Improvement of Security and Feasibility for Chaos-Based Multimedia Cryptosystem*

Jianyong Chen and Junwei Zhou

Department of Computer Science and Technology, Shenzhen University, Shenzhen, China 518060
Cjyok2000@hotmail.com

Abstract. Nonlinear dynamic filter (NDF) has been used in chaos-based multimedia cryptosystem. However, our study shows that the key of randomized arithmetic coding (RAC) based on NDF can be successfully recovered under chosen plaintext attack. Moreover, current ciphertext block can't be decoded unless preceding plaintext is available. In order to enhance the security and feasibility used in multimedia applications, the algorithm is improved by building a new correlation between ciphertext and coefficients. Its security is enhanced that can effectively resist chosen plaintext attack. Its feasibility is also improved that can decode ciphertext block without availability of preceding plaintext with which a user can play multimedia data starting at any place. The analysis and simulations show that the improved algorithm can evidently enhance both security and feasibility

Keywords: Chaos, Cryptography, Security, Arithmetic coding.

1 Introduction

The security and efficiency requirements of data transmission make data compression and encryption become more and more important. In order to improve performance and satisfy requirements of multimedia application such as playing a certain portion of a video or audio, it is worthwhile to joint compression and encryption in a united process [1, 2]. It is reported that the united scheme is more secure and effective than the classical separate compression-encryption schemes [3].

Arithmetic coding is a method for lossless data compression and performs excellence in many respects [4], which is widely used in a variety of multimedia application [5]. Recently, various studies have been taken to integrate cryptography into the arithmetic coding [6-13]. Among them, randomized arithmetic coding (RAC) is proposed with multimedia selective encryption including some randomization in the arithmetic coding procedure to achieve encryption [6]. In order to improve the security of RAC [6], Schemes [7 ,8] proposed two variants of RAC utilizing chaotic

* This work was supported by Shenzhen University Research and Development Fund (SZU R/D) with Grant No. 200903.

B. Murgante et al. (Eds.): ICCSA 2011, Part IV, LNCS 6785, pp. 604–618, 2011.

map as the pseudo-random number generator and making the random number bitstream associated with the plaintext. In the scheme [8], a kind of nonlinear dynamic filter (NDF) whose probability density function is distributed uniformly is adopted to expand key space and improve security. The plaintext is mapped into the chaos parameter space and thus the random number bitstream can associate with the plaintext. Unfortunately, after studying the scheme proposed in [8], it is found that the key of NDF is easily recovered under chosen plaintext attack scenario. Furthermore, function requirements, e.g., fast-forward, rewind and playing video or audio from arbitrary position at a user's discretion, are necessary in multimedia player. Because the random number bitstream depends on the preceding plaintexts, the decoder must firstly obtain the all preceding plaintext and then generate the random number bitstream. Finally, the decoder could decrypt the current ciphertext successfully. However, in multimedia application scenario, the starting point is arbitrary at a user's discretion and the decoder couldn't always get all previous plaintext to generate random number bitstream. Therefore, the encryption algorithms [7, 8] are limited in multimedia application since it depended on plaintext sequence.

In order to enhance the security and improve feasibility, a nonlinear correlation model between ciphertext and random number bitstream is established. The ciphertext instead of plaintext is mapped into the chaos parameter spaces based on a nonlinear map, and coefficients of NDF are derived from the ciphertext. Similarly, the random number bitstream depends on both initial value of NDF and the ciphertext, which can employ to flexible design of the coefficients of NDF [14]. Because of the nonlinear correlation model between ciphertext and random number bitstream, the security problem presented in this scheme can be solved. Meanwhile, coefficients of NDF are derived from the ciphertext instead of plaintext, the decoder could decrypt current ciphertext block successfully without any knowledge of preceding plaintext. This makes our approach to meet the needs of multimedia application, such as display of video and audio starts from arbitrary portion as user desire. In proposed algorithm, the randomness of the random number bitstream, which plays the most important role in proposed cryptosystem, is confirmed by the statistical test suite which is recommended by the U.S. National Institute of Standards and Technology (NIST) [15].

The rest of this paper is organized as follows. In next section, RAC and cryptanalysis of RAC based NDF are reviewed. Cryptanalysis of existing scheme is presented in section 3. The improved operation is proposed to enhance the security and the flexibility in Sections 4. Analyses and simulation results can be found in Sections 5. In the last section, conclusions are figured out.

2 Review of the RAC and Its Variants

2.1 RAC

The scheme of RAC [6] is a multimedia cryptography that its order of the symbol intervals is disturbed by secret random number bitstream. Only the decoder who obtains the random number bitstream could decode ciphertext correctly. The scheme

of RAC consists of two parts: One part is pseudo-random number generator for generating random number bitstream and disturbing the order of intervals. In [7], logistic map is used as the pseudo-random generator, while in [8], NDF is used as the generator. The other part uses public traditional arithmetic encoding to achieve compression. In the scheme of RAC and its variants, intervals used in arithmetic coding are swapped according to random number bitstream. Assuming that the probabilities of symbols 0 and 1 are 1/4 and 3/4, the corresponding intervals are [0, 1/4] and (1/4, 1]. In general, if random number bit r_i is equal to 0, corresponding intervals of both symbol 0 and 1 are kept with [0, 1/4] and (1/4, 1]. Otherwise, the interval of symbol is swapped, so the interval mapped to symbol 0 is (3/4, 1] and the interval mapped to symbol 1 is [0, 3/4]. Fig.1 is draft of RAC and its variants. The pseudo-random number generator of variants [7, 8] is correlation with plaintext, which can enhance the security of RAC. It is obvious that the random number bitstream is the most important part of security. Once the opponent obtained the key of the pseudo-random number generator, RAC can be broken easily.

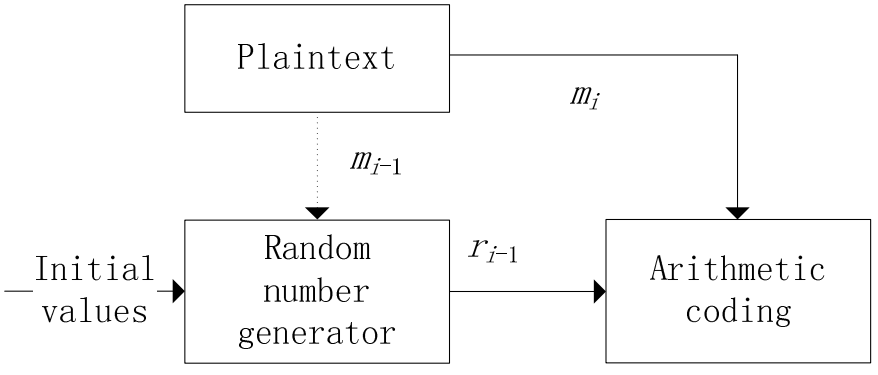


Fig. 1. Structure of the RAC and its variants where RNG is pseudo-random number generator and AC is traditional arithmetic encoding

Fig. 2 (a) shows procedure for encoding sequences 110 used in RAC. The order of intervals mapped to symbol 0 and 1 is determined by a secret random number bitstream $\{r_0, r_1, r_2\}$. Here, the probabilities of symbols 0 and 1 are 1/4 and 3/4, the corresponding intervals are [0, 1/4] and (1/4, 1]. The secret random number bitstream $\{r_0, r_1, r_2\}$ is 010 generated from pseudo-random number generator. Firstly, we encode plaintext block m_1=1. For the corresponding random number bit r_0=0, the order of intervals keeps the same. Now, we get interval [1/4, 1] after we encode plaintext block m_1 as arithmetic encoding. Sequentially, we encode plaintext block m_2=1. For the corresponding random number bit r_1=1, the order of intervals is swapped. After we encode plaintext block m_2=0, we get interval [1/4, 13/16]. Finally, we encrypt the third plaintext m_3, and we get final interval [1/4, 25/64]. For

comparison, the traditional arithmetic encoding is presented in Fig.2 (b). The order of interval keeps the same all the time. After three plaintext blocks are encoded, the final interval [7/16, 37/64] is obtained. Details of arithmetic coding process is not depicted in this figure, more details please refer to [6].

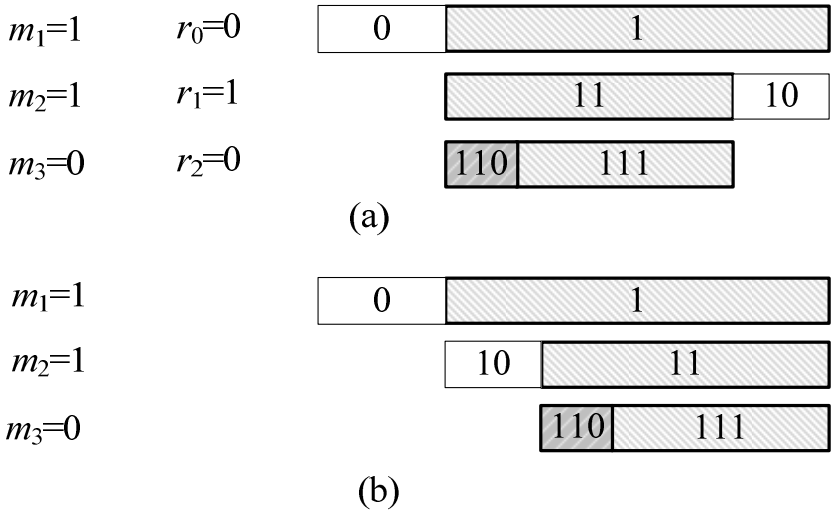


Fig. 2. Illustration of randomized arithmetic coding. (a) is for RAC and (b) is for traditional arithmetic coding

2.2 NDF

Since NDF has uniform distribution and large key space [14, 16], it has been successfully used in chaotic encryption algorithms [8, 17]. To enhance the security of RAC, the plaintext is mapped into the chaos parameter space. The binary random number bitstream produced by NDF is designed as follows.

Without loss of generality, the message is assumed as a sequence of symbols and the count of symbols is l, where $\{m_1, m_2 \ldots m_l\}$ is the ASCII value of original message. $\{r_1, r_2 \ldots r_t\}$ is the random number bitstream generated by NDF. $\{y_{-1}, y_0\}$, p and ϕ are the initial values of NDF.

1. The encoder gets z_{j-2} and z_{j-1} from Eq. (2) after getting ξ_{j-2} and ξ_{j-1} from Eq. (1). Here, m_{j-2} and m_{j-1} are the previous plaintext blocks with ASCII values.

$$\begin{aligned} \xi_{j-2} &= 3 + m_{j-2} / 256 \\ \xi_{j-1} &= 3 + m_{j-1} / 256 \end{aligned} \tag{1}$$

$$\begin{aligned} z_{j-2} &= \xi_{j-2} + \xi_{j-1} \\ z_{j-1} &= -\xi_{j-2} * \xi_{j-1} \end{aligned} \tag{2}$$

2. The encoder obtained variables $\{y_{i-2}, y_{i-1}\}$ from last step. Then, the encoder could get y_i from Eq. (3). The random number bit r_i can be obtained by the Eq. (4).

$$y_i = h \circ \mathrm{mod}(z_{j-2} \times y_{i-1} + z_{j-1} \times y_{i-2} + \phi) \tag{3}$$

$$r_i = \begin{cases} 1, & y_i \geq 0.5, \\ 0, & else \end{cases} \tag{4}$$

3. Repeat Steps 1) and 2), the encoder obtains the whole random number bitstream.

The function mod(.) of Eq. (3) is a modulo map described at Eq. (5), and the function of $h(.)$ represented in Eq. (6) is a piecewise linear map. Because the random number bitstream is key point for security of the algorithm, only the scheme of pseudo-random number generator is presented here. The encoding procedure of traditional arithmetic coding is the same as RAC [8].

$$\mathrm{mod}(v) = v - 2\lfloor (v+1)/2 \rfloor \tag{5}$$

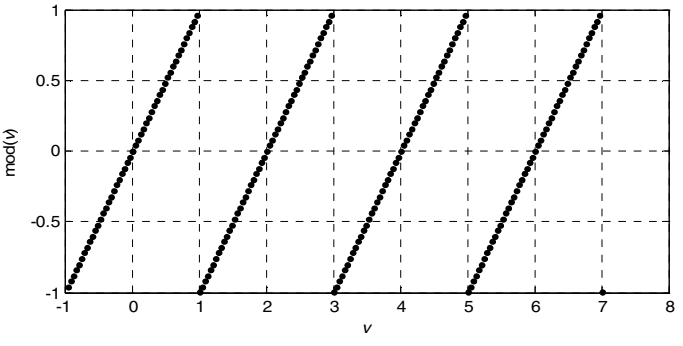
$$h(w) = \begin{cases} w/p, & 0 \leq w < p, \\ (w-p)/(0.5-p), & p \leq w < 0.5 \\ (1-w-p)/(0.5-p), & 0.5 \leq w < 1-p \\ (1-w)/p, & 1-p \leq w < 1 \\ h(-w), & w < 0 \end{cases} \tag{6}$$

3 Cryptanalysis of RAC Based NDF

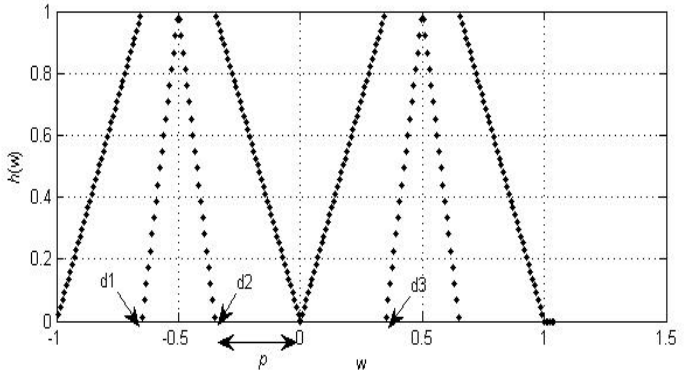
3.1 Chosen Plaintext Attack

A chosen-plaintext attack is an attack model for cryptanalysis which presumes that the attacker has the capability to choose arbitrary plaintext to be encrypted, and obtain the corresponding ciphertext. The goal of the attack is to gain usable information

which can reduce security of the encryption scheme. In the worst case, a chosen-plaintext attack could reveal the secret key. Here, a chosen-plaintext attack is used to show the vulnerability of the NDF. Assume that plaintext and corresponding ciphertext are exactly known to cryptanalyst in chosen plaintext attack scenario. It is easy to obtain the random number bitstream from the plaintext and corresponding ciphertext because the arithmetic coding is reversible operation. Therefore, random number bitstream generated by NDF can be considered as a known variable in chosen plaintext attack scenario.



(a) A plot of Eq. (5)



(b) A plot of Eq. (6)

Fig. 3. Plots of Eq. (5) and Eq. (6)

At the beginning of chosen-plaintext attack, various equations of NDF are examined first. Eq. (5) is a period-2 periodic function. Eq. (7) is an equivalent equation with Eq. (5). Fig.3 (a) shows that Eq. (5) is an identity transform when v is in

the range of [-1, 1]. These equations cannot evidently increase confusion of the algorithm. Here, Eq. (6) is the most important function in NDF which is depicted in Fig.3 (b). The plot of piecewise linear map $h(.)$ is constituted by the discrete points and consists of two distinct lines. Assume that there are a_1 points in the range of $[0, p]$ and a_2 points in the range of $[p, 0.5]$. Because the intervals of two points are equality, the length of $[0, p]$ is represented by a_1 and the length of $[p, 0.5]$ is represented by a_2.Now we know for sure that the Eq. (8) can reflect their relationship.

$$\begin{cases} f(x) = x, & x \in [-1,1], \\ f(x) = f(x+2), & else \end{cases} \tag{7}$$

$$\frac{a_1}{a_2} = \frac{p}{0.5-p} \tag{8}$$

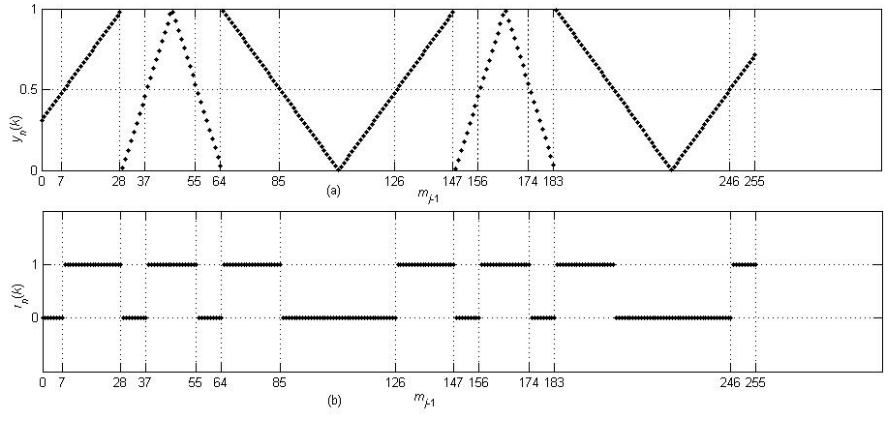


Fig. 4. Plots of plaintext m_{j-1} and the corresponding random number bit $r_n(k)$ and $y_n(k)$. (a) is a plot of m_{j-1} and $y_n(k)$. (b) is a plot of plaintext m_{j-1} and $r_n(k)$

In Eq. (3), z_{j-1}, z_{j-2} and modulo map mod(.) can be got from Eq. (1), Eq. (2) and Eq. (5). The result is presented in Eq. (9) where γ is integer and locates $\left[\frac{y_{n-1}}{256} - \frac{y_{n-2} \times (768 + m_{j-2})}{256^2}\right] * m_{j-1} + \phi_1$ within the range of [-1, 1]. Thus, the modulo map in Eq. (5) is an identity transform, and the operation

$\left[\frac{y_{n-1}}{256}-\frac{y_{n-2}\times(768+m_{j-2})}{256^2}\right]*m_{j-1}+\phi_1$ is a linear transformation of m_{j-1} if m_{j-2} is fixed. Assume that m_{j-1} is input variable, y_n is output and $\{y_{n-2}, y_{n-1}, p, \phi\}$ are constant values. The variable m_{j-1} is integer in the range of [0, 255] and the plaintext block m_{j-2} is set to 1. The corresponding sequence of y_n is $\{y_n(0), y_n(1)...y_n(k)\ldots, y_n(255)\}$ and the corresponding random number bitstream is $\{ r_n(0), r_n(1)...r_n(k)\ldots r_n(255)\}$. The plot of $\{y_n(0), y_n(1)...y_n(k)\ldots y_n(255)\}$ and corresponding m_{j-1} have two distinct parts: one is dense, the other is dilute depicted in Fig.4 (a). Since the cryptanalyst knows the random number bitstream $\{ r_n(0), r_n(1)...r_n(k)\ldots r_n(255)\}$ and the characteristics of distribution, they can easily obtain the value of p from Eq. (8) after getting the count of point a_1 located in dense part and a_2 located in dilute part.

There are still three unknown factors in $\left[\frac{y_{n-1}}{256}-\frac{y_{n-2}\times(768+m_{j-2})}{256^2}\right]\times m_{j-1}+\phi_1$. The cryptanalyst could find numbers of special points just like $\{d_1, d_2, d_3\}$ in Fig.3 (b) and estimate the approximate coordinates of these points. Furthermore, the approximation of $\{y_{n-1}, y_{n-2}, \phi_1\}$ can be got after numbers of $(y_n(k), m_{j-1})$ are substituted in Eq. (9). Furthermore, the cryptanalyst could reduce the error by a large number of statistical computing.

$$\begin{cases} y_n = h\circ \mathrm{mod}(\left[\frac{y_{n-1}}{256}-\frac{y_{n-2}\times(768+m_{j-2})}{256^2}\right]\times m_{j-1}+\phi_1) \\ \phi_1 = y_{n-1}\times\left(6+\frac{m_{j-2}}{256}\right)-y_{n-2}\times 3\times\left(3+\frac{m_{j-2}}{256}\right)+\phi-2\gamma \end{cases} \quad (9)$$

To confirm that algorithm NDF is vulnerable under chosen plaintext attack, a simulation is presented to recover the secret keys of NDF under chosen plaintext attack.

The key of NDF is $\{y_{-1}, y_0, p, \phi\}$ that is set to {0.2, 0.3, 0.6, 0.35}. $\{c_1, c_2\}$ is set to {5.7, 7} as recommendation of the scheme [8]. Fig.4 (a) is a plot of Eq. (9) when m_{j-1} is the input value in the range of [0, 255] and corresponding $y_n(k)$ as output value. The cryptanalyst must recover the keys of NDF only knowing the plaintext $\{m_{j-2}, m_{j-1}\}$ and the random number bit $r_n(k)$ corresponding to $y_n(k)$ in chosen plaintext attack scenario. The proposed chosen plaintext attack is described as follows.

1. In order to locate $\left[\frac{y_{n-1}}{256}-\frac{y_{n-2}\times(768+m_{j-2})}{256^2}\right]\times m_{j-1}+\phi_1$ within the range of [-1, 1], it is better to set y_{i-2} in the range [0.5, 1] and y_{i-1} in the range [0, 0.5), that means r_{i-2} must be equal to 1 and r_{i-1} must be equal to 0. In practical application, this condition is met easily. To simplify the procedure, y_{i-2} is arbitrarily set to 0.8 and y_{i-1} is arbitrarily set to 0.25. Plaintext value m_{j-2} is set to 1. Fig.4 (b) shows the plaintext and the corresponding random number bitstream.
2. As show in Fig.4 (b), we can count the number of points located in the range of [7, 28], and it is equal to 21. Meanwhile, we count the number of points located in the range of [28, 37], and it is equal to 9. Now, we know that a_1 is equal to 21and a_2 is equal to 9. Therefore, the cryptanalyst knows for sure that the approximation value of p is 0.35 from Eq. (8).
3. Put three special points (8, 0.5), (85, 0.5) and (106, 0) into Eq. (9), and then it is easy to obtain the approximation of coefficients $\{y_{i-2}, y_{i-1}, \phi\}$.
4. Repeat steps (1), (2) and (3) with several times, the cryptanalyst could reduce the error rate.

4 Improved Algorithm

4.1 Enhanced NDF

Because the plaintext is mapped into the coefficients of NDF directly, opponent can get these coefficients easily in chosen plaintext scenario. Making further investigation, the opponent could obtain information of other key as showing in section 3. The key problem is that Eq. (1) is linear correlation model and the coefficients of NDF relates to plaintext directly. With the linear correlation model, the opponent can obtain one part of key for NDF in chosen plaintext scenario. Therefore, nonlinear correlation model is necessary to resist the chosen-plaintext attack. In order to make this scheme flexibility in multimedia application, the coefficients must be mapped with the ciphertext. Here, the Eq. (10) is used to instead of Eq. (1). The operation $\oplus$ denotes XOR. The values of a_1 and a_2 are arbitrary positive integer.

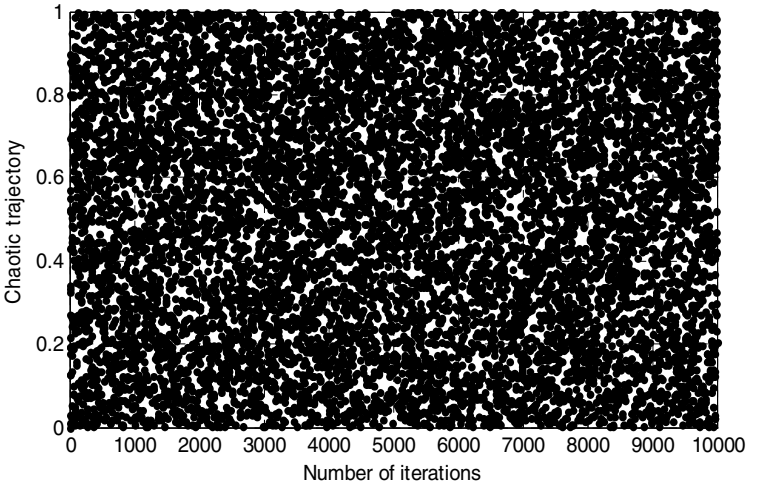
$$\begin{aligned}\xi_{j-2} &= a_0 \oplus C_{j-2} + 3 \\ \xi_{j-1} &= a_1 \oplus C_{j-1} + 3\end{aligned} \tag{10}$$

4.2 Effectiveness of Proposed Algorithm

Kelber [14] has proved that NDF is an ergodic chaotic system with n-D uniform distribution only if the coefficients are set as $z_n \in Z$ and $z_n \neq 0$, the function $h(w)$ is preserved with uniform distribution, and the system is not decomposable. Obviously, in proposed algorithm, z_n is positive integer meeting the first above condition. In a strict sense, the metric entropy is the rate of information generation with respect to the generating partitions of phase space. For 2-D NDF system, the metric entropy should be larger than 2 to obtain 2-bit information at one iteration. Ciphertext is translated to the corresponding ASCII numbers. By means of nonlinear transform, eigenvalues of NDF is obtained as Eq. (10). Then, the metric entropy is showed in Eq. (11), so it satisfies the Kelber condition [14].

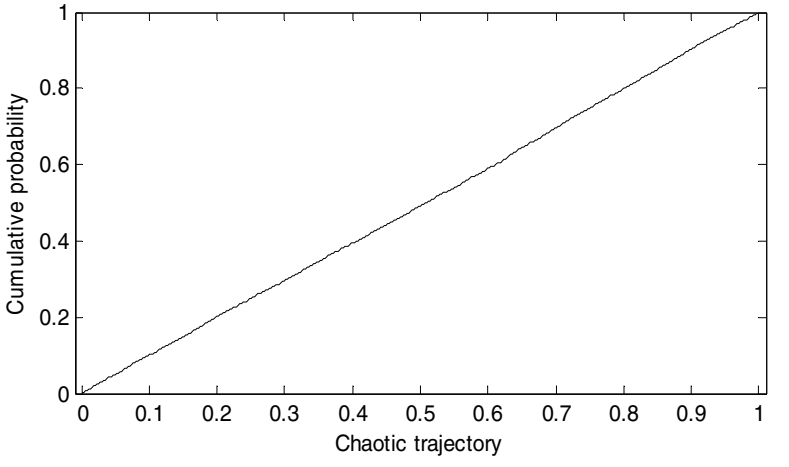
$$H = \sum_{i=1}^{2} \log \mid \xi_i \mid > 1 + 1 = 2 \tag{11}$$

Fig. 5(a) illustrated the trajectory of a second-order NDF map with the conditions that the initial ciphertext is randomly set in range of [0, 255], the initial values are a_1=25, a_2=23, ϕ = 0.6, p=0.35, $y_{-1}(0)$ = 0.2, y_{-2} = 0.3 and the number of iteration is 10,000. From the trajectory of a nonlinear dynamic filter and its distribution function as illustrated in Fig. 5(b), we can see that the chaotic property of the NDF map has the uniform probability density distribution.



(a)

Fig. 5. The uniform property of a variant NDF proposed in our scheme. (a) Trajectory of a variant NDF proposed in our scheme; (b) its distribution function.



(b)

Fig. 5. (*continued*)

5 Simulation Results and Analysis

5.1 Chosen Plaintext Attack

Coefficient of NDF is linearly related to plaintext, and two adjacent chaotic states are closely correlated. From analysis of the correlation between plaintext and random number bitstream in section 3, the coefficient of NDF, which is part of key, is recovered successfully in chosen plaintext attack scenario. In order to solve the problem, the system must guarantee that the plaintext is not closely related to both chaotic trajectory and coefficient of chaotic system. Here, a constructive model is presented in Eq. (10). The XOR operation ensures that the ciphertext is nonlinear related to coefficient. Even in chosen plaintext attack scenario, the opponent can't obtain the coefficient z_{j-2} and z_{j-1} for it doesn't get any knowledge of a_1 and a_2. In a similar way of Fig.4, Fig. 6 is a plot of ciphertext C_{j-1} versus the corresponding random number bit $r_n(k)$ and chaotic trajectory $y_n(k)$. Comparison Fig.4 with Fig.6, it is found that the chaotic trajectory is nonlinear related to ciphertext and the opponent can't get any information about key from this figure.

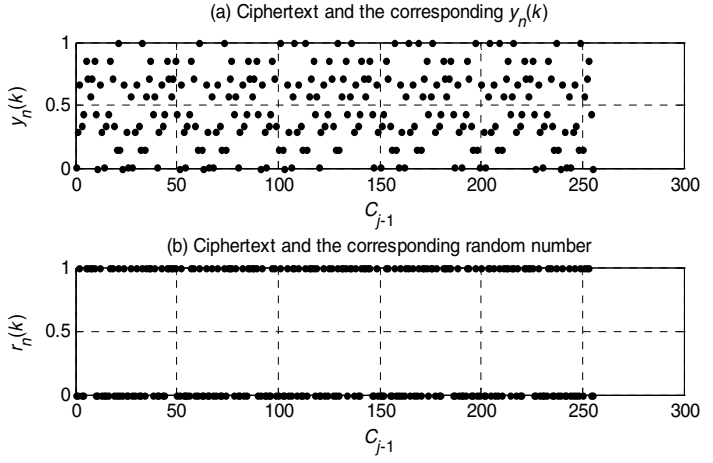


Fig. 6. Plots of ciphertext C_{j-1} and the corresponding chaotic trajectory $y_n(k)$ and random number bits $r_n(k)$ and. (a) is a plot of C_{j-1} versus $y_n(k)$, and (b) is a plot of Ciphertext C_{j-1} versus $r_n(k)$

Table 1. An analysis report for the statistical test suite which produces multiple P-values and proportions including the worst case

STATISTICAL TEST	PROPORTION	P-VALUE	RESULT
Frequency	0. 9880	0. 220159	Success
Block Frequency	0. 9880	0. 299251	Success
Cumulative Sums	0. 9880	0. 494392	Success
Runs	0. 9920	0. 974370	Success
Longest Run	0. 9860	0. 148653	Success
Rank	0. 9940	0. 827279	Success
Non-Overlapping Template	0. 9733	0. 000117	Success
Overlapping Template	0. 9860	0. 016261	Success
Universal	0. 9940	0. 162606	Success
Approximate Entropy	0. 9880	0. 246750	Success
Random Excursions	0. 9844	0. 014741	Success
Random Excursions Variant	0. 9875	0. 082702	Success
Serial	0. 9900	0. 319084	Success
Linear Complexity	0. 9860	0. 236810	Success

5.2 The Random Number Bitstream

The randomness of the random number bitstream is confirmed by the statistical test suite recommended by the U.S. National Institute of Standards and Technology (NIST) [15]. With 300 binary sequences, each of 1,000,000 bits is extracted for testing. They should pass 14 types of statistical tests including approximate entropy, block frequency, linear complexity, frequency, runs, longest run, rank and serial test. All proportion values from the multiple chaotic maps are bigger than the minimum pass rate. Therefore, the sequences are considered as random according to the NIST Special Publication 800–22 [15]. Table 1 is the analysis report from the statistical test suite. The item of proportion is the proportion of sequences passing a test, and the item of distribution of p-value is Chi-square Distribution value. If the value is bigger than 0.0001, it indicates that the sequence is uniformly distributed.

5.3 Multimedia Application Scenario

In multimedia application scenario, the users always move forward through an audio or video at a speed faster than that at which it would usually flow, and play audio or video at arbitrary portion as their wish. For scheme of [7, 8], Eq. (12) is a summarization of generating i^{th} random number bit. It shows that the decoder must obtain all preceding plaintext before getting the random number bit r^i and decoding the i^{th} ciphertext. Unfortunately, in multimedia application scenario, this condition is not always met. In the schemes of [7, 8], they maybe meet these requirements by blocking plaintext and reusing key vector repeatedly. However, in that way, these schemes will be similar to the classical approach to provide compression and encryption separately. And the security is even worse than that scheme for reusing the initial key vector repeatedly.

$$r_i = U(m_{-2}, m_{-1}, \cdots, m_{i-1}, \mathrm{y}_{-2}, \mathrm{y}_{-1}, \phi, p) \tag{12}$$

In proposed model, Eq. (13) is a summarization of generating i^{th} random number bit. For all of available ciphertext, the decoder could get the r^i and decode the i^{th} ciphertext.

$$r_i = U(C_{-2}, C_{-1}, \cdots, C_{i-1}, \mathrm{y}_{-2}, \mathrm{y}_{-1}, \phi, p, a_0, a_1) \tag{13}$$

6 Conclusion

The security of existing approach is analyzed. In the meantime, an enhanced algorithm is proposed with a new nonlinear correlation model between ciphertext and coefficients of NDF. For the nonlinear correlation model, the opponent can't obtain

the keys even in chosen plaintext attack scenario. The randomness of the pseudorandom number bitstream, which reflects security strength of RAC, is confirmed by the statistical test suite which is recommended by the U.S. National Institute of Standards and Technology (NIST). The improved algorithm can also meet users' individual requirements such as fast-forward, rewind or from arbitrary position to play video or audio at a user's discretion. The study in this paper shows that it is better to use ciphertext instead of plaintext as disturbing resource of encryption process for multimedia cryptosystem.

References

1. Wong, K.W., Yuen, C.H.: Embedding compression in chaos-based cryptography. IEEE Transactions on Circuits and Systems II-Express Briefs 55(11), 1193–1197 (2008)
2. Wu, C.P., Kuo, C.C.J.: Design of integrated multimedia compression and encryption systems. IEEE Transactions on Multimedia 7(5), 828–839 (2005)
3. Zhou, J.T., Au, O.C., Wong, P.H.W.: Adaptive chosen-ciphertext attack on secure arithmetic coding. IEEE Transactions on Signal Processing 57(5), 1825–1838 (2009)
4. Witten, I.H., Neal, R.M., Cleary, J.G.: Arithmetic coding for data compression. Communications of the ACM 30(6), 520–540 (1987)
5. Chen, R.C., Pai, P.Y., Chan, Y.K., Chang, C.C.: Lossless image compression based on multiple-tables arithmetic coding. Mathematical Problems in Engineering 2009, Article ID 128317 (2009)
6. Grangetto, M., Magli, E., Olmo, G.: Multimedia selective encryption by means of randomized arithmetic coding. IEEE Transactions on Multimedia 8(5), 905–917 (2006)
7. Mi, B., Liao, X.F., Chen, Y.: A novel chaotic encryption scheme based on arithmetic coding. Chaos Solitons & Fractals 38(5), 1523–1531 (2008)
8. Li, H.J., Zhang, J.S.: A secure and efficient entropy coding based on arithmetic coding. Communications in Nonlinear Science and Numerical Simulation 14(12), 4304–4318 (2009)
9. Wen, J.T., Kim, H., Villasenor, J.D.: Binary arithmetic coding with key-based interval splitting. IEEE Signal Processing Letters 13(2), 69–72 (2006)
10. Kim, H., Wen, J.T., Villasenor, J.D.: Secure arithmetic coding. IEEE Transactions on Signal Processing 55(5), 2263–2272 (2007)
11. Bose, R., Pathak, S.: A novel compression an encryption scheme using variable model arithmetic coding and coupled chaotic system. IEEE Transactions on Circuits and Systems I-Regular Papers 53(4), 848–857 (2006)
12. Li, M.: Generation of teletraffic of generalized cauchy type. Physica Scripta 81(2), 025007, 10 (2010)
13. Zhou, J.T., Au, O.C.: Comments on 'a novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system'. IEEE Transactions on Circuits and Systems I-Regular Papers 55(10), 3368–3369 (2008)
14. Kelber, K.: N-Dimensional uniform probability distribution in nonlinear autoregressive filter structures. IEEE Transactions on Circuits and Systems I-Fundamental Theory and Applications 47(9), 1413–1417 (2000)

15. Rukhin, A., et al.: A statistical test suite for the validation of random number generators and pseudo-random number generators for cryptographic applications Nat. Inst. Stand. Technol (NIST). Gaithersburg, MD, NIST Special Publication 800-22, May 15 (2001), http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html
16. Kelber, K., Gotz, M., Schwarz, W.: Generation of chaotic signals with n-dimensional uniform probability distribution by digital filter structures. In: Digital Signal Processing Workshop Proceedings, pp. 486–489 (1996)
17. Wang, X.M., Zhang, J.S.: Chaotic secure communication based on nonlinear autoregressive filter with changeable parameters. Physics Letters A 357(4-5), 323–329 (2006)