Borneo Journal of Sciences & Technology, 4(1): 51-55
DOI: http://doi.org/10.3570/bjost.2022.4.1-08
e-ISSN: 2672-7439
© 2018, UTS Publisher.
Submitted: 16th November 2021 Accepted: 20th December 2021 Published: 31st January 2022

Development of Bit-level Scrambling Encryption Algorithm for Radio Telescope Imageries

[1,3]Kung Chuang Ting, [1]Kim Ho Yeap, [1]Peh Chiong Teh, [2]Koon Chun Lai and [3]Florence Francis-Lothai

[1]Faculty of Engineering and Green Technology, Universiti Tunku Abdul Rahman, Kampar 31900, Perak, Malaysia
[2] Academe Incubator, 203, Beijing 3rd, Qingcheng, Qingyuan, Guangdong, China
[3]Faculty of Science and Technology, *i*-CATS University College, Kuching 93350, Sarawak, Malaysia

Abstract: Image security is a main issue in image transmission through the network especially with the involvement of sensitive data. Addressing to this issue, image encryption is one of the effective ways to protect the originality and security of the image to be transmitted. Thus, in this paper, we present the bit-level scrambling algorithm for radio telescope imageries using Random Generation Number method. Two types of scrambling algorithm are studied, namely Level I and Level II. The first algorithm scrambles the position between layers of bit-plane, whereas the latter scrambles randomly between bits in each of the bit-plane. We show that, by evaluating the stability and scrambling degree, Level II scrambling algorithm is much reliable in scrambling the radio telescope images used in the present study. The outcome of this study is evaluated based on the measurement of the image scrambling degree. The average between the highest and lowest value of the scrambling degree obtained are 0.845 and 0.865, and the gaps are 0.09 and 0.05, for Level I and Level II scrambling, respectively. Compared to Arnold transformation method, it has been shown that the proposed algorithm provides better performance in image encryption.

Keywords: bit-planes, radio telescope, scrambling, encryption, bit-level

INTRODUCTION

Digital image security issues increased rapidly nowadays due to the fast development of telecommunications. More digital images in various fields of medical, military, and astronomy are transmitted throughout the network. Therefore, digital image security methodologies are demanded in the market to protect the security of the image [1]. Many researches had been conducted for image encryption to improve the security of digital image. Encryption is simply coding or protecting the intelligible element of an image so as to turn it into hardly recognizable or decodable by anyone except the recipient [2].

Oyinloye and Gbolagade proposed a scrambling method utilizing the neighbourhood pixels [3]. Image scrambling is a method by scrambling the value in each pixel location of digital images in such a way that it is converted to become an unrecognizable image [4]. Due to the benefits of scrambling methodologies, some encryption algorithms had been studied in [5-7]. Arnold transformation is one of the most typical methodologies among all image scrambling methods [8]. However, this typical image encryption algorithm may not be applicable to the informative fine features found in medical, military, and astronomy images [9]. This is due to the fact that these types of images are larger and contain more information, and the Arnold transformation method only applies to square area of an image.

With the increasing number of research on space exploration, more telescope imageries are being transmitted. Hence, a reliable image encryption method is required to secure these images from unauthorized accesses. This paper proposes a 2-level scrambling encryption algorithm with bit-level decomposition. Radio telescope imageries are used as the test images in the analysis. It is targeted that the proposed encryption algorithm would resist attacks in the transmission of those imageries that contain sensitive information.

RELEVANT INFORMATION

In this section, the image formation from the use of radio telescope, bit-level image decomposition process and the scrambling encryption algorithms are discussed.

Radio Telescope Imagery

In general, radio telescope is made up of a parabolic reflector (primary) antenna and a hyperboloid (secondary) reflector [10]. It receives radio waves from celestial objects such as pulsars or active galaxies, typically by means of the primary antenna. The

Corresponding Author: Kung Chuang Ting. Universiti Tunku Abdul Rahman (UTAR) and *i*-CAT, email: tingkc@ppks.edu.my

incoming waves are then converted into electrical signals inside the receiver and processed to display the spectral and spatial information carried by the signal [11].

Bit-level Decomposition

Image decomposition process refers to the extraction of eight bit-planes from digital image. A digital image is constructed with *M* rows and *N* columns of pixels as descripted in equation 1. For a grayscale image, each pixel value is classified into four most significant bits (MSB) and four least significant bits (LSB) [12]. As in equation 2, the i^{th} bit-plane consists of all the i^{th} bits of binary representation of each pixel [13]. Higher bit-planes contain more significant visual information, whereas lower bit-planes contain more detail information. Figure 1(a) shows a grayscale image of Lena. This image is then decomposed into its eight layers of bit-plane using equation 2. The decomposed image is depicted in Figure 1(b) showing the MSB and LSB.

$$f(x,y) = \begin{bmatrix} f(0,0) & \cdots & f(0,N-1) \\ \vdots & \ddots & \vdots \\ f(M-1,0) & \cdots & f(M-1,N-1) \end{bmatrix} \quad (1)$$

$$f_{bit-plane\ i} = R\left[\frac{1}{2} floor\left(\frac{1}{2^i}[f(x,y)]\right)\right] \quad (2)$$

Scrambling Encryption Algorithm

Figure 2 defines our proposed image scrambling methodology in this study. First, a digital image is decomposed into 8 layers of bit-planes, followed by the level I of scrambling that involves random scrambling between bit planes. Then, repeat the random scrambling process by applying the Random Number Generation method [14] into level II which is scrambling on bits in each of the bit-plane.

Scrambling methodology is to change the position of each pixel in the original image without changing the value to grey level. It can be used to encrypt and decrypt the grey level image in any size based on random number generation algorithm, as explained by the following steps:

Encryption:
Step 1: Define image size as *x*(*i*), *y*(*j*)
Step 2: Start with the pixel where *i*, *j*=1, 2, …, *q*
Step 3: Assign non-repetitive random number for row (*m*) and for column (*n*), where *m*, $n \leq q$
Step 4: Generate new pixel position by replacing *i*, *j* with *m*, *n*
Step 5: Repeat the scrambling process for *k* times and record the sequence

Decryption:
Step 1: Apply the reverse sequence for the encrypted image
Step 2: Repeat the process for *k* times

RESULTS AND DISCUSSION

Figure 3 illustrates a grayscale image before and after the proposed scrambling methods. The image scrambling can be evaluated in term of scrambling degree (see equation 3) which is suggested by [15].

$$S(A) = \frac{\sum_{k=1}^{k}\left(\mu(k) \times \frac{H(k)}{H}\right)}{\sum_{k=1}^{k}\mu(k)} \quad (3)$$

where *H* are the entropy of whole transformed image, *H(k)* is the entropy of k^{th} block of transformed image, *μ(k)* is the average of differences between all two connective pixels block *k* of transformed image.

In order to assess the efficiency of the proposed scrambling method, Arnold transform was included in the evaluation for comparison. Arnold transform scrambles the intensity values of an image which results to an image in unrecognizable form. As it can be seen from Table 1, scrambling degree for Arnold transform ranges from 0.78 to 0.93. This range is determined by calculating the gap between the highest and the lowest value. Higher value of scrambling degree implies the pixel has been moved further away [14]. Although Arnold transform is able to provide higher degree of 0.93, it meanwhile gives low value of 0.78, making this scrambling method rather volatile. On the other hand, the relatively narrow range of degree for both Level I and Level II scrambling methods, which is 0.80 – 0.89 and 0.84 – 0.89, respectively, is preferable for better scrambling stability. When Level I scrambling was applied, the gap significantly reduced to 0.09 when compared to 0.15 using Arnold transform. This gap further reduced to 0.05 after applying the Level II scrambling. It is apparent that the second scrambling method provides better scrambling degree with lower gap value.

Figure 1: (a) Grayscale image, (b) 8 layers of bit plane from grayscale image

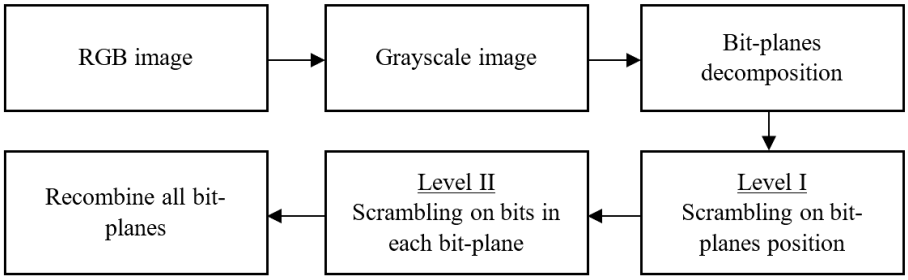

Figure 2: Block diagram of image scrambling

Figure 3: (a) Grayscale image, (b) After two levels scrambling algorithm

Table 1: Scrambling degree

Method	Range	Gap between highest and lowest	Average between highest and lowest
Arnold Transform	0.78 -0.93	0.15	0.855
Level 1 Scrambling	0.80-0.89	0.09	0.845
Level II Scrambling	0.84-0.89	0.05	0.865

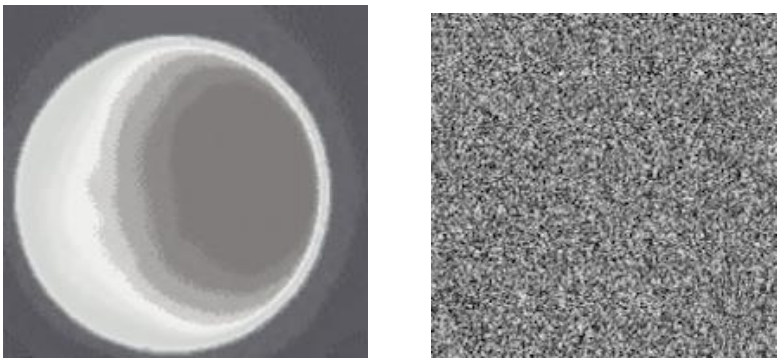

Figure 4: (a) Telescope image of moon, (b) After scrambling algorithm

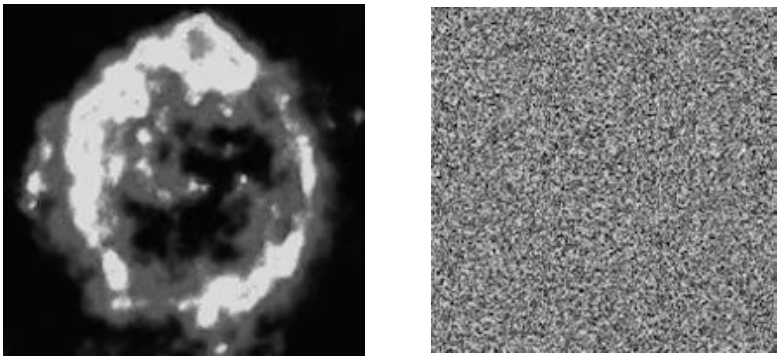

Figure 5: (a) Telescope image of supernova, (b) After scrambling algorithm

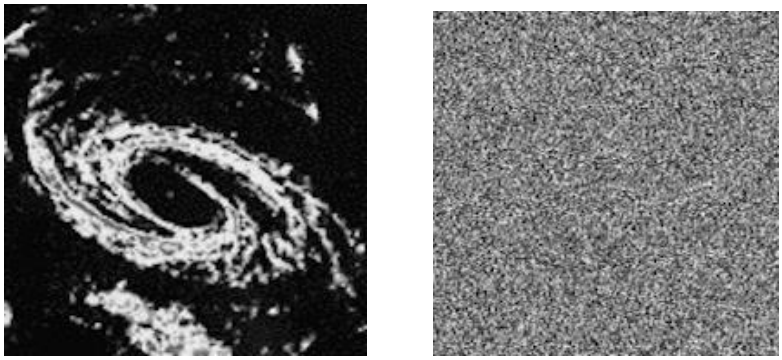

Figure 6: (a) Telescope image of galaxy, (b) After scrambling algorithm

Table 2: Comparison

Telescope image	Level II	
	Gap between highest and lowest	Average between highest and lowest
Moon	0.04	0.860
Supernova	0.05	0.850
Galaxy	0.05	0.840

To further study the encryption algorithm on the radio telescope imageries, three images are selected for evaluation as shown in Figs. 4-6. As it can be seen from Fig. 4-6, the gap between highest and lowest value are between 0.04 and 0.05 after applying Level II scrambling method. These findings are similar to that tabulated in Table 1 in which Level II scrambling method achieved better encryption. The average between highest and lowest value, ranges between 0.840 and 0.860, suggests that 2-levels scrambling is reliable in the encrypted process with low gap between highest and lowest value of the scrambling degree for the transmission of the digital telemetry images used in this study.

CONCLUSION

Two types of bit-level scrambling methodology, namely Level I scrambling (by scrambling position of bit-plane) and Level II scrambling (by scrambling position of bits in each of the bit-plane), have been implemented in this study. The outcome is evaluated based on the measurement of the scrambling degree and comparison with Arnold transformation method. The results showed that the proposed algorithm has ability to provide better performance when compared to Arnold transformation in terms of the gap value and average between higher and lowest value in the scrambling degree ranges. To further examine the proposed methodology, more tests e.g., correlation analysis, entropy analysis and robustness test will be carried out and discussed in our future reports.

ACKNOWLEDGEMENT

We would like to show our gratitude to *i*-CATS University College for supporting the publication financially.

REFERENCES

[1] Ghadirli H.M., Nodehi A., and Enayatifar R. 2019. An overview of encryption algorithms in color images. Signal Processing (164), 163-185.

[2] Wang T., and Wang M-h. 2020. Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding. Optics and Laser Technology (13).

[3] Oyinloye D.P., and Gbolagade K.A. 2018. An improved image scrambling algorithm using {2n - 1, 2n, 2n +1}. Computing & Information Systems (22), 1-7.

[4] Radu B., Cristina D.A., and Iustin P, Cristina, F. 2014. A new fast chaos-based image scrambling algorithm. 10th international Conference on Communications 1-4.

[5] Abhimanyu K.K.P., and Bibhudendra A. (2020). A secure block operation based bit-plane image encryption using chaotic maps. First International Conference on Power, Control and Computing Technologies, 411-416.

[6] Zhang H., and Cai R. 2010. Image encryption algorithm based on bit-plane scrambling and multiple chaotic systems combination. International Conference on Intelligent Computing and Integrated Systems, 113-117.

[7] Zhou R.G., Sun Y.J., Fan and P. 2015. Quantum image Gray-code and bit-plane scrambling. Quantum Information Processing (14), 1717-1734.

[8] Wang D., Chang C., Liu Y, Song G., and Liu L. 2015. Digital image scrambling algorithm based on Chaotic sequence and decomposition and recombination of pixel values. Journal of Network Security (17), 322-327.

[9] Dai Y. Wang, H. and Wang Y. 2016. Chaotic medical image encryption algorithm based on bit-plane decomposition. Biomedical Image Analysis (30).

[10] Yeap K.H. et. al., 2016. Analysis of reflector antennas in radio telescopes. Advanced Electromagnetics (5), 32-38.

[11] Yeap K.H. et. al. 2016.Abalysis of offset antennas in radio telescopes. International Journal on Advanced Science, Engineering and Information Technology (6), 997-1004.

[12] Liu X. Song Y. Jiang G.P. (2019). Hierarchical bit-level image encryption based on Chaotic map and Feistel network. International Journal of Bifurcation and Chaos (19).

[13] David B.L.B., Ting K.C., Wang Y.C. 2009. Novel face recognition approach using bit-level information and dummy blank images in feedforward neural network. Applications of Soft Computing, 483-490.

[14] Makera M.A., and Dena, R.A. 2015. Simple image scrambling algorithm based on random numbers generation. International Journal of Advanced Research in Computer Science and Software Engineering (5), 434-438.