Chaos-based true random number generator using image

Xuan Li
School of Computer Science and Engineering
South China University of Technology
Guangzhou, China

Guoji Zhang, Yuliang Liao
School of Science
South China University of Technology
Guangzhou, China

***Abstract*—This paper proposes a chaos-based true random number generator using image as nondeterministic entropy sources. Logistic map is applied to permute and diffuse the image to produce a random sequence after the image is divided to bit-planes. The generated random sequence passes NIST 800-22 test suite with good performance.**

Keywords-Random number generator; Nondeterministic entropy source; Logistic map;

I. INTRODUCTION

Random number is very useful in many applications such as communication systems, integrated circuits, stochastic optimization and so on. Especially, Random numbers are critical for cryptography: encryption keys, random authentication challenges, initialization vectors, key-agreement schemes and generating prime numbers. Random number generators can be broadly classified as either true random number generators (TRNG) or pseudorandom number generators (PRNG). A TRNG uses a nondeterministic source (i.e., the entropy source) along with a processing function (i.e., the entropy distillation process) to produce randomness. The use of distillation process is to overcome any nonrandom weakness in the entropy source (e.g., the occurrence of long strings of zeros and ones) [1]. The entropy source typically consists of physical sources such as thermal noise [2], atmospheric noise [3], and mouse movement [4]. The output of TRNG need to pass statistical tests before it is used. For example, a physical source such as electronic noise may contain a superposition of regular structures, such as waves or other periodic phenomena, which may appear to be random, yet are determined to be non-random using statistical tests [1]. PRNG use an initial input called seed and a deterministic algorithm to generate numbers that have statistical properties of randomness. The initial seed usually consist of one or two real-value parameters such as in chaotic maps or a binary vector such as in LFSR (Linear Feedback Shift Register). This seed is then used as initial value in a deterministic algorithm typically iterative equation to produce numbers one by one which compose a random sequence. The length of sequence (i.e., the number of iterations) is supplied by users. The common and well-studied pseudorandom number generators include LFSR [6], LCR (Linear Congruential Random Number Generators) [7, 8] and chaotic maps [9-14]. It's easy to notice that each element of the produced sequence by PRNG is reproducible from its seed. PRNG also have to pass statistical tests.

In this paper, a chaos-based true random number generator using image as nondeterministic entropy sources is proposed: Firstly, we convert the color image to grayscale image, then logistic chaotic maps is applied to permute image pixels position, and finally 8 bit-planes of the image is connected as a sequence and diffused with a chaotic sequence. TRNG in [5] uses an image of 512×512 pixels to produce 16384-bit random sequence. In our method, an image of $M \times N$ is able to generate a $8 \times M \times N$ bits random sequence while passing SP 800-22 test suite with good performance.

II. CHAOS-BASED TRUE RANDOM NUMBER GENERATOR USING IMAGE

In this paper, we consider random number generator used as key stream generator in cryptography application. For cryptographic purposes, the random sequence is required to be unpredictable, convenient and reproducible. Since PRNG use deterministic algorithms and produce pseudorandom numbers by iteration from an initial seed in PC, period is unavoidable [1]. In addition, the randomness of PRNG is also affected by undesired regularities (e.g., low linear complexity), which lead to weaker cryptographic properties [7]. So PRNG is not considered very suitable for cryptography. Various combinations of these PRNG are studied [8, 13] to enhance complexity and security of PRNG.

TRNG based on nondeterministic entropy sources satisfy unpredictable requirement. Physical entropy sources such as thermal noise and atmospheric noise are good for their unpredictable properties. However, on one side, TRNG based on them are inconvenient and expensive for a personal computer (PC), on the other side, it is hard to reproduce the random numbers from physical entropy sources. The method using mouse movement [4] is cheaper and more convenient for PC, but how to reproduce the random number is still a problem. So a reproducible entropy source and an accompanying processing function called the entropy distillation process are important for a good TRNG in cryptographic application. Although reproducible entropy source seems to have more nonrandom weakness than the irreproducible ones, this weakness can overcome once a good distillation process is designed carefully. For example, PRNG of good random properties can be used in the distillation

978-1-4244-9763-8/11/$26.00 ©2011 IEEE

process. The produced random number should also be checked by the statistical tests.

In [5], a TRNG using mobile telephone photos as the entropy source is first proposed. This method also designs a good distillation process and applies chaotic sequence to remove statistic weakness of the photos. A photo of 512×512 image is first transformed to the same size cipher binary image by differing method and chaotic encryption, and then divided to 4×4 blocks. Then sum of black pixels in each block is counted. Every block is assigned a value of 0 if the corresponding sum is even, otherwise a value of 1. Then all blocks are scanned in a zigzag order to generate a random sequence of 16384 bits. The sequence passes the statistic test, section 3 shows the result.

Digital information such as mobile telephone photos are convenient entropy sources for personal computer. In cryptography application, the transmitter and the acceptor could select the same image as their entropy source which is unknown and nondeterministic for other people. In this paper, we proposed a new chaos-based TRNG which relies on the bit-planes of images. NIST 800-22 is a statistical test suite published by American National Institute of Standards and Technology [1], which is specifically designed for random number generators in cryptographic applications. Our true random number generator using image as nondeterministic entropy source with chaotic distillation process is able to pass all 15 tests in NIST 800-22. In addition, a random sequence generator for cryptographic application should be unpredictable. Since image pixels especially neighbor pixels have definite correlation with each other, it's necessary to permute and diffuse image pixels. In recent years, chaotic system is widely applied in random number generation and image encryption [8-13]. Logistic map is one of the most studied nonlinear chaotic systems [15, 16]. The iterative equation of logistic map is given by:

$$x_{n+1} = \lambda x_n (1 + x_n), \quad \text{for } x_n \in (0,1), \text{ and } \lambda \in (3.99996, 4] \quad (1)$$

When the initial value x_0 and the parameter λ *are* determined, a chaotic sequence *of n* bits can be produced by *n* iterations $\{x_i\}_{i=1}^{n}$. Fig.1 shows the bifurcation diagram of logistic map. For $3.99996 < \lambda \le 4$, the logistic map becomes completely chaotic and the iterative sequence is sensitive to the initial value x_0. For $\lambda = 4$, the logistic map is ergodic.

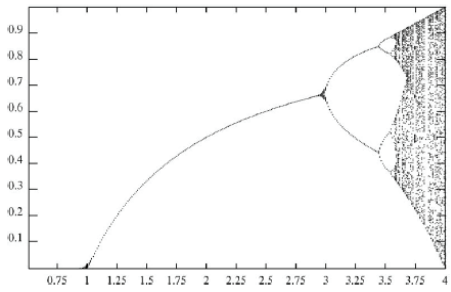

Figure 1 bifurcation diagram of logistic map

In this paper, we choose logistic maps to finish the permutation and diffusion of grayscale image. Given a color image of $M \times N$, the scheme includes following 6 steps:

Step1. Convert the color image to a grayscale image of same size.

Step2. Generate 9 chaotic sequences by logistic map where the first L produced bits are abandoned to guarantee a better random performance of the sequence:

$$X_k = \{\bar{x}_0^k, \bar{x}_1^k, \cdots, \bar{x}_{M\times N-1}^k\} = \{x_L^k, x_{L+1}^k, \cdots, x_{L+(M\times N-1)}^k\} \text{ for } k = 1,2,\cdots,9 \quad (2)$$

Parameters λ and L are set 4 and 250. The corresponding 9 Initial values are as follows:

$$\{x_0^1, x_0^2, \cdots, x_0^9\} = \{0.361, 0.362, 0.363, 0.364, 0.365, 0.366, 0.367, 0.368, 0.369\} \quad (3)$$

Step3. Sort the first chaotic sequence $X_1 = \{\bar{x}_i^1\}_{i=0}^{M\times N-1}$ in ascending order and obtain an index sequence $\{d_i\}_{i=0}^{M\times N-1}$. Then we permute the position of grayscale image pixels with the index sequence to get a new image as equation (4):

$$\text{newimage}(m,n) = \text{image}(d_{m\times N+n} \,\%\, N + 1, d_{m\times N+n} \bmod N) \quad (4)$$

Where $m = 0,1,\cdots,M-1$ and $n = 0,1,\cdots,N-1$

Step4. Turn each chaotic sequence X_k to bit sequence Y_k $(k = 2,3,\cdots,9)$ by using a threshold function [14]:

$$\bar{y}_i^k = F(\bar{x}_i^k) = \begin{cases} 0, \text{ if } \bar{x}_i^k < c \\ 1, \text{ otherwise} \end{cases} \quad (5)$$

Here c is the threshold value and $c = 0.5$ is a good choice [15].

Step5. Divide this permuted grayscale image to 8 bit-planes of size $M \times N$ and scan each bit-plane from left to right and from up to down to get bit sequences.

We denote the 8 bits sequence as $\{B_1, B_2, \cdots, B_8\}$ where $B_i = \{b_i^0, b_i^1, \cdots, b_i^{M\times N-1}\}$ for $i = 1,2,\cdots,8$.

Step6. Finally the binary random sequence $\{R_1, R_2, \cdots, R_8\}$, $R_i = \{r_i^0, r_i^1, \cdots, r_i^{M\times N-1}\}$ is obtained by confusing $\{Y_1, Y_2, \cdots, Y_8\}$ and $\{B_1, B_2, \cdots, B_8\}$ with a XOR operation:

$$r_i^k = (\bar{y}_i^k + b_i^k) \bmod 2 \quad for \quad k = 0,1,\cdots,M\times N-1 \quad (6)$$

III. THE RESULT OF STATISTICAL TESTS

In this section, we will apply NIST 800-22 test suite to evaluate the performance of TRNG we proposed above. There are 15 statistical tests in NIST 800-22. For each test, a relevant randomness statistic is chosen and used to calculate *P-value* which determine the acceptance or rejection of the null hypothesis 'the sequence being tested is random'. A significance level is chosen for the tests. If *P-value* $\ge \alpha$, then

the null hypothesis is accepted. If $P\text{-}value < \alpha$, then the null hypothesis is rejected, i.e., the sequence is nonrandom. The parameter α is usually chosen as 0.01. Meanwhile, the closer to 1 *P-value* is, the better random properties the sequence has [1].

Table 1 Result of NIST 800-22 test suite

Image Name	Kids. jpg	Sunrise. jpg	Lena. jpg	
			MASK	our method
Image Size	318×400	325×235	512×512	256×256
Sequence Length (bit)	900000	550000	16384	500000
Test name	*P-Value*	*P-Value*	*P-Value*	*P-Value*
Approximate Entropy	0.85	0.91	0.89	0.86
Block Frequency	0.77	0.56	0.84	0.74
Cumulative Sums	0.40	0.31	0.72	0.61
FFT	0.91	0.98	0.50	0.44
Frequency	0.37	0.23	0.89	0.81
Linear Complexity	0.50	0.10	0.19	0.87
Longest Run	0.47	0.52	0.95	0.18
Non-Overlapping Template	0.51	0.55	0.46	0.45
Overlapping Template	0.44	0.72	0.26	0.98
Random Excursions	0.58	0.70	0.45	0.49
Random Excursions Variant	0.38	0.51	0.42	0.62
Rank	0.24	0.84	0.59	0.12
Runs	0.85	0.75	0.60	0.18
Serial	0.13	0.97	0.36	1.00
Universal	0.78	0.07	0.54	0.35
Average	0.55	0.58	0.58	0.58

Table 1 shows the statistical test result of color images Kids. jpg, Sunrise. jpg and Lena. jpg. The last two columns compare our method with the algorithm MASK proposed in [5] which generates 16384-bits random number from mobile telephone photo Lena. jpg of size 512×512. The test result shows that our algorithm is able to generate a much longer random sequence of 500000 bits than the one generated by MASK while our generated sequence also shows a good performance in all 15 tests of NIST 800-22 test suite.

IV. CONCLUSION

Random number plays a very important role in modern digital communication systems. In this paper, image is used as entropy sources in TRNG and logistic map is applied to permute and diffuse the image to produce a true random bit sequence. Since the method uses bit-planes of image instead of converting the image to a binary one, we are able to generate a much longer random sequence than MASK in [5] while passing NIST 800-22 test suite with good performance.

ACKNOWLEDGMENT

The research was supported by the Natural Science Foundation of Guangdong Province (No. 8151064101000033)

REFERENCES

[1] NIST Special Publication 800-22 rev. 1. "A Statistical Test Suite for Random and pseudorandom number generators for cryptographic application", August 2008.
[Online].Available:http://csrc.nist.gov/publications/nistpubs/800-22-rev1/SP800-22rev1.pdf

[2] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, "A high speed random number source for cryptographic applications on a Smart Card", IEEE Trans. Computers, vol.52, no. 4, pp. 403–409, 2003.

[3] W. T. Holman, J.A. Connelly, and A. B. Downlatabad, "An integrated analog/digital random noise source", IEEE Trans. Circuits System I, vol. 44, no. 6, pp: 521–528, 1997.

[4] Q. Zhou, X. F. Liao, K. Wong, and Yue Hu, "True random number generator based on mouse movement and chaotic hash function", information sciences, 179, pp: 3442-3450, 2009.

[5] L. Zhao, X. F. Liao, and D. Xiao, "True random number generation from mobile telephone photo based on chaotic cryptography", Chaos Solitons & Fractals, 42, pp: 1692-1699, 2009.

[6] M. Sharaf, H. A. Mansour, and H. H. Zayed, "A complex Linear Feedback Shift Register Design for the A5 Key Steam Generator", Proceedings of the 22nd National Conference on Radio Science, 2005.

[7] Raj S. Katti, Rajesh G. Kavasseri, and Vyasa Sai, "Pseudorandom Bit Generation Using Coupled Congruential Generators", IEEE Trans Circuits and Systems Ⅱ: Express Briefs, vol. 57, No. 3, 2010.

[8] H. Y. Shen, P. Zhan, and K. Wang, "Improved linear congruential random number generators", Journal of Tsinghua University, vol. 49, No 2, 2009.

[9] F. Xiang and S. S. Qiu, "Analysis on Stability of Binary Chaotic Pseudorandom Sequence", IEEE Communications Letters, vol. 12, No. 5, May 2008.

[10] A. Akhshani, S. Behnia, A. Akhavan, and H. Abu Hassan, "A Novel Scheme for Image Encryption based on 2D piecewise chaotic maps", Optics, April 2010

[11] Y. Hu, X. F. Liao, and K. W. Wong, "A chaotic cryptography scheme for generator based on a spatiotemporal chaotic map", Physics Letters A, vol. 349, No. 6, pp: 467-473, 2006.

[12] X. Yi, Hash function based on chaotic tent maps, IEEE Transactions on Circuits and Systems II, vol. 52, pp: 354–357, 2005.

[13] S. Li, X. Mou, and Y. Cai, "Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography",. Proceedings of INDOCRYPT, Lecture notes in computer science, vol. 2247, pp: 316–29, 2001.

[14] Z. Kotulski, J. Szcepanski, K. Gorski, A. Gorska, and A. Paszkiewicz, "On constructive approach to chaotic pseudorandom number generators", In Proceedings of RCMCIS, pp: 191–203, 2000.

[15] S. C. Phatak and S. S. Rao, "Logistic map: a possible random-number generator", Physical Review E, vol. 51, no. 4, pp: 3670-3678, 1995.

[16] Ali Kanso, Nejib Smaoui, "Logistic chaotic maps for binary numbers generations", Chaos Solitons & Fractals , vol 40, pp: 2557-2568, 2009.