Vol 18 No 12, December 2009
1674-1056/2009/18(12)/5219-09

Chinese Physics B

© 2009 Chin. Phys. Soc.
and IOP Publishing Ltd

Digital chaotic sequence generator based on coupled chaotic systems*

Liu Shu-Bo(刘树波)[a)b)], Sun Jing(孙 婧)[a)b)],
Xu Zheng-Quan(徐正全)[b)†], and Liu Jin-Shuo(刘金硕)[a)]

[a)] *State Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, Computer School, Wuhan University, Wuhan* 430079, *China*

[b)] *State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, Wuhan* 430079, *China*

(Received 30 March 2009; revised manuscript received 14 May 2009)

Chaotic systems perform well as a new rich source of cryptography and pseudo-random coding. Unfortunately their digital dynamical properties would degrade due to the finite computing precision. Proposed in this paper is a modified digital chaotic sequence generator based on chaotic logistic systems with a coupling structure where one chaotic subsystem generates perturbation signals to disturb the control parameter of the other one. The numerical simulations show that the length of chaotic orbits, the output distribution of chaotic system, and the security of chaotic sequences have been greatly improved. Moreover the chaotic sequence period can be extended at least by one order of magnitude longer than that of the uncoupled logistic system and the difficulty in decrypting increases $2^{128}*2^{128}$ times indicating that the dynamical degradation of digital chaos is effectively improved. A field programmable gate array (FPGA) implementation of an algorithm is given and the corresponding experiment shows that the output speed of the generated chaotic sequences can reach 571.4 Mbps indicating that the designed generator can be applied to the real-time video image encryption.

Keywords: chaos, coupling structure, sequence generator
PACC: 0545

1. Introduction

Chaos system is related to the concepts of confusion and diffusion in cryptography by its ergodicity, mixing, and sensitivity to initial conditions. Therefore chaotic cryptography is formed based on this positive connection between chaos theory and cryptography. Since the 1980s, a variety of cryptographic systems and relevant analyses have emerged.[1−17] In almost all these algorithms digital chaotic systems are adopted. Theoretically speaking, chaotic system must be an infinite precision system to keep its ideal dynamical properties. But practically, an applied chaotic system is implemented by a digital system with finite computing precision, which will inevitably lead to the dynamical property degradation of chaos.[8,10,14,15,18] The threat caused by the dynamical degradation of digital chaos to the security of chaotic system has seriously impeded the practical application of chaotic stream cipher systems.[19]

Dynamical degradation of digital chaos refers to short cycle length, non-ideal distribution and lower linear complexity, which will turn the output sequences into short cycle length, and so they become vulnerable to attacks. Therefore, the problem of how to overcome dynamical degradation has been the central concern of research since chaos was first applied to cryptosystem. There are three main causes of degradation:[14] quantization noise, periodicity caused by finite precision, and zero measure effects of shadow period. Plenty of studies have been conducted to provide solutions to these three causes respectively,[8−13,19,20] which are effective to some extent, but none of them can thoroughly solve the problem. Among these studies, the most effective one is the algorithm with random perturbations for digital chaotic system, because it not only increases the length of chaotic orbits, but also improves the dynamic characteristics of non-ideal distribution.[14] However, the existing perturbation-based algorithms can neither well solve the uneven output distribution of chaotic system, nor overcome the flaw in the sys-

*Project supported by the National Basic Research Program of China (Grant No 2006CB303104) and the National Natural Science Foundation of China (Grant No 40871200).
†Corresponding author. E-mail: xuzq@whu.edu.cn

tem security itself. Based on the perturbation algorithms of digital chaotic sequences, in this paper we propose a new perturbation algorithm of logistic map cryptographic scheme, in which a coupling structure for chaotic systems is adopted. One of the chaotic systems generates the perturbation signal to disturb the control parameter of the other system. In this way, the dynamic characteristics of digital chaotic sequences will be improved, and the problem of dynamical degradation can be solved to a great extent.

2. Coupling structure based on coupled chaotic system

2.1. Perturbation algorithm of digital chaotic system

Firstly, due to the system sensitivity to initial conditions, even a very small error can be amplified, so the chaotic system is unpredictable in the long term. Secondly, the alignment of chaos does not conform to the principle of probability statistics and no stable distribution can be obtained, therefore random sequences can be generated. Thirdly, although the data set of the chaos alignment is real, it can be extended to complex set. Theoretically speaking, data encryption scheme based on chaotic system can prevent the frequency analysis attack, exhaustive attack, and so on, which can assure that the cipher is difficult to analyse and decrypte illegally. However, dynamical degradation can actually cause a decrease in the performance of digital chaos-based applications, so it becomes a very important issue in chaotic cryptosystem.

Some improvement measures have been proposed by researchers to control the dynamical degradation of digital chaos, which can be categorized into three groups: to improve the digital finite precision,[19,21] to connect the multiple class chaotic systems,[22] and to add pseudo random perturbation.[8−15,20,23,24]

In the measure of the first category, a higher finite precision is used to realize digital chaos, which can increase the mean length of pseudo chaotic orbits. However, it remains finite precision no matter how finite the utilized word-length is, and moreover, there still exist plenty of short chaotic orbits. So the problem of dynamical degradation of digital chaos remains unsolved.[18] In the second kind of measure cascading multiple chaotic systems are used, which can effectively increase the length of pseudo chaotic orbits. These will affect the dynamic characteristics of the output sequences, thus leading to more inhomogeneous distribution.[14] Better than the previous two kinds of measures, the third one can not only increase the length of pseudo chaotic orbits, but also help to effectively reduce the dynamical degradation under finite precision.[14] In this kind of measure, perturbations can happen to either control parameter or system variable, or both. Based on the analysis of the foregoing perturbation measures in Ref.[14], disturbance feedforward and disturbance feedback are both feasible, and disturbance feedback is better than disturbance feedforward. As shown in Fig.1, A is better than B.

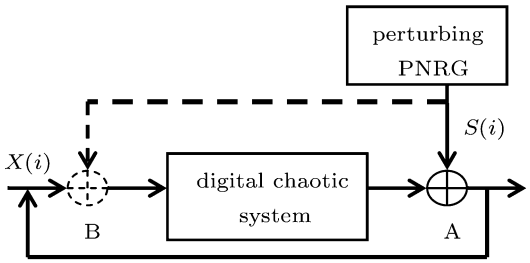


Fig.1. Two available configurations of the perturbation-based algorithm.

Philip and Joseph[12] pointed out that the finite precision had a negative effect on the dynamic characteristics of digital chaos. However, mixing of pseudo random sequences of finite precision can generate more complex random sequences with better dynamic characteristics.[25−28] Linear perturbed systems used in the previous studies turned these systems vulnerable to the known plain text attack and correlation attack.[29] To overcome the above drawback, a nonlinear perturbation algorithm based on a hybrid chaotic system was proposed in Ref.[12] as follows:

$$\begin{aligned} x_{n+1} &= 4\lambda x_n(1-x_n),\\ x'_{n+1} &= 4\lambda x'_n(1-x'_n),\\ p_n &= x_n \oplus x'_n,\\ x_n &= x_{n+1} \oplus c_n,\\ x'_n &= x'_{n+1}, \end{aligned} \tag{1}$$

where $0 < \lambda \leq 1$, $c_n = p_n \oplus y_n$, y_n is the plaintext, and the $\oplus$ operator represents the exclusive-OR (XOR) operation. In the proposed system of Eq.(1), two chaotic sequences of logistic map are adopted, and they are mixed by XOR operation. This mixing is equivalent to adding a continuous perturbation to a chaotic system, causing the system to jump from one unstable trajectory to another in accordance with the perturbation. In this way, the system can effectively

resist brute-force attack, such as known-plaintext attack and differential attack.

After studying the modified versions based on Baptista's cryptographic scheme, Jun Wei *et al*[24] pointed out that some of the remedial modifications introduced in Refs.[3]–[5] could only resist specific keystream attacks, but not all the keystream attacks. It is even doubtful whether the countermeasures can resist other attacks or not. Therefore, they proposed a modified method by perturbing control parameter of the chaotic system.

Suppose that the current chaotic state is x_i and its binary representation is $0b_1b_2\ldots b_j\ldots$. By defining three variables whose binary representation is $x_l = b_1\ldots b_{15}$, $x_m = b_{16}\ldots b_{30}$, $x_h = b_{31}\ldots b_{45}$, respectively, satisfying certain condition, renewing control parameter λ and making $\lambda_{\text{new}} = \lambda_0 + (\lambda_{\max} - \lambda_0) * g(\chi_i)/2^{15}$, the following equations are obtained

$$f(x_i) = x_l \oplus x_m \oplus x_h,$$
$$g(x_i) = f(x_1) \oplus f(x_2) \oplus \cdots \oplus f(x_i), \quad (2)$$
$$f(x_i) > \beta \cup \text{nop} > 200, \quad (3)$$
$$\lambda_{\text{new}} = \lambda_0 + (\lambda_{\max} - \lambda_0) \times g(x_i)/2^{15}, \quad (4)$$

where $\oplus$ denotes the bitwise XOR operation, $\cup$ is the logical OR operation, variable nop is the number of plaintext blocks that have been encrypted since the last update of λ, $\beta \in [0,\ 32767]$ is a coefficient that determines the updating frequency of λ. They suggested $\lambda_0 = 3.88$, and $\lambda_{\max} = 4$. Since $g(\chi_i) = 0, 1, 2, \ldots, 32767$, equation (4) leads to the case that the real control parameter λ belongs to the fixed set $B : B = \{\lambda_{\text{new}} | \lambda_0 + (\lambda_{\max} - \lambda_0)/2^{15} * g(\chi_i)\}$, $g(\chi_i) = (0, 1, 2, \ldots, 32767)$. Thus the value of λ_{new} only has 32768 kinds of possibilities, and some control parameters correspond to periodic windows, such as 3.90632507324219, 3.88607940673828, 3.96143920898438, etc. In order to avoid the condition that expression (3) still cannot be satisfied when iteration number is up to 65536, $c_{\max} = 65536$ is set to prevent any chaotic system from entering into the period state.

In both Ref.[12] and Ref.[24] perturbation algorithms were used to further strengthen the security of chaotic systems. In Ref.[12], the chaotic sequences generated by equation $\chi'_{n+1} = 4\lambda\chi'_n(1 - \chi'_n)$ under finite precision can still be periodic sequences. Moreover, in Ref.[24], the value of λ_{new} has only 32768 kinds of possibilities. Therefore, all the values of $\lambda \in [3.88, 4]$ cannot be obtained in computation.

2.2. Proposed algorithm

In order to overcome the shortcomings of existing correction methods such as non-ideal distribution and to avoid possible security risk as well, a modified algorithm is proposed as shown in Eqs.(5)–(8). This algorithm is applied only to the generation of digital chaotic sequences, which is the key step of chaotic system in cryptography, but not involved in such a follow-up application of these sequences as being used as a key stream of encryption, decryption, etc. Among the equations, Eqs.(5) and (6) are two independent chaotic systems. When the condition of Eq.(7) is satisfied, the control parameter b in Eq.(5) is substituted by the output variable in Eq.(6). In order to prevent frequent updating of the control parameter b, which affects calculation efficiency, the control parameter b should be updated after iterating Eq.(5) up to 200 times. At the same time, adjacent output variables of Eq.(6) are perturbed by arithmetical operation to increase the length of pseudo chaotic orbits as shown in Eq.(8).

$$x_{n+1} = bx_n(1 - x_n), \quad (5)$$

$$x'_{n+1} = b'x'_n(1 - x'_n), \quad (6)$$

$$b = 10x'_{n+1}(0.357 \le x'_{n+1} \le 0.4 \ \text{ and } cnt \ \ge 200), \quad (7)$$

$$x'_n = \begin{cases} (x'_{n+1} + x_{n+1}) - \lfloor x'_{n+1} + x_{n+1} \rfloor & ((x'_{n+1} + x_{n+1}) - \lfloor x'_{n+1} + x_{n+1} \rfloor \neq 0), \\ x'_{n+1} & ((x'_{n+1} + x_{n+1}) - \lfloor x'_{n+1} + x_{n+1} \rfloor = 0), \end{cases}$$
$$x_n = x_{n+1}, \quad (8)$$

where χ_n and χ'_n belong to the interval (0, 1), b and b' are the control parameters. Variable *cnt* is the iteration

number since the last update of b. The requirements for b and $b' \in [3.57, 4]$ guarantee better dynamical properties of the chaotic system.

When $cnt = cnt_{\max}(65536)$ but the condition $0.357 \leq \chi'_{n+1} \leq 0.4$ is still not satisfied, the formula $\chi'_n = \chi'_{n+1} \oplus \chi_{n+1}$ is established and equation (6) is treated again until the conditions are satisfied.

2.3. Implementation of the modified algorithm

For the modified algorithm, the initial condition $(\chi_0, b_0, \chi'_0, b'_0)$ is regarded as a key for both communication sides, which should be shared secretly. Encryption and decryption use the same algorithm, as shown in Fig.2.

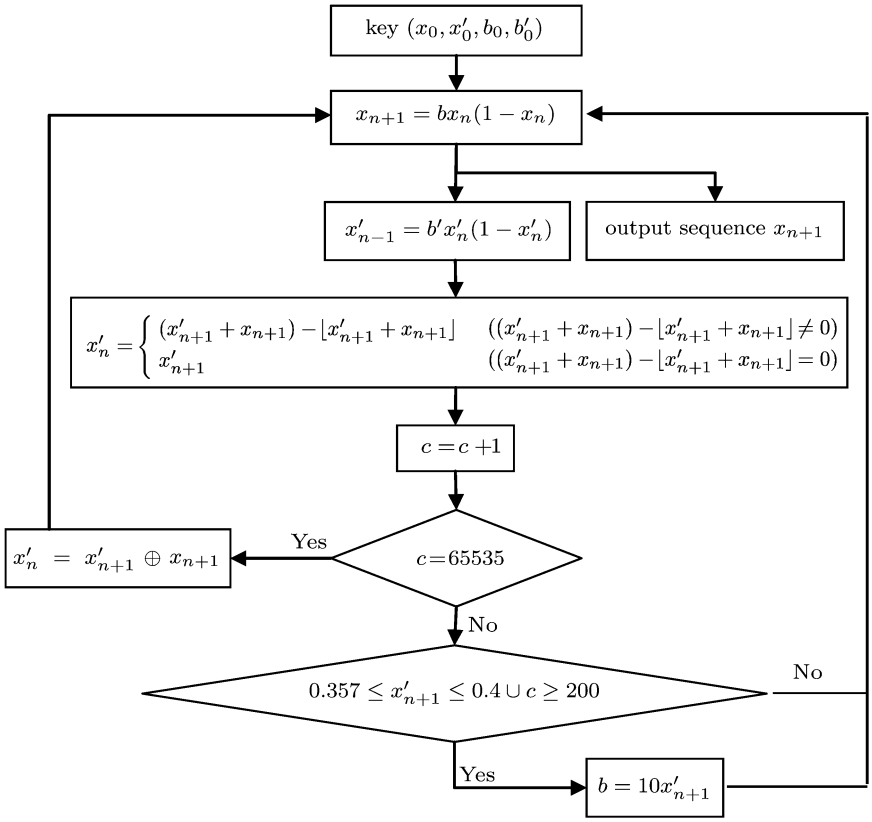


Fig.2. Flow diagram of the algorithm.

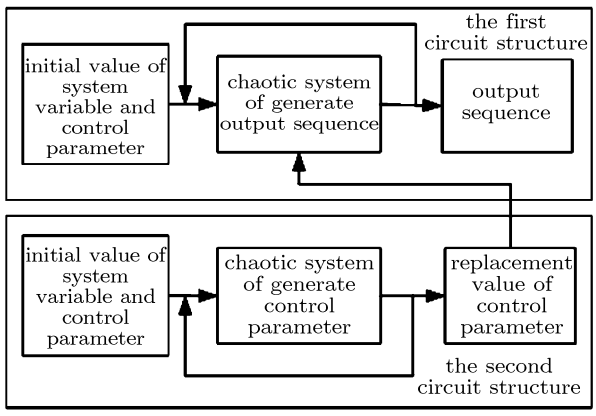


Fig.3. Parallel circuit structure of coupled chaotic system in VLSI.

The iteration process of this algorithm is complex because two chaotic systems are included. Every output sequence is regarded as the final output to enhance computation efficiency. The implementation efficiency of this algorithm on PC is low, but it is particularly suitable for parallel implementation in VLSI. Therefore, the two chaotic systems are designed as a parallel circuit structure in this paper, as shown in Fig.3.

3. Analyses and experimental results

The criteria to determine whether the proposed algorithm can effectively overcome degradation are (i) the short cycle length should be eliminated in the orbital period of output sequence; (ii) the randomness of output sequence should be strengthened; (iii) the

distribution of output sequence should be improved; (iv) the self-correlation of output sequence should be within a reasonable range. The algorithm is simulated first by using a software. The quantity of randomness, frequency distribution, and self-correlation of output sequence are investigated to verify whether this algorithm can effectively overcome degradation. Then the implementation efficiency is tested by FPGA study.

The simulation environment includes CPU Pentium IV-3.2 GHz and 512 MB RAM personal computer with the Software Platform MATLAB7.1 SP3. Moreover, the Verilog HDL code is compiled by using ALTERA QUATUS II 5.0. The synthesis of the architectures is carried out for STRATIX technology with EP1S30F780C5 target devices.

3.1. Randomness analysis

In order to verify the randomness of the output sequences, the logistic map and the modified algorithm under different control parameters are iterated 500 thousand times separately as shown in Fig.4. The measurements and the results show that the chaotic orbits display quite different dynamic characteristics under different control parameters but the same initial values. In Fig.4, it is seen that each control parameter corresponds to a single-orbit mapping and different control parameters correspond to different single-orbit mappings. Furthermore, short cycle length orbits appear as shown in Figs.4(a) and 4(b). However, in Figs.4(e)–4(h), all the different control parameters correspond to compound orbit mapping, and every compound orbit traverses all the orbit space of logistic map. It can also be seen that the chaotic orbits of the modified algorithm are basically the same, whether the control parameters are the same or not.

The experiments prove that the unpredictable updating of the control parameter b in the interval [3.57, 4] enables the chaotic orbits in Eq.(5) to jump from one trajectory to another, i.e. from one chaotic state to another. So the chaotic orbits display homogeneous dynamic characteristics under different control parameters and different iteration numbers, and the chaotic sequence period is extended to a large extent.

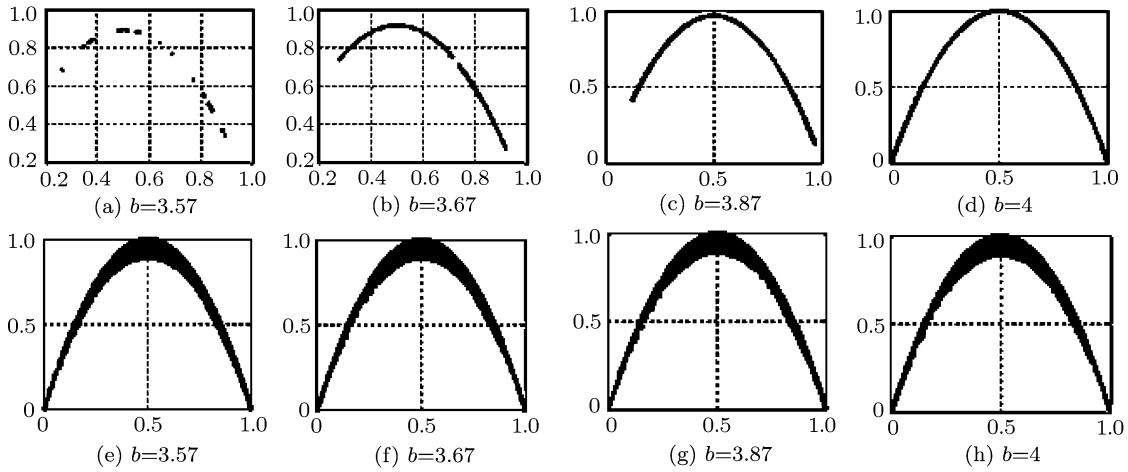


Fig.4. Chaotic orbits by iterating logistic map and the modified algorithm 500 thousand times respectively under different control parameters with $x_0 = 0.3986$. Panels (a), (b), (c) and (d) show the chaotic orbits by iterating logistic map, and panels (e), (f), (g) and (h) display the chaotic orbits by iterating the modified algorithm.

To determine whether the chaotic system in Eq.(5) falls into short period orbits accordingly when the chaotic system in Eq.(6) takes the same activity, three control parameters which can make logistic map fall into the short period orbits are chosen in the experiment to investigate the variations of the orbits as shown in Fig.5.

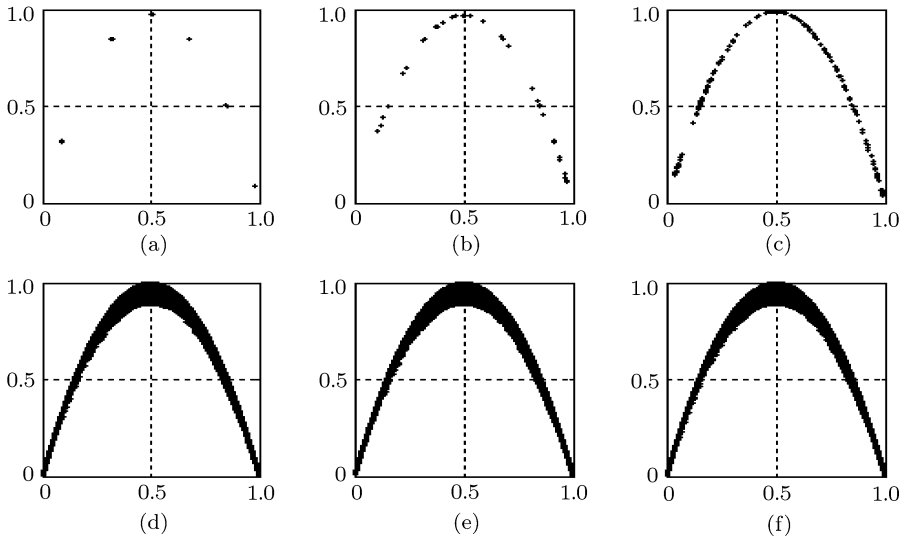


Fig.5. Chaotic orbits under the three control parameters which can make the chaotic system of Eq.(6) fall into short cycle length. Panels (a), (b), and (c) show chaotic orbits of Eq.(6), and panels (d), (e), and (f) indicate the corresponding orbits of Eq.(5), with the values of $b' = 3.90632507324219$ (a), 3.88607940673828 (b), 3.96143920898438 (c), and 3.68 (d), (e), and (f).

In Fig.5, the chaotic orbits of the output sequences can traverse the chaotic orbit space even when the chaotic system which generates control parameter enters into short-period orbits. And whatever short orbits the chaotic orbit which generates control parameter falls into, the output sequence orbits are basically the same as shown in Figs.5(d), 5(e), and 5(f).

In the modified algorithm, the spatial ergodicity of coupled chaotic system and the changing randomness of the orbit ensure the maximal randomness of the output sequences. Continuously updating the control parameter b can keep increasing the length of the chaotic orbits to overcome the short-orbit cycle, and thus effectively extending the chaotic sequence period. The experiments demonstrate that the chaotic sequence period of the modified algorithm can be extended at least by one order of magnitude longer than that of logistic map.

3.2. Frequency distribution

In order to investigate the frequency distribution of the chaotic sequences in the interval [0, 1], the interval [0, 1] of x axis is divided into 512 sections. One million output sequences are obtained after iterating one million times, and then they are classified into 512 sections and remarked according to their values. Finally, the number of each section is calculated to obtain the frequency distribution of each section as shown in Fig.6. Figure 7 shows the frequency distribution of output sequences after iterating logistic map one million times.

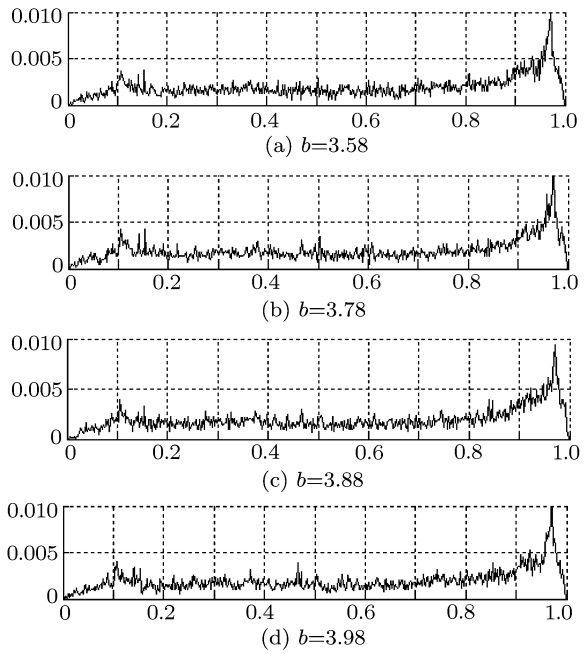


Fig.6. Frequency distributions of output sequence under different control parameters, with the modified algorithm iterated one million times. The range of output sequence x is [0, 1] as x-axis. The x-axis is divided into 512 sections, and the frequency distribution of each section is exhibited by y-axis.

The frequency distribution in Fig.6 is more uniform than that in Fig.7, and the frequency distribution curves are basically identical under different control parameters. With the intervals [0, 0.1] and [0.9, 1] removed, the frequency distributions of other intervals are basically homogeneous. In this way, the system can effectively resist cipher text attack and frequency attack.

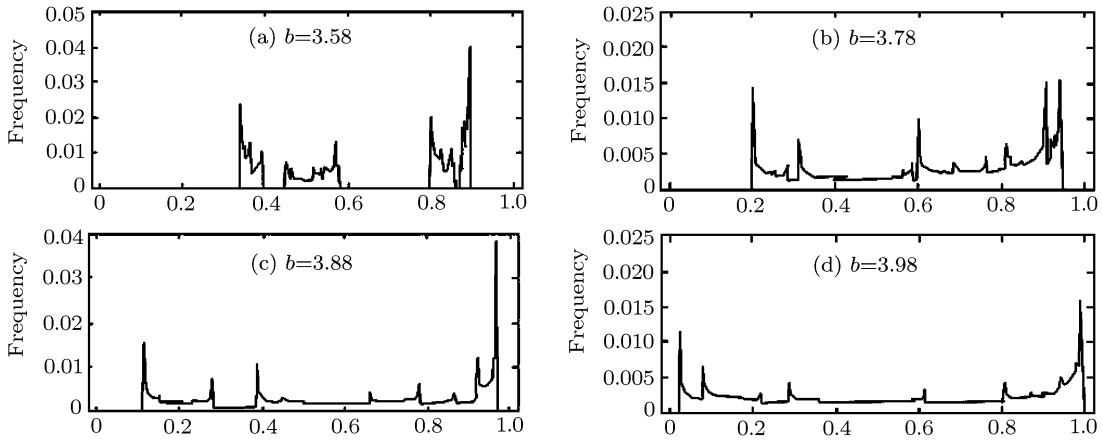


Fig.7. Frequency distributions of output sequence under different control parameters, which are given in Ref.[24], after iterating logistic map one million times. The range of output sequence x is [0, 1] as x-axis. The x-axis is divided into 512 sections, and the frequency distribution of each section is exhibited by y-axis.

3.3. Self-correlation

After iterating the proposed modified system 100 million times, four dada segments are generated at different time moments. The number of data segments is 10 thousand, and the first data of each segment is used as the starting point to study the self-correlation of this segment as shown in Fig.8.

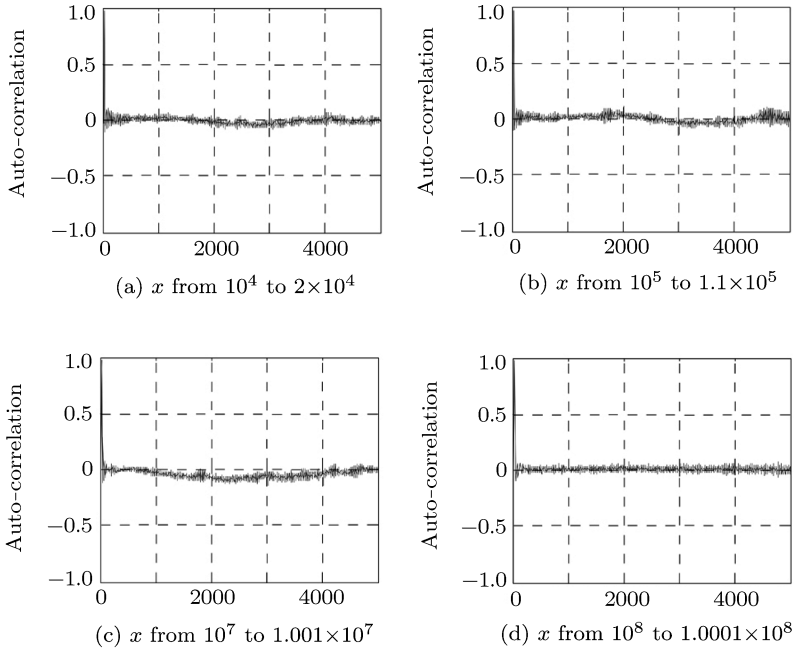


Fig.8. Self-correlation of four data segments.

In Fig.8, there is no degradation in the auto-correlation function of each data segment, which shows that no degradation appears at least in the investigated scope (100 million).

3.4. Security analysis

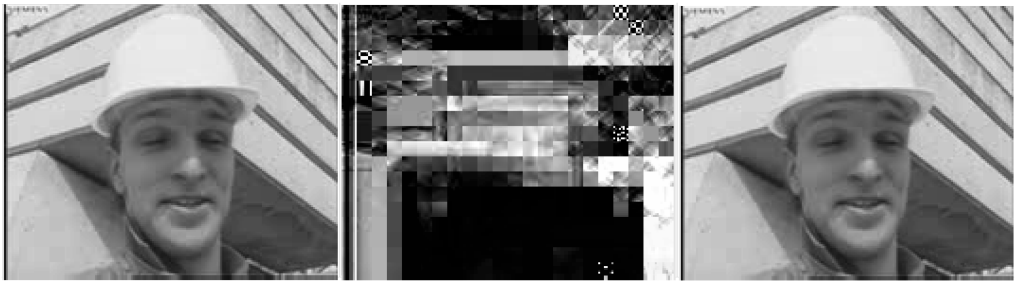
The above experimental results demonstrate that the randomness, the frequency distribution, and the self-correlation of output sequences are greatly improved. The problem of degradation can be solved to a certain extent, thereby removing a big obstacle in the way of practical application.

When no degradation appears, it is impossible to attack the proposed modified algorithm by intercepting the output sequences. This is because the attacker has to intercept a section of the output sequences first, and then calculates the key inversely. Since the parabolic mapping is obtained from the modified algorithm, and the control parameters are renewed continuously, the attack is just in vain. According to the experimental results and data analysis, the average number of renewal times of b is 229.67, and the system generates 128-bit sequence each time. To obtain the current value of b, the attacker may need as long as 229.67 iterations by the exhaustive method for 2^{128} times. And it is still no big deal even if the value of b is obtained by guess, because it will be renewed soon. So in order to decode the system, the attacker also needs to guess the initial value of the chaotic system which generates the control parameter, and finish it in 229.67 iterative times' period by exhaustive method for $2^{128}*2^{128}*2^{128}$ times (the time is about 25 μs in our FPGA implementation). In other words, it is impossible for the attackers to decode our system with the present computing ability.

Besides, since the frequency distribution of output sequences is basically homogeneous, the ability for the system to resist cipher text attack and frequency attack is further improved to a large extent.

3.5. Application in video encryption

The proposed modified algorithm is implemented by our research group in FPGA. The output speed of the generated chaotic sequences can reach 571.4 Mbps when the clock frequency is up to 35 MHz. And this is then applied to real-time video stream encryption. The experiments prove that the encryption speed for the PAL format of CIF image can be as fast as over 25 frames per second. For 300-frame image, data stream is increased by 0.048%, and most of the increased data are synchronized signals. The decoder has the same chaotic system and key stream as the encoder. The result in Fig.9 shows that the algorithm can ensure not only the output speed of the real-time video stream, but also the security in visual sense.



(a) Original image (b) Encrypted image (c) Decrypted image

Fig.9. Application in real-time video stream encryption.

4. Conclusion

Based on the analysis of the drawbacks in the existent algorithms, a modified version of Baptista's scheme of more security and efficiency is proposed. In the new algorithm, nonlinear coupled chaotic systems are used to extend the chaotic orbits and make the frequency distribution more uniform. Therefore, it can avoid the hidden security risk in application, and improve the anti-attack ability of the chaotic sequences. The experiments show that the length of chaos orbits, distribution and security of chaotic sequences have been greatly improved by using the perturbation based on coupled chaotic systems. It is also demonstrated in the experiments that the orbit length in our algorithm is extended by about one order of magnitude longer than the chaotic sequence period of logistic map.

In the modified algorithm, coupled chaotic systems are used, so the key length increases by 100% compared with that of the logistic map. Besides, other properties remain the same in the transmit channel.

References

[1] Baptista M S 1998 *Phys. Lett.* A **240** 50
[2] Lu H P, Wang S H, Li X W, Tang G N, Kuang J Y, Ye W P and Hu Gang 2004 *Chin. Phys.* **13** 625
[3] Gu Q L and Gao T G 2009 *Chin. Phys.* B **18** 84
[4] Wong K W 2003 *Phys. Lett.* A **307** 292
[5] Wong K W, Ho S W and Yung C K 2003 *Phys. Lett. A* **310** 67
[6] Palacios A and Juarez H 2002 *Phys. Lett.* A **303** 345
[7] Li S J, Mou X Q, Ji Z, Zhang J H and Cai Y L 2003 *Phys. Lett.* A **307** 22
[8] Kotulski Z and Szczepanski J 1997 *Annalen. Der. Physik.* **6** 381
[9] Sang T, Wang R L and Yan Y X 1998 *Electron. Lett.* **34** 873
[10] Masuda N and Aihara K 2002 *Int. J. Bifurcat. Chaos* **12** 2087
[11] Ambika G, Menon1 K and Harikrishnan K P 2006 *Eur. Phys. J.* B **49** 225
[12] Ninan Sajeeth P and K. Babu J http://arxiv.org/abs/cs.CR/0102012
[13] Wei J, Liao X F and Wong K W 2006 *Chaos, Solitons and Fractals* **30** 1143
[14] Li S J 2005 *Int. J. Bifurcat. Chaos* **15** 3119
[15] Li S J, Mou X Q and Cai Y L 2001 *Proceedings of 2^{nd} International Conference on Cryptology* (Germany: Springer) **2247** 316
[16] Zhang Y W, Wang Y M and Shen X B 2007 *Sci. Chin.* Ser. F **50** 334
[17] Yu S M, Qiu S S and Lin Q H 2003 *Sci. Chin.* Ser. F **46** 104
[18] Li S J, Mou X Q, Cai Y L, Ji Z and Zhang J H 2003 *Comput. Phys. Commun.* **153** 52
[19] Bernstein G M and Lieberman M A 1990 *IEEE T. Circ. Syst. Vid.* **37** 1157
[20] Li S J, Li Q, Li W M, Mou X Q and Cai Y L 2001 *In Cryptography and Coding—8th IMA Int. Conf. Proc.* (Germany: Springer) **2260** 205
[21] Ganguly N, Das A, Sikdar B and Chaudhuri P 2000 *Cellular Automata Conference* (Japan: Yakohama National University)
[22] Heidari-Bateni G and McGillem C D 1994 *IEEE. T. Commun.* **42** 1524
[23] Gernak J 1996 *Phys. Lett.* A **214** 151
[24] Wei J, Liao X F, Wong K W, Zhou T and Deng Y G 2006 *Phys. Lett.* A 354 101
[25] Ritter T 1990 *Cryptologia* 14 289
[26] MacLaren M and Marsaglia G 1965 *JACM* **22** 83
[27] Wolfram S 1986 *Proceedings of Advances in Cryptography-Crypto'85* (New York: Springer) **218** 429
[28] Pless V 1977 *IEEE T. Comput.* **C-26** 1133
[29] Siegenthaler T 1985 *IEEE T. Comput.* **C-34** 81