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

A REVIEW PAPER ON ENCRYPTION OF PICTURE IN WAVELET DOMAIN

Arun N
Faculty of Engineering and Technology, Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email ID: n.arun@jainuniversity.ac.in.

Abstract

A novel symmetric multiple image encryption algorithm is suggested in this paper. The device takes advantage of the characteristics of discrete wavelet transformation, finite ridgelet transformation, and chaotic maps to achieve a single encrypted image that secretly contains the original image information that is totally distorted and meaningless. The four original images are first transformed into the wavelet domain, followed by their HH bands' finite ridgelet transformations, to get two transformed matrices combined. This results in a final encrypted image on the rotation of pixel values using chaotic key image, mixing and then their shuffling using random sequences. To produce the chaotic main image and shuffling sequences, respectively, the piece-wise linear chaotic map and 2D gingerbreadman chaotic map are used. For a casual observer, the encrypted image is extremely skewed and without significance. The mean square error is less than 0.004 between the pairs of decrypted and original images. In addition, the experimental results and simulation analysis indicate that the low correlation factor, high key sensitivity and large key space have the advantage of the scheme..

Keywords: *Encryption, Image, Image Encryption, Video, Gingerbreadman, Ridgelet*

I. INTRODUCTION

In the area of networks, technical developments have made digital media information security, such as images, audio and video, more complex and demanding. The multimedia images in different applications are the most commonly and widely used multimedia data. Via the Internet and wired/wireless networks, sensitive multimedia images are transmitted or exchanged. The methods are used to encrypt images before transmission in order to safeguard and avoid the multimedia images sent over the attack-prone networks against the attack of an attacker [1]. The need for reliable and standardized methods of image encryption is continually increasing. Traditional encryption algorithms such as Data Encryption Standard, Advanced Encryption Standard, and Advanced Encryption Standard to satisfy the safety and

confidentiality criteria of multimedia images with the intrinsic features of bulk data capacity and high data redundancy [2].

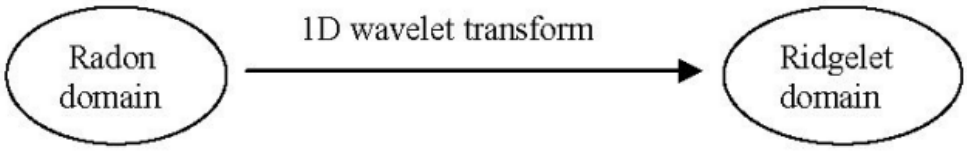

Figure 1: Illustrates the single level and two level decomposition [3]

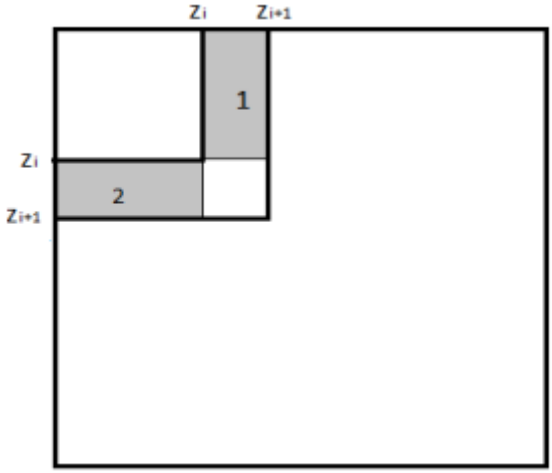

Figure 2: Illustrates the pixels Block 1 and 2 rendering to Z (i) and Z (i) [3]

Figure 3: Illustrates the real and encrypted images [4]

Figure 1: Illustrates the single level and two level decomposition. Figure 2: Illustrates the pixels Block 1 and 2 rendering to Z (i) and Z (i). Figure 3: Illustrates the real and encrypted images [5].

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

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

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

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

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

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

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

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

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

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

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

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

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

II. LITERATURE REVIEW

An analysis was carried out by Ji et al on various watermarking algorithms based on chaotic sequences. In the various phases of printing, sale and use, multiple digital watermarking techniques will solve the issues of multiple copyright claims and hold traces of digital goods. A multiple digital algorithm for watermarking based on chaotic sequences is suggested in this paper. There are the benefits of huge, high security, and weakest correlation in the chaotic sequences. Through 1-D chaotic maps, which are determined by various initial conditions and parameters, massive and independent digital watermark signals are created [4].

III. DISCUSSION AND CONCLUSION

A multiple image encryption algorithm for providing protection before transmitting multiple images over open networks is proposed in this paper. The proposed algorithm makes use of

discrete wavelet transformation characteristics, finite ridgelet transformation, and chaotic maps. The estimated wavelet coefficients of four images are combined to encrypt the original images' information value. The encryption method involves circular rotation based on chaotic-key-image; ridgelet transforms mixing based on pixel values and their random relocation using another chaotic map. Experimental and simulation tests demonstrate that the proposed encryption algorithm meets the security criteria of a successful form of multiple image encryption. This results in a low coefficient of correlation, high key sensitivity, large key space and a high degree of deviation from the original picture (s). In addition, the mean square error is very negligible between the decrypted and original image(s).

IV. REFERENCES

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

[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] A. Jain, M. Ahmad, and V. Khare, "A ridgelet based symmetric multiple image encryption in wavelet domain using chaotic key image," 2012, doi: 10.1007/978-3-642-32112-2_17.

[4] Z. Ji, W. Xiao, and J. Zhang, "Multiple watermarking algorithm based on chaotic sequences," 2003, doi: 10.1117/12.453509.

[5] J. Lang, "Color image encryption based on color blend and chaos permutation in the reality-preserving multiple-parameter fractional Fourier transform domain," Opt. Commun., 2015, doi: 10.1016/j.optcom.2014.10.049.

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

[7] Y. P. Zhang, Z. J. Zhai, W. Liu, X. Nie, S. P. Cao, and W. Di Dai, "Digital image encryption algorithm based on chaos and improved DES," 2009, doi: 10.1109/ICSMC.2009.5346839.