On the security of the Yen-Guo's domino signal encryption algorithm (DSEA)

Chengqing Li [a], Shujun Li [b,*] Der-Chyuan Lou [c] and Dan Zhang [d]

[a] *Department of Mathematics, Zhejiang University, Hangzhou 310027, China*

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

[c] *Department of Electrical Engineering, Chung Cheng Institute of Technology, National Defense University, Taiwan, China*

[d] *College of Computer Science, Zhejiang University, Hangzhou 310027, China*

Abstract

Recently, a new domino signal encryption algorithm (DSEA) was proposed for digital signal transmission, especially for digital images and videos. This paper analyzes the security of DSEA, and points out the following weaknesses: 1) its security against the brute-force attack was overestimated; 2) it is not sufficiently secure against ciphertext-only attacks, and only one ciphertext is enough to get some information about the plaintext and to break the value of a sub-key; 3) it is insecure against known/chosen-plaintext attacks, in the sense that the secret key can be recovered from a number of continuous bytes of only one known/chosen plaintext and the corresponding ciphertext. Experimental results are given to show the performance of the proposed attacks, and some countermeasures are discussed to improve DSEA.

Key words: DSEA, dominos, cryptanalysis, encryption, ciphertext-only attack, known-plaintext attack, chosen-plaintext attack

1 Introduction

In today's networked world, the security issues become more and more important, so various encryption algorithms have been developed to fulfill the needs

⋆ This paper has been published in *Journal of Systems and Software*, vol. 79, no. 2, pp. 253-258, 2006.

* The corresponding author, personal web site: `http://www.hooklee.com`.

of different applications (Schneier, 1996). In recent years, Yen and Guo et al. proposed a series of chaos-based [1] signal/image encryption schemes (Li et al., 2004b, Sec. 4.4.3), some of which have been broken according to the works reported in (Li and Zheng, 2002a,b; Li et al., 2005b, 2004a,c, 2005a). The present paper gives the cryptanalysis results on a new Yen-Guo encryption scheme called DSEA (Yen and Guo, 2003), which has not been cryptanalyzed before.

DSEA encrypts the plaintext block by block, which is composed of multiple bytes. The first byte of each block is masked by part of the secret key, and other bytes are masked by the previous cipher-byte, under the control of a chaotic pseudo-random bit sequence (PRBS). That is to say, DSEA works like the dominos. This paper analyzes the security of DSEA, and points out the following defects: 1) its security against the brute-force attack was overestimated; 2) it is not sufficiently secure against ciphertext-only attacks, and only one ciphertext is enough to get some information about the plaintext and to break the value of a sub-key; 3) it is insecure against known/chosen-plaintext attacks, in the sense that the secret key can be recovered from a number of continuous bytes of only one known/chosen plaintext and the corresponding ciphertext.

The rest of this paper is organized as follows. At first, Sec. 2 gives a brief introduction to DSEA. Then, the cryptanalysis results are presented in detail in Sec. 3, with some experimental results. Section 4 discusses how to improve DSEA. The last section concludes the paper.

2 Domino Signal Encryption Algorithm (DSEA)

Assume that the plaintext is $g = \{g(n)\}_{n=0}^{M-1}$ and that the ciphertext is $g' = \{g'(n)\}_{n=0}^{M-1}$, where $g(n)$ and $g'(n)$ denote the n-th plain-byte and cipher-byte, respectively. Then, the encryption procedure of DSEA can be described as follows (see also Fig. 1).

- *The secret key*: two integers, $L \in \{1, \cdots, M\}$, $initial\_key \in \{0, \cdots, 255\}$, the control parameter μ and the initial condition $x(0)$ of the following chaotic Logistic map(Devaney, 1989; Hao, 1993):

$$x(k+1) = \mu \cdot x(k) \cdot (1 - x(k)). \tag{1}$$

[1] Chaos is a dynamical phenomenon demonstrated in many dynamical systems (Devaney, 1989; Hao, 1993). Due to the tight relationship between chaos and cryptography, chaotic systems have been used to design encryption schemes since 1990s. For a survey of digital chaotic ciphers, see (Li, 2003, Chap. 2).

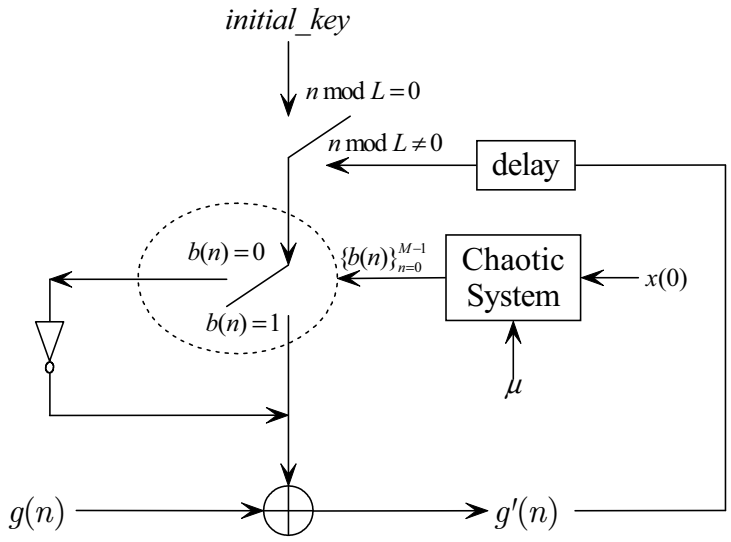


Fig. 1. The diagrammatic view of the encryption procedure of DSEA.

- *The initialization procedure*: under 8-bit finite computing precision, run the Logistic map from $x(0)$ to generate a chaotic sequence $\{x(k)\}_{k=0}^{\lceil M/8\rceil-1}$, and then extract the 8 significant bits of $x(k)$ to yield a PRBS $\{b(n)\}_{n=0}^{M-1}$, where $x(k)=\sum_{i=0}^{7}\left(b_{8k+i}\cdot 2^{-(i+1)}\right)=0.b_{8k+0}\cdots b_{8k+7}$.
- *The encryption procedure*: for $n=0\sim M-1$, do

$$g'(n)=\begin{cases} g(n)\oplus true\_key, & b(n)=1,\\ g(n)\oplus \overline{true\_key}, & b(n)=0,\end{cases}$$

where

$$true\_key=\begin{cases} initial\_key, & n \bmod L=0,\\ g'(n-1), & n \bmod L\neq 0,\end{cases}$$

and $\oplus$ denotes the bitwise XOR operation.

The decryption procedure is identical with the above encryption procedure, since XOR is an invertible operation.

3 Cryptanalysis

3.1 Brute-force attack

The brute-force attack is the attack of exhaustively searching the secret key from the set of all possible keys (Schneier, 1996). Apparently, the attack complexity is determined by the size of the key space and the complexity of verifying each key. The secret key of DSEA is $(L, initial\_key, \mu, x(0))$, which

has $M \cdot 2^{3\cdot 8} = M \cdot 2^{24}$ possible values. Taking the complexity of verifying each key into consideration, the total complexity of searching for all possible keys is $O\left(2^{24} \cdot M^2\right)$. When the plaintext is selected as a typical image of size 256×256, the complexity will be $O(2^{56})$, which is much smaller than $O(2^M \cdot M) = O(2^{65552})$, the complexity claimed in (Yen and Guo, 2003). Note that the real complexity is even smaller since not all values of μ can ensure the chaoticity of the Logistic map (Devaney, 1989; Hao, 1993). That is, the security of DSEA against brute-force attacks was over-estimated much in (Yen and Guo, 2003). In today's digitized and networked world, the complexity of order $O(2^{128})$ is required for a cryptographically-strong cipher (Schneier, 1996), which means DSEA is not practically secure.

3.2 Ciphertext-only attacks

Ciphertext-only attacks are such attacks in which one can access a set of ciphertexts (Schneier, 1996). Since the transmission channel is generally insecure, the security against ciphertext-only attacks are required for any ciphers. However, it is found that DSEA is not sufficiently secure against ciphertext-only attacks, since much information about the plaintext and the secret key can be found from even one ciphertext.

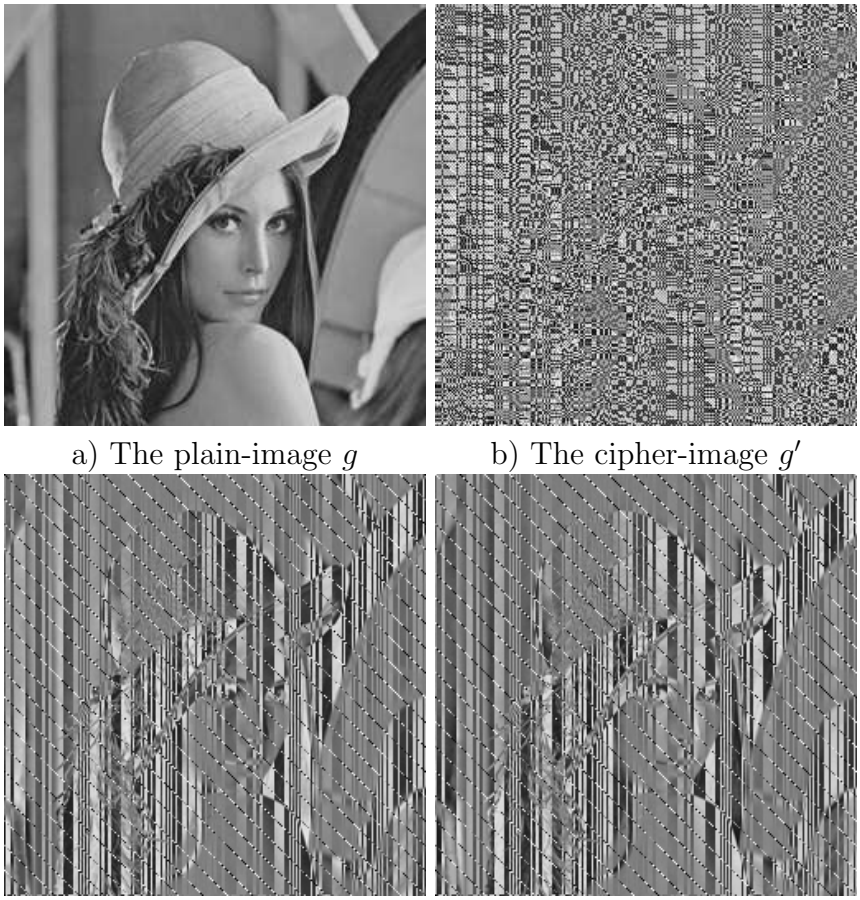
Given an observed ciphertext g', generate two mask texts, g_0^* and g_1^*, as follows: $g_0^*(0) = 0$, $g_1^*(0) = 0, \forall\ n = 1 \sim M-1$, $g_0^*(n) = g'(n) \oplus \overline{g'(n-1)}$, $g_1^*(n) = g'(n) \oplus g'(n-1)$. From the encryption procedure of DESA, it can be easily verified that the following result is true when $n \bmod L \neq 0$:

$$g(n) = \begin{cases} g_0^*(n), & b(n) = 0, \\ g_1^*(n), & b(n) = 1, \end{cases} \tag{2}$$

which means that $g(n)$ is equal to either $g_0^*(n)$ or $g_1^*(n)$. Assuming that each chaotic bit distributes uniformly over $\{0, 1\}$, one can deduce that the percentage of right plain-pixels in g_0^* and g_1^* is not less than $\frac{L-1}{L} \cdot \frac{1}{2} = \frac{1}{2} - \frac{1}{2L}$. When L is large, about half pixels in g_0^* and g_1^* are plain-pixels in g, and it is expected that some visual information of the plain-image can be distinguished from g_0^* and g_1^*.

To verify the above idea, one 256×256 image, "Lenna", has been encrypted to get g_0^* and g_1^*, with the following secret parameters: $L = 15$, $initial\_key = 170$, $\mu = 251/2^6 \approx 3.9219$, $x(0) = 69/2^8 \approx 0.2695$. The experimental results are shown in Fig. 2. In g_0^* there are 27726 pixels that are identical with those in g, and in g_1^* there are 33461 such pixels. Observing Figs. 2 c and d, one can see that the plain-image roughly emerges from both g_0^* and g_1^*.

In addition, from either g_0^* or g_1^*, it is possible to directly get the value of



a) The plain-image g b) The cipher-image g'

c) The mask image g_0^* d) The mask image g_1^*

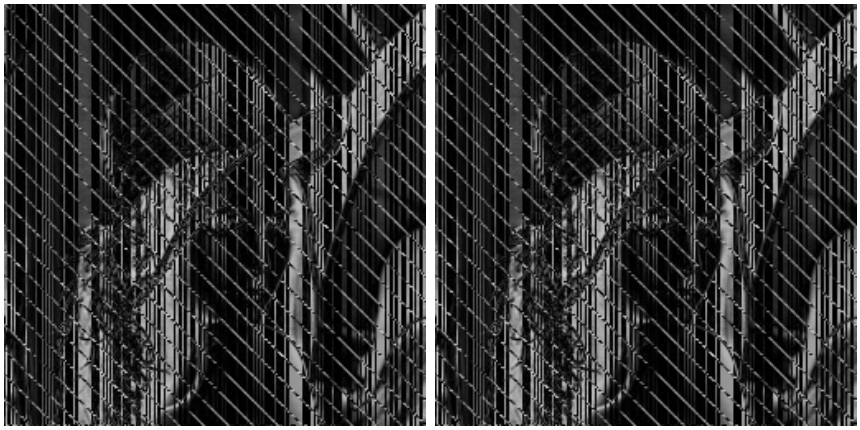
Fig. 2. A ciphertext-only attack to DSEA.

L, if there exists strong correlation between adjacent bytes of the plaintext (speeches and natural images are good examples). This is due to the probability difference existing between the following two kinds of plain-bytes:

- when $n \bmod L \neq 0$, $g_0^*(n) = g(n)$ and $g_1^*(n) = g(n)$ with a probability of $\frac{1}{2}$;
- when $n \bmod L = 0$, $g_0^*(n) = g(n)$ and $g_1^*(n) = g(n)$ with a probability [2] of $\frac{1}{256}$: $g_0^*(n) = g(n)$ if and only if $g'(n-1) = \overline{initial\_key}$; $g_1^*(n) = g(n)$ if and only if $g'(n-1) = initial\_key$.

When there exists strong correlation between adjacent bytes, the above probability difference implies that there exists strong discontinuity around each position satisfying $n \bmod L = 0$ (with a high probability). The fixed occurrence period of such discontinuous bytes will generate periodically-occurring straight lines in the mask text when it is an image or displayed in 2-D mode, as shown in Figs. 2c and d. Then, it is easy to determine the occurrence period, i.e., the value of L, by checking the horizontal distance between any

[2] Without loss of generality, it is assumed that each cipher-byte distributes uniformly in $\{0, \cdots, 255\}$.



a) $g^*_{d,0}$ b) $g^*_{d,1}$

Fig. 3. The differential images of g^*_0 and g^*_1.

two adjacent lines. To make the straight line clearer, one can calculate the differential images of g^*_0 and g^*_1, as shown in Fig. 3, where the differential image of an image $g = \{g(n)\}_{n=0}^{M-1}$ is defined as follows: $g_d(0) = g(0)$ and $\forall\ n = 1 \sim M-1$, $g_d(n) = |g(n) - g(n-1)|$. Note that the two differential images of g^*_0 and g^*_1 are identical according to the following theorem, from which one can get that $|g^*_0(n) - g^*_0(n-1)| = |g'(n) \oplus \overline{g'(n-1)} - g'(n-1) \oplus \overline{g'(n-2)}| = |g'(n) \oplus g'(n-1) - g'(n-1) \oplus g'(n-2)| = |g^*_1(n) - g^*_1(n-1)|$.

Theorem 1 *For any three s-bit integers, a, b, c, it is true that $|(a \oplus b) - (b \oplus c)| = |(a \oplus \bar{b}) - (b \oplus \bar{c})|$.*

Proof: Introduce four new variables, $A = a \oplus b$, $B = b \oplus c$, $A' = a \oplus \bar{b}$, $B' = b \oplus \bar{c}$. It can be easily verified that $A' = \overline{A}$ and $B' = \overline{B}$, since $a \oplus \bar{b} = a \oplus b \oplus b \oplus \bar{b} = a \oplus b \oplus (2^s - 1) = \overline{a \oplus b}$. That is, $(a \oplus b) - (b \oplus c) = A - B$ and $(a \oplus \bar{b}) - (b \oplus \bar{c}) = \overline{A} - \overline{B}$. Let $A = (A_0 \cdots A_{s-1})_2 = \sum_{i=0}^{s-1} A_i \cdot 2^i$, $B = (B_0 \cdots B_{s-1})_2 = \sum_{i=0}^{s-1} B_i \cdot 2^i$. Since $\forall\ A_i, B_i \in \{0, 1\}$, $A_i - B_i = \bar{B}_i - \bar{A}_i$, it is obvious that $A - B = \sum_{i=0}^{s-1}(A_i - B_i) \cdot 2^i = \sum_{i=0}^{s-1}(\bar{B}_i - \bar{A}_i) \cdot 2^i = \overline{B} - \overline{A}$. As a result, $|(a \oplus b) - (b \oplus c)| = |A - B| = |\overline{B} - \overline{A}| = |\overline{A} - \overline{B}| = |(a \oplus \bar{b}) - (b \oplus \bar{c})|$, which completes the proof. ■

3.3 Known/chosen-plaintext attacks

Known/chosen-plaintext attacks are such attacks in which one can access/choose a set of plaintexts and observe the corresponding ciphertexts (Schneier, 1996). In today's networked world, such attacks occur more and more frequently. For a cipher with a high level of security, the security against both known-plaintext and chosen-plaintext attacks are required. Although it was claimed that DSEA can resist this kind of attacks (Yen and Guo, 2003, Sec. IV.B), we found this claim is not true: with a limited number of continuous plain-bytes

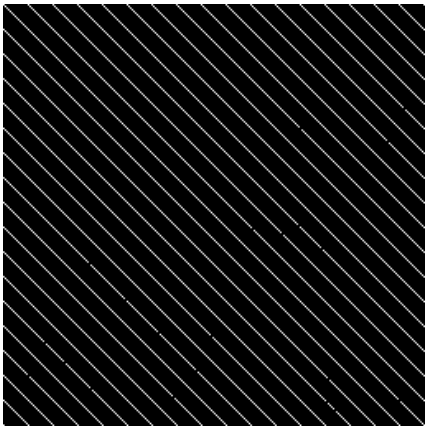


Fig. 4. The enhanced differential image g_d^*.

of only one known/chosen plaintext, one can completely break the secret key to decrypt other unknown plain-bytes of the known/chosen plaintext and any new ciphertexts encrypted with the same key. Apparently, even when the secret key is changed for each plaintext (as mentioned in (Yen and Guo, 2003, Sec. IV.B)), DSEA is insecure against known/chosen-plaintext attacks. In the following, let us discuss how to break the four sub-keys, respectively.

1) Breaking the sub-key L: as mentioned above, once one gets a ciphertext, he can easily deduce the value of L by observing the periodically-occurring straight lines in the two constructed mask texts, g_0^* and g_1^*. Furthermore, since the plaintext is also known, it is possible to generate an enhanced differential image, g_d^*, as follows: $g_d^*(0) = 0$, and $\forall\ n = 1 \sim M - 1$,

$$g_d^*(n) = \begin{cases} 0, & g(n) \in \{g_0^*(n), g_1^*(n)\}, \\ 255, & g(n) \notin \{g_0^*(n), g_1^*(n)\}. \end{cases} \tag{3}$$

See Fig. 4 for the enhanced differential image corresponding the cipher-image shown in Fig. 2b. Compared with Fig. 3, one can see that the straight lines become clearer.

2) Breaking the initial_key: for all values of n that satisfy $n \bmod L = 0$, it is obvious that

$$initial\_key = \begin{cases} g(n) \oplus g'(n), & b(n) = 1, \\ \overline{g(n) \oplus g'(n)}, & b(n) = 0. \end{cases} \tag{4}$$

Note that it is possible to uniquely determine the value of *initial_key*, when there may exist pixels satisfying $n \bmod L = 0$ and $g_d^*(n) = 0$, i.e., $g(n) \in \{g_0^*(n), g_1^*(n)\} = \left\{g'(n) \oplus \overline{g'(n-1)}, g'(n) \oplus g'(n-1)\right\}$. Considering $g'(n) =$

$g(n) \oplus initial\_key$, one can immediately deduce that

$$initial\_key = \begin{cases} g'(n-1), & g(n) = g_1^*(n), \\ \overline{g'(n-1)}, & g(n) = g_0^*(n). \end{cases} \tag{5}$$

3) Breaking the chaotic PRBS and the other two sub-keys: once L and $initial\_key$ have been determined, the chaotic PRBS, $\{b(n)\}_{n=0}^{M-1}$, can be immediately derived as follows:

- when $n \bmod L \neq 0$: if $g(n) = g_0^*(n)$ then $b(n) = 0$, else $b(n) = 1$;
- when $n \bmod L = 0$: if $initial\_key = g(n) \oplus g'(n)$ then $b(n) = 1$, else $b(n) = 0$.

Once $\{b(n)\}_{n=0}^{M-1}$ is uniquely determined, $x(0) = 0.b(0) \cdots b(7)$ can be immediately recovered.

With 16 consecutive chaotic bits, $b(8k+0) \sim b(8k+15)$, one can further derive two consecutive chaotic states: $x(k) = 0.b(8k+0) \cdots b(8k+7)$ and $x(k+1) = 0.b(8k+8) \cdots b(8k+15)$, and then derive an estimation of the sub-key μ as

$$\widetilde{\mu} = \frac{x(k+1)}{x(k) \cdot (1 - x(k))}. \tag{6}$$

Due to the quantization errors introduced in the finite-precision arithmetic, generally $x(k+1) \neq \mu \cdot x(k) \cdot (1 - x(k))$, so $\widetilde{\mu} \neq \mu$. Fortunately, following the error analysis of $\widetilde{\mu}$ in (Li et al., 2004a, Sec. 3.2), the following result has been obtained: when $x(k+1) \geq 2^{-n}$ $(n = 1 \sim 8)$, $|\widetilde{\mu} - \mu| < 2^{n+3} \cdot 2^{-8}$. Specially, when $x(k+1) \geq 2^{-1} = 0.5$, $|\widetilde{\mu} - \mu| < 2^4 \cdot 2^{-8}$, which means that one can exhaustively search for $2^4 = 16$ values in the neighborhood of $\widetilde{\mu}$ to find the right value of μ. To verify which searched value is the right one, one can iterate the Logistic map from $x(k+1)$ for some times to get some new chaotic states and then check the coincidence between these chaotic states and corresponding recovered chaotic bits.

With the above steps, the whole secret key $(L, initial\_key, \mu, x(0))$ can be recovered, and then be used for decryption. For the plain-image "Lenna", a breaking result is shown in Fig. 5. It can be verified that the complexity of the known/chosen-plaintext attacks is only $O(M)$, which means a perfect breaking of DSEA.

4 Improving DSEA

In this section, we study some possible remedies to DSEA to resist the proposed attacks. It is concluded that DSEA cannot be simply enhanced to resist known/chosen-plaintext attacks.

Fig. 5. The recovered plain-image of "Lenna" in a known-plaintext attack.

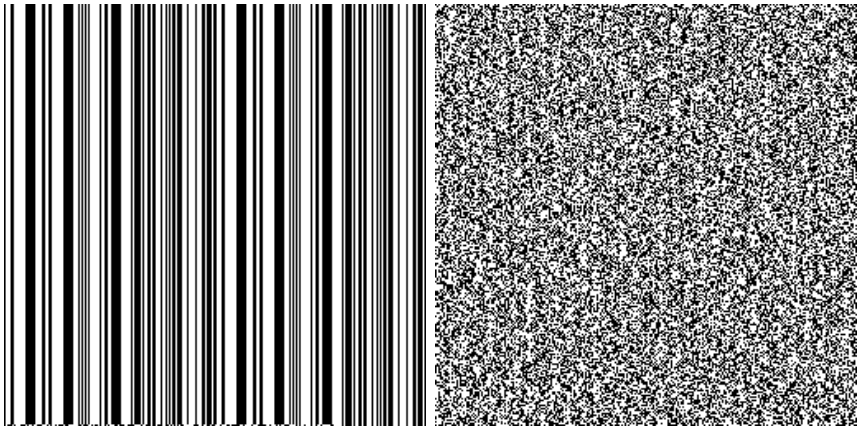
To ensure the complexity of the brute-force attack cryptographically large, the simplest idea is to increase the presentation precision of $x(0)$ and μ. Binary presentations of $x(0)$ and μ with 64-bit (long integers) are suggested to provide a complexity not less than $O(2^{128})$ against the brute-force attack.

Apparently, the insecurity of DSEA against ciphertext-only and known/chosen-plaintext attacks is mainly due to the invertibility of XOR operations. This is actually the weakness of all XOR-based stream ciphers. To make DSEA securer, one has to change the encryption structure and/or the basic masking operations, in other words, one has to design a completely new cipher, instead of enhancing DSEA to design a modified cipher.

In addition, there exists a special flaw in DSEA. According to (Li, 2003, Sec. 2.5), when a chaotic system is implemented in s-bit finite computing precision, each chaotic orbit will lead to a cycle whose length is smaller than 2^s (and generally much smaller than 2^s). Figure 6a shows the pseudo-image of the chaotic PRBS recovered in a known-plaintext attack. It is found that the cycle of the chaotic PRBS is only $2^6 = 64$ and the period of the corresponding chaotic orbit is only $2^3 = 8$. Such a small period of the chaotic PRBS will make all attacks easier. To amend this defect, using a higher implementation precision or floating-point arithmetic is suggested. Figure 6b gives the pseudo-image of the chaotic PRBS when the chaotic states are calculated under double-precision floating-point arithmetic. It is obvious that the short-period effect of the chaotic PRBS is effectively avoided.

5 Conclusion

In this paper, the security of a recently-proposed signal security system called DSEA (Yen and Guo, 2003) has been studied in detail. It is pointed out that DSEA is not secure enough against the following attacks: the brute-force



a) 8-bit fixed-point arithmetic b) double-precision floating-point arithmetic

Fig. 6. The pseudo-image of the chaotic PRBS, under two different finite-precision arithmetics.

attack, ciphertext-only attacks, and known/chosen-plaintext attacks. Experimental results are also given to support the theoretical analysis. Also, some remedies of enhancing the performance of DSEA are discussed. As a conclusion, DSEA is not suggested in serious applications requiring a high level of security.

6 Acknowledgements

This research was partially supported by the National Natural Science Foundation, China, under grant no. 60202002, and by the Applied R&D Centers of the City University of Hong Kong under grants nos. 9410011 and 9620004.

References

Devaney, R. L., 1989. An Introduction to Chaotic Dynamical Systems. Addison-Wesley, Redwood City, California.

Hao, B.-L., 1993. Starting with Parabolas: An Introduction to Chaotic Dynamics. Shanghai Scientific and Technological Education Publishing House, Shanghai, China, (In Chinese).

Li, C., Li, S., Chen, G., Chen, G., 2005a. Cryptanalysis of a new signal security system for multimedia data transformation. accepted by EURASIP J. Applied Signal Processing, preprint available online at `http://www.hooklee.com/pub.html`.

Li, C., Li, S., Zhang, D., Chen, G., 2004a. Cryptanalysis of a chaotic neural network based multimedia encryption scheme. In: Advances in Multimedia

Information Processing - PCM 2004 Proceedings, Part III. Vol. 3333 of Lecture Notes in Computer Science. Springer-Verlag, pp. 418–425, preprint available online at http://www.hooklee.com/pub.html.

Li, C., Li, X., Li, S., Chen, G., 2005b. Cryptanalysis of a multistage encryption system. accepted by IEEE Int. Symposium on Circuits and Systems, preprint available online at http://www.hooklee.com/pub.html.

Li, S., 2003. Analyses and new designs of digital chaotic ciphers. Ph.D. thesis, School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China, available online at http://www.hooklee.com/pub.html.

Li, S., Chen, G., Zheng, X., 2004b. Chaos-based encryption for digital images and videos. In: Furht, B., Kirovski, D. (Eds.), Multimedia Security Handbook. CRC Press, LLC, Ch. 4, pp. 133–167, preprint available online at http://www.hooklee.com/pub.html.

Li, S., Li, C., Chen, G., Mou, X., 2004c. Cryptanalysis of the RCES/RSES image encryption scheme. Cryptology ePrint Archive: Report 2004/376, available online at http://eprint.iacr.org/2004/376.

Li, S., Zheng, X., 2002a. Cryptanalysis of a chaotic image encryption method. In: Proc. IEEE Int. Symposium on Circuits and Systems (ISCAS'2002). Vol. II. pp. 708–711.

Li, S., Zheng, X., 2002b. On the security of an image encryption method. In: Proc. IEEE Int. Conference on Image Processing (ICIP'2002). Vol. 2. pp. 925–928.

Schneier, B., 1996. Applied Cryptography – Protocols, Algorithms, and Souce Code in C, 2nd Edition. John Wiley & Sons, Inc., New York.

Yen, J.-C., Guo, J.-I., 2003. The design and realization of a new domino signal security system. Journal of the Chinese Institute of Electrical Engineering 10 (1), 69–76.