A Stream Ciphering Method using a Chaotic System

Hyun-Jun Choi, Young-Ho Seo and Dong-Wook Kim, *Member, KIMICS*

***Abstract*— In this paper, we presented a ciphering method whose target data is any kind of digital bit-stream. It uses a chaotic system as the main encrypting tool, MISR (Multi-Input Signature Register), and shift-and-rotation function, all of which are exclusive-ORed with the plaintext. Also, it incorporates a cipher text feedback mode such that part of the previously ciphered data is fed back to encrypt the current data. The encryption block size and the amount of feedback data are different at each ciphering operation. Experimental results with the image/video date showed that this method has enough speed and encryption effect with negligible latency time. Thus, we are expecting it to have various application areas that need high speed stream ciphering with high security level.**

***Index Terms*— stream cipher, encryption, chaotic system, image encryption.**

I. INTRODUCTION

CURRENT multimedia era should satisfy the users' demand for more information-implicative, more kinds of media, and larger amount of data. These satisfactions have made the communication of digital data become very common so that much of the data is private or contents on business, which in turn, needs to hide information inside the contents themselves. Also a various kinds of data compression techniques have been developed for various kinds of contents, which result in communicating various serial data streams through various wired/wireless networks. These compression processes include lossless and/or lossy functions. From the property of encryption that a single bit difference in a cipher text results in the whole information unrecoverable by de-ciphering, a stream ciphering method whose target data is the stream after compression is most proper for these multimedia data.

Encryption techniques are classified by several criteria. The first one is the kind of encryption key, which divides them into symmetric-key methods (DES, triple-DES, AES, etc) and public-key methods (RSA, ECC, etc) [1]. Another classification divides them into block cipher and stream cipher, which is by the amount of data to be encrypted each time. While a block cipher usually processes relatively large block of data, a stream cipher encrypts from one bit to several byte of data at a time.

So far, small amount of researches have been accomplished for stream ciphering compared to block ciphering. The representative researches are the ones using LFSR (Linear Feedback Shift Register) [2], SEAL [3], RC4 [4], etc. The LFSR method has its inherent defect of low security level because of its linearity. SEAL was designed to fit to a 32-bit machine and its pre-computation and look-up table of 3K bytes in size increases its complexity and processing time. It has been used more as a key-stream generator for a stream cipher. RC4 has enough key space but still uses linear function mainly although it includes a nonlinear function.

Chaos-based encryption systems have been purposed by many researches [5][6]. In secure communication and transmission, the chaotic signal is used to ciphering information signals by a predefined arithmetic calculation. Extraction of information by a receiver is done by chaos synchronization. But the synchronization matching of the chaotic result between a transmitter and a receiver can be difficult and might be lost due to transmission noise. If the cipher text encrypted by a chaos-based system is involved in the data signal and included in the standard protocol or syntax, it is not required to consider the synchronization problem.

This paper is to propose a stream cipher method whose security level is high enough and processing time is low enough. For this, we adopt a chaotic system which is a nonlinear system. In data scrambling, both this system and a shift function are incorporated. Also we include a cipher text feedback mode. The size of encryption block and the amount of feedback are randomly chosen for each encryption.

II. CHAOTIC SYSTEM

A chaotic system is a deterministic nonlinear dynamic system [7]. The major property of it is that a small difference in the initial values makes huge difference as the function proceeds, which results in unpredictable convergence value if a certain condition is satisfied. This property increases the level of security in an encryption system dramatically.

Manuscript received July 12, 2010; revised July 20, 2010; accepted July 31, 2010.

Young-Ho Seo is with Department of Electronic Materials Engineering, Kwangwoon University, 447-1, Wolgye-Dong, Nowon-Gu, Seoul, Korea (Email: yhseo@kw.ac.kr)

One chaotic system is defined as Eq. (1),

$$x(n+1)=\gamma x(n)[1-x(n)] \tag{1}$$

that is a recursive system and it is graphically shown in Fig. 1. As can see in the figure, when <3.5 x(n) is converged to a certain value (a), while when >3.5 it does not converge to one value. Fig. 2 shows the convergence value for various values of and x(0) which is the initial value of x(n). It shows that the convergence value are deterministic if <3.5. However, if >3.5, the convergence value is unpredictable for any or x(0), which is called as a chaotic zone. It means that, if we choose >3.5, a small difference in x(0) results in indeterministic difference in the convergence values. Also it includes the fact that the function values in each iteration are indeterministic if >3.5. Fig. 3 shows an example of this sensitivity to when (a) =3.5 and (b) =3.5000001. Until iteration number of 20, both systems have the same value, but since then two values are diverse unpredictably.

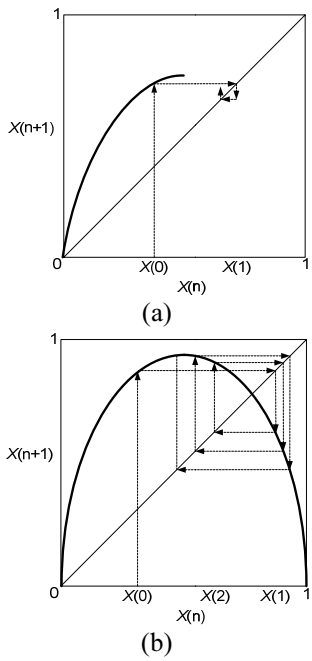


Fig. 1. Recursive operation of eq. (1); (a) γ<3.5, (b) γ>3.5.

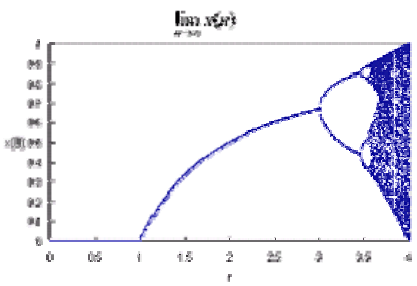


Fig. 2. Bifurcation diagram of *x(n)* in eq. (1)

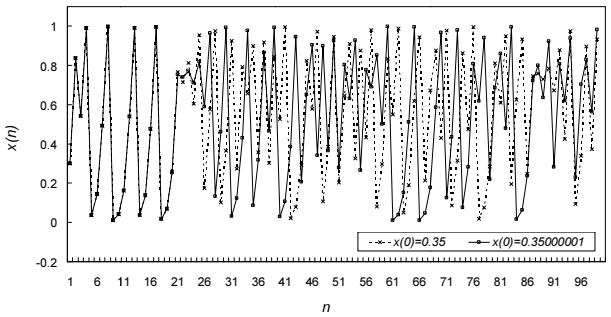


Fig. 3. Scatter plot for sensitivity to initial condition

III. THE PROPOSED STREAM CIPHER

The ciphering/de-ciphering algorithm we are proposing here can be expressed with Eq. (2) and (3), and the encryption process is depicted as a block diagram in Fig. 4. As the two equations, the ciphering and the de-ciphering processes are the same.

$$C_i=SR_{R1,i}[T_{R2,i}(C_{i-1})] \oplus S_i \oplus P_i \tag{2}$$

$$P_i=SR_{R1,i}[T_{R2,i}(C_{i-1})] \oplus S_i \oplus C_i \tag{3}$$

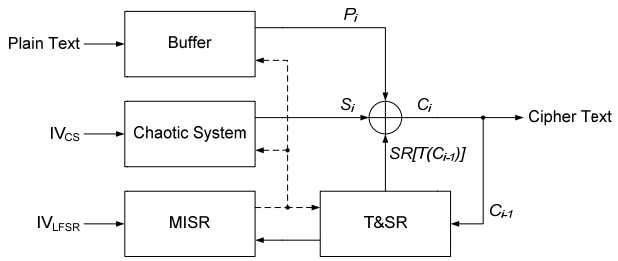


Fig. 4. The proposed stream cipher method

The ciphering process performs exclusive-OR operation whose inputs are the plaintext, the output of chaotic system, and the refined result of a part of the previous cipher text. The refinement process which is marked as T&SR in Fig. 3 includes a shift-and-rotate (SR) function as well as truncating a part of the previous cipher text. The size of truncated bits and the amount of SR are different in each encryption time and they are dependent of the value from chaotic system (CS).

The size of the data block, that is, the amount of data to be encrypted (S_i and P_i) is determined for each encryption by a part of outputs from MISR (Multiple Input Signature Register) who accepts a part of the previous cipher text as its parallel inputs, which forms a cipher text feedback mode [1]. The amount of feedback bits also depends on the value from CS.

From output bits from MISR, the size of the cipher block would be,

$$L_i = f(k) + a_{k-1}2^{k-1} + a_{k-2}2^{k-2} + \cdots + a_1 2^1 + a_0 \quad (4)$$

where, $f(k)$ is an arbitrary function. Eq. (1) or (2) takes ad SRs the L_i bits of the previously ciphered data (C_{i-1}) indicated by the eq. 4 which is calculated with the outputs from the current (i) MISR state. Then, the result is exclusive-ORed to make the current cipher text (C_i). Because this process takes place at each encryption time, the amount and the position of the previously ciphered data for cipher text feedback is arbitrary. Note that the number of bits to be SRed is also determined by a value from CS which is different from L_i.

The security of this scheme depends on the following factors:

- **The size of key**: The key consists of $x(0)|\gamma|IV_{MISR}$, where IV_{MISR} means the initial value of MISR, | represents concatenation, and $x(0)$ is the initial value of $x(n)$ (IV_{CS}). The size of IV_{MISR} is fixed if the number of stages in MISR is determined. But $x(0)$ and γ have arbitrary sizes. The larger the key size is, the higher the security level is.
- **Unpredictability of the chaotic system**: As explained before, the main security of our scheme depends on the chaotic system. It affects directly to the cipher text, the size of cipher block, number of bits taken from the previous cipher text, and number of bits to be SRed. The CS in Fig. 4 also re-initialized periodically. When it re-starts, the new initial value is taken from MISR.
- **The recursive inputting scheme of cipher text to MISR**: A part of previous cipher text is inputted to the MISR in parallel at each ciphering process. Even though MISR itself is a linear system, the nonlinear input values induce the nonlinear effect on the system.
- **The recursive feedback scheme of the cipher text**: This feedback mode chains the cipher text recursively. It means that the whole cipher text cannot be separated even though the size of each cipher block is determined separately. Thus, the processing data unit to hack the data or extract the key extends to the whole cipher text.

These factors increase the security level of our scheme enough to be used a secure stream cipher for any kind of bit stream data.

IV. EXPERIMENTAL RESULTS

scheme in Fig. 4 was implemented in S/W and experimented in a PC with Intel Pentium IV 2.66GHz processor. The test data was image, voice, and text bit streams. Fig. 5 shows an encryption example of Lena image. Here we used 3.75 and 0.75 as γ and $x(0)$, respectively, and the size of image was 256×256 pixels. It is clear that any information in the figure (b) cannot be recognized.

One of the most important properties in a stream cipher is the ciphering/de-ciphering speed. To show the encryption speed and latency time of our scheme, we applied our scheme with varying the encryption block size by changing k and $f(k)$ in eq. (4). The results are shown in Fig. 6, which includes both encryption speed (left vertical axis, in [Mbps]) and latency time (right axis, in [ns]). As in the figure, both the ciphering speed and the latency time increases as the block size increases. This result shows a trade-off relationship between them. However, the latency times are less than 1[μs] which is negligible. Also this scheme shows enough speed in all the range of ciphering block size. The result shows the better performance than the previous researches [5][6]. Thus, we expect that this scheme would be a good stream ciphering method with high strength of security.

(a) **(b)**

Fig. 5. Encrypted result of the Lena image; (a) original, (b) encrypted.

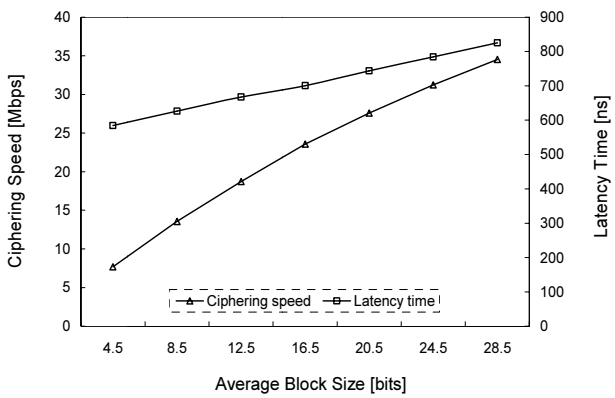


Fig. 6. Experimental results for speed and latency time

V. CONCLUSIONS

In this paper, we proposed a stream ciphering scheme which uses a chaotic system, shift-and-rotation operation and cipher text feedback mode to enhance the security level. It is also characterized by the cipher block size and the amount of feedback bits in each ciphering iteration. These characteristics of the proposed cryptosystem increase the security level enough to be used in the applications which need high security level.

From experimental results, all the considered contents cannot be recognized after encryption with our method. It also has enough speed such as more than 20Mbps when the cipher block size is 16 bits, with the latency time of 0.7μs which is negligible.

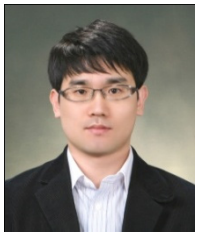
Thus, we conclude this paper that the proposed scheme has enough security level and operational speed as a stream cipher method and we are expecting that it has various application areas in various kinds of stream data.

ACKNOWLEDGMENT

This work was supported by the IT R&D program of KEIT. [KI002058, Signal Processing Elements and their SoC Developments to Realize the Integrated Service System for Interactive Digital Holograms.]

REFERENCES

[1] W. Stallings, “Cryptography and Network Security Encryption”, Prentice Hall, 2003
[2] M. Robshaw, Stream Ciphers, RSA Lab. Technical Report TR-701, RSA Lab., Redwood City, July 1995.
[3] R. Rogaway and D. Coppersmith, "A Soft-ware-oriented Encryption Algorithm", Cambridge Security Workshop, pp. 56-63, 1994.
[4] R. L. Rivest, The RC4 Encryption Algorithm, RSA Data Security Inc., March 1992.
[5] K. Klomkarn, A. Jansri, and P. Sooraksa, “A Design of Stream Cipher Based on Multi-Chaotic Functions”, ISCIT2004, pp.26-29, 2004.
[6] S. Lian, J. Sun, Z. Wang, and Y. Dai, “A Fast Video Encryption Scheme Based-on Chaos”, ICCARV2004, pp.126-131, 2004.
[7] Hirsch, Morris W , “Differential Equations, Dynamical Systems, and an Introduction to Chaos”, Academic Pr, 2003.



Hyun-Jun Choi has received his M.S. and Ph.D. degrees in 2005 and 2009 from Dept. of Electronic Materials Engineering of Kwangwoon University in Seoul, Korea. He was a research professor in Realistic Media Institute at Kwangwoon University. He is currently an assistant professor with the department of Information and Communication Engineering, Anyang University, Anyang-si, Korea. He is research interests are in optical image processing and 3D display.

Young-Ho Seo has received his M.S and Ph.D degree in 2000 and 2004 from Dept. of Electronic Materials Engineering of Kwangwoon University in Seoul, Korea. He was a researcher at Korea Electrotechnology Research Institute (KERI) in 2003 to 2004. He was a research professor in Dept. of Electronic and Information Engineering at Yuhan College in Buchon, Korea in 2005. He was an professor of Dept. of Information and Communication Engineering at Hansung University in Seoul, Korea in 2006 to 2007. He is now an assistant professor of College of Liberal Arts at Kwangwoon University in Seoul, Korea and a director of research institute in Ten Technology Inc. His research interests include 2D/3D digital image processing, SoC design and contents security

Dong-Wook Kim (S’82–M’85) received the B.S. and M.S. degrees from the Department of Electronic Engineering, Hangyang University, Seoul, Korea, in 1983 and 1985, respectively, and the Ph.D. degree from the Department of Electrical Engineering, Georgia Institute of Technology, Atlanta, in 1991. He is currently a Professor and the Dean of Academic Affairs at Kwangwoon University, Seoul. His current research interests include digital system design, digital testability and design-for-test, digital embedded systems for wired and wireless communication, and design of digital signal processors.