A Selective Compression-Encryption Of Images Based On SPIHT Coding and Chirikov Standard MAP

Mimoun Hamdi, Rhouma Rhouma, Safya Belghith

www.elsevier.com/locate/sigpro

PII: S0165-1684(16)30237-7
DOI: http://dx.doi.org/10.1016/j.sigpro.2016.09.011
Reference: SIGPRO6266

To appear in: *Signal Processing*

Received date: 5 June 2016
Revised date: 13 August 2016
Accepted date: 13 September 2016

Cite this article as: Mimoun Hamdi, Rhouma Rhouma and Safya Belghith, A Selective Compression-Encryption Of Images Based On SPIHT Coding and Chirikov Standard MAP, *Signal Processing* http://dx.doi.org/10.1016/j.sigpro.2016.09.011

A Selective Compression-Encryption Of Images Based On SPIHT Coding and Chirikov Standard MAP

Mimoun Hamdi, Rhouma Rhouma, Safya Belghith

Ecole Nationale d'Ingénieurs de Tunis, BP 37 Belvedere 1002, Tunisia

Abstract

In this paper, we propose a partial compression-encryption of images using chaotic system and Discrete Wavelet Transform (DWT) combined with Set Partitioning in Hierarchical Trees (SPIHT). The proposed cryptosystem adopts three stages for confusion and diffusion which are well integrated into the compression chain. The chaotic system used in this approach is Chirikov Standard Map. Some cryptographic tests and metrics are applied to measure the degree of security and analyze the performance of the partial compression-encryption scheme. The evaluation and simulation analysis indicate that our proposal possesses excellent statistical and cryptographic properties; it is extremely sensitive to the small change in secret key, resists against common cryptanalytic attacks, has a high speed and provides high picture quality of the reconstructed image.

Keywords Image Compression, Discrete Wavelet Transform (DWT), SPIHT coding, Partial encryption, Chaotic systems, Chirikov Standard Map.

1 Introduction

The compression and the security of images are the most challenging aspects of image storage and circulation in the Internet and network applications. The need for these two factors is required progressively by technological developments. For example, today the size of a three-color image would require more than 15 Megabytes of memory and need more than 1 hour to send it in a transmission channel with 64 kbit/s. But if this image is compressed at the ratio of 20 :1, the memory required would be just 500 KB and its transmission time become around 3 minutes. It is therefore necessary, for a real-time communication to apply a compression algorithm which also facilitates the transfer security. We try always to give new methods which ensure the ease and the speed of encoding and encryption operations. These methods should also preserve the original image after the reconstruction and guarantee the strength of the transmission process to propagation errors.

Coming to safety, some researches suggest encryption applied directly to images without compression [1-5], this approach is not always useful because the information to be transmitted requires a lot of bandwidth. Others propose encryption after the compression [6,7] which needs a significant additional time and memory and it is sometimes difficult to enable an encryption algorithm to be into the integrated system. However, very little research proposed encryption before compression [8,9], in this case the randomness of cipher text will dramatically reduce the compression efficiency. However some novel schemes have also been proposed to realize joint compression and encryption [10-14]. We adopt this approach with the use of a security algorithm based on the chaotic encryption technique. This concept allows to improve safety compared to the use