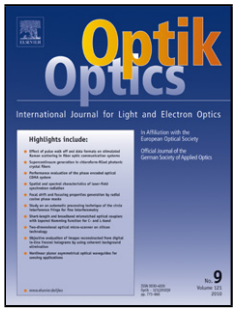

Title: Cryptanalysis and security improvement for a symmetric color image encryption algorithm

Author: Thang Manh Hoang Hoang Xuan Thanh

PII: S0030-4026(17)31285-8
DOI: https://doi.org/doi:10.1016/j.ijleo.2017.10.072
Reference: IJLEO 59808

To appear in:

Received date: 15-7-2016
Revised date: 11-10-2017
Accepted date: 14-10-2017

Please cite this article as: Thang Manh Hoang, Hoang Xuan Thanh, Cryptanalysis and security improvement for a symmetric color image encryption algorithm, *<![CDATA[Optik - International Journal for Light and Electron Optics]]>* (2017), https://doi.org/10.1016/j.ijleo.2017.10.072

Cryptanalysis and security improvement for a symmetric color image encryption algorithm

Thang Manh Hoang[1], Hoang Xuan Thanh

School of Electronics and Telecommunications,
Hanoi University of Science and Technology,
1 Dai Co Viet, Hanoi, Vietnam

Abstract

This paper presents the weaknesses in the cryptosystem proposed by W. Zhang and his colleagues. The proposed method to restore the permutation rule is based on the chosen-ciphertext attack. The method is successful in restoration of the permutation rule in the case of multiple encryption rounds without any knowledge about the cyptosystem. In order to improve the security of W. Zhang's cryptosystem, the proposed modifications are made to the equations to resist against the chosen-ciphertext attack. The specific examples will demonstrate the cryptanalysis and the security improvement.

Keywords: image encryption, chosen-ciphertext attack, cryptanalysis

1. Introduction

Chaotic systems with characteristics of sensitivity on initial conditions, control parameters, psuedo-randomness and ergodicity [1, 2, 3] are considered as good candidates for for cryptographic application [4, 5]. Chaos-based image encryption, e.g. [6, 7, 8, 9, 10, 11] has been interested and pursued in research community. Chaotic systems are used for designing cryptosystem in various ways (see [12] and therein). So far, there are three main ways of using chaos in encryption, i.e. creating position permutation matrices, generating psuedo-random bit sequences for mixing with plaintext, and producing ciphertext with the use of plaintext as initial condition of chaotic map. The architecture of substitution-permutation network suggested provides most prominent in providing high security for data encryption [13, 4], and recently it is widely employed in many chaotic cryptosystems, e.g. [14, 2, 15]. Specifically, chaos-based permutation is performed some location permutation for either pixels e.g. [16, 17, 6, 18, 8, 19, 20] or bits [21, 22]. The diffusion process using chaos can be realized in some ways, and in most cryptosystems, chaotic systems are used as random sequence generators for diffusion process. Chaotic random sequences are mixed with plain words in various fashions, e.g. [23, 24, 25, 17, 26]. However, flaws in designing encryption algorithms make chaos-based cryptography vulnerable. The strength of chaotic cryptosystems is still a controversial issue in literature [27], and many cryptosystems have been broken, e.g. [28, 12, 29, 30]. In the literature, to the best knowledge of the authors, there are limited success in attacking on chaos-based substitution-permutation networks with multiple encryption rounds, especially for the case of multiple encryption rounds, e.g. [31].

Email address: thang.hoangmanh@hust.edu.vn (Thang Manh Hoang)

October 24, 2017