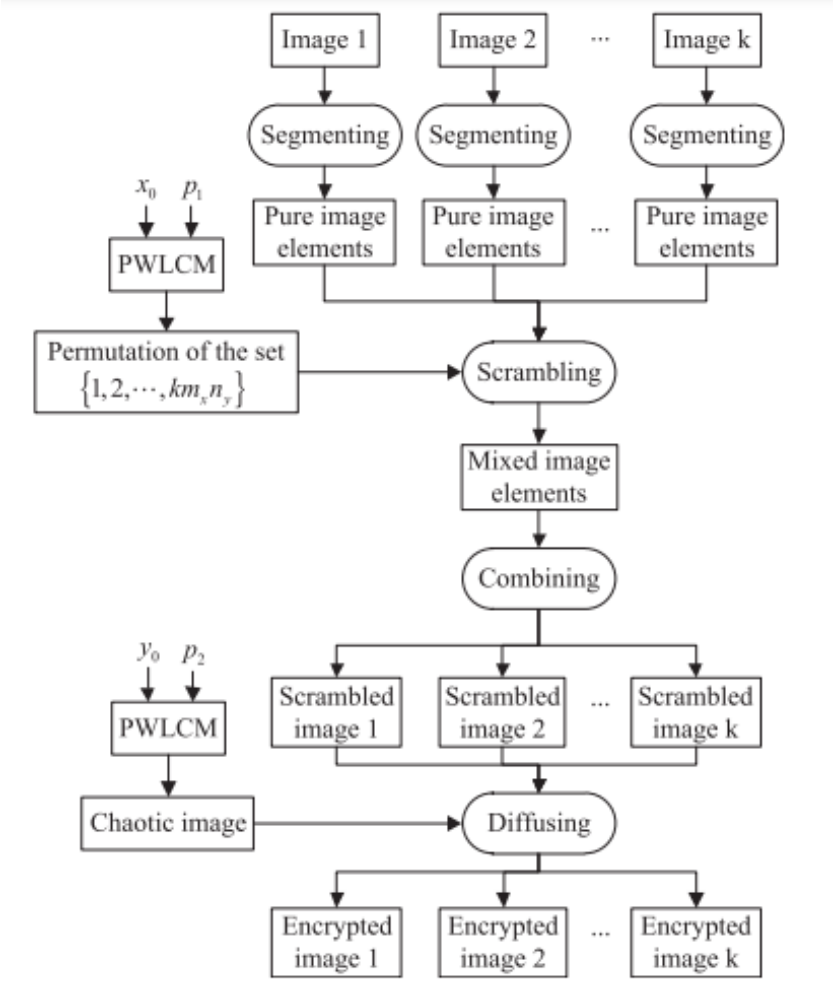

Fig. 2: Illustrates the flow chart for the proposed encryption approach [4]

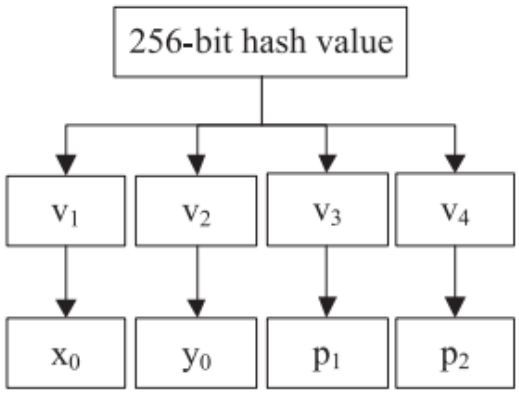

Fig 3: Illustrates the procedure for key generation [5]

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

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

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

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

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

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

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

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

II. LITERATURE REVIEW

A study was conducted on the Chaos-based image encryption algorithm by Chang et al. In this letter, a new image encryption scheme is implemented in which shuffling the positions and changing the grey values of the image pixels are combined to confuse the relationship between cipher-image and plain-image. Firstly, the Arnold cat map is used to shuffle the image pixels' spatial-domain positions. The discrete output signal of the Chen chaotic device is then preprocessed to be adequate for grayscale image encryption, and the shuffled image is encrypted by the preprocessed signal pixel by pixel. The experimental results show that the key space is large

enough to withstand the attack of brute force and there is a random-like behavior in the distribution of the grey values of the encrypted image [6].

III. DISCUSSION AND CONCLUSION

This paper proposes a MIE algorithm that can encrypt k images at once, based on the mixed image element and permutation, where k can be designated by the consumer. This paper explains the concepts of pure and mixed image elements and, with the chaotic system, designs a method to produce a permutation and chaotic image. Comparison tests are performed with the transform algorithm of Arnold and the algorithm of Tang. For the latest algorithm, to encrypt 4 original images of the same size 512 × 512, the encryption processing time is only 0.7103 s. Experimental results and algorithm analysis show that the new algorithm, which is suitable for realistic image encryption, is very successful and stable. For example, military, aerospace, national security, electronic government, personal affairs, and other fields may apply the new algorithm.

IV. REFERENCES

[1] 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.

[2] S. Kumar, A. Gupta, and A. Arya, *Triple Frequency S-Shaped Circularly Polarized Microstrip Antenna with Small Frequency-Ratio*. International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)/ISSN(Online): 2320-9801, 2016.

[3] E. N. Kumar and E. S. Kumar, "A Simple and Robust EVH Algorithm for Modern Mobile Heterogeneous Networks- A MATLAB Approach," 2013.

[4] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Opt. Lasers Eng.*, 2014, doi: 10.1016/j.optlaseng.2013.12.003.

[5] X. Zhang and W. Chen, "A new chaotic algorithm for image encryption," 2008, doi: 10.1109/ICALIP.2008.4590187.

[6] C. C. Chang, M. S. Hwang, and T. S. Chen, "A new encryption algorithm for image cryptosystems," *J. Syst. Softw.*, 2001, doi: 10.1016/S0164-1212(01)00029-2.