Joint image compression and encryption based on order-8 alternating transforms

Peiya Li, Kwok-Tung Lo

PII: S1047-3203(17)30027-5
DOI: http://dx.doi.org/10.1016/j.jvcir.2017.01.021
Reference: YJVCI 1941

To appear in: *J. Vis. Commun. Image R.*

Received Date: 3 June 2016
Revised Date: 29 October 2016
Accepted Date: 17 January 2017

Please cite this article as: P. Li, K-T. Lo, Joint image compression and encryption based on order-8 alternating transforms, *J. Vis. Commun. Image R.* (2017), doi: http://dx.doi.org/10.1016/j.jvcir.2017.01.021

Joint image compression and encryption based on order-8 alternating transforms

Peiya Li, Kwok-Tung Lo

Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong, China

Abstract

In this paper, we propose a novel joint image compression and encryption scheme based on JPEG standard. We realize image encryption at JPEG's transformation stage. Instead of only using 8×8 discrete cosine transform (DCT) for transformation, we generate new orthogonal transforms by embedding an extra rotation angle of π to different stages' butterflies in 8×8 DCT's flow-graph, and then apply them alternatively for transformation according to a predefined secret key. By carefully controlling the number of rotation angles embedded, the quality control of encrypted images can also be achieved. The encryption algorithm is further enhanced by performing block permutation before the entropy encoding stage. Extensive experiments have been conducted to show the good protection and compression performance of our encryption schemes. Finally, a detailed security analysis is provided to show the encryption schemes' resistance to various cryptanalysis methods, such as brute-force attack, key sensitivity analysis, replacement attack and statistical attack.

Keywords: Image encryption, orthogonal transforms, security analysis, JPEG standard

Email addresses: yolanda.peiya@connect.polyu.hk (Peiya Li), kwok.tung.lo@polyu.edu.hk (Kwok-Tung Lo)