Signal-Dependent Chaotic-State-Modulated Digital Secure Communication

Omar Farooq and Sekharjit Datta

ABSTRACT—In this letter, a discrete state, discrete time chaotic pseudo random number generator (CPRNG) is presented for stream ciphering of text, audio, or image data. The CPRNG is treated as a finite state machine, and its state is modulated according to the input bit sequence of the signal to be encrypted. The modulated state sequence obtained can be transmitted as a spread spectrum or encrypted data.

Keywords—Chaos, cryptography, finite state machines, spread spectrum communication.

I. Introduction

Chaos is a deterministic, random-like process found in a non-linear dynamical system that is non-periodic, non-converging, and bounded. The fundamental characteristics of chaos, such as ergodicity, mixing property, and sensitivity to initial conditions/control parameters are properties of good ciphers, which also include confusion/diffusion, balance, and avalanche effect [1]. A chaotic sequence has also been used for a spread-spectrum sequence in place of a pseudo random number sequence in conventional CDMA direct sequence spread spectrum communication systems [2]. Chaotic pseudo random number generators (CPRNGs) have particular attractive properties that guarantee the uniqueness of the generated sequences for any chosen seed and the independence of the generated numbers along an obtained trajectory [3].

There are several sufficient conditions to be satisfied by a dynamic system to guarantee chaos, among which sensitivity to the initial conditions and topological transitivity are the most common [4]. An important property of a chaotic system defined by $f(\ )$ is bifurcation, which is measured by Lyapunov exponent (λ). Lyapunov exponent (λ) is a measure of the trajectory of function $f(\ )$ in the neighborhood of χ_0 and, as in [4], is defined for a continuous state discrete time system by

$$\lambda(\chi_0) = \lim_{n\to\infty}\lim_{\varepsilon\to 0}\frac{1}{n}\log\left|\frac{f^n(\chi_0-\varepsilon)-f^n(\chi_0)}{\varepsilon}\right|. \quad (1)$$

For encryption process E on plain text P, let the encryption key space be denoted by K; then, the encryption scheme (or cipher in a system) that gives cipher text C is given by

$$E: P^* \times K \to C^*. \quad (2)$$

The received cipher text C is decrypted as

$$D: C^* \times K \to P^*, \quad (3)$$

such as for each $e \in K$ there exists a unique key $d \in K$ and

$$\begin{aligned} &D_d = E_e^{-1} \\ &\Rightarrow \forall p \in K, e \in K,\ \exists d \in K : p = D(E(p,e),d). \end{aligned} \quad (4)$$

Symmetric encryption based on a logistic map has been suggested in [5]-[8] with an initial seed and α being a hidden parameter or key [5]. However, hiding both the initial seed and scale α is not sufficient for security [6], and an iterative approach [7] may reveal the key if a very large encrypted sequence is captured. In [7], the tent map was used as a sequence generator. It has also been shown [8] that if the chaotic scheme is unknown, then a return map will provide a clue as to the family that the chaotic scheme belongs to. This means that the attractor, the parameter, and the initial seed can be discerned from the encrypted data allowing the message to

Manuscript received Sept. 12, 2005; revised Nov. 25, 2005.

Omar Farooq (phone: +91 571 2721148, email: omarfarooq70@gmail.com) is with the Department of Electronics Engineering, Aligarh Muslim University, Uttar Pradesh, India.

Sekharjit Datta (email: s.datta@lboro.ac.uk) is with the Department of Electronic and Electrical Engineering, Loughborough University, Loughborough, UK.

be decoded given a sufficiently large sequence.

In order to overcome the above problem, a new algorithm has been proposed that uses two CPRNGs, their states modulated separately by two other CPRNGs. The scheme is inspired by the chaos shift keying proposed for analog communication [9]. In this letter, the proposed algorithm has been tested for encrypting text messages, audio streams, and images over an IP network.

II. Chaotic-State-Modulated Spread Spectrum

For the generation of a chaotic sequence, there are many existing functions that can be used such as Chebyshev map, Tent map, Logistic map, and so on [4], [5]. In this work , two new functions are proposed:

$$y(i+1) = 6.259075 * y(i) * (1 - \log_{10}(y(i))) \text{, and} \quad (5)$$

$$y(i+1) = 3.3726 * y(i) * (1 - \tan(y(i))) . \quad (6)$$

These functions iterate, and a number is outputted as a part of a chaotic sequence. A chaotic sequence generator is ideally an infinite state machine that is converted into a finite state machine by quantizing its output using a 'B' bit quantizer as shown in Fig. 1(a). The output of this generator is pseudo random and is used for spreading the input signal. For the generation of a state modulated spread spectrum, two CPRNGs use different generation equations, for example, (5) and (6), with different initial seeds. However, for message recovery, the same initial seeds and equations are known at the receiver as well. Even a small change in the seeds will cause different numbers to be generated, and the message will not be recovered. For each binary message bit, both the CPRNGs make state transitions from their initial state to a new one. The new state achieved may not be the immediate next state, but rather during this process many states may be skipped. In the case of a '0' in the input message, CPRNG3 goes from the *i*-th state to the (*i*+M)th state, while in the case of '1', CPRNG4 goes from the *j*-th state to the (*j*+N)th state, that is, CPRNG3 iterates M times while CPRNG4 iterates N times. This results in state modulation of the finite state machine according to the input bit. If the current bit is '0', the value of CPRNG3 is selected, while in the case of a '1', the output of CPRNG4 is selected. The selected output is then transmitted instead of the input bit giving a bandwidth expansion of 'B' times. Figures 1(b) and 1(c) show block diagram implementations of the chaotic spread spectrum transmitter and receiver.

To increase the complexity, two more CPRNGs (CPRNG1 and CPRNG2, as shown in Fig. 1) are used with their outputs

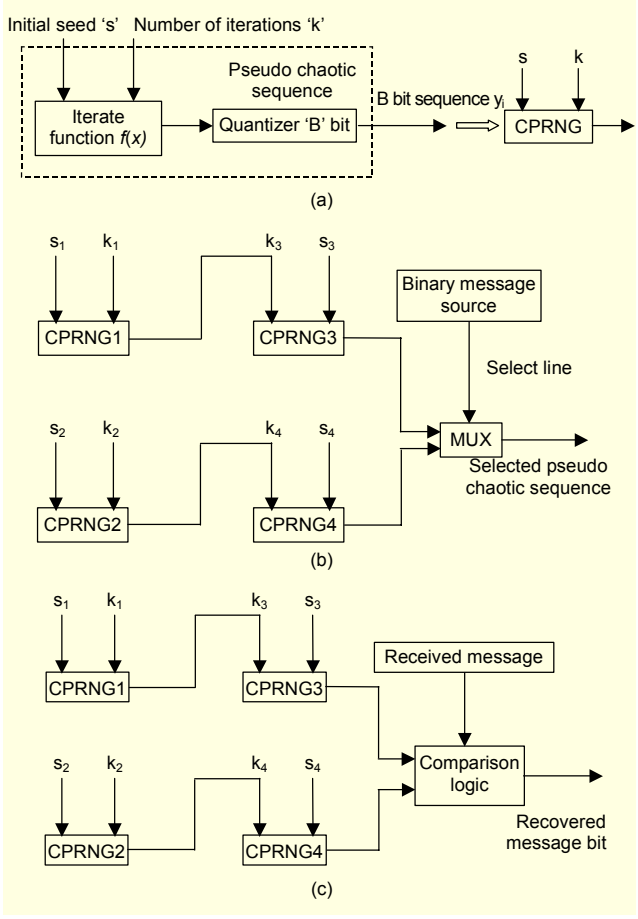

Fig. 1. Block diagrams of (a) chaotic pseudo random number generator used in chaotic state modulated spread spectrum, (b) transmitter, and (c) receiver.

connected to k_3 and k_4. Thus, instead of using fixed values of 'M' and 'N', the number of states skipped varies and depends upon the outputs of the previous CPRNGs. This results in a chaotic modulation of states for the two CPRNGs, and the signal transmitted is thus a chaotic-state-modulated spread spectrum signal.

At the receiver, when the 'B' bits are received, CPRNG1 and CPRNG2 make a transition from their initial state to the next state ($k_1 = k_2 = 1$ both for the transmitter and receiver). Both of these new states are given to CPRNG3 and CPRNG4 in order to decide on the number of times these CPRNGs (CPRNG3 and CPRNG4, as shown in Fig. 1) will have to iterate. The values, obtained after k_3 and k_4 numbers of iterations from CPRNG3 and CPRNG4, respectively, are compared with the received input bits. If the received input bit matches with the CPRNG3 output, then a '0' is decided, and if it matches with the CPRNG4 output, then a '1' is decided. An ambiguity may arise at the receiver if the two CPRNGs (CPRNG3 and CPRNG4) are in the same state. In order to avoid this situation, the quantized values of both CPRNG3 and CPRNG4 are checked at the transmitter, and if found equal, both CPRNGs iterate once more

to the next states until they reach distinct states. Thus, at the receiver, if for received 'B' message bits, both CPRNGs have the same value, the generators will be incremented to the next states until they reach distinct states. This avoids ambiguity at the receiver and helps in making the correct decision.

III. Chaotic-State-Modulated Encryption

In order to avoid bandwidth expansion, which may be desirable in many applications where limited bandwidth is available, the quantizer chosen for CPRNG3 and CPRNG4 can be of one bit, while the quantizer used for CPRNG1 and CPRNG2 can be of 'B' bits. Thus, the proposed chaotic-state-modulated encryption technique can be applied to the spread spectrum communication as well as encryption of the signal. The above state-modulated encryption algorithm was applied on the Lena image of size 128 × 128. The values of k_1 and k_2 were chosen to be 1, and 'B' was taken as 4 for CPRNG1 and CPRNG2. The chaotic number generators CPRNG1 and CPRNG2 were implemented using (5), and CPRNG3 and CPRNG4 were implemented using (6). The encryption scheme simulated used equal values of *e* and *d*, given in (4), which is decided by the initial seed/state (s_i) of the four CPRNGs. The initial seeds are floating-point numbers represented by 32 bits in the range of 0 to 1. Since encryption was to be performed, a one-bit quantizer was used for CPRNG3 and CPRNG4. The original/recovered and encrypted images are shown in Figs. 2(a) and 2(b), respectively. The histogram of the encrypted image is found to be more flat when compared to the original image, as shown in Figs. 2(c) and 2(d). The standard deviation of pixel intensity for the encrypted image was found to be 11.13 compared to 52.75 of the original image, which shows a fairly uniform distribution of pixel intensities. To extract the original message from the encrypted data, the receiver must have information about the initial seed values, the chaos generating functions used for the generation of pseudo random numbers, and the quantizing thresholds used.

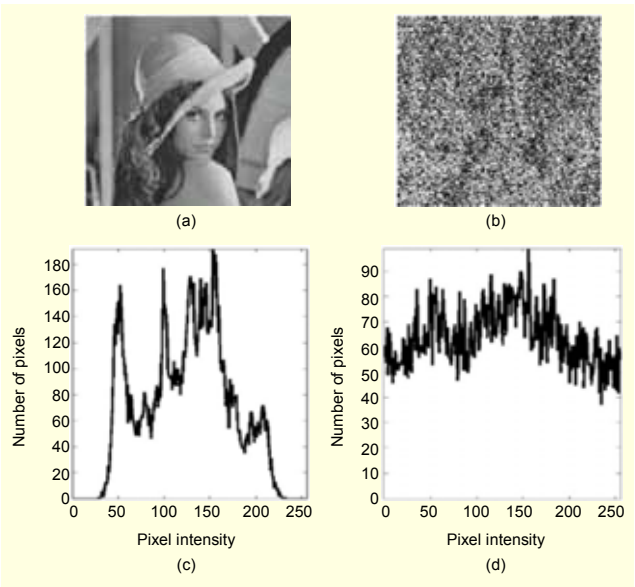

Fig. 2. (a) original image, (b) encrypted image, (c) histogram of the original image, and (d) histogram of the encrypted image.

IV. Conclusion

Since different generating functions are used and the states are also modulated, it is difficult to get information about the attractor and the initial seed. The encryption scheme proposed is signal dependent, and the outcomes of the generators are not consecutive states. Therefore, even if a long sequence of data is decrypted, and the state sequences are obtained, it will not be the same for a different input signal. Also, for continuous strings of 1's or 0's, the number generated was found to be random. Complexity of the system can be increased by using all four CPRNGs with different generating equations. Since data transmission over a TCP/IP link is error free, the proposed scheme has no problem as long as the data is received correctly in sequence as it was transmitted.

References

[1] B. Schneier, *Applied Cryptography Practical Algorithms and Source Codes in C*, John Wiley, New York, 1996.

[2] Ghobad Heidari-Bateri and Clare D. McGillem, "A Chaotic Direct-Sequence Spread Spectrum Communication System," *IEEE Trans. on Communications*, vol. 42, iss. 234, 1994, pp. 1524-1527.

[3] J. Szczepański, K. Górski, Z. Kotulski, A. Paszkiewicz, and A. Zugaj, "Some Models of Chaotic Motion of Particles and Their Application to Cryptography," *Archives of Mechanics,* 51, no.3-4, 1999, pp. 509-528.

[4] R. Brown and L. O. Chua, "Clarifying Chaos: Examples and Counter Examples," *Int. J. Bifurcation and Chaos*, vol. 6, no. 2, 1996, pp. 219-249.

[5] M. S. Baptista, "Cryptography with Chaos," *Physics Letters A,* vol. 240, 1998, pp. 50-54.

[6] L Kocarev and G Jakimoski, "Logistic Map as a Block Encryption Algorithm," *Physics Letters A*, vol. 289, 2001, pp. 199-206.

[7] G Jakimoski and L Kocarev, "Analysis of Some Recently Proposed Chaos Based Encryption Algorithms," *Physics Letters A*, vol. 291, 2001, pp. 381-384.

[8] T. Yang, L-B Yang, and C-M Yang, "Cryptanalyzing Chaotic Secure Communications Using Return Maps," *Physics Letters A*, vol. 245, 1998, pp. 495- 510.

[9] M. P. Kennedy, R. Rovatti, and G Setti, *Chaotic Modulation Schemes, Chaotic Electronics in Telecommunications*, CRC Press, 2000.