A novel chaotic stream cipher and its application to palmprint template protection*

Li Heng-Jian(李恒建) and Zhang Jia-Shu(张家树)†

Sichuan Province Key Lab of Signal & Information Processing, Southwest Jiaotong University, Chengdu 610031, *China*

(Received 23 April 2009; revised manuscript received 25 October 2009)

Based on a coupled nonlinear dynamic filter (NDF), a novel chaotic stream cipher is presented in this paper and employed to protect palmprint templates. The chaotic pseudorandom bit generator (PRBG) based on a coupled NDF, which is constructed in an inverse flow, can generate multiple bits at one iteration and satisfy the security requirement of cipher design. Then, the stream cipher is employed to generate cancelable competitive code palmprint biometrics for template protection. The proposed cancelable palmprint authentication system depends on two factors: the palmprint biometric and the password/token. Therefore, the system provides high-confidence and also protects the user's privacy. The experimental results of verification on the Hong Kong PolyU Palmprint Database show that the proposed approach has a large template re-issuance ability and the equal error rate can achieve 0.02%. The performance of the palmprint template protection scheme proves the good practicability and security of the proposed stream cipher.

Keywords: chaotic stream cipher, coupled nonlinear dynamic filter, biometric protection, cancelable competitive code

PACC: 0545

1. Introduction

Chaotic cryptography has received much attention in recent years. Chaotic systems are well known to be very sensitive to both initial states and system parameters. Furthermore, based on characteristics such as ergodicity, unstable periodic orbits, one-way property, pseudo-randomness and mixing properties, many cryptosystems based on chaos have been proposed. Also, chaos-based approaches have great potential applications in many fields, such as protecting multimedia content,[1,2] constructing hash function[3−5] and enhancing biometrics security and privacy.[6]

A lot of stream ciphers based on chaos have been proposed in recent years.[2,7−10] Usually, a good chaotic stream cipher depends on its generation mechanism and the chaotic map employed. Both of them determine the key space and the security strength. Perturbations can also improve the cryptographical properties.[2,7] A coupled piecewise linear map chaotic system (CCS) is employed to generate a pseudorandom bit generator (PRBG) and to construct stream ciphers for its excellent cryptographic properties.[9] The NDF chaotic map, which has a uniform distribution and large key space, can generate n-dimensional uniform probability distribution chaotic signals up to n-th-order.[11] Inspired by CCS, a coupled NDF with the same flow is employed to generate multiple bits per iteration.[10] However, only one output of them is employed via circular left (right) shift operation to obtain multiple bits. To improve the security and make full use of the n-dimensional uniform distribution, a novel structure where the flows of the coupled NDF are in an inverse direction is proposed to generate multiple bits effectively via comparison with the output of each other.

With the growing use of biometrics, there is rising concern about the security and privacy of the biometric data itself.[12] Ratha *et al.* analysed the basic vulnerabilities of biometrics systems and addressed systematically eight potential attacks in Ref. [13]. In all the vulnerabilities, the security of biometric templates is particularly important due to their irrevocable nature. Another important reason is that biometric templates play a key role in biometric verification/identification. One of the template protection schemes mainly depends on irreversible transforms to

*Project supported by the National Natural Science Foundation of China (Grant No. 60971104), the Basic Research Foundation of Sichuan Province, China (Grant No. 2006J013-011), and the Outstanding Young Researchers Foundation of Sichuan Province, China (Grant No. 09ZQ026-091), and the Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20090184110008).

†Corresponding author. E-mail: jszhang@home.swjtu.edu.cn

© 2010 Chinese Physical Society and IOP Publishing Ltd

generate cancelable biometrics templates.[14,15] But these techniques have an impractical hidden assumption that users never share or lose their token keys, and a detailed analysis is given in Ref. [16]. Therefore, based on a competitive code,[17] invertible transform is suggested and a random orientation filter bank (ROFB) is employed as a feature exactor to generate noise-like feature codes.[18] Although this method has some problems, for example, the ability of template re-issuance usually depends on the cryptography not the theoretical analysis, it provides a compromise between security and accuracy in the palmprint verification. In this paper, the bitwise of the palmprint competitive code are encrypted by chaotic stream ciphers to generate renewable and privacy preserving binary palmprint templates, which can increase the inter-class divergence and maintain the intra-class variance. Several experimental results of key sensitivity tests and key space analysis show that chaotic stream ciphers are very efficient and secure for protecting users' privacy; moreover, the proposed scheme can provide high-confidence cancelable palmprint verification performance with very large re-issuance power.

The rest of this paper is organized as follows. In Section 2, a novel chaotic stream cipher based on coupled NDF is presented. Based on it, a palmprint template protection scheme is given in Section 3. In Section 4, the performances of the palmprint template protection scheme are analysed and discussed. Finally, conclusions are given in Section 5.

2. Generating multiple pseudo-random bits based on coupled NDF

Constructing a stream cipher via a coupled chaotic system, which can provide higher security than that of one chaos, was first proposed in Ref. [9]. Recently, NDF has received attention for its n-dimensional uniform distribution, ergodicity and large key space.[5] In this section, we present a novel chaotic stream cipher where coupled NDF chaotic systems are employed to generate multiple pseudo-random bits.

2.1. The n-dimensional (n-D) nonlinear digital filter

Consider an n-D continue-value discrete-time NDF structure. The state space equation of the system is

$$\begin{aligned} &z_1(t+1) = h \circ \mathrm{mod}\left(\sum_{i=1}^{n} c_i z_i + \phi\right), \quad \phi \in \Phi = R, \\ &z_k(t+1) = z_{k-1}(t), \quad k = 2, 3, \ldots, n, \\ &y(t) = z_k(t+1) \in I, \end{aligned} \tag{1}$$

where

$$z = (z_1, z_2, \ldots, z_n)^{\mathrm{T}} \in Z = I^n$$

denotes the vector of state variables, $h(\cdot)$ is a piecewise linear map $h : I \to I, h(w) = m_k \cdot \omega + r_k$, $\omega \in W_k \subseteq I, k \in \{1, \ldots, M\}$. Without loss of generality, $I = [-1, 1)$, a popular piecewise linear map (PWL) can be given as follows:

$$h(w) = \begin{cases} w/p & 0 \le w < p, \\ (w-p)/(0.5-p) & p \le w < 0.5, \\ (1-w-p)/(0.5-p) & 0.5 \le w < 1-p, \\ (1-w)/p & 1-p \le w < 1, \\ h(-w) & w < 0, \end{cases} \tag{2}$$

where $\mathrm{mod}(\cdot)$ is a modulo map given by

$$\mathrm{mod}(v) = v - 2\left\lfloor \frac{v+1}{2} \right\rfloor. \tag{3}$$

Because of the periodicity of the modulo map, we restrict our consideration to the parameter interval $\Phi = [-1, 1)$. The eigenvalues of Eq. (1) are denoted by λ_i, $i = 1, \ldots, n$. Kelber[8] has proved that equation (1) is an ergodic chaotic system and the state vector Z has an n-D uniform probability density only if the following conditions are satisfied: (i) $h(\cdot)$ is uniform distribution preserving; (ii) the n-dimensional system cannot be decomposed into lower-dimensional independent subsystems, that is $|\lambda_i| \neq 1, i = 1, \ldots, n$; (iii) the system parameters satisfy $c_n \in Z$, $|c_n| > 1$ and $s_n \in Z$, $|s_n| > 1$. The n-th-order nonlinear filter satisfying the above conditions is an n-D chaotic system with good cryptographic properties.

2.2. Design of chaotic stream cipher based on the coupled NDF

Based on the entropy criterion and Kelber condition,[11] the well-designed NDF can generate multiple random bits per iteration. In this section, we use a novel structure in which the flows of the coupled NDF are in an inverse direction to construct a chaotic stream cipher. As illustrated in

Fig. 1, two independent NDFs with the same order but different coefficients are employed to construct an efficient chaotic stream cipher. The pseudorandom bit vector sequence $K(i)$ can be represented as $K(i) = \{k((i-1)*n+1), \ldots, k(i*n)\}$, $i = 1, 2, \ldots, N$, where n is the order of NDF, N is the length of the pseudorandom sequence, $k(i)$ is represented by $k(i) = g(Z_1(i), Z_2(n-i+1))$. Here $Z_1(i)$ is the output of NDF_1, $Z_2(i)$ is the order of NDF_2. The $g(\cdot)$ is defined as

$$g(x_1, x_2) = \begin{cases} 1, & x_1 > x_2, \\ \text{null}, & x_1 = x_2, \\ 0, & x_1 < x_2. \end{cases} \tag{4}$$

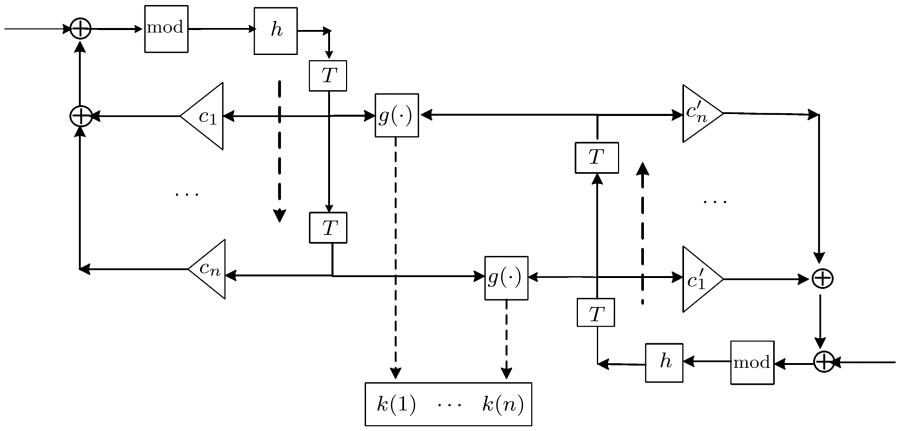


Fig. 1. Proposed coupled chaotic stream cipher.

Suppose that ξ_i is the system eigenvalue; it can be proved that the Lyapunov exponents of the system are $\lambda_i = \log|\xi_i|$. For multidimensional systems, metric entropy is a sum of all positive Lyapunov exponents. Thus the metric entropy h of NDF is given by

$$h = \sum_{\lambda>0} \lambda_i = \sum_{|\xi_i|>1} \log|\xi_i| = \log \prod_{|\xi_i|>1} |\xi_i|. \tag{5}$$

If $|\xi_i| > 1$ for $i = 1, 2 \ldots, n$; H will be simplified into

$$H = \log \prod_{i=1}^{n} |\xi_i| = \log|c_n|. \tag{6}$$

In a strict sense, the metric entropy is the information creation rate with respect to the generating partitions of phase space. Heuristically, H also characterizes the entropy of discrete information. In other words, $n \leq \lfloor H \rfloor$ should be satisfied for generating n bits at each NDF. For our proposed coupled NDF chaotic systems, the metric entropy should be the sum of that of each NDF. The properties of the proposed chaotic stream cipher will be discussed in detail below.

2.3. Statistical properties of coupled NDF–PRBG

According to Kolmogorov entropy theory,[19] $Z_1(i)$ and $Z_2(i)$ can be considered to be independent after several iterations. When the chaotic systems are realized in the finite precision form, the information will decrease even faster since the quantization errors make two orbits depart faster. So we can say that, as long as there is an initial difference between two chaotic orbits, they will become asymptotically independent as $i \to \infty$. The distributions of both NDF_1 and NDF_2 are uniform distributions. Defined within a scope $I = (-1, 1)$ in NDF, the orbits generated from almost all the initial conditions will lead to the same distribution functions $f_1(x)$ and $f_2(x)$. Therefore, the probabilities of $x_1 > x_2$ and $x_1 < x_2$ as $i \to \infty$ will be

$$P\{x_1 > x_2\} = \int_a^b \int_a^x f_1(x) f_2(y) \, \mathrm{d}y \mathrm{d}x,$$

$$P\{x_1 < x_2\} = \int_a^b \int_a^x f_2(x) f_1(y) \, \mathrm{d}y \mathrm{d}x.$$

Considering that $f_1(x)$ and $f_2(x)$ have the same uniform distributions, it can be inferred that

$$\begin{aligned} P\{x_1 > x_2\} &= P\{x_1 < x_2\} \\ &= \int_a^b \int_a^b f_1(x) f_2(y) \, \mathrm{d}y \mathrm{d}x \\ &= 0.5. \end{aligned} \tag{7}$$

Apparently, the above deduction is still based on the continuous conditions. When chaotic systems are discretely realized with perturbation, every chaotic orbit will be perturbed timely to a certain neighbour orbit by the small perturbing signal. Consequently, almost all orbits reach the discrete versions of $f_1(x)$ and $f_2(x)$. For the discrete condition, the above conclusion also holds if the integral operator is replaced by summation.

Therefore, the balance will be approximately preserved in the digital coupled CCS–PRBG. The independent and identical distributions (IIDs) of $Z_1(i)$ and $Z_2(i)$ as well as the balance between 0 and 1 imply that the proposed PRBG is an independent and identically distributed bit sequence. Therefore, it has a delta-like auto-correlation function and near-zero cross-correlation function. Moreover, the independent and identical distribution has half-length complexity. Some tests are illustrated in Fig. 2 to confirm the results. Figure 2(a) shows that the 0–1 ratio is balanced. Figure 2(b) illustrates the high linear complexity. Figures 2(c) and 2(d) give the autocorrelation and the cross-correlation of the random sequences, respectively. The autocorrelation looks like a δ function, and the cross-correlation curve lies near zero. All these properties make it suitable for stream cipher construction with high security.

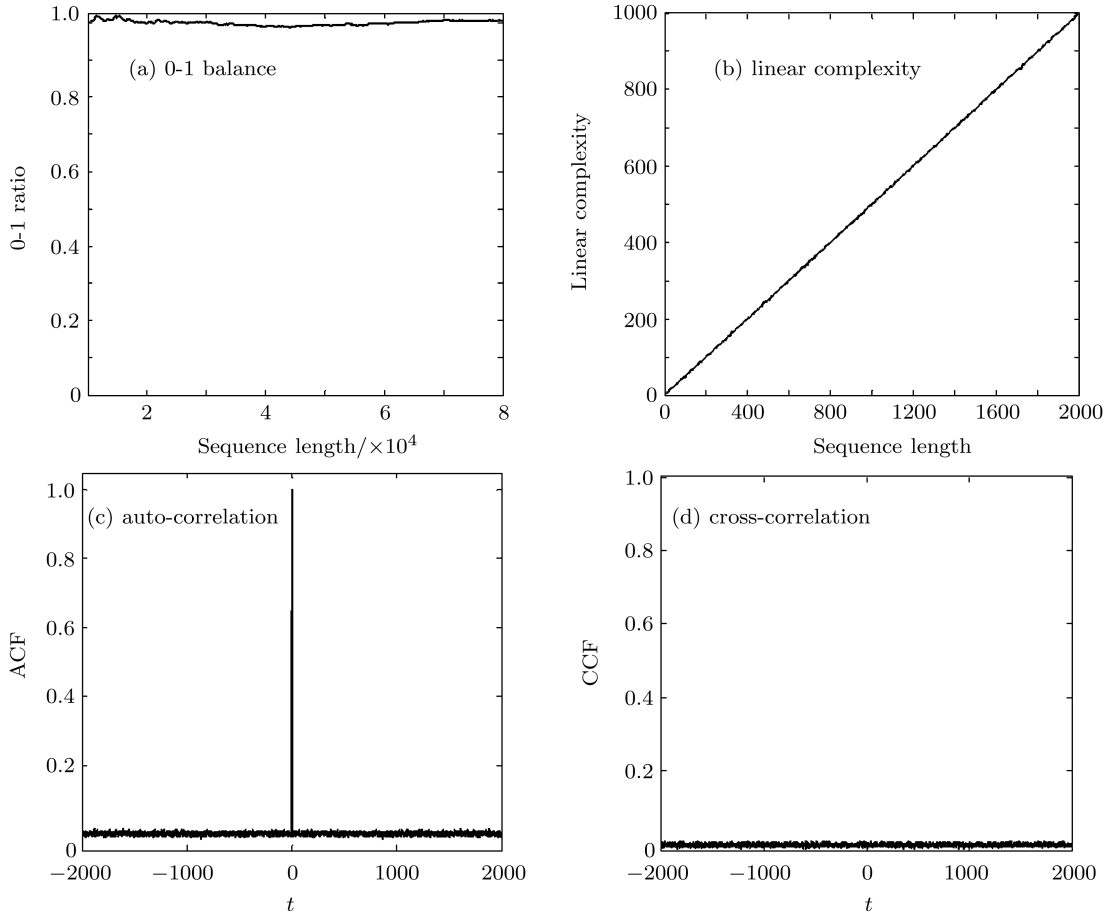


Fig. 2. Cryptographic properties of second-order coupled NDF–PRBG.

In order to verify the above cryptographic properties of coupled NDF–PRBG, some other experiments are conducted. Also, the pseudo-random sequence should pass all known statistical tests for randomness. Statistical tests determine whether the sequences possess certain attributes that truly random sequences would be likely

to exhibit. Hence, any random number generator which is proposed for the cryptographic applications must be subject to statistical tests. When a PRBG for cryptographic purposes is evaluated, the National Institute of Standards & Technology (NIST)[20] proposes a battery of statistical tests that must be performed. For the NIST test, the tests will be successful if the p-value is greater than 0.01 (99% confidence). Table 1 gives the test results, which pass all the test items as expected. The numbers of nonperiodic templates, random-excursions and random-excursions-variant are 148, 8, and 18, respectively, and all of them pass. In summary, we propose a novel chaotic pseudo-random bit generator named CCS–NDF, which is based on the metric entropy criterion and Kelber condition; the process meets the randomness requirement. The proposed novel has ideal cryptographic properties and a high bit generation rate.

Table 1. Randomness test results summary with NIST-142.

test type	p-value	test type	p-value
approximate entropy	0.304505	block frequency	0.792891
cumulative sums (Forward) (Reverse)	(F) 0.39527 (R) 0.596954	random-excursions (8)	all pass
FFT	0.392183	random-excursions-variant (18)	all pass
frequency	0.800771	rank	0.107324
linear complexity	0.843378	runs	0.504227
longest runs	0.476340	serial-1	0.899020
nonperiodic templates (148)	all success	serial-2	0.806959
overlapping template	0.421257	universal	0.758049

3. Cancelable competitive code based on coupled NDF

Palmprint-based biometric verification/identification has received extensive attention from researchers during recent years. However, there has been little research on palmprint security up to now and the existing cancelable template protection algorithms cannot work very well.[21] One potential scheme is a competitive code based on random field,[18] but the ability of template re-issuance is always limited by the key space, and performance needs to be further improved. To obtain a cancelable competitive code and provide high-confidence, a cancelable palmprint verification system based on the competitive code is proposed as illustrated in Fig. 3.

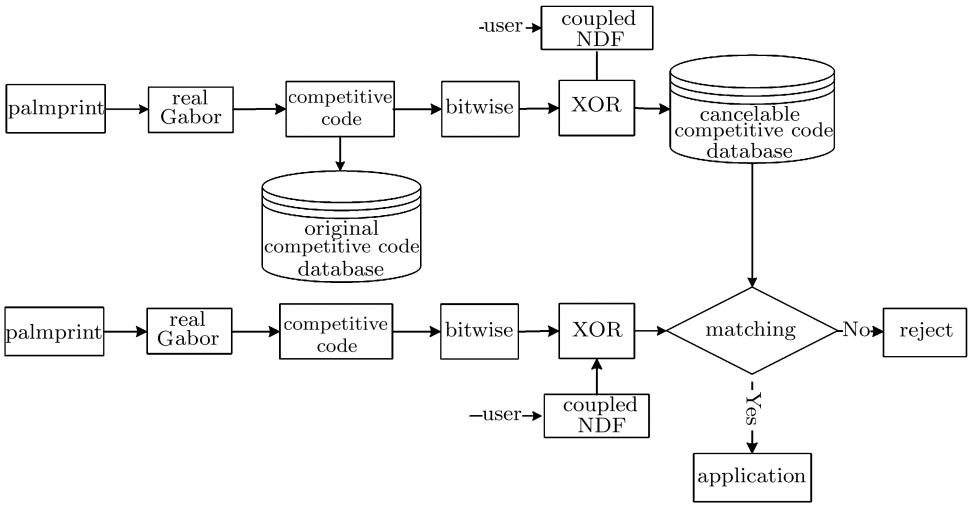


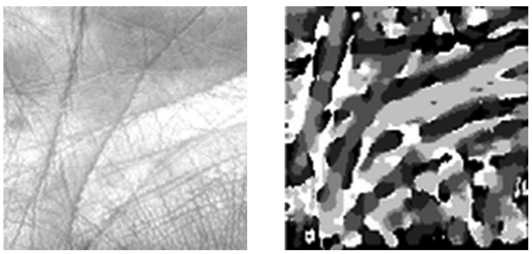
Fig. 3. Block diagram of a palmprint verification system based on cancelable competitive code. The system is mainly composed of three parts: part 1 for obtaining the competitive code, part 2 for generating a cancelable competitive code, and part 3 for matching. These parts will be described in detail below.

3.1. Basic concept of competitive code

The competitive coding scheme aims to encode the dominant orientations of palmprint lines. More concretely, letting $I(x, y)$ denote the preprocessed image and $G(\theta)$ be a real Gabor filter with orientation θ which can be found in Ref. [22], then the competitive rule will be a winner-take-all defined as

$$j = \arg\min \iint_{\theta} I(x, y) G(\theta) \, \mathrm{d}x \, \mathrm{d}y, \tag{8}$$

where j is the winning index. According to the neurophysiological findings, the simple cells are sensitive to specific orientations with an approximate bandwidth of $\pi/6$, thus, six filters with orientations $\theta_p = p \times \pi/6$, $p = \{0, 1, \ldots, 5\}$ are selected for competition. Figure 4(b) shows a competitive code of the preprocessed image illustrated in Fig. 4(a). The competitive rule is applied to each sample pixel and produces a 3-bit code as illustrated in Table 2. With this bitwise representation, the angular distance of two competitive codes can be efficiently computed with Boolean operators.



(a) (b)

Fig. 4. Palmprint image (a) and its competitive code (b).

Table 2. Bitwise representation of the competitive code.

winner indexes	bit 1	bit 2	bit 3
0	0	0	0
1	0	0	1
2	0	1	1
3	1	1	1
4	1	1	0
5	1	0	0

3.2. Generation of cancelable competitive code

To generate a cancelable competitive code, the bitwise representation of the competitive code is encrypted with a chaotic stream cipher based on the three-order coupled NDF via exclusive OR operation. The cancelable palmprint template is pseudorandom and its independence is enhanced, therefore, the standard deviation will decrease. The probability of "0" (p_0) in the encrypted template approximates to p_1, $p_0 = p_1 = 0.5$. From the theory of probability, the normalized Hamming distances between the two encrypted templates which are exacted from different palms are

$$s = 1 - p_0^2 - p_1^2 = 1 - 0.5^2 - 0.5^2 = 0.5, \tag{9}$$

while the Hamming distances between the cancelable templates from the same palms are the same as those of the original templates. Exclusive-OR (XOR) operations can maximally increase the inter-class divergence of different subjects while maintaining intra-class variance of the same subjects. Therefore, the verification performance can be improved dramatically. In the matching phase, the Hamming distance is employed to measure the similarity between different palmprint features and can be performed in the encryption domain directly, which can protect users' privacy and reduce the computation complexity.

3.3. Security analysis

Our basic design depends on two factors: a biometric token and a physical token. If only one factor is compromised, the system can still work well. For example, if the biometric token is shared, this does not conduce to the attacker because the key is randomly generated and only known to legality users. On the other hand, if the users lose their tokens, the palmprint system reverts to the original palmprint authentication system, and what is more interesting is that the authentication performance of the biometric system is not degraded since the Hamming distances are maintained in the reversible system. The system can provide different tokens from one application to another to ensure the security and privacy of biometric data. This prevents cross-matching databases, thereby ensuring the user's privacy. It is computationally very hard to recover the original palmprint images from the competitive code. This property prevents an adversary from creating a physical spoof of the palmprint. If an encryption template is compromised, it can easily be revoked, and re-issued by a new one just with another token, thus providing revocability. The ability of template re-issuance will be discussed in Subsection 4.3.

4. Experimental results and discussion

We choose a third-order nonlinear dynamic filter defined as

$$y(n) = h \circ \mathrm{mod}\left(c_1 y(n-1) + c_2 y(n-2)\right.$$

$$+ c_2 y(n-3) + \phi_0)\,. \tag{10}$$

The eigenvalues are set by $(\lambda_1, \lambda_2, \lambda_3) = (2, -3, 4)$ and $(\lambda_1', \lambda_2', \lambda_3') = (2, -4j, 4j)$, correspondingly, the control parameters of NDF_1 and NDF_2 can be obtained with the synthesis method[11] $(c_1, c_2, c_3) = (3, 10, -24)$ and $(c_1', c_2', c_3') = (2, -16, 32)$, respectively. The initial filter state values of NDF_1 and NDF_2 are (φ_0, $y(0)$, $y(1)$, $y(2)$) = (0.7109, 0.2315, 0.3431, 0.8425), and (φ_0', $y(0)'$, $y(1)'$, $y(2)'$) = (0.6587, 0.3564, 0.8021, 0.3215) respectively. The control parameter p in PWL is 0.35. The generation information entropy can be achieved at $h = \log 24 + \log 32 = 6.6438 > 3$. The experiments are conducted on a personal computer configured with an XP operating system and Matlab 7.6 with image processing toolbox and VC++6.0 platform.

4.1. Database and experiment settings

All the experiments are performed on the Hong Kong PolyU palmprint database that contains 7752 greyscale images captured from 193 individuals, 386 different palms.[23] The samples of each individual are collected in two sessions, where the average interval between the first and second sessions is around two months. The resolution of all the original palmprint images is 384 × 284 pixels at 75 dpi. In our paper, the palmprint is orientated and the region of interest, whose size is 128×128, is cropped.

The performance of a verification method is often measured by false acceptance rate (FAR), false reject rate (FRR) and equal error rate (EER). With regard to the evaluation of the separation between the genuine and the imposter distributions, the discriminating index d' (d-prime)[24] is computed to measure how well the non-match score probability density and the match score probability density are separated. The d' is defined as

$$d' = \frac{\mu_1 - \mu_2}{\sqrt{(\sigma_1^2 + \sigma_2^2)/2}}, \tag{11}$$

where μ_1 and σ_1 are the mean and variance of the match scores of genuine populations, respectively; μ_2 and σ_2 are the mean and variance of the match scores of imposter populations, respectively.

4.2. Verification test

To obtain the verification accuracy of our palmprint system, each of the palmprint images is matched with all the others in the database. A matching is said to be genuine if two palmprint images are from the same palm. None of the matching Hamming distances is zero. The failure to enrol rate is zero. The peak/mean value of imposter matching (the peak value approximates the mean value for the imposter matching and nearly satisfies symmetrical distribution) increases from 0.4608 to 0.4804 while the genuine matching score distribution is maintained as shown in Table 3, where those obtained from the original competitive code are also listed for comparison. What is more, the variance decreases from 2.7717×10^{-4} to 3.1438×10^{-5}. d'-primes is also computed, and its increase is increased by 0.7389 via matching in the encryption domain. The matching process in the encrypted domain can reduce the variance of the imposter matching scores since the randomness and the independence of encryption template are enhanced.

Table 3. Comparisons between the original competitive code and the cancelable competitive code.

	genuine distribution		imposter distribution		EER (%)	d'-prime
	mean	variance	mean	variance		
original competitive code	0.2335	0.0029	0.4608	2.7717×10^{-4}	0.13	5.6764
cancelable competitive code	0.2335	0.0029	0.4804	3.1148×10^{-5}	0.02	6.4162

From Fig. 5, the genuine and imposter matching score distributions can be separated at the threshold between 0.38 and 0.46. However, the operation threshold in this range is not best in the applications since the FAR is very high in a range of 0.40–0.46 in the token-stolen case as illustrated in Fig. 6. Therefore, considering all the aspects, the optimized threshold in our system is between 0.38 and 0.40. More interestingly, the FRR within the cancelable palmprint template is zero while GAR is very high (GAR is 99.85% when the threshold is set to be 0.39) if the operating range is from 0.37 to 0.39. The threshold in this range leads the security level to be very high and a user may try many times to reduce the FAR in the real application systems.

Finally, figure 7 depicts the corresponding receiver operation characteristic (ROC) curves, which are plots of false reject rate against false acceptance rate. From Fig. 7, we can see that the EER is 0.02%, nearly perfect zero EER, while the competitive code (competitive code –FOFB, whose performance is the same as those of the original competitive code) is 0.13%. In particular, the GAR of the proposed approach (99.94%) is about

1.79% higher than that of the original competitive code (98.15%) while the FAR is 1×10^{-5}%. The accuracy of the proposed palmprint authentication is improved by the token, and so is the security.

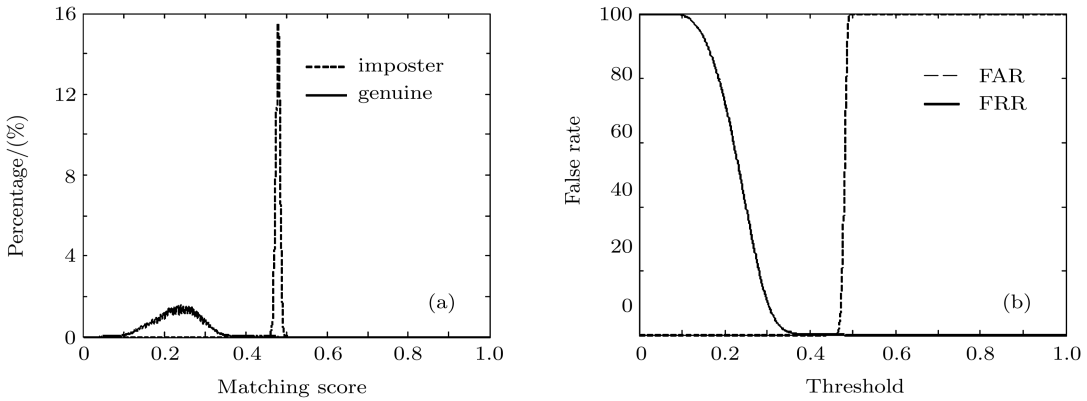


Fig. 5. Verification test results obtained with cancelable competitive code, where (a) is for genuine and imposter distributions of matching score and (b) for FAR and FRR curves.

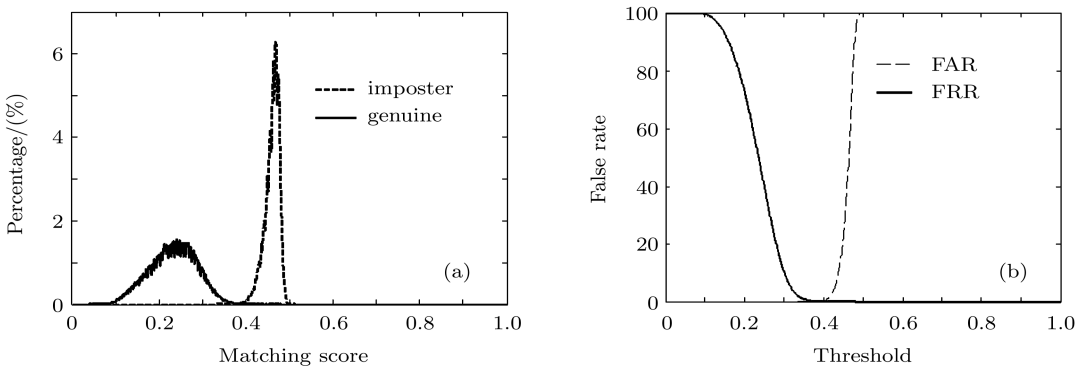


Fig. 6. Verification test results in the token-stolen scenarios (also the original competitive code), (a) is for genuine and imposter distributions of matching scores, and (b) for FAR and FRR curves.

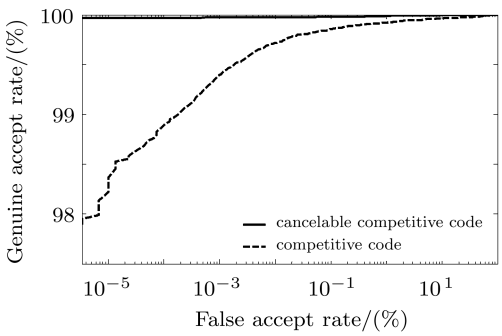


Fig. 7. ROC curves of cancelable competitive code (ROFB) and competitive code.

4.3. Ability of palmprint template re-issuance

The ability of palmprint template re-issuance is characterized by the key space of the employed chaotic stream cipher. The key space size depends on the total number of different keys that can be used in the encryption. A good cancelable palmprint authentication system indicates that the cancelable templates are completely sensitive to all the secret keys and the ability of template re-issuance should be large enough to make brute-force attacks unfeasible. According to the experiments in Subsection 4.2, the optimized threshold range is from 0.37 to 0.39 in our system, which means that the imposter matching scores should be bigger than 0.39 if the FAR is expected to be zero. Therefore, at least one of the parameters in NDF_1 and that in NDF_2 must vary simultaneously to make the system satisfy sufficient security. Otherwise, the matching score is approximately 1/3, which tends to lower the decision threshold, that is, it leads to false acceptance. The conclusion can be proven below.

Supposing that the four sequences $\{s_1\}$, $\{s_2\}$, $\{s_3\}$ and $\{s_4\}$ are IIDs and satisfy uniform distributions, then the ideal matching score in the encryption domain is approximately

$$p\,(s_3 > s_4\,|s_1 > s_2\,) = p\,(s_3 > s_4) = 0.5,$$

corresponding to that in Eq. (9). For a special case, we can infer

$$p\left(s_3 > s_4 \left| s_1 > s_2 \right.\right) \neq p\left(s_3 > s_4\right) = 0.5$$

on the condition that $\{s_2\} = \{s_4\}$ is satisfied since $p\left(s_1 > s_2\right)$ and $p\left(s_3 > s_2\right)$ are not independent. However, the equation attains the following form:

$$\begin{aligned} p\left(s_3 > s_4 \left| s_1 > s_2 \right.\right) &= p\left(s_3 > s_2 \left| s_1 > s_2 \right.\right) \\ &= 1/3. \end{aligned} \tag{12}$$

The proof is given in sequence. If $s_1 > s_2$ and $s_3 > s_2$, which implies $\min\left(s_1, s_2, s_3\right) = s_2$ and yields

$$p\left(s_3 > s_2 \left| s_1 > s_2 \right.\right) = p\left(\min\left(s_1, s_2, s_3\right) = s_2\right), \tag{13}$$

then $\{s_1\}$, $\{s_2\}$ and $\{s_3\}$ are IIDs. Consequently,

$$\begin{aligned} & p\left(\min\left(s_1, s_2, s_3\right) = s_1\right) \\ = \; & p\left(\min\left(s_1, s_2, s_3\right) = s_2\right) \\ = \; & p\left(\min\left(s_1, s_2, s_3\right) = s_3\right). \end{aligned} \tag{14}$$

There is an implied condition

$$\sum_{i=1}^{3} p\left(\min\left(s_1, s_2, s_3\right) = s_i\right) = 1. \tag{15}$$

Therefore, we can obtain

$$p\left(\min\left(s_1, s_2, s_3\right) = s_i\right) = 1/3, \quad i = 1, 2, 3. \tag{16}$$

The proof is completed. In order to validate the conclusion and investigate the key space size, the following experiments are performed. The results are shown in Table 4. From the last row and last column in Table 4, we can draw a conclusion that the coupling of NDF could result in a reduction to half of the original key space. The coupled component of the key scales down from initial values by a ratio of 10^{-1} separately, and the corresponding ciphertext ratios are shown in Table 4 (we also have tested the other parameter pairs, and they have a similar character). The results in Table 4 show that the ciphertext variation rates approximate to 0.5 when the parameters in NDF_1 and NDF_2 are both changed to 10^{-16} and they approximate to 1/3 when only one of the two parameters is changed to 10^{-17}. Considering all the other coupled key components and noting that NDF has three parameters, we can easily derive the size of the key space to be $0.5 \times 10^{16\times4\times2} = 0.5 \times 10^{128}$. The number of effective cancelable templates is numerous, which is enough to re-issue many templates resistant to all kinds of brute-force attacks.

Table 4. Key sensitive test.

NDF_2	an initial value scales down by a ratio of 10^{-1} in NDF_1							
	$1.\times10^{-1}$	$1.\times10^{-2}$	$1.\times10^{-3}$	$1.\times10^{-4}$	$1.\times10^{-5}$	$1.\times10^{-6}$	$1.\times10^{-7}$	$1.\times10^{-8}$
$1.\times10^{-1}$	0.5015	0.5033	0.5019	0.4935	0.5009	0.5055	0.5042	0.5025
$1.\times10^{-2}$	0.4969	0.4993	0.5011	0.4899	0.4949	0.4955	0.5043	0.5073
$1.\times10^{-3}$	0.4991	0.5031	0.5021	0.4939	0.5062	0.5043	0.5043	0.5019
$1.\times10^{-4}$	0.5009	0.5020	0.5073	0.4987	0.5043	0.5031	0.5015	0.5055
$1.\times10^{-5}$	0.4947	0.4967	0.5018	0.4932	0.4929	0.5019	0.5012	0.5009
$1.\times10^{-6}$	0.5052	0.5066	0.5072	0.4997	0.5058	0.5076	0.5114	0.5081
$1.\times10^{-7}$	0.4996	0.4999	0.5049	0.4915	0.5041	0.4989	0.5034	0.5041
$1.\times10^{-8}$	0.4936	0.5029	0.5016	0.4954	0.5015	0.5001	0.5019	0.4981
$1.\times10^{-9}$	0.5007	0.5033	0.5039	0.4959	0.5031	0.5050	0.5063	0.5047
$1.\times10^{-10}$	0.4994	0.5027	0.5057	0.4917	0.5036	0.5039	0.5054	0.5023
$1.\times10^{-11}$	0.4943	0.4932	0.4977	0.4881	0.4939	0.5043	0.5005	0.4973
$1.\times10^{-12}$	0.5014	0.4991	0.5007	0.4971	0.5063	0.5015	0.5048	0.5028
$1.\times10^{-13}$	0.4985	0.4988	0.5006	0.4943	0.4981	0.5039	0.5035	0.5014
$1.\times10^{-14}$	0.4984	0.5021	0.4998	0.4905	0.4949	0.4986	0.5033	0.4969
$1.\times10^{-15}$	0.5031	0.5017	0.5039	0.4966	0.5049	0.5064	0.5067	0.5068
$1.\times10^{-16}$	0.4991	0.5006	0.5064	0.4962	0.4963	0.5075	0.5061	0.5010
$1.\times10^{-17}$	**0.3307**	**0.3311**	**0.3417**	**0.3281**	**0.3353**	**0.3321**	**0.3350**	**0.3338**

NDF_2	an initial value scales down by a ratio of 10^{-1} in NDF_1								
	$1.\times10^{-9}$	$1.\times10^{-10}$	$1.\times10^{-11}$	$1.\times10^{-12}$	$1.\times10^{-13}$	$1.\times10^{-14}$	$1.\times10^{-15}$	$1.\times10^{-16}$	$1.\times10^{-17}$
$1.\times10^{-1}$	0.5015	0.5018	0.4975	0.5056	0.4977	0.5069	0.5057	0.5020	**0.3361**
$1.\times10^{-2}$	0.5018	0.4995	0.5009	0.5051	0.4947	0.5024	0.5007	0.4989	**0.3341**
$1.\times10^{-3}$	0.5054	0.4982	0.4973	0.5056	0.4945	0.5070	0.5081	0.4995	**0.3381**
$1.\times10^{-4}$	0.5023	0.5057	0.4997	0.5071	0.4971	0.5041	0.5090	0.5013	**0.3448**
$1.\times10^{-5}$	0.4969	0.4956	0.4933	0.5039	0.4912	0.4977	0.4974	0.4932	**0.3306**
$1.\times10^{-6}$	0.5123	0.5089	0.5013	0.5087	0.4995	0.5094	0.5093	0.5076	**0.3409**
$1.\times10^{-7}$	0.5043	0.5023	0.4987	0.5047	0.5004	0.5073	0.5050	0.5007	**0.3408**
$1.\times10^{-8}$	0.5030	0.4958	0.4949	0.5023	0.4952	0.5040	0.4998	0.4951	**0.3325**
$1.\times10^{-9}$	0.5057	0.5037	0.4969	0.5054	0.4967	0.5039	0.5025	0.4969	**0.3370**
$1.\times10^{-10}$	0.5060	0.5031	0.4985	0.5049	0.4931	0.5019	0.5069	0.4990	**0.3386**
$1.\times10^{-11}$	0.4977	0.4965	0.4941	0.4999	0.4933	0.4983	0.4984	0.4937	**0.3329**
$1.\times10^{-12}$	0.5043	0.5009	0.4954	0.4971	0.4999	0.5013	0.5020	0.5026	**0.3385**
$1.\times10^{-13}$	0.5037	0.4991	0.4980	0.4993	0.5005	0.5061	0.5030	0.4953	**0.3373**
$1.\times10^{-14}$	0.5033	0.4965	0.4905	0.4955	0.4956	0.4999	0.5019	0.4995	**0.3287**
$1.\times10^{-15}$	0.5077	0.5073	0.5021	0.5056	0.5057	0.5082	0.5065	0.5002	**0.3419**
$1.\times10^{-16}$	0.5088	0.5057	0.5021	0.5026	0.4990	0.5070	0.5083	0.5034	**0.3347**
$1.\times10^{-17}$	**0.3411**	**0.3327**	**0.3335**	**0.3363**	**0.3265**	**0.3353**	**0.3354**	**0.3289**	**0**

5. Conclusion

In this paper, a coupled NDF is used to construct an efficient chaotic stream cipher. The analysis and the simulation results prove that the proposed chaotic stream cipher satisfies the security requirements. The chaotic stream ciphers encrypt the palmprint templates to generate cancelable palmprint templates in parallel, which can quickly implement and increase the inter-class divergence of different subjects and maintain intra-class distance of the same subjects. Even in the stolen–token scenario, the result just reverts to the original performance without loss in performance, which still achieves high verification accuracy. The experimental results of verification on the Hong Kong Polyu Palmprint Database show that the proposed approach has a large template re-issuance ability and a better separation between the genuine and imposter populations with a very low EER.

References

[1] Xu S J, Wang J Z and Yang S X 2008 *Chin. Phys.* B **17** 4027

[2] Lian S G, Sun J S, Wang J W and Wang Z Q 2007 *Chaos, Solitons and Fractals* **34** 851

[3] Sheng L Y, Li G Q and Li Z W 2006 *Acta Phys. Sin.* **55** 5700 (in Chinese)

[4] Yang Q T and Gao T G 2008 *Chin. Phys.* B **17** 2388

[5] Zhang J S, Wang X M and Zhang W F 2007 *Phys. Lett.* A **362** 439

[6] Khan M K, Zhang J S and Tian L 2007 *Chaos, Solitons and Fractals* **32** 1749

[7] Xiang F and Qiu S S 2008 *Acta Phys. Sin.* **57** 6132 (in Chinese)

[8] Zhou Q, Hu Y and Liao X F 2008 *Acta Phys. Sin.* **57** 5413 (in Chinese)

[9] Li S J, Mou X and Cai Y 2001 in *Progress in Cryptology—INDOCRYPT* (Chennai, India: Springer-Verlag) 2247

[10] Wang X M and Zhang J S 2007 *Chin. Phys. Lett.* **24** 1166

[11] Kelber K 2000 *IEEE Trans. Circuits Syst.* I **47** 1413

[12] Prabhakar S, Pankanti S and Jain A K 2003 *IEEE Security Privacy Magazine* **1** 33

[13] Ratha N, Connell J and Bolle R 2001 *IBM Systems Journal* **40** 614

[14] Connie T, Teoh A B J, Goh M and Ngo D 2005 *Inf. Process. Lett.* **1** 1

[15] Teoh A B J, Goh M and Ngo D 2006 *IEEE Trans. PAMI* **12** 1892

[16] Kong A, Zhang D, Kamel M and You J 2006 *Pattern Recognition* **41** 13291

[17] Kong A and Zhang D 2004 *ICPR* **2** 520

[18] Kong A, Zhang D and Kamel M 2008 *Pattern Recognition* **41** 13291

[19] Bernstein G M and Lieberman M A 1990 *IEEE Trans. Circuits Syst.* **37** 1157

[20] *NIST Special Publication 800-22* 2001 http://csrc.nist.gov/rng/rng2.html

[21] Kong A, Zhang D and Kamel M 2009 *Pattern Recognition* **7** 1408

[22] Lee T S 1996 *IEEE Trans. on PAMI* **18** 959

[23] PolyU Palmprint database available: http://www4.comp.polyu.edu.hk/∼biometrics/

[24] Daugman J 2003 *Pattern Recognition* **36** 279