Title: Crypt analysis of an image compression-encryption algorithm and a modified scheme using compressive sensing

Author: P. Devaraj C. Kavitha

PII: S0030-4026(17)30886-0
DOI: http://dx.doi.org/doi:10.1016/j.ijleo.2017.07.063
Reference: IJLEO 59459

To appear in:

Received date: 6-9-2016
Revised date: 21-6-2017
Accepted date: 30-7-2017

Please cite this article as: P. Devaraj, C. Kavitha, Crypt analysis of an image compression-encryption algorithm and a modified scheme using compressive sensing, *<![CDATA[Optik - International Journal for Light and Electron Optics]]>* (2017), http://dx.doi.org/10.1016/j.ijleo.2017.07.063

Crypt analysis of an image compression-encryption algorithm and a modified scheme using compressive sensing

P. Devaraj

School of Mathematics, Indian Institute of Science Education and Research, Thiruvananthapuram, Kerala, India.

C. Kavitha

Department of Mathematics, College of Engineering, Guindy, Anna University Chennai, Chennai-25, India.

Abstract

Compressive sensing acquires image in the form of linear measurements. Utilizing compressive sensing in image encryption makes most of the algorithm vulnerable, due to the linearity property of compressive sensing retained in the encryption process. In this paper, a compression - encryption algorithm based on compressive sensing is analysed. It is demonstrated that chosen plain-text attack can be performed successfully for the scheme mentioned above. This paper shows that the encryption combined with compression adapted in the scheme under analysis can be represented as a single linear transformation. The corresponding matrix of transformation can be computed using the chosen plain-text attack. This matrix enables to encrypt or decrypt any image without knowing the keys. A modified scheme is proposed in which the encryption process is designed to change dynamically depending on the values of the plain image. The dynamic nature of the scheme makes it nonlinear and hence the scheme is secure against the chosen plain text attack.

Keywords: Compressive sensing, Modified Logistic Map, Hadamard matrix, Chosen plain-text attack

1. Introduction

Invention of smart devices and the reach of the technology to the wider range of people has increased the use of multimedia data. Due to the increased usage and the bulky nature of the multimedia data, they are compressed before storage and transmission. Compressive sensing introduced in [1, 2], is a new signal acquisition and compression technique with less sampling rate than usual Nyquist rate. Along with the development of compressive sensing, many security algorithms are designed to suit the compressive sensing scenario. Drori in [3], considers compressive sensing as an encryption technique with the measurement matrix kept as secret. In [4], it is shown that the secrecy achieved in compressive sensing is not perfect but still due to its computational complexity it can guarantee a required level of secrecy. Applying compressive

Email addresses: `devarajp@iisertvm.ac.in` (P. Devaraj), `kavistha@gmail.com` (C. Kavitha)