Performance analysis of Jakimoski-Kocarev attack on a class of chaotic cryptosystems

Shujun Li [a,*], Xuanqin Mou [a], Zhen Ji [b], Jihong Zhang [b] and Yuanlong Cai [a]

[a] *Institute of Image Processing, School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an, Shaanxi 710049, P. R. China*

[b] *College of Information Engineering, Shenzhen University, Shenzhen, Guangdong 518060, P. R. China*

Abstract

Recently G. Jakimoski and L. Kocarev cryptanalzed two chaotic cryptosystems without using chaotic synchronization – Baptista cryptosystem and Alvarez cryptosystem. As a result, they pointed out that neither of the two cryptosystems are secure to known-plaintext attacks. In this letter, we re-study the performance of Jakimoski-Kocarev attack on Baptista cryptosystem and find that it is not efficient enough as a practical attack tool. Furthermore, a simple but effective remedy is presented to resist Jakimoski-Kocarev attack, and the detailed discussion on its performance are given.

Key words: chaotic encryption system; cryptanalysis; cryptography

1 Introduction

The tight relationship between chaos and cryptography makes it natural to employ chaotic systems to design new crytposystems [1–3]. From 1989 on, many different chaotic encryption systems have been proposed, including secure communications based on chaotic synchronization of analog circuits [3] and chaotic cryptosystems without using chaotic synchronization (most are designed for implementation on digital circuits or computers) [2, 4–18]. Since cryptanalytic works [19, 20] have shown that most chaotic secure communications based on chaotic synchronization are not secure enough, the alternative

[⋆] This paper has been published in *Physics Letters A*, 307(1):22-28, 2003.

[*] Corresponding author: Shujun Li (`http://www.hooklee.com`).

idea of designing chaotic encryption systems without chaotic synchronization has attracted more and more attention recently. Among the chaotic cryptosystems without chaotic synchronization, some [8–11] have been known to be insecure from strong cryptographic viewpoint [21–24], and others are still waiting for further cryptanalytic works to measure their security exactly.

In the past few years, two recently-proposed chaotic cryptosystems without using chaotic synchronization have attracted much attention - *Baptista cryptosystem* [12] and *Alvarez cryptosystem* [11]. In [13], W.-K. Wong et al. enhanced *Baptista cryptosystem* with some modifications. In [23], *Alvarez cryptosystem* is successfully cryptanalyzed by four different attacks. In [14], two essential defects of *Alvarez cryptosystem* have been distinguished and an improved version of *Alvarez cryptosystem* is proposed to resist the four known attacks in [23]. In [25], G. Jakimoski and L. Kocarev analyzed both of the above two chaotic cryptosystems and pointed out that neither of them are secure to known-plaintext attacks.

This letter studies the performance and countermeasure of one Jakimoski-Kocarev attack presented in [25], which is originally claimed to attack *Baptista cryptosystem* in [12], but can also be easily extended to break the modified *Baptista cryptosystem* in [13] and the improved *Alvarez cryptosystem* in [14]. Our study leads to a different result from the one given in [25]: Jakimoski-Kocarev attack is not efficient enough to break related chaotic cryptosystems, and a simple remedy can be used to effectively resist this attack.

2 Related chaotic cryptosystems

Firstly, let us give a brief introduction of original *Baptista cryptosystem* [12]. Here a rather different way from the one in [12] is used to make the description clearer. Given a one-dimensional chaotic map $F: X \to X$, divide an interval $[x_{min}, x_{max}) \subseteq X$ into S ϵ-intervals $X_1 \sim X_S$: $X_i = [x_{min} + (i-1)\varepsilon, x_{min} + i\varepsilon)$, where $\varepsilon = (x_{max} - x_{min})/S$. Assume plain messages are composed by n different characters $\alpha_1, \alpha_2, \cdots, \alpha_S$, use a bijective map

$$f_S : \boldsymbol{X_\epsilon} = \{X_1, X_2, \cdots, X_S\} \to \boldsymbol{A} = \{\alpha_1, \alpha_2, \cdots, \alpha_S\} \tag{1}$$

to associate the different ϵ-intervals with different characters. Define a new function $f'_S : X \to \boldsymbol{A}$: $f'_S(x) = f_S(X_i)$, if $x \in X_i$.

Given a plain-message $M = \{m_1, m_2, \cdots, m_i, \cdots\}$ ($m_i \in \boldsymbol{A}$), *Baptista cryptosystem* can be described as follows.

The chaotic system: Logistic map $F = bx(1-x)$.

The secret key: the association map S [1], the initial condition x_0 and the control parameter b of the logistic system.

Encryption procedure: i) The first plain-character m_1 – Iterate the chaotic system from x_0 to find a chaotic state x that satisfies $f'_S(x) = m_1$, and record the iteration number C_1 as the first cipher-message unit and $x_0^{(1)} = F^{C_1}(x_0)$; ii) The i^{th} plain-message character m_i – Iterate the chaotic system from $x_0^{(i-1)} = F^{C_1+C_2+\cdots+C_{i-1}}(x_0)$ to find a chaotic state x satisfying $f'_S(x) = m_i$, record the iteration number C_i as the i^{th} cipher-message unit and $x_0^{(i)} = F^{C_i}(x_0^{(i-1)})$.

Decryption: For each ciphertext unit C_i, iterate the chaotic system for C_i times from the last chaotic state $x_0^{(i)} = F^{C_1+C_2+\cdots+C_{i-1}}(x_0)$, and then use $x_0^{(i)} = F^{C_i}(x_0^{(i-1)})$ to derive the plain-character m_i by the association map f_s.

Constraints of C_i: Each cipher-message unit C_i should yield to the constraint $N_0 \leq C_1 \leq N_{max}$ ($N_0 = 250$ and $N_{max} = 65532$ in [12]). Since there exist many options for each C_i in $[N_0, N_{max}]$, an extra coefficient η is used to choose a right number: if $\eta = 0$, C_i is chosen as the minimal number satisfying $f'_S(x) = m_i$; if $\eta \neq 0$, C_i is chosen as the minimal number satisfying $f'_S(x) = m_i$ and $\kappa \geq \eta$ simultaneously, where κ is a pseudo-random number with normal distribution within the interval $[0, 1]$.

The above cryptosystem has two defects: a) the distribution of the plaintext is not balanced, and the occurrence probability decays exponentially as C_i increases from N_0 to N_{max}; b) at least N_0 chaotic iterations are needed to encrypt a plain-character, which makes the encryption speed very slow compared with other conventional ciphers. In [13], the above original cryptosystem is improved by the following modification: for each plain-character m_i, firstly generate a pseudo-random number r distributed uniformly between 0 and a pre-defined maximum r_{max}, iterate the chaotic system for r times and then iterate it until find a chaotic state x satisfying $f'_S(x) = m_i$, record the iteration number as the cipher-message unit C_i. Such a modified cryptosystem can avoid the first defect of the original one, but cannot overcome the second defect efficiently (only a better trade-off between the two defects is provided).

The improved *Alvarez cryptosystem* proposed in [14] is rather different from the original *Baptista cryptosystem* (an entirely different method is used to associate the different plain-characters and different chaotic states), but it also uses the number of chaotic iterations in the ciphertext to find a position corresponding to the current plaintext unit. This feature makes it possible to extend Jakimoski-Kocarev attack to attack this cryptosystem. Here, we omit technical details, and the readers are suggested referring to [11, 14, 23].

[1] We think that the map f_S should not be included in the secret key from implementation consideration and Kerckhoffs' principle [26].

Table 1
An association table constructed from two known plaintexts “subject” and “to”

n	*254*	*272*	*521*	*530*	*835*	*1120*	*1434*	*1710*	*2132*
m_i	t	s	o	u	b	j	e	c	t

In the following contexts, to simplify description, we will chiefly focus our attention on the original *Baptista cryptosystem* in [12]. Please note that the analysis can be easily extended to the chaotic cryptosystems presented in [13, 14].

3 Jakimoski-Kocarev attack and its performance

3.1 Jakimoski-Kocarev attack

In [25], G. Jakimoski and L. Kocarev proposed a known-plaintext attack to break the original *Baptista cryptosystem*. The cryptanalysis is based on the following fact: one can establish an association table between the moment of interest and the plain-characters by observing plaintext/ciphertext pairs, where “the moment of interest” of the ciphertext unit C_i is $n = \sum_{j=1}^{i} C_j$ (the *total* number of chaotic iterations from x_0). The table can be used to decrypt the corresponding plain-characters if the same moment n re-occurs in the ciphertext. In [25], an example is given to explain this attack: assume “subject” and “to” are two known plaintexts and they are encrypted as *272 258 305 285 314 276 422* and *254 267* respectively. Then one can obtain an association table shown in Table 1. Using the constructed table, he can decrypt any ciphertext that corresponds to a recorded moment. For example, a ciphertext *272 249* can be immediately decrypted as “so” (*272* denotes “s” and *272* + *249* = *512* denotes “o”). Apparently, if more plaintext/ciphertext pairs are known, this table will contain more associations, and then more ciphertexts can be decrypted by this table. Conceptually, such an attack is also available to break the modified *Baptista cryptosystem* [13] and the improved *Alvarez cryptosystem* [14].

3.2 Performance of Jakimoski-Kocarev attack

In [25], the authors stated that “*Statistical tests show that over 90% of the moments of interest can be recovered using only 4000 plaintext/ciphertext pairs*”. It seems that this attack is rather perfect as a tool to break related chaotic cryptosystems. However, we will point out that its performance is not so effective as G. Jakimoski and L. Kocarev claimed. Let us consider the following facts about this attack.

Fact 1: *to decrypt one ciphertext unit, averagely more than one plain-characters should be known.* If an attacker gets to know a plaintext with i different characters, he can construct a table with i different associations, and then he can use the i associations to decrypt i ciphertext units. That is to say, to decrypt one ciphertext unit, one plain-character must be known firstly. When the number of known plain-characters N_p increases, the number of decrypted ciphertext units (i.e., the moments of interest) N_c will also increase. However, the increment ratio of N_c will be less than the ratio of N_p, since plain-characters in different plaintexts may generate the same associations in the table. As the number of plaintexts increases, the ratio of N_c will become even less and less. See Fig. 1 for an experimental curve about the increment of N_c with respect to N_p. Consequently, to decrypt one ciphertext unit, averagely more than one plain-characters are required. Apparently, Jakimoski-Kocarev attack is more of an exhaustive attack than an intelligent and effective one.

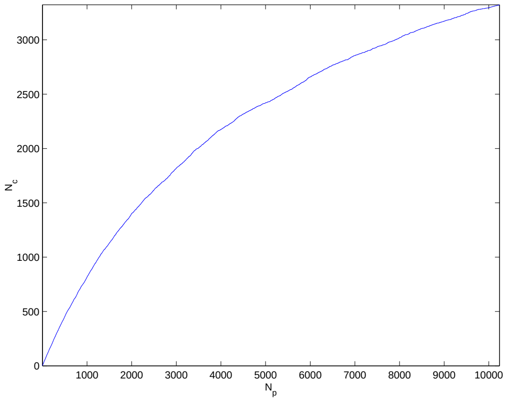

Fig. 1. The increment of N_c with respect to N_p
(Related parameters are $S = 256$, $b = 3.78$, $x_0 = 0.43203125$, $x_{min} = 0.2$, $x_{max} = 0.8$. 1024 plaintexts with 10 random plain-characters are used.)

Fact 2: *if all known plaintexts contain at most i plain-characters, it is almost impossible to decrypt any plain-character whose position is far beyond i and absolutely impossible to decrypt any plain-character whose comment of interest is beyond $i \cdot N_{max}$.* For a given plaintext, if the first i plain-characters (and the corresponding ciphertext units) are known, it is absolutely impossible to decrypt any following plain-character in this plaintext. What's more, even if the first i plain-characters of a lot of plaintexts are known, it is probabilistically impossible to decrypt any plain-character whose position is far beyond i. In fact, because of the exponentially decayed occurrence probability of C_i (please see Fig. 3 of [12] and Fig. 1 of [13]), the probability of successful attack will decrease exponentially as the plain-character goes away from i and decrease to zero once the comment of interest becomes larger than $i \cdot N_{max}$. For example, given a plaintext "Can you give me any help to break this chaotic cryptosystem" encrypted by the original *Baptista cryptosystem*, assume an attacker can only get to know plaintexts with 3 plain-characters, it will be almost (probabilistically) impossible for him to decrypt the last word “cryptosystem” although he can decrypt the first word “Can” with rather high probability.

Fact 3: *Baptista cryptosystem is more of a stream cipher than a block cipher, since same plain-characters may be encrypted as different ciphertext units. But Jakimoski-Kocarev attack is designed following the idea of breaking block ciphers, which is not suitable for stream ciphers.* Consider a general XOR-based stream cipher with the secret key-stream $\{k_i\}$, there exists a similar known-plaintext attack to Jakimoski-Kocarev's: once the first l plain-characters of one plaintext are known by an attacker, he can XOR the plain-characters and corresponding cipher-characters to derive the first l keys $k_1 \sim k_l$, and then the first l plain-characters of any plaintext encrypted with a same key-stream can be decrypted successfully (but all following plain-characters still remain secure). Generally speaking, such an attack cannot be considered as a practical attack from strict cryptographic viewpoint, since it cannot break the secret key generating the key-stream $\{k_i\}$ and cannot reveal the following plain-characters by previous known ones [26]. Similarly, Jakimoski-Kocarev attack is not a strong tool to break related chaotic cryptosystems, either.

Fact 4: *it will be impossible to decrypt the i^{th} plain-character in a plaintext, if not all previous $i-1$ units of the ciphertext are known.* To calculate the comment of interest of a ciphertext unit C_i, all $i-1$ previous ciphertext units $C_1 \sim C_{i-1}$ must be known: $n = \sum_{j=1}^{i} C_j$. As a natural result, it will be absolutely impossible for an attacker to decrypt even one plain-character if he does not observe and record all previous plain-characters. For example, given a plaintext “Who am I”, if an attacker only observes the ciphertext units of “ho am I”, he cannot get any association to decrypt other ciphertexts. This fact lowers the practical applicability of Jakimoski-Kocarev attack.

From the above facts, we can see that Jakimoski-Kocarev attack is not so effective as the authors argued in [25]. But how to understand the statement “*... over 90% of the moments of interest can be recovered using only 4000 plaintext/ciphertext pairs*”? Assume the maximal length of plaintexts is l_{max}, the maximal value of comments of interest will be $(N_{max} - N_0 + 1) \cdot l_{max}$. From Fact 1 and 2, the number of comments of interest N_c that can be obtained from 4000 known plaintexts will satisfy $N_c < N_p = 4000$, which is much smaller than $90\% \cdot (N_{max} - N_0 + 1) \cdot l_{max} = 0.9 \cdot (65532 - 250 + 1) \cdot l_{max} = 58754.7 \cdot l_{max}$. Apparently, the statement of “90%” is ambiguous and inadequate. In fact, it is conceptually right that 90% of S values of plain-characters can be obtained in the association table by 4000 plaintext/ciphertext pairs. But such a fact cannot be used to show the effectiveness of the attack at all, because different ciphertext units may correspond to the same plain-characters in *Baptista cryptosystem* (recall Fact 3).

4 A remedy to resist Jakimoski-Kocarev attack

Although Jakimoski-Kocarev attack is not very effective to break related chaotic cryptosystems, it can still be useful in some situations. In this section, we will present a simple remedy to provide satisfactory resistance to Jakimoski-Kocarev attack. Such a remedy is available for all related cryptosystems [12–14].

4.1 Description

Before explaining the remedy, let us see why Jakimoski-Kocarev attack works. As we know, each ciphertext unit C_i is the iteration number for the chaotic system (from $x_0^{(i-1)}$) to reach the ϵ-interval representing the current plain-character m_i, then $C_1 \sim C_i$ can be accumulated together to recover the comment of interest $n = \sum_{j=1}^{i} C_j$. If the plain-character m_i is known by an attacker, he can directly get the association between the comment of interest n and the plain-character m_i, and use this association to decrypt any ciphertext unit that corresponds to the same comment of interest n.

Apparently, if we cut off the way to construct the associations between the comments of interest and the plain-characters, Jakimoski-Kocarev attack will be disabled immediately. Here, we will employ chaotic masking algorithm to realize such a task. Chaotic masking algorithm is somewhat like "whitening" used in DES$^{\mathrm{X}}$, Khufu and Khafre cryptosystems [26, §15.6].

A natural idea to frustrate Jakimoski-Kocarev attack is to cut off the way of an attacker to calculate the value of $n = \sum_{j=1}^{i} C_j$. How can we do so? A simple answer is to mask the ciphertext C_i with the current chaotic state $x_0^{(i)} = F^{C_1+C_2+\cdots+C_{i-1}}(x_0)$. Since C_i is a 16-bit number ($250 \leq C_i \leq 65532$) and generally $x_0(i)$ has more bits, some bit-extracting function should be used to select 16 bits from the binary representation of $x_0^{(i)}$ to mask C_i. Please note that the bit extracting function cannot be freely selected to avoid information leaking of the current chaotic state, which will be discussed in the next subsection. The masking operation can be either XOR or modular addition.

Assume the bit-extracting function is $f_{be}(\cdot)$ and the masking operation is $\oplus$, we can use the remedy to enhance the original *Baptista cryptosystem* as follows.

Encryption. For each plain-character m_i, iterate the chaotic system from $x_0^{(i-1)}$ to find a suitable chaotic state x satisfying $f_S'(x) = m_i$ (and other requirements defined by N_0, N_{max}, η, κ), record the number of chaotic iterations from $x_0^{(i-1)}$ as $\widetilde{C}_i$ and $x_0^{(i)} = F^{\widetilde{C}_i}(x_0^{(i-1)})$. Then the i^{th} cipher-message unit of

m_i is $C_i = \widetilde{C}_i \oplus f_{be}(x_0^{(i)})$.

Decryption. For each ciphertext unit C_i, firstly iterate the chaotic system for N_0 times and set $\widetilde{C}_i = N_0$, then do the following operations (if $\eta \neq 0$, such operations can be made only when $\kappa \geq \eta$): if $\widetilde{C}_i \oplus f_{be}(x) = C_i$ then use x to derive the plain-character m_i and goto the next ciphertext unit C_{i+1}; otherwise iterate the chaotic system once and $\widetilde{C}_i + +$, repeat the procedure until the above condition is satisfied (where x represents the current chaotic state).

4.2 Discussion

Apparently, the above modified *Baptista cryptosystem* is essentially immune to Jakimoski-Kocarev attack, since it is impossible for an attacker to calculate $\sum_{j=1}^{i} C_j$ only by observing plaintext/ciphertext pairs.

However, we should carefully configure the modified *Baptista cryptosystem* to avoid a new insecurity problem induced by the bit extracting function: because of the unbalanced distribution of the ciphertext in the original *Baptista cryptosystem*, it may be possible for an attacker to guess some bits of the current chaotic state with high probability. Assume $f_{be}(x_0^{(i)})$ extracts 16 bits directly from the binary representation of $x_0^{(i)} = 0.b_1 b_2 \cdots b_j \cdots$, we can explain such insecurity about information leaking of $x_0^{(i)}$. As we know, although the ciphertext units C_i are 16-bit integers, the probability of $C_i \geq 2^{12}$ is very small (please see Fig. 3 of [12] and Fig. 1 of [13]). Hence, if we assume that the four most significant bits are all zeros, such an assumption will be true with high probability, i.e., 4-bit information of $x_0^{(i)}$ is leaked from $f_{be}(x_0^{(i)})$. For $i = 1$, such information can be then used to exhaustively search $F^{C_1}(x_0)$ with a complexity less than the complexity of exhaustive attack to x_0. Once $F^{C_1}(x_0)$ is obtained by the attacker, he can use it to decrypt any cipher-unit that is not smaller than C_1.

The above analysis shows that $f_{be}(x_0^{(i)})$ should not leak information of $x_0^{(i)}$, that is to say, it should be cryptographically hard for an attacker to derive any useful information about $x_0^{(i)}$ from $f_{be}(x_0^{(i)})$. In the following we will give two classes of such bit extracting functions, as examples to demonstrate how to make $f_{be}(x_0^{(i)})$ cryptographically strong. With the two classes of functions, it is rather difficult for an attacker to derive $x_0^{(i)}$ from partial bits of $f_{be}(x_0^{(i)})$.

The first class is

$$f_{be}(x_0^{(i)}) = f'_{be}\left(\bigoplus_{j=0}^{C_1+\cdots+C_{i-1}} F^j(x_0)\right) = f'_{be}\left(x_0 \oplus F(x_0) \oplus \cdots \oplus x_0^{(i)}\right), \quad (2)$$

where $f'_{be}(x)$ can be *any* function that extracts 16 bits from the binary representation of x. Using this class of bit extracting functions, an attacker can only get some information about $\bigoplus_{j=0}^{C_1+\cdots+C_{i-1}} F^j(x_0)$. Consider $C_i \geq N_0 = 250$, it is almost impossible for an attacker to get any useful information about $x_0^{(i)}$.

The second class is

$$f_{be}(x_0^{(i)}) = \sum_{j=0}^{15} 2^j \cdot b\left(F^j(x_0^{(i)}), \left\lfloor F^{j+m}(x_0^{(i)}) \cdot 2^n \right\rfloor \bmod 16\right), \tag{3}$$

where $m \geq 1, n \geq 4$ and $b(x,j) = \lfloor x \cdot 2^j \rfloor \bmod 2$. In this class of bit extracting functions, all 16 bits are extracted from different chaotic states, and the positions of extracted bits are determined by chaotic states that are different from the ones the bits are extracted from ($m \geq 1$). Apparently, this class can be easily extended to many variants, for example, we can change $j+m$ to $j-m$ or change the definition of $b(\cdot)$. Also, we can combine the above two classes to realize more complex bit extracting functions, which will further enhance the security.

What's more, by cancelling the unbalance of the ciphertext in the original *Baptista cryptosystem*, another two methods can also be used to avoid the information leaking of $f_{be}(x_0^{(i)})$ effectively. With the following methods, bit extracting function can be *freely* selected.

- *Method 1.* Using the modified *Baptista cryptosystem* proposed by W.-K. Wong et al. in [13]: the distribution of the ciphertext has been modified to be nearly balanced, then the information leaking becomes practically impossible (please refer to Fig. 2 of [13]).
- *Method 2.* Introducing compression mechanism: after $\widetilde{C}_i$ is obtained, compress it with any lossless entropy compression algorithm (such as Huffman compression algorithm [27]) to cancel the information redundancy (i.e., to make the distribution of $\widetilde{C}_i$ nearly balanced) and then mask the compressed $\widetilde{C}_i$ with $f_{be}(x_0^{(i)})$. Here, please note that the smaller $\widetilde{C}_i$ is, the larger the occurrence probability will be, and the smaller the length of the compressed C_i will be, i.e., the less bits will be needed to mask the compressed $\widetilde{C}_i$.

From the above discussions, we can see that our modified *Baptista cryptosystem* is more secure than the original *Baptista cryptosystem.* To break our modified cryptosystem, the initial condition x_0 and the control parameter b of the chaotic systems must be broken firstly to get $x_0^{(i)}$, which just means exhaustive attack of the secret key. Of course, there still exists one defect: the encryption/decryption speed is relatively (but not much) slower than the original one.

5 Conclusion

In this letter, we re-study the performance and countermeasure of one cryptanalysis presented by G. Jakimoski & L. Kocarev in [25], which can be used to attack *Baptista cryptosystem* in [12] and another two chaotic cryptosystems [13,14]. Our analysis points out that Jakimoski-Kocarev cryptanalysis is not so efficient as the authors claimed in [25]. Also, we present a simple remedy to essentially resist Jakimoski-Kocarev attack. Our work shows that more delicate works should be done in the future to exactly measure the security of the chaotic cryptosystems in [12–14].

Acknowledgements

The authors would like to thank the anonymous reviewers for their valuable comments on this Letter, which is used to enhance the discussion on the performance of the modified *Baptista cryptosystem* proposed by us to resist Jakimoski-Kocarev attack. Also, we would like to thank Ms. Yanghui Cao for her help on the manuscript and the final paper.

References

[1] R. Brown, L. O. Chua, Clarifying chaos: Examples and counterexamples, Int. J. Bifurcation and Chaos 6 (2) (1996) 219–249.

[2] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, Int. J. Bifurcation and Chaos 8 (1998) 1259–1284.

[3] G. Alvarez, G. P. F. Monotoya, M. Romera, Chaotic cryptosystems, in: Proc. IEEE 33^{rd} Annual Int. Carnahan Conf. Security Technology, IEEE, 1999, pp. 332–338.

[4] F. Dachselt, W. Schwarz, Chaos and cryptography, IEEE Trans. Circuits and Systems–I 48 (12) (2001) 1498–1509.

[5] L. Kocarev, Chaos-based cryptography: A brief overview, IEEE Circuits and Systems Maganize 1 (3) (2001) 6–21.

[6] R. Schmitz, Use of chaotic dynamical systems in cryptography, J. Franklin Institute 338 (4) (2001) 429–441.

[7] L. Shujun, M. Xuanqin, C. Yuanlong, Pseudo-random bit generator based on couple chaotic systems and its application in stream-ciphers cryptography, in: Progress in Cryptology - INDOCRYPT 2001, Lecture Notes in Computer Science 2247, Springer-Verlag, Berlin, 2001, pp. 316–329.

[8] R. Matthews, On the derivation of a 'chaotic' encryption algorithm, Cryptologia XIII (1) (1989) 29–42.

[9] T. Habutsu, Y. Nishio, I. Sasase, S. Mori, A secret key cryptosystem by iterating a chaotic map, in: Advances in Cryptology - EuroCrypt'91, Lecture Notes in Computer Science 0547, Spinger-Verlag, Berlin, 1991, pp. 127–140.

[10] S. Papadimitriou, T. Bountis, S. Mavaroudi, A. Bezerianos, A probabilistic symmetric encryption scheme for very fast secure communications based on chaotic systems of difference equations, Int. J. Bifurcation and Chaos 11 (12) (2001) 3107–3115.

[11] E. Alvarez, A. Fernández, P. García, J. Jiménez, A. Marcano, New approach to chaotic encryption, Physics Letters A 263 (1999) 373–375.

[12] M. S. Baptista, Cryptography with chaos, Physics Letters A 240 (1998) 50–54.

[13] W.-K. Wong, L.-P. Lee, K.-W. Wong, A modified chaotic cryptographic method, Computer Physics Communications 138 (2001) 234–236.

[14] S. Li, X. Mou, Y. Cai, Improving security of a chaotic encryption approach, Physics Letters A 290 (3-4) (2001) 127–133.

[15] G. Jakimoski, L. Kocarev, Chaos and cryptography: Block encryption ciphers based on chaotic maps, IEEE Trans. Circuits and Systems–I 48 (2) (2001) 163–169.

[16] S. Li, X. Zheng, X. Mou, Y. Cai, Chaotic encryption scheme for real-time digital video, in: Real-Time Imaging VI, Proceedings of SPIE vol. 4666, 2002, pp. 149–160.

[17] Z. Kotulski, J. Szczepanski, Application of discrete chaotic dynamical systems in cryptography – DCC method, Int. J. Bifurcation and Chaos 9 (6) (1999) 1121–1135.

[18] N. Masuda, K. Aihara, Cryptosystems with discretized chaotic maps, IEEE Trans. Circuits and Systems–I 49 (1) (2002) 28–40.

[19] M. J. Ogorzatek, H. Dedieu, Some tools for attacking secure communication systems employing chaotic carriers, in: Proc. IEEE Int. Symposium Circuits and Systems 1998, Vol. 4, IEEE, 1998, pp. 522–525.

[20] K. M. Short, Signal extraction from chaotic communications, Int. J. Bifurcation and Chaos 7 (7) (1997) 1579–1597.

[21] D. D. Wheeler, R. Matthews, Supercomputer investigations of a chaotic encryption algorithm, Cryptologia XV (1991) 140–151.

[22] E. Biham, Cryptanalysis of the chaotic-map cryptosystem suggested at EuroCrypt'91, in: Advances in Cryptology - EuroCrypt'91, Lecture Notes in Computer Science 0547, Spinger-Verlag, Berlin, 1991, pp. 532–534.

[23] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of a chaotic encryption system, Physics Letters A 276 (2000) 191–196.

[24] S. Li, X. Mou, B. L. Yang, Z. Ji, J. Zhang, Problems with a probabilistic encryption scheme based on chaotic systems, accepted by Int. J. Bifurcation and Chaos, initially scheduled to be published in vol. 13, no. 10, 2003, preprint available online at `http://www.hooklee.com/pub.html`.

[25] G. Jakimoski, L. Kocarev, Analysis of some recently proposed chaos-based encryption algorihtms, Physics Letters A 291 (6) (2001) 381–384.

[26] B. Schneier, Applied Cryptography – Protocols, algorithms, and souce code in C, 2nd Edition, John Wiley & Sons, Inc., New York, 1996.

[27] K. R. Castleman, Digital Image Processing, Prentice Hall Inc., New York, 1996.