IMAGE ENCRYPTION BY USING VARIABLE LENGTH KEY: A STATE OF THE ART SURVEY

Ravi Kant
Faculty of Engineering and Technology,
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: ravi.kant@jainuniversity.ac.in.

Abstract

Centered on a modified tent map, we propose a new image encryption algorithm with a variable length running key. This modified tent map will produce a uniform pseudo-random number sequence for distribution. In the proposed image encryption, we use the variable length running key strategy that extends key value space, the one-time running key strategy that is immune to known/chosen plaintext attack, the cypher disruption strategy that minimizes the dynamic degradation of digital chaos. Simulations have been carried out and the findings show our system's good survival potential. In every area of human life and development, the advancement of digital and multimedia techniques makes imaging devices deeply involved. In the field of life, to catch beautiful moments, people use handheld terminals such as mobile phones, personal digital assistants (PDAs), and other portable devices. People use ultrasonic, computed tomography (CT), magnetic resonance imaging, and positron emission tomography imaging in the field of medical imaging to verify the health of people.

Keywords: *Computed Tomography, Cloud, Encryption, Image, Magnetic imaging, Resonance imaging.*

I. INTRODUCTION

People use an infrared imager to catch the night scene in the security area. In the aviation sector, in meteorological disaster detection, people make use of satellite remote sensing technology and so on [1]. The broad use of these imaging devices results in a vast number of photographs appearing thus facilitating the lives of people. Some related to personal privacy, some involving business secrets, some involving national security, are among these photos. Generally, these images are stored on a computer or in a cloud [2]. Therefore, current systems naturally strive to deter opponents from theft of image data. However, experience shows that the intruder is still able to find ways to break in and steal data. Therefore, how data-centered approaches secure those data is a major challenge facing the industry and the scientific community [3].

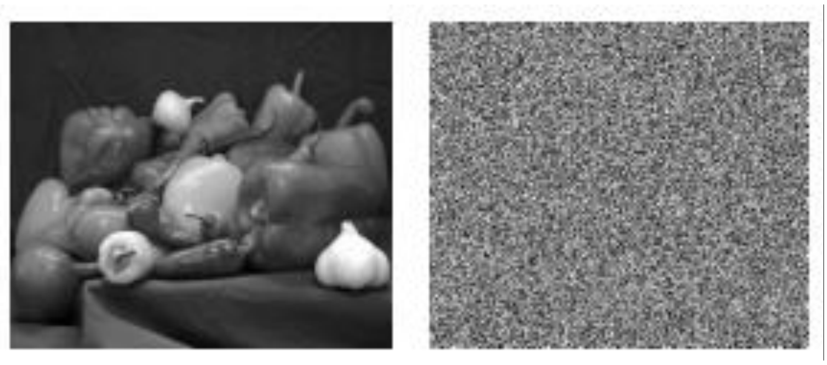

Figure 1: Illustrates the Real Images and Encrypted Image

II. IMAGE ENCRYPTION BY USING VARIABLE LENGTH KEY

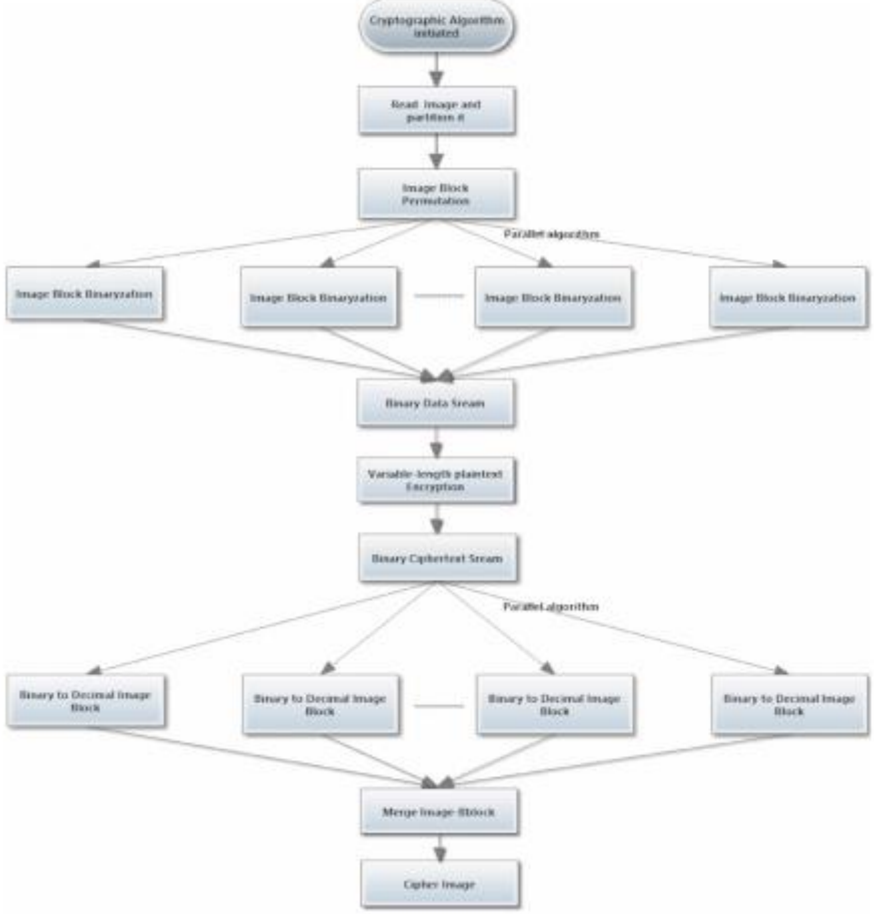

Figure 2: Illustrates the block diagram [4]

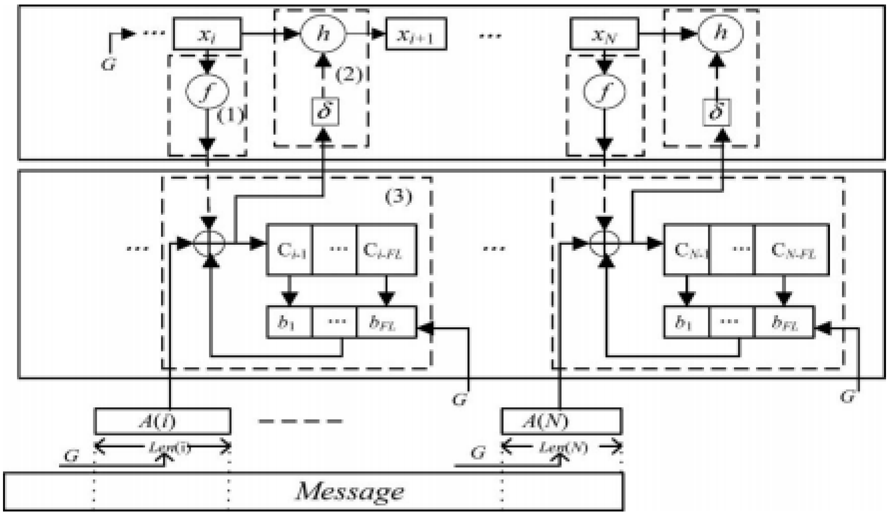

Figure 3: Illustrates the Framework of the core encryption algorithm [5]

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

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

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

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

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

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

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

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

The correlation coefficient is another essential constraint to ensure that how much efficient is the encryption algorithm [6].

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

Where $C(x,y), D(x)$ and $D(y)$ can be evaluated by using the following equations [7].

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

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

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

III. LITERATURE REVIEW

A symmetric image encryption scheme based on 3D chaotic cat maps was suggested by Liu et al. Image encryption differs from that of texts because of certain inherent characteristics of images, such as bulk storage capability and high redundancy, which are typically difficult to handle by traditional methods. Chaos-based encryption has proposed a modern and effective way to deal with the intractable issue of easy and highly secure image encryption, thanks to the extremely desirable properties of mixing and sensitivity to initial conditions and parameters of chaotic maps. In this paper, the two-dimensional chaotic cat map is generalized to 3D for designing a real-time secure symmetric encryption scheme [8].

IV. DISCUSSION AND CONCLUSION

The security benefits are a driving factor in the process of developing the image encryption algorithm, often with pace as a secondary consideration. We propose an image encryption scheme with a variable length running key that uses a modified tent map, based on this concept. The uniform distribution chaotic sequence has improved the security of the cryptosystem due to the given new function in the modified tent map dynamic. Of course, if PDF is known, the modified tent map can also be replaced by some other chaotic map. A chaos-based picture cryptosystem is key to the encryption policy. The degradation of digital chaos is effectively minimized by the disturbing chaotic sequence of cypher text. The key space is expanded by a variable length running key. A one-time key is immune to a known/selected plaintext attack.

V. REFERENCES

[1] J. Li, J. Sheng Li, Y. Yang Pan, and R. Li, “Compressive optical image encryption,” Sci. Rep., 2015, doi: 10.1038/srep10374.

[2] S. H. Kamali, M. Hedayati, R. Shakerian, and M. Rahmani, “A new modified version of Advanced Encryption Standard based algorithm for image encryption,” 2010, doi: 10.1109/ICEIE.2010.5559902.

[3] S. Li and X. Zheng, “Cryptanalysis of a chaotic image encryption method,” Proc. - IEEE Int. Symp. Circuits Syst., 2002, doi: 10.1109/ISCAS.2002.1011451.

[4] E. Thambiraja, R. G., and R. Umarani, “A Survey on Various Most Common Encryption Techniques,” Int. J. Adv. Res. Comput. Sci. Softw. Eng., 2012.

[5] 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.

[6] S. Hanis and R. Amutha, “Double image compression and encryption scheme using logistic mapped convolution and cellular automata,” Multimed. Tools Appl., 2018, doi: 10.1007/s11042-017-4606-0.

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

[8] S. Liu, C. Guo, and J. T. Sheridan, “Optics & Laser Technology,” Opt. Laser Technol., 2014.