Available online at www.sciencedirect.com

ScienceDirect

The Journal of Systems and Software 81 (2008) 1130–1143

The Journal of Systems and Software

www.elsevier.com/locate/jss

Cryptanalysis of the RCES/RSES image encryption scheme

Shujun Li [a,*], Chengqing Li [b], Guanrong Chen [b], Kwok-Tung Lo [c]

[a] *FernUniversität in Hagen, Lehrgebiet Informationstechnik, Universitätsstraße 27, 58084 Hagen, Germany*
[b] *Department of Electronic Engineering, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong SAR, China*
[c] *Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong SAR, China*

Received 13 April 2007; received in revised form 9 July 2007; accepted 26 July 2007
Available online 14 September 2007

Abstract

Recently, a chaos-based image encryption scheme called RCES (also called RSES) was proposed. This paper analyses the security of RCES, and points out that it is insecure against the known/chosen-plaintext attacks: the number of required known/chosen plain-images is only one or two to succeed an attack. In addition, the security of RCES against the brute-force attack was overestimated. Both theoretical and experimental analyses are given to show the performance of the suggested known/chosen-plaintext attacks. The insecurity of RCES is due to its special design, which makes it a typical example of insecure image encryption schemes. A number of lessons are drawn from the reported cryptanalysis of RCES, consequently suggesting some common principles for ensuring a high level of security of an image encryption scheme.

Keywords: Image encryption; Chaotic cryptography; RCES/RSES; Cryptanalysis; Known-plaintext attack; Chosen-plaintext attack; CKBA

1. Introduction

In the digital world today, the security of digital images becomes more and more important, since the communications of digital products over networks occur more and more frequently. Furthermore, special and reliable security in storage and transmission of digital images is needed in many applications, such as pay-TV, medical imaging systems, military image database and communications as well as confidential video conferencing, etc. In recent years, some consumer electronic devices, especially mobile phones and hand-held devices, have also started to provide the function of saving and exchanging digital images via the support of multimedia messaging services over wireless networks.

To meet the challenges arising from different applications, good encryption of digital images is necessary. The simplest way to encrypt an image is to consider the 2D image stream as a 1D data stream, and then encrypt this 1D stream with any available cipher (Dang and Chau, 2000). Although such a simple way is sufficient to protect digital images in some civil applications, encryption schemes considering special features of digital images, such as the bulky size and the large redundancy in uncompressed images, are still needed to provide better overall performance and make the adoption of the encryption scheme easier in the whole image processing system.

Since the 1990s, many specific algorithms have been proposed, aiming to provide better solutions to image encryption (Bourbakis and Alexopoulos, 1992; Alexopoulos et al., 1995; Chung and Chang, 1998; Cheng and Li, 2000; Chang et al., 2001; Pommer, 2003; Maniccam and Bourbakis, 2004; Scharinger, 1998; Fridrich, 1998; Mao et al., 2004; Yano and Tanaka, 2002; Bhargava et al., 2004; Wu and Kuo, 2005; Mao and Wu, 2006; Yen and Guo, 1999, 2000a,b, 2003; Chen et al., 2002, 2003; Chen and Yen, 2003). At the same time, cryptanalytic work on proposed image encryption schemes has also been developed, and some existing schemes have been found to be insecure (Jan and Tseng, 1996; Qiao, 1998; Cheng, 1998; Chang and Yu, 2002; Li and Zheng, 2002a,b; Li et al., 2005,

[*] Corresponding author.
URL: http://www.hooklee.com (S. Li), .

0164-1212/$ - see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2007.07.037

2006, 2007; Cannière et al., 2005). Due to the tight relationship between chaos and cryptography (Li, 2003, Chapter 2), chaotic systems have been widely used in image encryption to realize diffusion and confusion in a good cipher (Scharinger, 1998; Fridrich, 1998; Yano and Tanaka, 2002; Mao et al., 2004; Yen and Guo, 1999, 2000a,b; Chen et al., 2002; Chen and Yen, 2003). For a more comprehensive survey of the state of the art about image encryption schemes, see (Uhl and Pommer, 2005; Furht et al., 2004; Li et al., 2004).

The present paper focuses on a new chaos-based image encryption scheme proposed by Chen et al. (2002) and Chen and Yen (2003), which was originally called RSES (random seed encryption system) in Chen et al. (2002) and then renamed to be RCES (random control encryption system) in Chen and Yen (2003). RCES can be considered as an enhanced version of a previously-proposed image encryption scheme called CKBA (chaotic key-based algorithm) (Yen and Guo, 2000b), which has been cryptanalyzed by Li and Zheng (2002b). The present paper evaluates the security of RCES, and points out that RCES is as weak as CKBA, though it seems more complicated than CKBA. In known/chosen-plaintext attack, only one or two known/chosen plain-images are enough to break this image encryption scheme. In addition, we also show that the security of RCES against brute-force attack was much overestimated in Chen et al. (2002) and Chen and Yen (2003).

Due to the special design of RCES, some of its essential security defects are very useful for revealing several general principles of designing secure image encryption schemes. This magnifies the cryptanalysis presented below, though RCES is not a very delicate cipher from the cryptographical point of view.

This paper is organized as follows. Section 2 briefly introduces RCES and its parent version CKBA. A detailed cryptanalysis of RCES is presented in Section 3, where some experimental results are given to support the theoretical analysis. Section 4 discusses some design principles drawn from the essential security defects of RCES. The last section concludes the paper.

2. Introduction to RCES

2.1. CKBA (Yen and Guo, 2000b) – The Parent Version of RCES

Assume that the size of the plain-image for encryption is $M \times N$,[1] CKBA can be described as follows.

2.1.1. The secret key

The secret key includes two bytes $key1$, $key2$, and the initial condition $x(0) \in (0,1)$ of the following chaotic Logistic map:

$$x(n+1) = \mu \cdot x(n) \cdot (1 - x(n)), \tag{1}$$

which is a well-studied chaotic system in chaos theory and behaves chaotically when $\mu > 3.5699\ldots$ (Devaney, 1989).

2.1.2. Initialization

Run the chaotic system to generate a chaotic sequence, $\{x(i)\}_{i=0}^{\lceil MN/8\rceil-1}$, where $\lceil a\rceil$ denotes the smallest integer that is not less than a. From the 16-bit binary representation of $x(i) = 0 \cdot b(16i+0)b(16i+1)\cdots b(16i+15)$, derive a pseudo-random binary sequence (PRBS), $\{b(i)\}_{i=0}^{2MN-1}$.

2.1.3. Encryption

For the plain-pixel $f(x,y)$ $(0 \leqslant x \leqslant M-1$, $0 \leqslant y \leqslant N-1)$, the corresponding cipher-pixel $f'(x,y)$ is determined by the following rule:

$$f'(x,y) = \begin{cases} f(x,y) \oplus key1, & B(x,y) = 3, \\ f(x,y) \odot key1, & B(x,y) = 2, \\ f(x,y) \oplus key2, & B(x,y) = 1, \\ f(x,y) \odot key2, & B(x,y) = 0, \end{cases} \tag{2}$$

where $B(x,y) = 2 \times b(x \times N + y) + b(x \times N + y + 1)$, and $\oplus$ and $\odot$ denote XOR and XNOR operations, respectively. Since $a \odot b = \overline{a \oplus b} = a \oplus \bar{b}$, the above equation is equivalent to

$$f'(x,y) = \begin{cases} f(x,y) \oplus key1, & B(x,y) = 3, \\ f(x,y) \oplus \overline{key1}, & B(x,y) = 2, \\ f(x,y) \oplus key2, & B(x,y) = 1, \\ f(x,y) \oplus \overline{key2}, & B(x,y) = 0. \end{cases} \tag{3}$$

2.1.4. Decryption

The decryption procedure is like that of the encryption, since $\oplus$ is an involutive operation.[2]

2.1.5. A constraint

Because not all values of $key1$ and $key2$ can make well-disorderly cipher-images, it is required that $key1$ and $key2$ have four different bits (a half of all). In fact, this constraint ensures that the encryption results of $key1$ and $key2$ are sufficiently far.

In Li and Zheng (2002b), CKBA was cryptanalyzed and the following facts were pointed out:

- the security of CKBA against the brute-force attack was over-estimated;
- CKBA is not secure against known/chosen-plaintext attacks, since only one known/chosen plain-image is enough to get an equivalent key, a mask image f_m, by XORing the plain-image f and the cipher-image f', pixel by pixel: $f_m = f \oplus f'$;

[1] In this paper, $M \times N$ is in the form "width × height".

[2] An involutive encryption operation satisfies $f(f(x,k),k) = x$ for any x and k.