International Journal of Information Processing, 7(3), 92-99, 2013
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Wavelet Transform Based Approach for Partial Image Encryption

Parameshachari B D[a], K M Sunjiv Soyjaudah[b], Sumithra Devi K A[c] Panduranga H T[d]

[a]Department of ECE, Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India (Research Scholar, Department of ECE, Jain University, Bangalore.), Contact: parameshbkit@gmail.com

[b]Professor, Department of EEE, University of Mauritius, Reduit, Mauritius.

[c]Professor, Department of MCA, RVCE, Bangalore, Karnataka, India.

[d]Department of Electronics, Hemogangothri PG center, University of Mysore, Hassan, Karnataka, India.

Advances in digital content transmission have increased in the past few years. Security and privacy issues of the transmitted data have become an important concern in multimedia technology. In this paper proposed partial image encryption algorithm consists of two stages: first stage is *c* scan (continuous raster scan) and second is Band permutation stage. The c scan is done by both column wise and row wise. Band permutation means to permute the coefficients in the frequency bands. The coefficients positions are permuted in each frequency band or subblock. The transformed image is composed of seven frequency bands, that is, LL_1 LH_1, HL_1, HH_1, LH_0, HL_0 and HH_0. The scan mapping and Band permutation are often inserted between quantization and entropy coding. Performance of the proposed technique is evaluated by differential Analysis and also quantifying Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). The experimental results show that the proposed encryption technique is efficient and has high security features.

Keywords : Band Permutation, *C* Scan, Differential Analysis, Partial Encryption.

1. INTRODUCTION

The use of image communication has increased dramatically in recent years. The World Wide Web and video conferencing are two examples. When there is a need to protect the transmission from eavesdroppers, the transmitted data must be encrypted [1]. Unfortunately, the processing time for encryption and decryption is a major factor in real-time image communication. Encryption and decryption algorithms are too slow to handle the tremendous amount of data transmitted. Ciphering of images is actually an important issue. One essential difference between text data and image data is that the size of image data is much larger than the text data. The time is a very important factor for the image encryption. We find it at two levels, one is the time to encrypt, and the other is the time to transfer images. To minimize the time, the first step is to choose a robust, rapid and easy method to implement cryptosystem [2]. Wavelet Transform is one of the most powerful tools in digital signal processing. The image components are decomposed into different decomposition levels using a wavelet transform. These decomposition levels contain a number of subbands, which consist of coefficients that describe the horizontal and vertical spatial frequency characteristics of the original image component [3]. Power of 2 decompositions are allowed in the form of standard decomposition.

To perform the forward DWT, the standard uses a 2D subband decomposition of a 2-D set of samples into low-pass samples and high-pass samples. Low-pass samples represent a down sampled low-resolution version of the original set. High-pass samples represent a downsam-

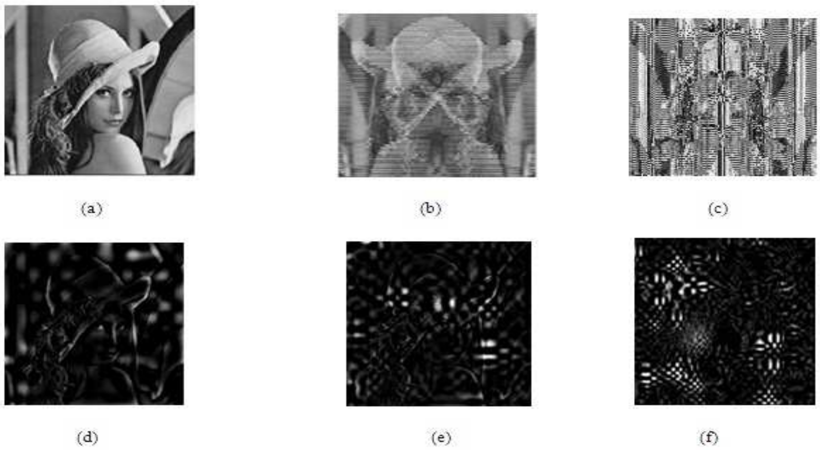

Figure 5. Partially Encrypted Images: (a) Original Image (b) C Scan (Row wise) (c) C Scan (Column wise)(d) Band Permutation (First 4 Bands) (e) Band Permutation (First 7 Bands) (f) Band Permutation (First 10 Bands)

(PSNR) for the proposed technique has been computed for different images. It is known that, as the MSE increases, PSNR decreases, resulting more randomness in the encrypted image. MSE is calculated using the formula.

$$MSE = \frac{1}{MN} \sum_{i=1}^{N} \sum_{j=1}^{M} [C(i,j) - C'(i,j)]^2 \quad (6)$$

where $C(i,j)$ and $C'(i,j)$ be the ith row and jth column pixel of two images C and C', respectively. M and N are number of rows and columns of original image. PSNR can be computed by

$$PSNR = 10 \times log_{10} \left[\frac{R^2}{MSE} \right] \quad (7)$$

Where R is 255 as 8 bit image has been used in this experiment. Calculated results of MSE and PSNR are tabulated in Table 2.

7. CONCLUSION AND FUTURE WORK

In this paper, scrambling analysis of image scrambling encryption algorithm is presented. The performance of the proposed approach is evaluated based on the Differential Analysis, MSE, and PSNR. From the experiment results and the differential analysis can be concluded that the proposed algorithm is secure from various attacks which aim to find the secret keys or pixels in plain images. As MSE increases PSNR decreases, resulting more randomness in the encrypted image. Increases in the value of NPCR and UACI shows that there is an improvement in the amount of encryption. The proposed method proves to be highly secure and decreases the probability of detection of the secret data present in the cover image. As a future work, many other scanning methods can be analyzed. Also, in the same image, a composite scanning path can be introduced by incorporating different scanning paths in different areas of the image.

Table 2
Results of MSE and PSNR

Name of the Input Image	PSNR	MSE
Lena	25.7862	81.7768
Cameraman	25.6257	80.2147
Step	25.7501	75.8352

REFERENCES

1. Cheng H. Partial Encryption for Image and

Video Communication, in *M.Sc. Thesis, Department of Computing Science, University of Alberta*, 1998.

2. Borie J, Puech W, Dumas M. Crypto-Compression System for Secure Transfer of Medical Images, *in 2nd International Conference on Advances in Medical Signal and Information Processing (MEDSIP2004)*, September 2004.
3. Uehara T, Safavi-Naini R, Ogunbona P. Securing Wavelet Compression with Random Permutations, in *Proceedings of the 2000 IEEE Pacific Rim Conference on Multimedia, Sydney*, 332-335, 2000.
4. Usevitch B E. A Tutorial on Modern Lossy Wavelet Image Compression:Foundations ofJPEG 2000, in *IEEE Transactions on Image Processing Magazine*, 2001.
5. Ch.Samson, V U K Sastry. A Novel Method for Image Encryption Supported by Compression using Multilevel Wavelet Transform, in *International Journal of Advanced Computer Science and Applications*, 3(8), August 2012.
6. Varma K, Bell A. JPEG2000-Choices and Tradeoffs For Encoders, in *IEEE Transactions on Image Processing Magazine*, 2004.
7. Norcen R, *et al.,* Confidential Storage and Transmission of Medical Image Data, in *Computers in Biology and Medicine 33*, pages 277-292, 2003.
8. Parameshachari B D, K M Sunjiv Soyjaudah and Sumithra Devi K A. Secure Transmission of an Image using Partial Encryption based Algorithm, in *International Journal of Computer Applications, Published by Foundation of Computer Science, New York, USA*, 63(16): 33–36, 2013.
9. Parameshachari B D and Chaitanyakumar M V. Image Security using SCAN Based Encryption Method, in *42nd IETE Mid-term symposium on Telecom Paradigms - Indian Scenario, Bangalore*, pages 115–118, 2011.
10. C Kachris, et al., A Reconfigurable Logic based Processor for the SCAN Image and Video Encryption Algorithm, in *IJPP*, 31(6):489–506, Dec 2003.
11. Panduranga H T and Naveen Kumar S K, Hybrid Approach for Image Encryption Using SCAN Patterns and Carrier Images, in *IJCSE*, 2010.
12. Antonini M, Barlaud M, Daubechies I. Image Coding Using Wavelet Transform, in *IEEE Transactions on Image Processing*, 1(2): 1716–1740, 1992.
13. Baxes G A. Digital Image Processing: Principles and Applications, in *John Wiley and Sons, Inc., USA*.
14. Saha S. Image Compression-From DCT to Wavelet: A Review, in *ACM Crossroads Student Magazine, The ACMs First Electronic Publication*, 2001.
15. Xiong Z, Ramchandran K, Orchard M T, Zhang Y. A Comparative Study of DCT and Wavelet-Based Image Coding, in *IEEE Transactions on Circuits and Systems for Video Technology*, 9(5), 1999.
16. Yue Wu, Joseph P. Noonan and Sos Agaian. NPCR and UACI Randomness Tests for Image Encryption, in *Cyber Journals: Multidisciplinary Journals in Science and Technology, JSAT*.

Parameshachari B D working as a Associate Professor and Department Coordinator in the Department of Electronics and Communication Engineering at Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India, affiliated to University of Calicut. Worked as a Senior Lecturer and incharge HOD in the Department of Electronics and Communication Engineering at JSS Academy of Technical Education, Mauritius. He worked at JSSATE, Mauritius for Three years and also worked as a Lecturer at Kalpatharu Institute of Technology, Tiptur for Seven years. He obtained his BE in Electronics and Communication Engineering from Kalpatharu Institute of Technology, Tiptur and MTech in Digital communication Engineering from B M S college of Engineering, Bangalore, affiliated to Visveswaraiah Technological University, Belgaum. He is pursuing his Ph.D in Electronics and Communication Engineering at Jain University, Bangalore, Karnataka, India under the guidance of Dr. K M Sunjiv Soyjaudah, Professor, University of Mauritius, Reduit, Republic of Mauritius and Co-guidance of Dr. Sumithra Devi K A, Professor and Director, Department of MCA, R V College of Engineering, Bangalore. Parameshachari area of interest and research include Image Processing, Cryptography and Communication. He has published several Research papers in international Journals/conferences. He is a Member of ISTE, IETE, IACSIT, IAEST, IAENG, SDWIC and AIRCC.

Professor K M Sunjiv Soyjaudah received his B.Sc (Hons) degree in Physics from Queen Mary College, University of London in 1982, his M.Sc. Degree in Digital Electronics from Kings College, University of London in 1991 and his Ph. D. degree in Digital Communications from University of Mauritius in 1998. He is presently Professor of Communications Engineering in the Department of Electrical and Electronic Engineering of the University of Mauritius. His current interest includes Source and Channel Coding Modulation, Image Processing, Cryptography, Voice and Video through IP, as well as Mobile Communication. Dr. K M S Soyjaudah is a member of the IEEE, Director in the Multicarrier (Mauritius), Technical expert in the Energy Efficiency Management Office, Mauritius. Registered Ph.D Guide in University of Mauritius, Reduit, Mauritius and Jain University, Bangalore, Karnatka, India.

Dr. Sumithra Devi K A Professor and Director, in Master of Computer Applications at R V College of Engineering, Bangalore, India. She received BE from Malnad College of Engineering, Hassan. She received ME and Ph.D from UVCE, Bangalore and Avinashilingam University for Women, Coimbatore, INDIA respectively. Reviewer for many International Journals / Conferences like WEPAN, WICT, EDAS, IACSIT, ISCAS, JEMS, Published 14 journals and 65 International/ National Conferences. Professional Member in many IEEE, IETE, CSI, ISTE. Member in BoS and BoE, for Visvesvaraiah Technological University, Belgaum, Karnataka. Registered Ph.D Guide in Visvesvaraiah Technological University, Belgaum; Jain University, Bangalore; Prist University, Sathyabhama University, Tamilnadu. Authored a chapter CAD algorithm for VLSI design in the book "VLSI Design ", published by In-Tech Publications, ISBN 979-953-307-512-8, 2011 and authored book on Operating System, published by Shroff Publisher India.

Panduranga H T obtained his M.Tech degree in Digital Electronics and Communication System from Visvesvaraya Technological University, Karantaka in the year 2006. Currently pursuing research in Depatment of studies in Electronics, University of Mysore, Mysore, Karnataka . His current research includes Image Processing and Information Security