Commun Nonlinear Sci Numer Simulat 27 (2015) 22–29

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

journal homepage: www.elsevier.com/locate/cnsns

Secure binary arithmetic coding based on digitalized modified logistic map and linear feedback shift register

Yushu Zhang [a,b], Di Xiao [b,*], Wenying Wen [c], Hai Nan [b], Moting Su [d]

[a] School of Electronics and Information Engineering, Southwest University, Chongqing 400715, China
[b] College of Computer Science, Chongqing University, Chongqing 400044, China
[c] School of Information Technology, Jiangxi University of Finance and Economics, Nanchang 330013, China
[d] School of Economics and Business Administration, Chongqing University, Chongqing 400044, China

ARTICLE INFO

Article history:
Received 22 October 2013
Received in revised form 17 February 2015
Accepted 28 February 2015
Available online 6 March 2015

Keywords:
Randomized arithmetic coding
Digitalized modified logistic map
Linear feedback shift register
Shift
Perturbance

ABSTRACT

In this paper, we propose a novel secure arithmetic coding based on digitalized modified logistic map (DMLM) and linear feedback shift register (LFSR). An input binary sequence is first mapped into a table, which is then scrambled by two cyclic shift steps driven by the keys resulting from DMLM–LFSR. Next, each column is encoded using traditional arithmetic coding (TAC) and randomized arithmetic coding (RAC). During the RAC process, the exchange of two intervals is controlled by the keystream generated from the DMLM. At the same time, a few bits of the present column sequence are extracted to interfere the generation of new keystream used for the next column. The final ciphertext sequence is obtained by XORing the compressed sequence and the keystream generated by the LFSR. Results show the compression ratio of our scheme is slightly higher than that of TAC, but the security is improved due to the architecture of shift–perturbance. DMLM and LFSR theories also ensure high sensitivity and strong randomness. The appended complexity is only $O(N)$, where N is the number of the input symbols.

© 2015 Elsevier B.V. All rights reserved.

1. Introduction

Arithmetic coding (AC) [1,2] has been widely developed over several decades and is incorporated into image and video coding standards like JPEG2000 [3] and H.264 [4]. AC is optimal since it can be arbitrarily close to the true entropy of the probability. Due to similarity between AC and cryptography, it is also regarded as an encryption scheme for some specific applications. Moreover, the current state in an adaptive model depends directly or indirectly upon the initial conditions and all of the messages encoded so far, therefore the adaptive AC approach may offer high level of security [5]. Nevertheless, it was proved that neither fixed AC model nor adaptive AC model can provide well-pleasing level of security [6–8]. Furthermore, many variant versions were researched and reported for the purpose of enhancing the security [9–14]. In [9], a secure compression method was presented by renovating the coding probabilities in random time intervals. The poor synchronization property of AC is utilized to design an encryption scheme by processing only the first few bits of the generated bit stream [10,11]. Random bit substitution is used to construct a cryptosystem during the encoding process of AC [12]. Randomized arithmetic coding (RAC) and key-based interval splitting AC were proposed in [13,14], respectively. However, they are vulnerable to some classic attacks as the result of the fact that the same key is used to encode many messages [15–17]. Besides, the security enhancement version of key-based interval splitting AC [15] was also cryptanalyzed in [18–20].

* Corresponding author.
E-mail address: xiaodi_cqu@hotmail.com (D. Xiao).

http://dx.doi.org/10.1016/j.cnsns.2015.02.025
1007-5704/© 2015 Elsevier B.V. All rights reserved.

Because of the deterministic randomness and unpredictable behavior of chaos, chaotic ciphers [21–28] have attracted a great deal of attention in recent years. Chaotic intrinsic properties provide good cryptography for the AC. Recently, there existed a few novel encryption schemes based on AC combing chaos theory [29–34]. Wong et al. [29] proposed a simultaneous AC and encryption scheme using piecewise linear chaotic maps and integer skew tent map. Lin et al. [30] further presented a novel idea that a discrete piecewise linear chaotic map is employed to perform the generalized AC and then proposed a joint compression and encryption scheme based on integer skew tent map. Bose and Pathak [31] integrated a variable model AC with couple chaotic system for designing a cryptosystem (it has been commented by Zhou and Au [35]). Mi et al. [32] presented a chaotic encryption scheme under the combination of AC and logistic map. Li and Zhang [33] proposed a security arithmetic coding algorithm based on nonlinear dynamic filter which is employed to generate the pseudorandom number generator (PRNG). Masmoudi et al. [34] designed a joint lossless compression and encryption scheme combing a binary AC with a pseudo random bit generator (PRBG) based on a stand chaotic map and an Engel Continued Fraction map. However, these chaotic systems used in the schemes [31–34] including couple chaotic map, logistic map, nonlinear dynamic filter etc., have at least one of two flaws: (i) high-cost computation. AC is a highly efficient coding whereas the iterative computation with respect to chaotic maps is a time-consuming process. Thus, these chaos-based AC may be not suitable for practice sometimes; (ii) poor randomness quality. With multiple iterations of chaotic system, the randomness will degrade on account of finite precision of computing devices. To overcome the above two disadvantages, in this paper, we propose a novel secure arithmetic coding based on digitalized modified logistic map (DMLM) [36] and linear feedback shift register (LFSR) [37]. An input binary sequence P of length N is first mapped into a table having q columns and $\lceil N/q \rceil$ rows according to raster-order ($\lceil N/q \rceil > q$). A permutation is then applied in the table by two key-driven cyclic shift steps operating on the columns and rows, respectively. The keys used in the shifts result from a q-bit DMLM–LFSR. Each column in the table is scanned to find out the number of distinct symbols including "0" and "1" and the corresponding probabilities of occurrence. Next, for the lth column, the first $\lceil N/q \rceil - q$ symbols are encoded using TAC while the last q symbols are compressed by utilizing RAC in which the keystream $\bar{c}_1$ controls the exchange of the two intervals. At the same time, the last τ bits of the symbol sequence *Column_l* in the lth ($1 \leqslant l \leqslant \lceil N/q \rceil - 1$) column are extracted to interfere the generation of the keystream $\bar{c}_{l+1}$. The final ciphertext sequence is obtained by XORing the compressed sequence and the keystream generated by the LFSR.

The rest of this paper is organized as follows. The next section firstly gives the basic background, primarily on the theories of DMLM and LFSR, and then proposes a secure arithmetic coding. Section 3 provides experimental results on the performance and security issues of the proposed scheme. Finally, we draw some conclusions in Section 4.

2. Secure arithmetic coding based on DMLM and LFSR

This section first gives the basic background, primarily on the theories of DMLM and LFSR on which we base our security and efficiency. Then a secure arithmetic coding is designed.

2.1. DMLM and LFSR

A general logistic map is given by

$$x_{i+1} = \lambda x_i(1 - x_i), \quad x_i \in (0, 1), \quad \lambda \in (3.5699456, 4]. \tag{1}$$

The trajectory generated by a parameter λ in short periodic window easily enters a short cycle and is not suitable for applications in security. In order to digitalize a logistic map, Chen et al. [36] defined a q-bit DMLM as

$$x_{i+1} = \lfloor [\lambda x_i(1 - x_i)] (\mathrm{mod}\ 1) \rfloor_q, \lambda \geqslant 4, \tag{2}$$

where $\lfloor x \rfloor_q$ is a truncation function to preserve the most significant q bits of x and drop others. Numerical results including bifurcation analysis and discrete Lyapunov Exponent verified the pseudochaotic properties of DMLM [36]. Furthermore, q-bit DMLM is modified by the following form

$$x_{i+1} = \left\lfloor [2^{\lceil q/2 \rceil} x_i(1 - x_i)] (\mathrm{mod}\ 1) \right\rfloor_q. \tag{3}$$

To increase the randomness quality, Eq. (3) can be rewritten as $x_{i+1} = c\{\lceil q/2 \rceil + 1 : \lceil q/2 \rceil + q\}$ by extracting the most significant $2q$ bits in the result c of $x_i(1 - x_i)$. Additionally, the multiplication of $\lambda = 2^{\lceil q/2 \rceil}$ only requires a shift operation in hardware implementation such that the computation cost is reduced. Iterating DMLM one time requires only one multiplication.

To solve the short cycle problem for chaotic cryptography systems, Sang et al. [37] proposed an algorithm based on a class of perturbance. The maximal length LFSR is a suitable candidate for the perturbing signal generator because its generated sequences have the following advantages: (i) definite cycle length $(2^L - 1)$ (here L is the degree); (ii) uniform distribution; (iii) double-valued auto-correlation function; (iv) easy implementation; (v) controllable maximum signal magnitude given by $2^{-p}(2^L - 1)$ when used in our P-precision system. Hence, it is a very useful and widely used method by exploiting a LFSR to scramble several least significant bits. For example, Chen et al. [36] proposed DMLM–LFSR by using LFSR to scramble the output of DMLM. More details on the DMLM–LFSR can be found in [36].

Download English Version:

https://daneshyari.com/en/article/758290

Download Persian Version:

https://daneshyari.com/article/758290

Daneshyari.com