Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm

David Arroyo [a,*], Chengqing Li [b], Shujun Li [c], Gonzalo Alvarez [a] and Wolfgang A. Halang [c]

[a] *Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas, Serrano 144, 28006 Madrid, Spain*

[b] *Department of Electronic Engineering, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong SAR, China*

[c] *FernUniversität in Hagen, Chair of Computer Engineering, 58084 Hagen, Germany*

Abstract

Chaotic systems have been broadly exploited through the last two decades to build encryption methods. Recently, two new image encryption schemes have been proposed, where the encryption process involves a permutation operation and an XOR-like transformation of the shuffled pixels, which are controlled by three chaotic systems. This paper discusses some defects of the schemes and how to break them with a chosen-plaintext attack.

Key words: Chaotic encryption, Lorenz system, Chen's system, hyper-chaos, logistic map, chosen-plaintext attack, permutation-only encryption algorithms, cryptanalysis

PACS: 05.45.Ac, 47.20.Ky.

* Corresponding author: David Arroyo (david.arroyo@iec.csic.es).

1 Introduction

When we think about exchanging information we are very interested in finding a way to make it fast and secure. Modern telecommunications technologies allow to send and receive files, images, and data in a relatively short time depending on the bandwidth available. Nowadays, the use of traditional symmetric and asymmetric cryptography is the way to secure the information exchange [1,2]. However, applications involving digital images and videos demand other encryption schemes. Indeed, the bulky size and the large redundancy of uncompressed videos/images make it necessary to look for new methods to deal with those features in order to facilitate the integration of the encryption in the whole processing procedure. For recent surveys on image and video encryption, please refer to [3–6].

The main features of chaotic systems (sensitivity to initial conditions, ergodicity, mixing property, simple analytic description and high complex behavior) make them very interesting to design new cryptosystems. Image encryption is an area where chaos has been broadly exploited. In fact, chaotic systems have been used to mask plain-images through XOR-like substitution operations [7], spatial permutation [8] or the combination of both techniques [9]. This paper is focused on two image encryption schemes proposed in [10,11]. In both papers the image encryption is based on a secret permutation derived from the logistic map, and a masking of the gray-scale values of the shuffled pixels with a keystream generated from one or two chaotic systems. The only difference between the two encryption schemes is that in [10] two chaotic systems (Lorenz and Chen's systems) are used to generate the keystream, while in [11] only one hyper-chaotic system is used. Because such a difference is independent of the security, we only focus on the cryptanalysis of the scheme proposed in [10].

The rest of this paper is organized as follows. The scheme under study is described briefly in the next section. In Section 3 some important problems of the cryptosystem are remarked. Then, a chosen-plaintext attack is described in Section 4 along with some experimental results. In the last section the conclusion is given.

2 The encryption scheme

Assuming that the size of the plain-image $\mathbf{I}$ is $M \times N$ and the cipher-image is $\mathbf{I}'$, the encryption scheme proposed in [10] can be described by the following two procedures. Please note that we use different notations from the original ones in [10] to get a simpler and clearer description.

- *Shuffling procedure*

    In this procedure, the plain-image $\mathbf{I}$ is permuted to form an intermediate image $\mathbf{I}^*$ according to a total shuffling matrix $\mathbf{P}^*$, which is derived by pseudo-randomly permuting the rows and columns of the original position matrix $\mathbf{P} = [(i, j)]$. The pseudo-random row and column permutations are generated by iterating the logistic map $x_{n+1} = 4x_n(1 - x_n)$ from a given initial condition x_0.
- *Masking procedure*

    In this procedure, the intermediate image $\mathbf{I}^*$ is further masked by a keystream $\{B(i)\}_{i=1}^{MN}$ as follows: $\forall i = 1 \sim MN$, $I'(i) = I^*(i) \oplus B(i) \oplus I'(i-1)$, where $I(i)$, $I'(i)$ denote the i-th pixels of $\mathbf{I}^*$ and $\mathbf{I}'$ (counted from left to right and from top to bottom), respectively, and $I'(0) = 128$.

    The keystream $\{B(i)\}_{i=1}^{MN}$ is generated by iterating the Lorenz and Chen systems and doing some postprocessing on all the 6 chaotic variables (the first N_0 iterations of the Lorenz system and the first M_0 iterations of Chen's system are discarded to enhance the security). Because our cryptanalysis succeeds regardless of the keystream's generation process, we ignore this part and readers are referred to Sec. 2.3 of [10] for details.

In [10], it is claimed that the secret key includes the initial values of the Lorenz and Chen systems and the number of initial iterations N_0, M_0. It is quite strange why the initial condition of the logistic map is not claimed to be part of the key, since the image encryption scheme is based on "a new total shuffling algorithm" (as can be seen in the title of [10]). In this cryptanalysis paper, we assume that the initial condition of the logistic map is also part of the key. We believe it is also the original intention of the authors of [10]. In addition, note that both $\mathbf{P}^*$ and $\{B(i)\}_{i=1}^{MN}$ are independent of the plaintext and ciphertext, so they can be used as an equivalent key.

3 Design weaknesses

In this section, we discuss some defects of the scheme under study.

3.1 Low sensitivity to the change of plain-image

It is well known that the ciphertext of a secure encryption scheme should be very sensitive to the change of plaintext [12, Rule 9]. Unfortunately, the encryption scheme under study fails to satisfy this requirement. Given two plain-images $\mathbf{I}_0$ and $\mathbf{I}_1$ with only one pixel difference at the position (i, j), the difference will be permuted to a new position (i^*, j^*) according to the shuffling matrix $\mathbf{P}^*$. Then, because all plain-pixels before (i^*, j^*) are identical

(a)

(b)

(c)

Fig. 1. Illustration of the low sensitivity to the change of the plain-image: (a) the first plain-image $\mathbf{I}_0$; (b) the second plain-image $\mathbf{I}_1$ (only the center pixel is different from $\mathbf{I}_0$); (c) the differential cipher-image $\mathbf{I}'_0 \oplus \mathbf{I}'_1$.

for the two plain-images, the ciphertexts will also be identical. This shows the low sensitivity of the image encryption scheme to changes in the plain-image. Figure 1 gives an example of this problem. It can be seen how the differential cipher-image is equal to zero for any pixel before (i^*, j^*) and equal to a constant value after that position.

3.2 Reduced key space

As claimed in [10], N_0 and M_0 are also part of the key. However, from an attacker's point of view, he/she only needs to guess the chaotic states after the N_0 and M_0 chaotic iterations as the initial conditions of the Lorenz and Chen's systems. In this way, N_0 and M_0 are removed from the key and the

key space is reduced.

3.3   Problem with chaotic iterations of Lorenz' and Chen's systems

In [10], the authors did not say anything about the time step τ of iterating the Lorenz and Chen systems. However, the randomness of the keystream $\{B(i)\}_{i=1}^{MN}$ is tightly dependent on the value of the time step. As an extreme example, if $\tau = 10^{-20}$, we will get a keystream of identical elements (according to the algorithm described in Section 2.3 of [10]). As a matter of fact, the value of τ is dependent on the multiplication factor 10^{13} occurring in Step 4 of the encryption process (see Section 2.3 of [10]): $x_i = \mathrm{mod}((\mathrm{abs}(x_i) - \mathrm{Floor}(\mathrm{abs}(x_i))) \times 10^{13}, 256)$.

3.4   Low encryption speed

Because the chaotic iterations of Lorenz' and Chen's systems involve complicated numerical differential functions, the encryption speed is expected to be very slow compared with other traditional ciphers. To asses this fact, we derived a modified encryption scheme from the original one by replacing the Lorenz and Chen systems with the logistic map, and then compared the encryption speeds of the two cryptosystems. Both cryptosystems were implemented using MATLAB on a PC with a 1.6 GHz processor and 512 MB of RAM. For images of size 256×256, the typical encryption time for the original cryptosystem in [10] was around 5.8 s, while the modified cryptosystem based on the logistic map required on average around 1.2 s to encrypt an image. The experiments have clearly shown that using continuous chaotic systems can drastically reduce the encryption speed. Since there are also no other obvious merits in using continuous chaotic systems rather than a simple discrete-time chaotic map, the use of the Lorenz and Chen systems in the image encryption scheme under study is unnecessary. Instead, these continuous chaotic systems can be replaced by a simpler discrete-time chaotic map without compromising the security.

4   Chosen-plaintext attack

When a variation of stream cipher is created, as in the case under study, obtaining the keystream is totally equivalent to obtaining the key whenever different plain-images are encrypted using the same key. In this section, we

present a chosen-plaintext attack which allows to recover both the keystream and the shuffling matrix.

Let us choose a plain-image $\mathbf{I}_1$ such that $\forall i, j = 1 \sim MN$, $I_1(i) = I_1(j) = a$. In this case, the shuffling part does not work, so we have $\mathbf{I}_1^* = \mathbf{I}_1$. Then, we can recover the keystream as follows: $\forall i = 1 \sim MN$, $B(i) = I_1(i) \oplus I_1'(i) \oplus I_1'(i-1)$.

After removing the masking part, we can try to recover the shuffling matrix. According to the general cryptanalysis on permutation-only ciphers in [13], only $\lceil \log_{256}(MN) \rceil$ chosen plain-images are needed to recover the shuffling matrix $\mathbf{P}^*$. In total we need $\lceil \log_{256}(MN) \rceil + 1$ chosen plain-images to perform this chosen-plaintext attack.

With the aim of verifying the proposed attack, several experiments have been done. One of the examples is shown in Fig. 2, where the images are of size 256×256 and the secret key involved is shown in Table 1. As it was mentioned above, the shuffling process is broken using $\log_{256}(MN) = 2$ chosen plain-images, while the masking procedure cryptanalysis requires one chosen plain-image. The three chosen plain-images allow to decipher the cipher-image included in Fig. 2a and thus to get the corresponding plain-image (Fig. 2b), even when the secret key is unknown. To conclude this section, it is necessary to point out that the chosen-plaintext attack proposed here was independently worked out, although a similar attack was reported by other researchers in [14] to cryptanalyze [11].

Table 1
Key value used in the experiment.

$x_1(0)$	$x_2(0)$	$x_3(0)$	$x_4(0)$	$x_5(0)$	$x_6(0)$	N_0	M_0	x_0
0.3	-0.4	1.2	10.2	-3.5	4.4	3000	2000	0.4
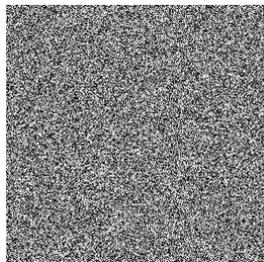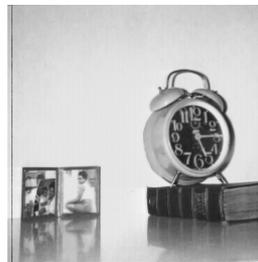
(a)   (b)

Fig. 2. The result of the chosen-plaintext attack: (a) a cipher-image encrypted with the key as shown in Table 1; (b) the decrypted plain-image using the equivalent key $\left(\mathbf{P}^*, \{B(i)\}_{i=1}^{MN} \right)$ obtained via the chosen-plaintext attack.

5 Conclusions

The security of the image encryption scheme proposed in [10] has been analyzed in detail. The cryptanalytic results are also valid for the other scheme proposed in [11]. It has been shown that the equivalent secret key can be recovered in a chosen-plaintext attack with only $\lceil \log_{256}(MN) \rceil + 1$ chosen plainimages. In addition, some other defects have also been distinguished in the scheme under study. Among those defects, it is necessary to emphasize the one concerning the encryption speed, since it informs about the non-convenience of continuous-time chaotic systems for implementing fast encryption procedures. The weak security properties frustrate the usage of the scheme in practice.

Acknowledgments

References

[1] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.

[2] B. Schneier, Applied Cryptography, 2nd Edition, John Wiley, New York, USA, 1996.

[3] S. Li, G. Chen, X. Zheng, Chaos-based encryption for digital images and videos, in: B. Furht, D. Kirovski (Eds.), Multimedia Security Handbook, CRC Press, LLC, 2004, Ch. 4, pp. 133–167.

[4] A. Uhl, A. Pommer, From Digital Rights Management to Secured Personal Communication, Springer, 2005.

[5] B. Fuhrt, E. Muharemagic, D. Socek, Image encryption algorithms, in: Multimedia Encryption and Watermarking, Springer, 2005, Ch. 5, pp. 79–120.

[6] W. Zeng, H. Yu, C.-Y. Lin (Eds.), Multimedia Security Technologies for Digital Rights Management, Academic Press, 2006.

[7] H.-C. Chen, J.-C. Yen, A new cryptography system and its VLSI realization, J. Systems Architecture 49 (7-9) (2003) 355–367.

[8] J.-C. Yen, J.-I. Guo, Efficient hierarchical chaotic image encryption algorithm and its VLSI realisation, IEE Proceedings - Vision, Image and Signal Processing 147 (2) (2000) 167–175.

[9] G. Chen, Y. Mao, C. K. Chui, A symmetric image encryption scheme based on 3d chaotic cat maps, Chaos, Solitons and Fractals 21 (3) (2004) 749–761.

[10] T. Gao, Z. Chen, Image encryption based on a new total shuffling algorithm, Chaos, Solitons and Fractals 38 (1) (2008) 213–220.

[11] T. Gao, Q. Gu, Z. Chen, A new image encryption algorithm based on hyer-chaos, Phys. Lett. A 372 (4) (2007) 394–400.

[12] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, Int. J. Bifurcation and Chaos 16 (8) (2006) 2129–2151.

[13] S. Li, C. Li, G. Chen, N. G. Bourbakis, K.-T. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, Signal Processing: Image Communication 23 (3) (2008) 212–223.

[14] R. Rhouma, S. Belghith, Cryptanalysis of a new image encryption algorithm based on hyper-chaos, Phys. Lett. A 372 (38) (2008) 5973–5978.