Research Journal of Information Technology

ISSN 1815-7432

Academic
Journals Inc.

www.academicjournals.com

OPEN ACCESS Research Journal of Information Technology

ISSN 1815-7432
DOI: 10.3923/rjit.2016.82.87

Research Article
Tri Layer Image Encryption Based on Quantum Principle

[1]R. Sridevi, [1]P. Philominathan, [2]Padmapriya Praveenkumar, [2]John Bosco Balaguru Rayappan and [2]Rengarajan Amirtharajan

[1]Department of Physics, A.V.V.M. Sri Pushpam College, Thanjavur, Tamil Nadu, India
[2]Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

Abstract

Background: The growth in the field of communication has enabled the people at miles apart to communicate easily. Once the online sharing of information is made possible. It is necessary to ensure about the security of the information that is shared. **Materials and Methods:** In this study, three levels of encryption process has been carried out. Quantum Key Distribution(QKD) with bit XOR forms the first level of encryption. Flipping and swapping of the ciphered block images were done using quantum walk principle forms the second and the third level of encryption. **Results and Discussion:** To prove the robustness of the proposed scheme, image encryption metrices like horizontal, vertical, diagonal correlations, No. of Pixel Change Rate (NPCR), Unified Average Changing Intensity(UACI) were estimated and compared with the available literature. **Conclusion:** The QKD and quantum walks forms the basic level of image encryption and offers NPCR 99.68 and UACI of 30.50. Flipping, swapping and bit XOR of the ciphered block images were done. To verify the robustness of the proposed method and the values are found to be better.

Key words: QKD, quantum walk, image encryption, NPCR, UACI

Received: March 26, 2016 Accepted: June 20, 2016 Published: September 15, 2016

Citation: R. Sridevi, P. Philominathan, Padmapriya Praveenkumar, John Bosco Balaguru Rayappan and Rengarajan Amirtharajan, 2016. Tri layer image encryption based on quantum principle. Res. J. Inform. Technol., 8: 82-87.

Corresponding Author: Rengarajan Amirtharajan, Department of Electronics and Communication Engineering,
School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

Competing Interest: The authors have declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

INTRODUCTION

Various techniques have been introduced to maintain the secrecy of the information transferred. The most popular technique thus used is the encryption[1,2]. Encryption is the process of altering the original information, so as to make it unrealizable for the third party[3,4]. The encryption process carries No. of stages depending upon the complexity of the encryption algorithm used[5-7]. More the complexity more will be the security[8,9].

Quantum cryptography used to factorize the large integer within seconds and compute the discrete algorithm using quantum mechanics and quantum polarization angle based encryption[10,11]. Quantum Key Distribution (QKD) uses quantum mechanics for secure communication. Quantum distribution has the unique property to detect the intruder trying to gain the knowledge of the key. The QKD provides perfect secrecy since it is based on the uncertainty principle of quantum physics[12,13].

Quantum walks are the quantum analogue of traditional random walks. Quantum random walk using optimal query algorithm which is slightly differs from classical walk. It mainly used for design the randomized algorithm and provides the high polynomial speed than the classical walk[8,14].

In classical walk, the current state of the walker is identified by the probability distribution over positions where as quantum walk, the walker position is described by superposition of position[15,16]. The quantum walk is classified as discrete-time quantum walks and continuous-time quantum walks[17,18]. The application of quantum random walk used as the model of universal computation[19,20].

In the proposed scheme, the original image is split into 64 blocks and each block is bit XORed with MSB of the key which is generated by quantum walk. Bitwise XOR provides the better result when compared to other gates for image encryption.

MATERIALS AND METHODS

Proposed methodology: A bitwise XOR performs exclusive OR operation between the two bit patterns of same length as given in Fig. 1. Bit XORed image is combined and again split into sixteen equal blocks. Each pixel value is flipped from LSB to MSB based on the quantum walk. The process of flipping produce the mirror inverted of original image.

The swapping is the process in which the position of the pixels is changed. The flipped images are split into four equal blocks according to the quantum walk each value of the pixels is swapped. The random number generator generates the sequence of bits which is used as the key and bit XORed with swapped images. The random key is generated by pseudorandom number generator or random number generator. The same key is used for both encryption and decryption process.

Encryption algorithm:

- Read the gray scale image of size 256×256
- Split the image into 64 blocks of an image
- Apply bit-XOR operation between the MSB of pixel and quantum key, then it forms an encrypted image of level 1
- Combine the encrypted blocks and split the image into 16 blocks
- Flip the pixel value from LSB to MSB according to the quantum walk, then it forms the encrypted image of level 2
- Combine the level 2 encrypted blocks and split the image into 4 blocks
- Swapping the pixel value according to the quantum walk, then it forms an encrypted image of level 3
- Combine the blocks and apply bit XOR operation between the results obtained from above step and random key
- Store the resultant image as the multilevel encrypted image

Decryption algorithm:

- Read the multilevel encrypted image
- Apply bit XOR operation between the results obtained from 1st step and random key,then it forms a decrypted image of level 1, further to split the image into 4 blocks
- Swapping the pixel to an original position according to the quantum key, then it forms decrypted image of level 2
- Combine the blocks and split the image into 16 blocks
- Flip the pixel value from MSB to LSB according to the quantum walk, then it forms a decrypted image of level 3
- Combine the level 3 decrypted image blocks and split the image into 64 blocks
- Apply bit-XOR operation between the MSB of pixel value and quantum key, then it forms decrypted image of level 1
- Combine the blocksof decrypted image into an image
- Store the resultant image as the decrypted image

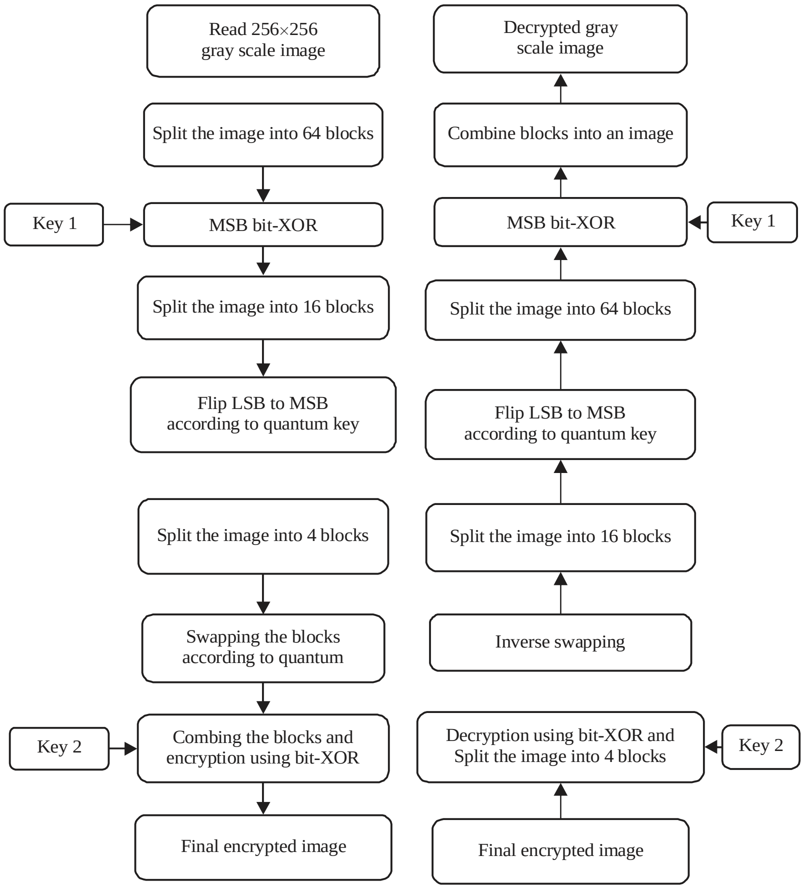

Fig. 1: Proposed encryption/decryption scheme

RESULTS AND DISCUSSION

For analysis the statically and security test such as horizontal, vertical, diagonal correlation, NPCR and UACI were calculated for gray scale image of size 256×256. The estimated values were compared with[8,9,14].

Figure 2-8 describe the encryption stages. Figure 2 and 3 are the original lena images and its histogram, respectively. Figure 4 is the first level of encrypted image obtained by applying bit-XOR operation between MSB of the each pixel value and quantum key. Figure 5 is the second level of encrypted image is obtained by flipping. Swapping of the encrypted image depicts in Fig. 6. The final encrypted image using bit-XOR is shown in Fig. 7. Figure 8 depicts the uniform pixel distribution of Fig. 7.

Figure 9-12 are the decryption stage. Decryption using swapping is illustrated in Fig. 9. Figure 10 is the decrypted image after applying the flipping operation. The final decrypted image is shown in Fig. 11. The histogram of decrypted image is depicted in Fig. 12. The NPCR, UACI and correlation coefficient were calculated using the following formula:

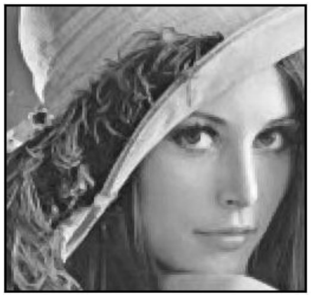

Fig. 2: Original image

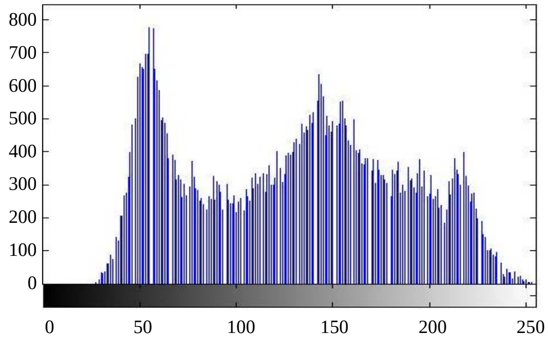

Fig. 3: Histogram of Fig. 1

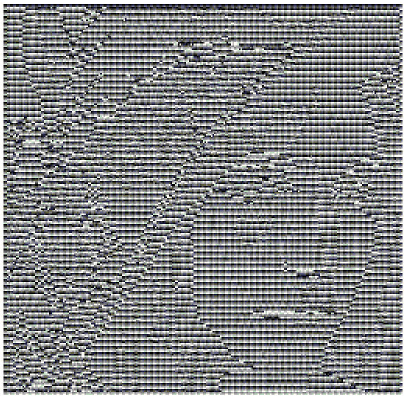

Fig. 4: MSB Bit-XOR with quantum key

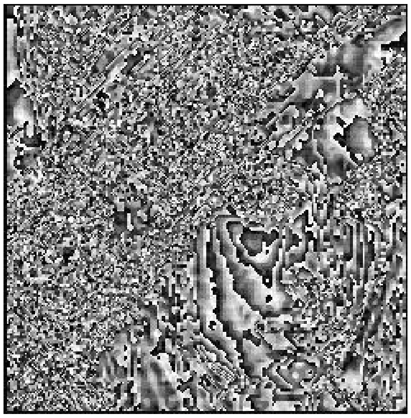

Fig. 5: Encryption using flipping

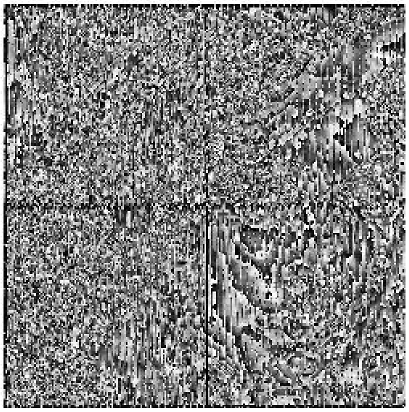

Fig. 6: Encryption using swapping

NPCR: The NPCR is expanded as No. of changing pixel rate and it is used to determine the strength of the encryption algorithm beyond attacks:

$$\text{NPCR} = \left(\frac{1}{n}\sum_{i=0}^{n-1} d_i\right) \times 100\%$$

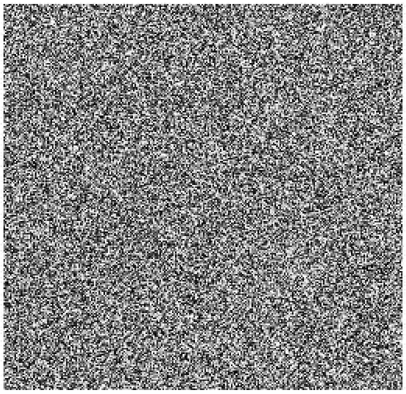

Fig. 7: Final encrypted image using bit -XOR

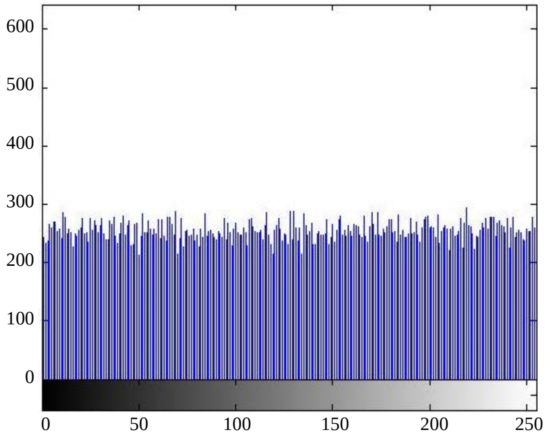

Fig. 8: Histogram of Fig. 7

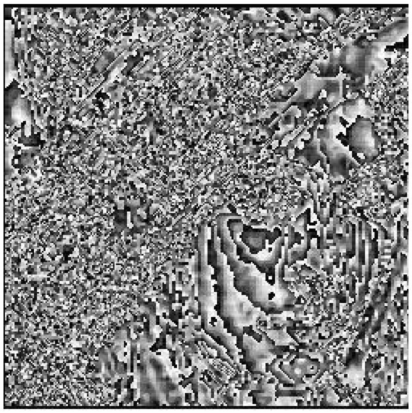

Fig. 9: Decryption uses swapping

X, Y is the original image and encrypted image:

$$d_i = 0 \text{ if } X_i^2 = Y_i^2$$

$$d_i = 1 \text{ if } X_i^2 \neq Y_i^2 \quad \text{for any } i \in \{0, 1, \ldots, n-1\}$$

Table 1: Metrics considering images of size 256×256

Metrics	Proposed lena	Zhou *et al.*[8] lena	Sivakumar and Venkatesan[9] lena	Proposed peppers	Zhou *et al.*[8] peppers	Sivakumar and Venkatesan[9] peppers
Vertical correlation	-0.0026	0.0018	0.0066	-0.00033	-0.0115	0.0007
Horizontal correlation	-0.0072	-0.005	0.0161	-0.0038	0.0137	0.0063
Diagonal correlation	-0.0090	0.0069	0.0075	0.0063	0.0104	0.0029
NPCR	99.6885	NA	99.670	99.664	NA	99.6490
UACI	30.5067	NA	28.3340	30.61	NA	30.1392

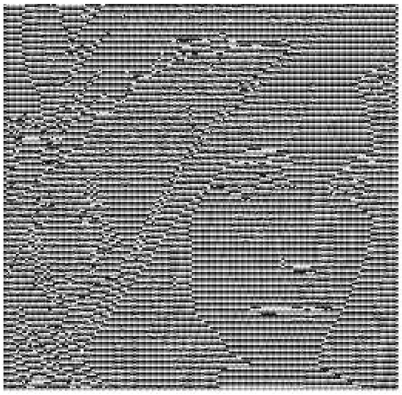

Fig. 10: Decryption using flipping

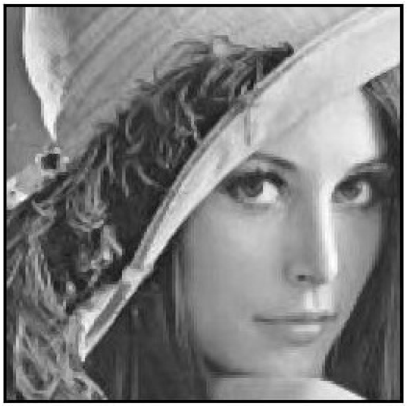

Fig. 11: Final decrypted image

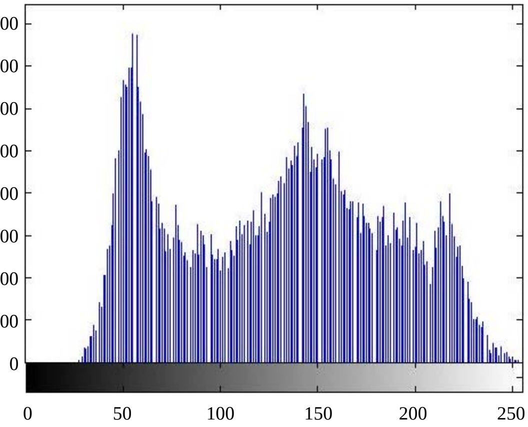

Fig. 12: Histogram of Fig. 11

UACI: Unified Average Change in Intensity (UACI) is a measure of the average intensity difference between two cipher images.

Correlation coefficient: The correlation is found out between two pixel values in an image, so as to determine the quality of the encryption technique applied to the image. This correlation can be calculated for an encrypted image diagonally, vertically and horizontally. As far the correlation values are lesser the encryption methodology can be claimed as better efficient:

$$\rho(X,Y)=\frac{E\left[(X-\mu_X)(Y-\mu_Y)\right]}{\sigma_X\,\sigma_Y}$$

Table 1 containing the metrics calculated for gray scale image such as lena and peppers. The metrics calculated by proposed algorithm is compared with the other existing method. Since, the correlation values are obtained in negative range and comparatively lesser, the algorithm is more preferable.

CONCLUSION

In this study, QKD and quantum walks forms the basic level of encryption. Flipping, swapping and bit XOR of the ciphered block images were done to improve the robustness of the proposed scheme. To verify the sterness of the proposed scheme, correlations, NPCR and UACI were calculated and the values were compared with the available literature.

ACKNOWLEDGMENT

Its our work, no grant and contribution numbers.

REFERENCES

1. Praveenkumar, P., R. Hemalatha, R. Uma, K. Madhunisha, K. Thenmozhi and R. Amirtharajan, 2014. Image Zoning→encryption. Res. J. Inform. Technol., 6: 368-378.

2. Praveenkumar, P., G. Ashwin, S.P.K. Agarwal, S.N. Bharathi, V.S. Venkatachalam, K. Thenmozhi and R. Amirtharajan, 2014. Rubik's cube blend with logistic map on RGB: A way for image encryption. Res. J. Inform. Technol., 6: 207-215.
3. Praveenkumar, P., P. Rajalakshmi, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2016. Horse DNA runs on image: A novel road to image encryption. Res. J. Inform. Technol., 8: 1-9.
4. Praveenkumar, P., R. Nisha, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2016. Image merger encryptor: A chaotic and chebyshev key approach. Res. J. Inform. Technol., 8: 10-16.
5. Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2015. Triple chaotic image scrambling on RGB-a random image encryption approach. Secur. Commun. Networks, 8: 3335-3345.
6. Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2015. Pixel scattering matrix formalism for image encryption-a key scheduled substitution and diffusion approach. AEU-Int. J. Electron. Commun., 69: 562-572.
7. Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2015. Medical data sheet in safe havens-a tri-layer cryptic solution. Comput. Biol. Med., 62: 264-276.
8. Zhou, N.R., T.X. Hua, L.H. Gong, D.J. Pei and Q.H. Liao, 2015. Quantum image encryption based on generalized Arnold transform and double random-phase encoding. Quantum Inform. Process., 14: 1193-1213.
9. Sivakumar, T. and R. Venkatesan, 2014. A novel image encryption method with Z-order curve and random number. Int. J. Comput. Applic., 103: 17-25.
10. Abd El-Latif, A.A., L. Li, N. Wang, Q. Han and X. Niu, 2013. A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. Signal Process., 93: 2986-3000.
11. Akhshani, A., A. Akhavan, S.C. Lim and Z. Hassan, 2012. An image encryption scheme based on quantum logistic map. Commun. Nonlinear Sci. Numer. Simul., 17: 4653-4661.
12. Seyedzadeh, S.M., B. Norouzi, M.R. Mosavi and S. Mirzakuchaki, 2015. A novel color image encryption algorithm based on spatial permutation and quantum chaotic map. Nonlinear Dyn., 81: 511-529.
13. Yan, F., A.M. Iliyasu and S.E. Venegas-Andraca, 2016. A survey of quantum image representations. Quantum Inform. Process., 15: 1-35.
14. Yang, Y.G., Q.X. Pan, S.J. Sun and P. Xu, 2015. Novel image encryption based on quantum walks. Scient. Rep., Vol. 5. 10.1038/srep07784
15. Song, X.H., S. Wang, A.A. Abd El-Latif and X.M. Niu, 2014. Quantum image encryption based on restricted geometric and color transformations. Quantum Inform. Process., 13: 1765-1787.
16. Wang, S., X. Song and X. Niu, 2014. A novel encryption algorithm for quantum images based on quantum wavelet transform and diffusion. Adv. Intell. Syst. Comput., 298: 243-250.
17. Hua, T., J. Chen, D. Pei, W. Zhang and N. Zhou, 2015. Quantum image encryption algorithm based on image correlation decomposition. Int. J. Theoret. Phys., 54: 526-537.
18. Zaghloul, A., T. Zhang, M. Amin and A.A. Abd El-Latif, 2014. Color encryption scheme based on adapted quantum logistic map. Proceedings of the 6th International Conference on Digital Image Processing, April 5-6, 2014, Athens, Greece.
19. Guanghui, C., Z. Jun, Z. Yizhi, J. Yueling and Z. Xing, 2014. Quantum chaotic image encryption with one time running key. Int. J. Secur. Applic., 8: 77-88.
20. Song, X.H. and X.M. Niu, 2014. Comment on: Novel image encryption/decryption based on quantum fourier transform and double phase encoding. Quantum Inform. Process., 13: 1301-1304.