Cryptanalysis of a chaotic image encryption scheme based on permutation-diffusion structure

Ming Li, Yuzhu Guo, Jie Huang, Yang Li

PII: S0923-5965(18)30017-1
DOI: https://doi.org/10.1016/j.image.2018.01.002
Reference: IMAGE 15317

To appear in: *Signal Processing: Image Communication*

Received date : 8 June 2017
Revised date : 10 December 2017
Accepted date : 5 January 2018

Please cite this article as: M. Li, Y. Guo, J. Huang, Y. Li, Cryptanalysis of a chaotic image encryption scheme based on permutation-diffusion structure, *Signal Processing: Image Communication* (2018), https://doi.org/10.1016/j.image.2018.01.002

Cryptanalysis of a chaotic image encryption scheme based on permutation-diffusion structure

Ming Li[a,b], Yuzhu Guo[a], Jie Huang[a] and Yang Li[a,*]

[a] *School of Automation Science and Electrical Engineering, Beihang University, Beijing 100191, China*

[b] *College of Computer and Information Engineering, Henan Normal University, Xinxiang 453007, China*

***Abstract*:** Chaos-based image encryption algorithms have been widely studied since the permutation-diffusion structure (PDS) was proposed. However, the PDS is not secure from attacks, which may lead to security vulnerabilities of PDS based chaotic cryptosystems. In this study, the security problems of PDS are investigated. Then, a new PDS based chaotic image encryption scheme is cryptanalyzed. In the original scheme, a 3D bit matrix permutation was used to address the intrinsic deficiencies of traditional pixel/bit level permutation of image encryption. The double random position permutation provides a high security level. However, it is not unattackable. In this study, a novel attack method will be introduced where all the chaotic mappings or parameters which are functionally equivalent to the keys used in the permutation and diffusion stages of the original cryptosystem can fully be revealed. The encrypted images can then be completely recovered without knowing the secret keys. Both mathematical analysis and experimental results are given to illustrate the effectiveness of the proposed method.

Key words: Cryptanalysis, permutation-diffusion structure, image encryption, chaos, chosen plaintext attack.

1. Introduction

With the rapid development of communication and network technology, the protection of digital images

* Corresponding author.

E-mail addresses: liming@htu.edu.cn (M. Li), liyang@buaa.edu.cn (Y. Li).