On the cryptanalysis of Fridrich's chaotic image encryption scheme

Eric Yong Xie, Chengqing Li, Simin Yu, Jinhu Lü

www.elsevier.com/locate/sigpro

PII: S0165-1684(16)30265-1
DOI: http://dx.doi.org/10.1016/j.sigpro.2016.10.002
Reference: SIGPRO6277

To appear in: *Signal Processing*

Received date: 27 July 2016
Revised date: 1 October 2016
Accepted date: 3 October 2016

Cite this article as: Eric Yong Xie, Chengqing Li, Simin Yu and Jinhu Lü, On the cryptanalysis of Fridrich's chaotic image encryption scheme, *Signal Processing*, http://dx.doi.org/10.1016/j.sigpro.2016.10.002

On the cryptanalysis of Fridrich's chaotic image encryption scheme

Eric Yong Xie[a], Chengqing Li[a,*], Simin Yu[b], Jinhu Lü[c]

[a] *Hunan Province Cooperative Innovation Center for Wind Power Equipment and Energy Conversion, College of Information Engineering, Xiangtan University, Xiangtan 411105, Hunan, China*
[b] *College of Automation, Guangdong University of Technology, Guangzhou 510006, Guangdong, China*
[c] *Academy of Mathematics and Systems Sciences, Chinese Academy of Sciences, Beijing 100190, China*

Abstract

Utilizing complex dynamics of chaotic maps and systems in encryption was studied comprehensively in the past two and a half decades. In 1989, Fridrich's chaotic image encryption scheme was designed by iterating chaotic position permutation and value substitution some rounds, which received intensive attention in the field of chaos-based cryptography. In 2010, Solak *et al.* proposed a chosen-ciphertext attack on the Fridrich's scheme utilizing influence network between cipher-pixels and the corresponding plain-pixels. Based on their creative work, this paper scrutinized some properties of Fridrich's scheme with concise mathematical language. Then, some minor defects of the real performance of Solak's attack method were given. The work provides some bases for further optimizing attack on the Fridrich's scheme and its variants.

Keywords: Chaotic encryption, chosen-ciphertext attack, cryptanalysis, differential attack.

1. Introduction

The complex dynamics of chaotic systems attracts researchers to utilize them as a new way to design secure and efficient encryption schemes [1, 2, 3, 4, 5]. The first chaos-based encryption scheme was proposed in 1989 [6], where a chaotic equation

$$g(x) = (\beta + 1)(1 + 1/\beta)^{\beta} x(1 - x)^{\beta}, \quad \beta \in [1, 4] \qquad (1)$$

was derived to generate pseudo-random number sequence and then mask the plaintext with modulo addition. Soon after publication of [6], it was pointed out that period of the sequence generated by iterating Eq. (1) may be very short, especially when it is implemented with small computing precision, which may seriously compromise the security level of the scheme [7]. Some special defects and properties of chaotic systems may facilitate cryptanalysis of chaos-based encryption schemes, e.g. chaotic synchronization [8], chaotic ergodicity [9], and parameter identification of chaotic system [10]. The inadequate combination of chaotic dynamics and encryption architectures makes the complexity of recovering its secret key from some pairs of plain-texts and the corresponding cipher-texts, encrypted with the same secret key, lower than that of brute-force attack [11, 12, 13, 14]. Some general rules on evaluating security of chaos-based encryption schemes can be found in [15, 16].

As quantitatively analyzed in [17, 18], any position permutation-only encryption scheme can be efficiently broken with only $O(\lceil \log_L(H \cdot W) \rceil)$ known/chosen plaintexts and the computational complexity of magnitude $O(H \cdot W \cdot \lceil \log_L(H \cdot W) \rceil)$, where L denotes the number of different gray-values of the plaintexts, and $H \times W$ (height×width) is the size of the encryption scheme's *permutation domain* , whose every element denotes the mapping relation between the relative position of a permuted element in the plaintext and that in the corresponding ciphertext. As suggested in [19], iterating position permutation and value substitution sufficient rounds can make an encryption scheme very strong against all kinds of attacks. Considering significant impact of the structure of Fridrich's scheme on a great number of chaotic encryption schemes, Solak's chosen-ciphertext attack method proposed in [20] can be considered as a breakthrough in the field of chaotic cryptanalysis.

According to the record of *Web of Science*, both papers [21] and [22] have been cited more than 500 times up to Aug 2016. Inspired by using space network (function graph) for attacking hash function in [23], we re-summarized some properties of Fridrich's chaotic image encryption scheme with the methodology of complex networks (binary matrix). Then, we further evaluated the real

*Corresponding author.
Email address: DrChengqingLi@gmail.com (Chengqing Li)