Journal of Advanced Research in Signal Processing and Applications
Volume 3, Issue 2 - 2021, Pg. No. 1-5
Peer Reviewed Journal

Article

Design of Encryption Algorithm in Combined Spatial and Frequency Domains for Telescope Grayscale and Bayer Images

Ting KC[1], Yeap KH[1], Teh PC[1], Lai KC[2], Florence Francis-Lothai[3]

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

I N F O

Corresponding Author:
Ting KC, Faculty of Engineering and Green Technology, Universiti Tunku Abdul Rahman Perak.
E-mail Id:
tkchuang2000@hotmail.com
How to cite this article:
Ting KC, Yeap KH, Teh PC et al. Design of Encryption Algorithm in Combined Spatial and Frequency Domains for Telescope Grayscale and Bayer Images. *J Adv Res Sig Proc Appl* 2021; 3(2): 1-5.

Date of Submission: 2021-11-05
Date of Acceptance: 2021-12-07

A B S T R A C T

Digital images transmission has grown dramatically over the past years in various applications, for instance, transmission of telescope images. In this research, a novel encryption algorithm that combines both spatial and frequency domains is studied. Telescope images in grayscale and Bayer array are applied in our algorithm. Effectiveness of the proposed algorithm has been analyzed in terms of several key analyses, such as histogram distribution, Number of Pixel Changing Rate (NPCR), Unified Average Changing Intensity (UACI), Peak Signal to Noise Ratio (PSNR), Information Entropy and Structural Similarity Index (SSIM). Empirical results suggest that our proposed algorithm can be practically applied to encrypt both grayscale and Bayer telescope images.

Keywords: Encryption, Bit Planes, Bayer, Image Security

Introduction

Over the past decades, the amount of digital images transmission has grown dramatically. This includes the transmission of telescope images. As digital image contains sensitive information, it is crucial to encrypt the image so as to protect it from being accessed by unauthorized users. In recent years, various methods of digital image encryption have been introduced, e.g. Latin squares,[1,2] skew tent map,[3] DNA sequence[4,5] and ciphertext feedback.[7] A symmetric-key Latin square image with probabilistic encryption was introduced in.[1] It was an improved method of traditional Latin square. Likewise, a self- orthogonal Latin square was proposed in[2] that uses 2D map for image permutation. In another approach, pixel combination was applied to encrypt the red, green and blue components of an image.[3] Skew tent map and hyper chaotic system of 6th-order CNN, on the other hand, was used to encrypt the pixel value of the image. A few researches of image encryption that based on DNA sequence were also conducted. Wei et al.[4] proposed a color image encryption algorithm based on DNA sequence that converts original image into R, G, and B matrices, and applied a similar method in,[3] i.e., hyper chaotic maps, to scramble the DNA elements' locations. The encrypted image was constructed based on the decoded DNA sequence and R, G, B channels combination.

Zhang et al.[7] presented a gray image-based encryption method that uses a single round permutation-diffusion chaotic cipher. Temp-value feedback mechanisms were introduced to defend against the known attacks on the image. A secret key was then generated from the diffusion of the employed plaintext or ciphertext feedback. Many of the proposed methods showing a promising level of

security, however, there are certain concerns that need to be addressed. Firstly, the suitability of the Latin square in image encryption is uncertain even though it was reported to have some fine characteristics. Also, a well-equipped and pricey laboratory is required to conduct the experiment for DNA cryptography, making it as not as a great option than others. Meanwhile, security level of the method proposed in is not confirmed even though it has a better encryption effect when compared to.[5]

In this paper, we propose a novel encryption algorithm that combines spatial and frequency domains to improve the encryption. Two types of telescope images were selected in the experiments, i.e. grayscale and Bayer images. Fourier Transform (FT), bit levels decomposition and scrambling methods were applied in the algorithm. Effectiveness of the proposed algorithm was then analyzed on several key indicators namely histogram distribution, Number of Pixel Changing Rate (NPCR), Unified Average Changing Intensity (UACI), Peak Signal to Noise Ratio (PSNR), information entropy and Structural Similarity Index (SSIM). The experimental results demonstrate that the proposed algorithm has achieved good encryption effect.

Relevant Information

Radio Telescope Images

Ground radio telescope such as Atacama Large Millimeter/submillimeter Array (ALMA) receives signal emission from celestial objects such as stars, pulsars or active galaxies.[8] The incoming waves are then converted into electrical signals inside the receiver and processed into electrical signals for displaying the spatial information carried by signal.[9] Figure 1, shows the original RGB radio telescope images.

Figure 1.Original RGB Images

Grayscale Image

Images in RGB color model consists of three component images, commonly said Red, Green and Blue components.[10] Based on the model in Figure 2, these RGB images can be converted into Grayscale images following equation (1).

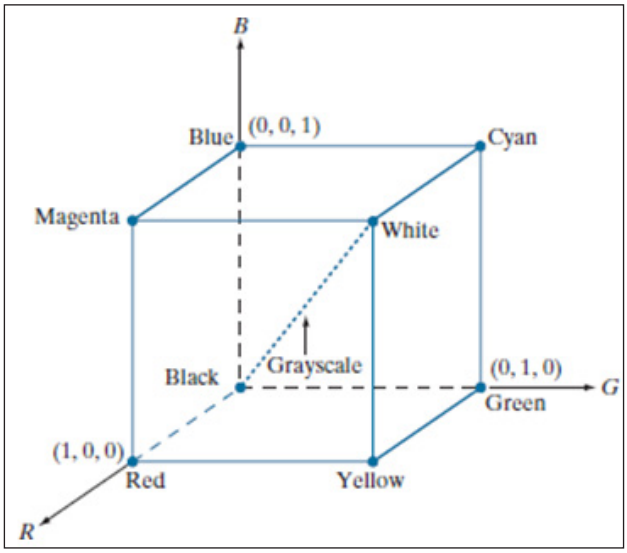

Figure 2.RGB Color Model

$$Grayscale = \frac{(R + G + B)}{3} \quad (1)$$

Bayer Image

A digital color image has three components R, G and B, where R represents red, G represents green and B represents blue. A Bayer image is a filtered array of color in which three color components are filtered and arranged on a grid of photosensors. The pattern of a Bayer image consists of 50% green, 25% red and 25% blue components from original RGB image. Figure 3, shows the RGB image and corresponding Bayer image.

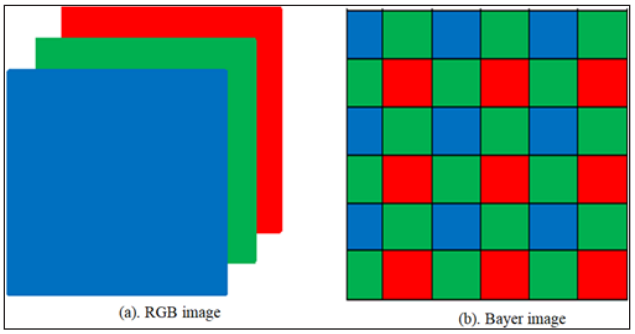

Figure 3.RGB and Corresponding Bayer Image

Bit Plane

Digital image decomposition is the process of extraction of eight bit-planes from any grayscale image. A digital image is constructed with M rows and N columns of pixels as

descripted in equation (2). For a grayscale image, each pixel value is classified into four Most Significant Bits (MSB) and four least significant bits (LSB).[11] The i-th bit-plane consists of all the i-th bits of binary representation of each pixel.[12]

$$(x,y) = \begin{bmatrix} f(0,0) & \cdots & f(0,N-1) \\ \vdots & \ddots & \vdots \\ f(M-1,0) & \cdots & f(M-1,N-1) \end{bmatrix} \quad (2)$$

$$f_{bit\_plane\ i} = R\left[\frac{1}{2} floor\left(\frac{1}{2^i} | f(x,y) |\right)\right] \quad (3)$$

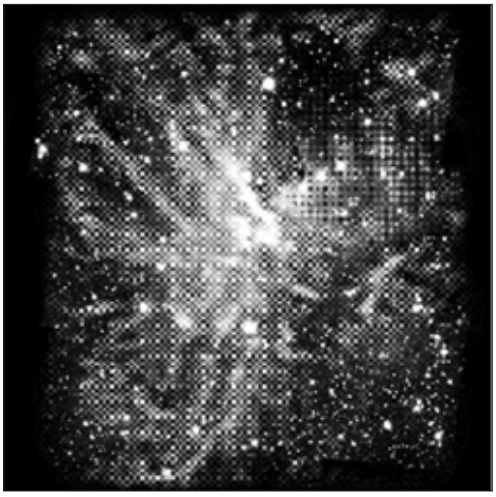

Figure 4.Bayer Image

Fourier Transfrom

The FT process the decompose process of an image into a sum of elementary signals. It has the property of being eased to implement and observe.[13] The discrete Fourier Transform (DFT) of an image f (m, n) of size M x N is defined.[14]

Note that modules in the first and second quadrants are equal to the coefficient in third and fourth quadrants, respectively, due to the Hermitian symmetry properties of Fast Fourier Transform (FFT).

Proposed System

In this paper, a combined spatial and frequency domains algorithm was proposed on grayscale and Bayer images. It is worth noting that FT is for frequency domain, meanwhile bit levels decomposition for spatial domain. Figure 4, shows an RGB image was converted into grayscale or Bayer image before FT. Then, grayscale or Bayer image were decomposed into eight layers of bit-planes, namely bit-plane 0 to bit-plane 7. Two levels of scrambling algorithm were applied: the first level scrambling was on the bit-plane position. Whereas, second level scrambling was applied whereby the value of the pixels in each bit-plane was randomly scrambled and restructured with random position to the bit-planes position. New grayscale image was thus re-formed by 8 bit-planes. The scrambling methodology is commonly utilized to exchange position of pixels without changing the value of pixels. It can be used to encrypt and decrypt the grayscale image in any size on random number generation algorithm.

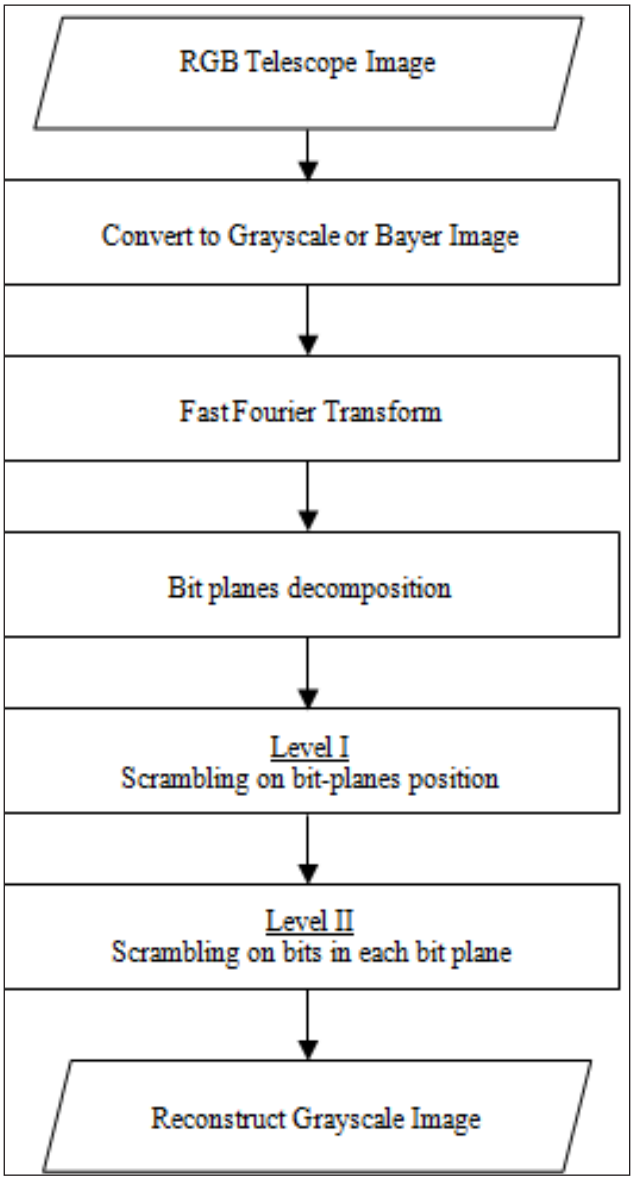

Figure 5.Proposed System

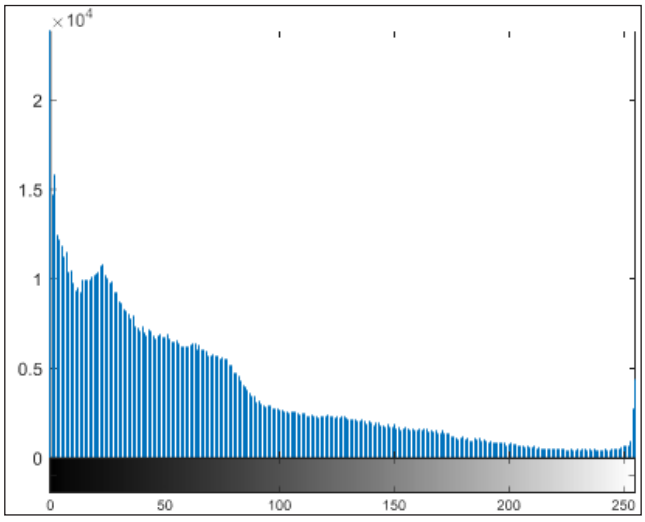

Figure 6.Histogram Distribution from Original Image

Result and Discussion

Histogram

Distribution of the image pixels after encryption can be observed through the histogram of the cipher text pixels. A qualified encryption algorithm can make the image pixels more evenly distributed between 0 and 255.[16] As it can be seen from Figures 6 and 7, it is apparent that pattern of histogram is amended if compared to the original histogram. Figure 7, shows an improvement of histogram distribution after combined spatial and frequency domains were applied in the image encryption process.

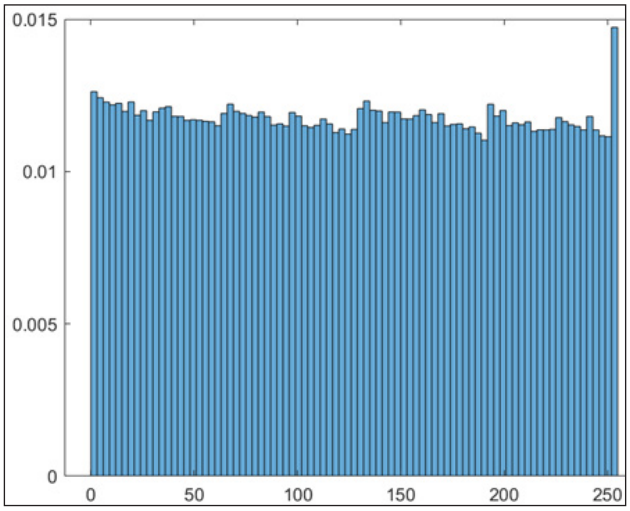

Figure 7.Histogram Distribution after Proposed System

Key Sensitivity Analysis

Two important measurements in analyzing the ability to resist different attacks are NPCR and UACI. NPCR is rate of change of pixel changes and its theoretical expectation value is 99.694%.[17]

On the other hand, UACI refers to the normalized average intensity of pixels.[19] The theoretical expectation value of UACI is 33.4635%.[20]

It is stated in[17] that the scheme has the power to withstand differential attacks if the NPCR > 90% and UACI ≈ 33%. Therefore, the NPCR and UACI values of five different images in the proposed algorithm were tabulated and compared. It is clear that our proposed algorithm is suitable for security transmission due to its high NPCR (>90) and good UACI (≈33%).

PSNR

The PSNR is used as an objective criterion for evaluating the image quality and the index to measure the level of correlation between the chipertext image and the plain text image. Lower value of the PSNR value implies higher security rank in the encryption algorithm.

Two approximate images should get a PSNR index not lower than 30. In other words, small value of PSNR index indicates that the two measured images are not approximate.[18] As a result of the calculation, the entropy value of the proposed encryption with combined spatial and frequency domain with grayscale images and Bayer images are found to be 8.2730 and 8.2007 respectively.

Information Entropy

The information entropy analysis can be used to decide the complexity of encrypted data. The encrypted data is supposed to be so complex that no information about the original data can be obtained out of it. The information entropy analysis can be measured.

The optimum information entropy value for an encryption is 8.[16] The quality of encryption becomes higher when the value of information entropy is closer to 8. The calculation shows the entropy value of our proposed encryption with combined spatial and frequency domain is recorded at 6.5400 for Grayscale Image and 6.5425 for Bayer Image, that are close to the optimum point.

SSIM

SSIM is used to compare the index of similarity between original and encrypted images. Dissimilarity level will be increased if the value of SSIM is low. Lower value of SSIM indicates the dissimilarity between two digital images is higher. The SSIM index between the original image and encrypted image.

Conclusion

Two types of telescope images are selected for the experiments of proposed novel encryption algorithm that combines spatial and frequency domains. The effectiveness of the proposed algorithm is then analyzed based on several key analyses such as histogram distribution, Number of Pixel Changing Rate (NPCR), Unified Average Changing Intensity (UACI), Peak Signal to Noise Ratio (PSNR), information entropy and Structural Similarity Index (SSIM). The empirical results confirm that the proposed algorithm has demonstrated good encryption effects.

Acknowledgment

We would like to show our gratitude to Universiti Tunku Abdul Rahman for technical guidance and financial assiatance.

References

1. Wu Y, Zhou Y, Noonan JP et al. Design of image cipher using latin squares. *Inf Sci* 2014; 264: 317-339.
2. Xu M, Tian Z. A novel image encryption algorithm based on self- orthogonal Latin squares. *Optik (Stuttg)*2018; 171: 891-903.
3. Kadir A, Hamdulla A, Guo WQ. Color image encryption using skew tent map and hyper chaotic system of 6th-

order CNN. *Optik (Stuttg)* 2014; 125(5): 1671-1675.
4. Wei X, Guo L, Zhang Q et al. A novel color image encryption algorithm based on DNA sequence operation and hyper- chaotic system. *J Syst Softw* 2012; 85(2): 290-299.
5. Gehani A, LaBean T, Reif J. DNA-based Cryptography. Aspects of Molecular Computing. *Lecture Notes in Computer Science* 2950.
6. Ning K. A Pseudo DNA Cryptography Method.
7. Zhang LY, Hu X, Liu Y et al. A chaotic image encryption scheme owning temp-value feedback. *Commun Nonlinear Sci Numer Simul* 2014; 19(10): 3653-3659.
8. Yeap KH, Lai KC, Ting KC et al. Optimization of Reflector Antennas in Radio Telescope. *Malaysian Journal of Fundamental and Applied* 2017.
9. Yeap KH. Analysis of offset antennas in radio telescopes. *International Journal on Advanced Science, Engineering and Information Technology* 2016; 6: 997-1004.
10. Gonzalez RC, Woods RE. Digital Image Processing. New York, NY: Pearson. 2018.
11. Liu X, Song Y, Jiang GP. Hierarchical bit-level image encryption based on Chaotic map and Feistel network. *International Journal of Bifurcation and Chaos* 2019; 19.
12. David BLB, Ting KC, Wang YC. Novel face recognition approach using bit-level information and dummy blank images in feedforward neural network. *Applications of Soft Computing* 2009; 483-490.
13. Chapeau-Blondeau F, Belin E. Fourier-transform quantum phase estimation with quantum phase noise. *Signal Processing* 2020; 170.