International Journal of Information Processing, 8(3), 31-41, 2014
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Fisher-Yates Chaotic Shuffling Based Image Encryption

Swaleha Saeed[a], M Sarosh Umar[a], M Athar Ali[a], Musheer Ahmad[b]

[a]Department of Computer Engineering, ZH College of Engineering and Technology,
Aligarh Muslim University, Aligarh 202 002, India,
Contact: {swalehasaeed, saroshumar, atharali}@zhcet.ac.in

[b]Department of Computer Engineering, Faculty of Engineering and Technology,
Jamia Millia Islamia, New Delhi 110 025, India, Contact: musheer.cse@gmail.com

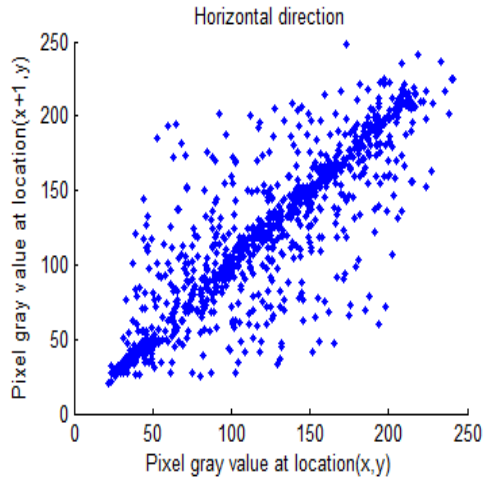
In Present era, information security is of utmost concern and encryption is one of the alternatives to ensure security. Chaos based cryptography has brought a secure and efficient way to meet the challenges of secure multimedia transmission over the networks. In this paper, we have proposed a secure Grayscale image encryption methodology in wavelet domain. The proposed algorithm performs shuffling followed by encryption using states of chaotic map in a secure manner. Firstly, the image is transformed from spatial domain to wavelet domain by the Haar wavelet. Subsequently, Fisher Yates chaotic shuffling technique is employed to shuffle the image in wavelet domain to confuse the relationship between plain image and cipher image. A key dependent piece-wise linear chaotic map is used to generate chaos for the chaotic shuffling. Further, the resultant shuffled approximate coefficients are chaotically modulated. To enhance the statistical characteristics from cryptographic point of view, the shuffled image is self keyed diffused and mixing operation is carried out using keystream extracted from one-dimensional chaotic map and the plain-image. The proposed algorithm is tested over some standard image dataset. The results of several experimental, statistical and sensitivity analyses proved that the algorithm provides an efficient and secure method to achieve trusted gray scale image encryption.

Keywords : Fisher-Yates Shuffle, Haar Wavelet Transform, Piece-wise linear Chaotic Map, Self Keyed Diffusion.

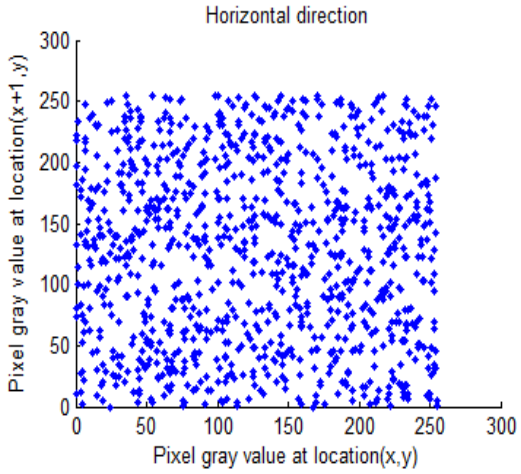
1. INTRODUCTION

Nowadays, public networks are not suitable for the direct transmission of confidential messages because of the rapidly rising problem of security threats. As a result, security is still an open challenge in spite of the tremendous advancement in internet technologies. This is an important challenge in the areas where reliable, secure, fast and robust transmission of information is the major requirement especially in the field of military and medical systems. To deal with the problem of secure transmission of information over the networks, numerous encryption algorithms have been proposed based on different methodologies and ideas [1][2][3].

Traditional ciphers RSA, DES, AES, can be used to encrypt image, but these are not ideal for two reasons [4]. First, since image size is generally much greater than text. This results in conventional ciphers taking much more time to encrypt images. Second, image data has high correlation among adjacent pixels. Consequently, it is rather difficult for these ciphers to shuffle and diffuse image data effectively. Chaos-based cryptosystems usually have higher speeds and lower costs. In this regard, chaos based encryption techniques have demonstrated exceptionally good behavior because these technique have faster speed, reasonable computation overheads without compromising the security. Moreover, chaotic systems have many important properties such as the sensitivity to initial conditions and system parameters, pseudorandom property, non-periodicity and topological transitivity [1]. These optimistic features make the chaotic al-



(a) Original Image



(b) Cipher Image

Figure 6. Distribution of Adjacent Pixels in Horizontal Direction

make shuffling key dependent. Moreover, the chaotic modulation of shuffled approximate coefficients results a good quality of shuffled image. Then, in second phase the shuffled image is self keyed diffused and mixing operation is carried out with the generated keystream sequence and shuffled image. The simulation and experimental analyses proved that the proposed encryption algorithm is secure, efficient, and highly robust towards cryptanalysis.

REFERENCES

1. M Ahmed and M S Alam. A New Algorithm of Encryption and Decryption of Images using Chaotic Mapping, *International Journal on Computer Science and Engineering*, 2(1):46–50, 2009.
2. Ismail, Mohammed Amin and Hossam Diab. A Digital Image Encryption Algorithm based on a Composition of Two Chaotic Logistic Maps, *International Journal of Network Security*, 11(1):1–10, 2010.
3. Said E El-Khamy, Mohammad Abou El-Nasr and Amina H El-Zein. A Partial Image Encryption Scheme Based on the DWT and ELKNZ Chaotic Stream Cipher, *MASAUM Journal of Basic and Applied Sciences*, 1(3):389–394, November 2009.
4. Narendra K Pareek, Vinod Patidar and Krishan K Sud. Diffusion-Substitution based Gray Image Encryption Scheme, *Digital Signal Processing, Elsevier*, 23(3):894–901, 2013.
5. Guoji Zhang and Qing Liu. Novel Image Encryption Method based on Total Shuffling Scheme, *Optics Communications, Elsevier*, 284(12):2775–2780, 2011.
6. M Ahmed, O Farooq and J M Blackedge. Chaotic Image Encryption Algorithm based on Frequency Domain Scrambling, *School of Electrical Engineering Systems Articles, Dublin Institute of Technology*, 2010.
7. R Durstenfeld. Algorithm 235: Random Permutation, *Communications of the ACM*, 1964.
8. D E Knuth. The Art of Computer Programming, *AddisonWesley*, 1969.
9. H Alsafasfeh and A A Arfoa. Image Encryption based on the General Approach for Multiple Chaotic System, *Journal of Signal and Information Processing*, 2:238–244, 2011.
10. Zhi-liang Zhu, Wei Zhang, Kwok-Wo Wong and Hai Yu. A Chaos-based Symmetric Image Encryption Scheme using a Bit-level Permutation, *Information Sciences*, 181(6):1171–1186, 2010.
11. Xiping He Qionghua Zhang. Image Encryption Based on Chaotic Modulation of Wavelet Coefficients, *Congress on IEEE Image and Signal Processing*, pages 622–626, 2008.
12. Dong Enxeng, Chen Zengqiang, Yuan Zhuzhi and Chen zaiping. A Chaotic Images Encryption Algorithm with The Key Mixing Proportion Factor, *2008 International Conference on Information Management, Innova-*

tion Management and Industrial Engineering, pages 169–174, 2008.
13. Ch Samson and V U K Sastry. An RGB Image Encryption Supported by Compression using Multilevel Wavelet Transform, *International Journal of Advanced Computer Science and Applications*, 3(9):36–41, 2012.
14. I Ozturk and I Sogukpinar. Analysis and Comparison of Image Encryption Algorithm, *International Journal of Information Technology*, 1(2):108-111, 2004.
15. Zhengjun Liu, She Li, Wei Liu, Yanhua Wang and Shutian Liu. Image Encryption Algorithm by using Fractional Fourier Transform and Pixel Scrambling Operation Based on Double Random Phase Encoding, *Optics and Lasers in Engineering, Elsevier*, 51(1):8–14, 2013.

Swaleha Saeed obtained her B. Tech and M. Tech degrees from Department of Computer Engineering, Zakir Hussain College of Engineering and Technology, Aligarh Muslim University, India in 2012 and 2014, respectively. She has profound interest in application-end research work and projects that contribute to a social cause. Her areas of research interest are Cryptography, Graphical User Authentication Systems and Image Processing Techniques.

M Sarosh Umar is working as Associate Professor in the Department of Computer Engineering, Zakir Hussain College of Engineering and Technology, Aligarh Muslim University, India. He has teaching/research and industrial experience of more than 25 years in India as well as abroad. He has various articles, research papers and published patents to his credit. His research interests are User Authentication using Graphical Methods, Computer Security and Software Engineering.

M Athar Ali is currently employed as an Assistant Professor in the Department of Computer Engineering, Zakir Hussain College of Engineering and Technology, Aligarh Muslim University (AMU), India. Dr. Ali earned his PhD from Loughborough University, England, United Kingdom and his masters and graduate degrees from AMU. His areas of interest include but are not limited to Image and Video coding/processing, information security and cryptography.

Musheer Ahmad received his B. Tech and M. Tech degrees from Department of Computer Engineering, Zakir Hussain College of Engineering and Technology, Aligarh Muslim University, India in 2004 and 2008, respectively. He is with Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India, as Assistant Professor. He has published about 30 research papers in refereed academic journals and international conference proceedings. His areas of research interest include Multimedia Security, Chaos-based Cryptography, Cryptanalysis and Image Processing.