Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 13, December 2019

A REVIEW PAPER ON MULTI—IMAGE ENCRYPTION METHOD

Dr. P. Pradeepa
Associate Professor, Department of EEE, Faculty of Engineering and Technology, Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: p.pradeepa@jainuniversity.ac.in

Abstract

Noise-like images are cypher images that are produced using encryption algorithms, which display a clear indication of encrypted data being present. The noise-like picture lures an opponent to carry out attacks. This paper provides an approach to generating a visually meaningful multiple-image encryption scheme. In the insignificant real data of a host image, multiple cypher image data is embedded. The high-quality output of the proposed approach is expressed by simulation results and security assessments. The proposed framework has a greater ability to embed more images with less distortion to the visual perspective of the host image in comparison with Bao and Zhou and Kanso and Ghebleh visually significant image encryption schemes.

Keywords: *Encryption, Image, Internet, Multimedia, Data protection, Safety, Compression.*

I. INTRODUCTION

The advent of technology has provided internet users the opportunity to exchange multimedia information (e.g. text, audio, picture, video) with just a fingertip. Any of the information is private and needs protection against unauthorized access. By converting the plain data to some unintelligible format, encryption will provide protection to a data process [1]. Another technique is steganography, where information is hidden in host data without giving an eavesdropper any space to detect it. Authors have developed various algorithms to provide the confidential image with protection for storage and transmission through encryption process. One of the strategies commonly studied and implemented by different authors to perform image encryption is the chaotic method [2].

Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 13, December 2019

Figure 1: Illustrates the real and encrypted images [3]

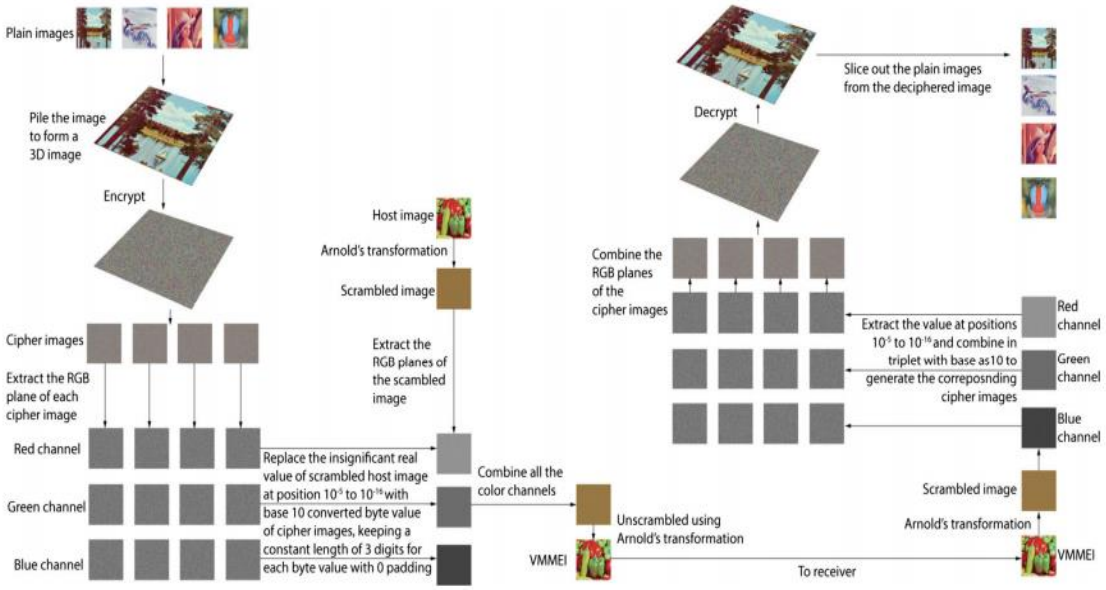

Figure 2: Illustrates the flow diagram of the presented algorithm for safe communication

$$MSE = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W}[P(i,j) - E(i,j)]^2}{W \times H}$$

$$MAE = \frac{1}{W \times H}\sum_{i=1}^{H}\sum_{j=1}^{W}|p(i,j) - E(i,j)|$$

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

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

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

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

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

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

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

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

The correlation coefficient is another essential constraint to ensure that how much efficient is the encryption algorithm [4].

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

Where $C(x,y)$, $D(x)$ and $D(y)$ can be evaluated by using the following equations[5].

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

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

II. LITERATURE REVIEW

Elhoseny et al. proposed a symmetric image encryption scheme based on 3D chaotic cat maps. Due to some inherent characteristics of images, such as bulk data capacity and high redundancy, which are usually hard to manage by conventional methods, image encryption varies from that of texts. Thanks to the extremely desirable properties of mixing and sensitivity to initial conditions and parameters of chaotic maps, Chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of simple and highly protected image encryption. In this paper, for designing a real-time protected symmetric encryption scheme, the two-dimensional chaotic cat map is generalized to 3D [6].

III. DISCUSSION AND CONCLUSION

This paper presents an approach to the generation of a visually meaningful multi-image encryption scheme. Multiple cypher image data is encoded in a scrambled host image's meaningless real data, which is later unscrambled, creating a multiple encrypted image that is visually meaningful. Comparison with current visually meaningful encryption schemes indicates that with almost no degradation of the host image, the proposed scheme has a better

capacity to insert more data. For Bao and Zhou, and Kanso and Ghebleh, the PSNR and SSIM values of the embedded host image (real data) are (27.1831, 0.9790) and (34.1624, 0.9949), respectively, while the proposed PSNR and SSIM method values are (86.6209, 0.9999). Against various classical attacks and other attacks such as salt and pepper noise attack and occlusion attack, the proposed scheme is robust. The proposed scheme can be used without enticing the attacker to transmit several cypher images using a host image, which is usually the case in a noise-like image. In the future, before performing encryption operations, the number of cypher images embedded in the host image can be increased using a compression technique on the plain images.

IV. REFERENCES

[1] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez, and O. R. Acosta Del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos," Signal Processing, 2015, doi: 10.1016/j.sigpro.2014.10.033.

[2] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Image and Vision Computing, 2006, doi: 10.1016/j.imavis.2006.02.021.

[3] S. Liu, C. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," Optics and Laser Technology, 2014, doi: 10.1016/j.optlastec.2013.05.023.

[4] 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.

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

[6] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure Medical Data Transmission Model for IoT-Based Healthcare Systems," IEEE Access, 2018, doi: 10.1109/ACCESS.2018.2817615