工程科学学报，第 37 卷，第 1 期：125－131，2015 年 1 月
Chinese Journal of Engineering，Vol. 37，No. 1：125－131，January 2015
DOI：10.13374/j.issn2095－9389.2015.01.019；http://journals.ustb.edu.cn

基于与 Tent Map 拓扑共轭系统的混沌流加密方案设计

田　清[1)]✉，徐正光[1)]，田　立[2)]

1）北京科技大学自动化学院，北京 100083　2）北京航空航天大学宇航学院，北京 100191
✉ 通信作者，E-mail：qingtiantq@hotmail.com

摘　要　利用与 Tent Map 拓扑共轭的两类混沌系统，以及产生独立均匀分布密钥流的方法，设计了一种通用的流加密方案．此方案类似数字信封，但传递过程中不传输具体加密使用的密钥流，只传输随机产生的 Tent Map 初值以及两个系统的参数值作为系统密钥，产生两列独立同分布的密钥流对原始图像进行两次密文反馈异或加密．该方案达到初始值掩盖的目的，增加了截获者破译的难度．图像加密的实验结果显示该方案安全且有效．

关键词　图像通信；密码术；混沌系统；图像处理；拓扑
分类号　TP391

Chaotic stream encryption scheme based on topological conjugate chaotic systems of Tent map

TIAN Qing[1)]✉，*XU Zheng-guang*[1)]，*TIAN Li*[2)]

1）School of Automation，University of Science and Technology Beijing，Beijing 100083，China
2）School of Astronautics，Beihang University，Beijing 100191，China
✉ Corresponding author，E-mail：qingtiantq@hotmail.com

ABSTRACT　A general chaotic stream encryption scheme is proposed by using two chaotic systems which topologically conjugate with Tent map and a method to generate independent and identically distributed chaotic streams. The stream encryption scheme is similar to the digital envelop，but the difference is that we only transport the initial values of Tent map and the parameters of the two chaotic systems as the initial key. According to the conjugate relation，the initial values of the chaotic systems are obtained to achieve the purpose of masking these initial values. We calculate two independent and identically distributed chaotic key streams based on the two chaotic systems to encrypt the plaintext through twice feedback XOR. An application result of image cryptograph illustrates that the stream encryption scheme is effective and secure.

KEY WORDS　image communications；cryptography；chaotic systems；image processing；topology

流密码也称为序列密码，其基本思想是将待加密的明文分成连续的字符或比特，然后用相应的密钥流对之进行加密，密钥流由种子密钥通过密钥流生成器产生，具有实现简单、便于硬件实施、加解密处理速度快、没有或只有有限的错误传播等特点[1－3]．流密码的核心技术是伪随机发生器，当流密钥序列是具有均匀分布的离散无记忆随机序列时，在理论上是不可破译的，其常用的方法有线性反馈移位寄存器法（LFSR）、非线性反馈移位寄存器法（NLFSR）、有限自动机法、线性同余法等．如今，流密码技术已经广泛的应用于移动通信、数字多媒体等，常用的流密码算法有 RC4 算法、SEAL 算法、A5 和 Rambutan 算法[3－5]．

混沌系统具有初始条件敏感、无周期、伪随机等基本特性，并且与密码学之间有着紧密的联系，吸引越来

收稿日期：2013－11－27
基金项目：国家自然科学基金资助项目（60573058）

越多的学者进行混沌密码学的研究[6-7]. 混沌流密码的研究主要是基于混沌系统伪随机序列发生器(PRNG)相关算法的研究，大部分采用特定的混沌系统，如一维混沌系统 Logistic 映射和 Tent 映射、二维混沌系统 Henon 映射和标准映射、三维混沌系统 Lorenz 映射等生成的伪随机序列采用二进制化、放大函数、区间划分等方法来抽取特定比特流作为密钥流来掩盖明文，也有结合其他方法如鼠标移动等方法，产生伪随机序列. 图像由于自身数据量大、像素相关性强等特点，需要高效实时加密的需求，使得传统密码(如 DES 和 AES)在图像加密上不是一个最佳选择. 混沌流密码具有速度快等优点，很适合应用在图像上. 目前的混沌图像加密方法有图像位置置乱、图像像素值扩散以及位置置乱与像素扩散相结合的方法[8-9]. 在图像位置置乱中，很多使用二维混沌映射如 Anold[10] 映射、标准映射[11]、Baker 映射[12]以及其他映射等方法置乱图像的位置[13-24]，本质上还是对图像的像素进行了重排.

文献[1-2]提出了独立同分布混沌密钥流的产生方法. 本文基于此方法，提出了一种加密方案，在加密过程中，只对混沌图像的像素值进行扩散. 此方案类似数字信封，但不传输具体加密使用的密钥流，只传输随机产生的 Tent Map 初值，两个系统参数以及密文，通信双方根据初值，系统参数产生密钥流进行加解密，增加了截获者破译的难度. 将该方法应用在图像上，实验结果表明，本文提出的加密协议安全有效，并能够提高图像加密的速率.

1　独立均匀分布密钥流快速算法设计

1.1　理论内容

引理 1[2]　对于 Tent Map，

$$x_{k+1}=g(x)=\begin{cases}2x_k, & 0\leqslant x_k\leqslant 1/2;\\ 2-2x_k, & 1/2\leqslant x_k\leqslant 1.\end{cases} \tag{1}$$

当 $ma=-2$ 时，

$$y_{k+1}=f(y_k)=my_k^2+a, y_k\in[-|a|,|a|] \tag{2}$$

与 $g(x)$ 关于

$$y_k=h(x_k)=-a\cos\pi x_k \tag{3}$$

共轭，且通过下面的采样规则可以产生独立同分布的混沌密钥流.

(1) 如果 $a>0$，将 $[-a,a]$ 划分成 $N=2^n$ 子区间 $\tau_i,\tau_i=[t_i,t_{i+1})$，其中 $t_i=h\left(\frac{i}{N}\right), i=0,1,\cdots,N-1$，$t_N=h\left(\frac{N}{N}\right)=a.$

(2) 如果 $a<0$，将 $[a,-a]$ 划分成 $N=2^n$ 子区间 $\tau_i,\tau_i=[t_i,t_{i+1})$，其中 $t_i=h\left(\frac{N-i}{N}\right), i=0,1,\cdots,N-1,t_N=h\left(\frac{N-N}{N}\right)=-a.$

(3) 定义混沌密钥流 $\{s_i\}_0^\infty$ 如下：

如果 $y_k\in\tau_i$，那么 $s_k=i$，并设定采样步长为 n，即 $y_{k+1}=f^n(y_k)$.

引理 2[1]　对于 Tent 映射(1)当 $ma=-4$ 时，

$$f(x_k)=mx_k^2+4x_k, x_k\in[\min\{0,a\},\max\{0,a\}] \tag{4}$$

与 $g(x)$ 关于

$$h(x_k)=a\sin^2\frac{\pi x_k}{2}, a\neq 0 \tag{5}$$

共轭，且对于映射 $f(x_k)=mx_k^2+4x_k$，选择采样间隔 n 通过下面的方法可以产生独立同分布的混沌密钥流 $\{s_i\}_0^\infty$.

如果 $a>0$，将混沌区间 $[0,a]$ 划分成 $N=2^n$ 子区间 $\tau_i,\tau_i=[t_i,t_{i+1})$，$t_i=h\left(\frac{i}{N}\right), i=0,1,\cdots,N-1$；

如果 $a<0$，将混沌区间 $[a,0]$ 划分成 $N=2^n$ 子区间 $\tau_i,\tau_i=[t_i,t_{i+1})$，$t_i=h\left(\frac{N-i}{N}\right), i=0,1,\cdots,N-1.$

定义混沌密钥流 $\{s_i\}_0^\infty$ 如下：

如果 $x_k\in\tau_i$，那么 $s_k=i$，并设定采样步长为 n，即 $x_{k+1}=f^n(x_k)$.

1.2　快速算法设计

一个可用的加密系统需要具有快速的加密速度. 文献[25]给出了引理 2 快速产生独立同分布密钥流的方法. 同样对于引理 1，从式(3)可以看出，区间的划分是不等分的，判断 y_{kn} 所处区间较为复杂，作变换 $y_k=h(\theta)=-a\cos\pi\theta$，在 $-a\leqslant\theta\leqslant a$ 时，式(3)的逆变换为

$$\theta=\frac{1}{\pi}\arccos\left(-\frac{y_k}{a}\right)=\frac{1}{\pi}\left[\pi-\arccos\left(\frac{y_k}{a}\right)\right]. \tag{6}$$

通过式(6)的变换，使得混沌吸引子上的非均匀划分 $\{\tau_i\}_{i=0}^{N-1}(N=2^n)$ 与 θ 的变化区域 $[-a,a]$ 上的均匀划分 $\{\tau_i'\}_{i=0}^{N-1}$ 一一对应，$\tau_i'=[t_i',t_{i+1}')$，$i=0,1,\cdots,N-2,\tau_{N-1}=[t_{N-1}',t_N']$，其中

$$t_i'=\frac{i}{N}, i=0,1,\cdots,N-1. \tag{7}$$

显然，通过判断 y_{kn} 对应的 θ_k 所处的划分子区间容易得出 y_{kn} 所处的划分子区间. 图 1 为快速算法框图(针对图像序列长度为 $W\times H$，采样间隔为 n)，具体算法如下：

(1) 令 $k=0$，对式(4)进行迭代，每间隔 n 取值一次.

(2) 把采样的值 y_k 代入式(6)计算出对应的 θ 值.

(3) 按照 $s_k = \lfloor \theta \times N \rfloor + 1$ 计算出对应的 s_k.

(4) 判断 $k < W \times H$,是,则回到 2; 否则结束.

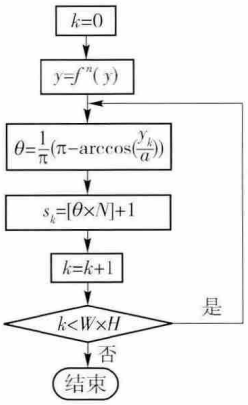

图 1　引理 1 密钥流快速算法

Fig. 1　Key stream fast algorithm of Lemma 1

2　加密方案设计

根据数字信封设计原理,设计了一个加密方案,目的在于 Alice 和 Bob 共享与帐篷映射共轭的两个混沌共轭系统式(2)和式(4);不同于数字信封,双方不传输密钥流,只传递随机产生的 Tent Map 初值为 m_1、m_2、n 和 T. 假设 Alice 和 Bob 约定共享系统(2)和系统(4),并共享对称加密算法 $C_s/M = T_s(M/C_s, K)$,以及非对称算法 $C_a = T_{as}(M, K^P_{pub})$ 和 $M = T_{as}(C_a, K^P_{pri})$ 其中 M 为明文,K 为对称密钥,K^P_{pub} 为实体 P 的公钥,K^P_{pri} 为实体 P 的私钥. 对称加密算法采用反馈方式,设明文图形长 W、宽 H 的图像 M,$M(i)$,$i = 1,2,3,\cdots,W \times H$ 分别表示图像的像素值,首先用 K_1 对像素值进行反馈异或得到中间加密图像 E,过程如下:

$$\begin{cases} E(1) = M(1) \oplus K_1(1) \oplus M(W \times H), & i = 1; \\ E(i) = M(i) \oplus K_1(i) \oplus E(i), & i \neq 1. \end{cases} \tag{8}$$

再用 K_2 对 E 像素值进行反馈异或得到密文图像 C_D,过程如下:

$$\begin{cases} C_D(1) = E(1) \oplus K_2(1) \oplus E(W \times H), & i = 1; \\ C_D(i) = E(i) \oplus K_2(i) \oplus C_D(i-1), & i \neq 1. \end{cases} \tag{9}$$

解密时,首先得到中间加密图像 E,再利用密钥流 K_1,异或得到明文图像,过程如下:

$$\begin{cases} E(1) \oplus E(W \times H) = C_D(1) \oplus K_2(1), & i = 1; \\ E(i) = C_D(i) \oplus K_2(i) \oplus C_D(i-1), & i \neq 1. \end{cases} \tag{10}$$

$$\begin{cases} M(1) \oplus M(W \times H) = E(1) \oplus K_1(1), & i = 1; \\ M(i) = E(i) \oplus K_1(i) \oplus E(i-1), & i \neq 1. \end{cases} \tag{11}$$

加解密方案的设计如图 2 所示.

具体的通信方案如图 3 所示,通信过程具体步骤描述如下:

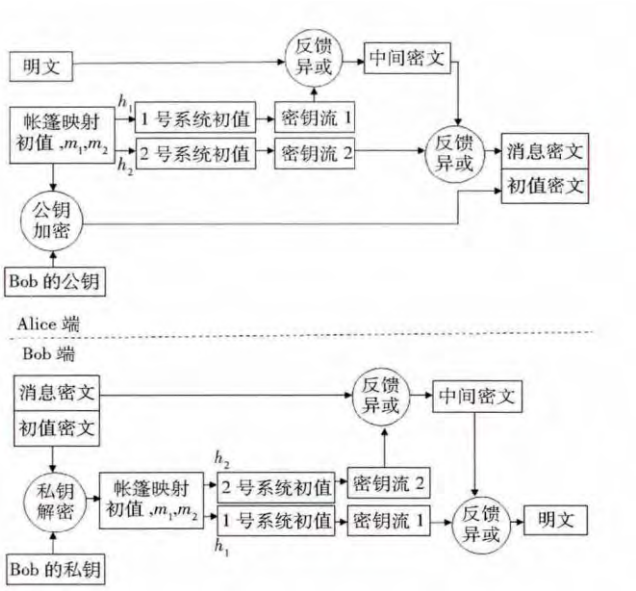

图 2　加密方案

Fig. 2　Encryption scheme

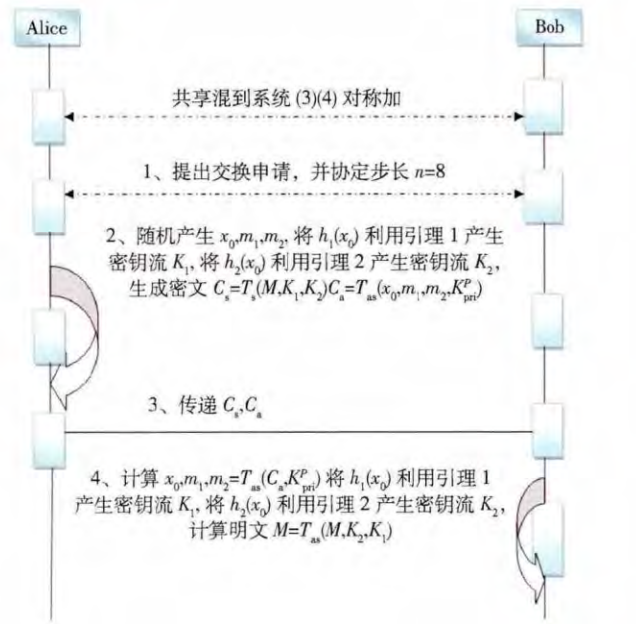

图 3　Alice 与 Bob 通信方案

Fig. 3　Alice and Bob communication scheme

(1) Alice 与 Bob 共享引理 1 和引理 2;

(2) Alice 与 Bob 提出交换申请,约定对图像加密取采样步长 $n = 8$;

(3) Alice 选择帐篷映射的初始值 x_0、m_1、m_2 和 T 用 Bob 的公钥进行加密生成初值密文,并根据引理 1 和引理 2 产生密钥流 1 和密钥流 2,使用对称算法加密进行图像加密生成消息密文,Alice 把初值密文及消息密文传递给 Bob;

(4) Bob 用自己的私钥解开初值密文 x_0、m_1 和 m_2,同样根据引理 1 和引理 2 计算出密钥流 1,密钥流 2.

Bob 用对称解密算法进行消息密文解密，得到明文图像.

3　应用实例及加密效果分析

3.1　应用实例

对于引理 1 和引理 2，Alice 与 Bob 共享如下系统，当取 $m_1 = -3, a_1 = 2/3, m_2 = 1/2, a_2 = -8$ 时，得到:

$$f(x) = -3x^2 + 2/3, x \in [-2/3, 2/3], \quad (12)$$

$$h(x) = -2/3\cos \pi x, x \in [0, 1], \quad (13)$$

$$f(z_k) = -2z_k^2 + 2z_k, z_k \in [-2, 2], \quad (14)$$

$$h(z) = -2\sin \frac{\pi z_k}{2}, z \in [0, 1]. \quad (15)$$

Alice 使用 $n = 8, T = 100, x_0 = 0.00111111111111$，根据引理 1 和引理 2 产生密钥流 1 和密钥流 2，进行明文图像加密，选用公钥算法 RSA，$m_1 = -3, m_2 = 1/2, x_0 = 0.00111111111111$ 用公钥进行加密后传送给 Bob.

在对图像进行对称加密过程中，使用两轮密文反馈异或方式，第一次用密钥流 1 与明文图像 P 像素进行异或取模后得到密文图像 E，得到的密文图像再用密钥流 2 进行异或取模得到最终的密文图像 C_D.

3.2　实验结果分析

3.2.1　密钥空间分析

一个安全的密码系统需要有较大的密钥空间，上述加密方案中，选择 m_1、m_2 和 x_0 为双精度，混沌前 T 次迭代结果进行截断，如果选择 T 的范围为 (0 ~ 5000)，那么密钥空间可以估算为 $10^{15} \times 10^{15} \times 10^{15} \times 5000 \approx 0.5 \times 10^{49}$，由此可见密钥空间足以抵抗对密钥的穷举攻击. 低维系统具有计算速度快的优势，加上本文采用独立均匀分布密钥流产生的快速算法，在加密过程中只进行两轮反馈异或加密，没有多伦迭代，相比于其他的一位混沌系统的加密方法，本文提出的方法具有密钥空间大、计算时间短的特点.

3.2.2　密钥敏感性分析

图 4(a) ~ (c) 分别为原始图像、加密后的图像以及用正确密钥解密后的图像. 为了测试方案的密钥敏感性，我们将其中一个密钥的数值进行微小的改变，其他密钥不变，实验结果如图 4(d) ~ (f) 所示，分别表示 $m_1 = -3.0000000001, x_0 = 0.00111111111110, T = 99$ 时，从解密图像中可以看出，当密钥有一点微小的改动后，解密出的图像与原始明文图像完全不同. 实验结果表明该加密算法能够抵抗各种基于敏感性的攻击.

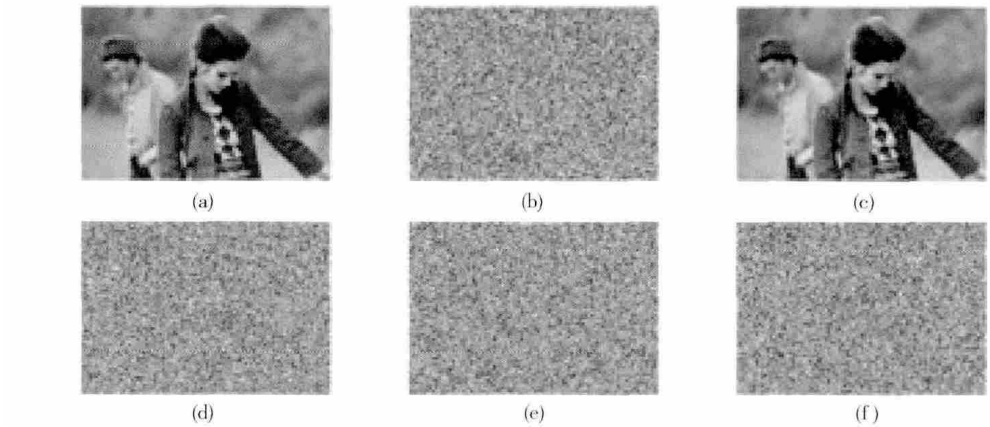

图 4　加解密结果. (a) 原始图像; (b) 加密后图像; (c) 解密后图像; (d) 改变 m_1 解密图像; (e) 改变 x_0 解密图像; (f) 改变 T 解密图像

Fig. 4　Encryption and decryption results: (a) plain-image; (b) cipher-image; (c) correctly decrypted image; (d) decrypted image with m_1 change in the key; (e) decrypted image with x_0 change in the key; (f) decrypted image with T change in the key

3.2.3　差分攻击

差分攻击基本思想是通过分析特定明文差分对相应密文差分影响来获得尽可能大的密钥. 如果对明文图像的微小改变会导致密文图像较大变化，则差分攻击为无效. 通常用 NPCR 和 UACI 来描述一个像素的改变对密文的影响.

对一副大小为 $N \times N$ 的图像，$c(i,j)$ 和 $c'(i,j)$ 分别为改变明文图像 $p(i,j)$ 的一个像素值而得到的两个加密图像，用 γ_{NPCR} 度量两个图像间像素的变化率，定义为

$$\gamma_{NPCR} = \frac{\sum_i \sum_j Q(i,j)}{N \times N} \times 100\%,$$

其中

$$Q(i,j) = \begin{cases} 1 & c(i,j) \neq c'(i,j), \\ 0 & c(i,j) = c'(i,j). \end{cases}$$

用 γ_{UACI} 来度量像素的平均改变强度，定义如下:

$$\gamma_{UACI} = \frac{1}{N \times N}\left[\sum_i \sum_j \frac{|c(i,j) - c'(i,j)|}{255}\right] \times 100\%.$$

对于两个完全随机的图像，NPCR 和 UACI 的理论值分别为 99.60937% 和 33.46354%.

本文中 $\gamma_{NPCR} = 99.5850\%$，$\gamma_{UACI} = 33.2177\%$，非常接近其理论值，说明加密方案对明文图像的微小改变非常敏感，因此本加密方案具有良好的抵抗差分攻击

的能力.

3.2.4　统计特性分析

相邻像素的相关性: 图像相邻像素的相关性很大，密文图像要尽可能地破坏明文图像的这种相关性来抵抗统计分析. 若 A 表示两个相邻像素的灰度值，则 $M \times N$ 图像的相关性 r 计算如下:

$$\mathrm{cov}_{\mathrm{Hori}}(A) = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N-1}(A(i,j) - E(A))(A(i,j+1) - E(A)),$$

$$\mathrm{cov}_{\mathrm{Ver}}(A) = \frac{1}{M\times N}\sum_{j=1}^{N}\sum_{i=1}^{M-1}(A(i,j) - E(A))(A(i+1,j) - E(A)),$$

$$\mathrm{cov}_{\mathrm{Diag}}(A) = \frac{1}{M\times N}\sum_{i=1}^{M-1}\sum_{j=1}^{N-1}(A(i,j) - E(A))(A(i+1,j+1) - E(A)).$$

$$r_{\mathrm{Hori}}(A) = \frac{\mathrm{cov}_{\mathrm{Hori}}(A)}{D(A)}, r_{\mathrm{Veri}}(A) = \frac{\mathrm{cov}_{\mathrm{Veri}}(A)}{D(A)},$$

$$r_{\mathrm{Veri}}(A) = \frac{\mathrm{cov}_{\mathrm{Diag}}(A)}{D(A)}.$$

这里

$$E(A) = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}A(i,j),$$

$$D(A) = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(A(i,j) - E(A))^2.$$

图 5(a) ~(c) 分别描述了明文图像水平、垂直及对角线方向相邻像素的相关性; 图 5(d) ~(f) 分别描述了密文图像水平、垂直及对角线方向相邻像素的相关性. 由图 3 可以看出明文图像相邻像素之间相关性高，加密后的图像相邻像素相关性分布均匀. 表 1 分别计算了明文图像和密文图像相关系数的计算结果. 由结果可知: 原始明文图像的相邻像素是高度相关的，相关系数接近于 1; 而加密图像的相邻像素相关系数接近于 0，相邻像素已基本不相关，像素分布比较均匀，有效隐藏了图像的统计特性.

表 1　明文和密文相邻像素的相关系数

Table 1　Correlation coefficient of plaintext and ciphertext adjacent pixels

方向	明文图像图 3(a)	密文图像图 3(b)
水平方向	0.9701	0.0022
垂直方向	0.9763	0.0028
对角线方向	0.9580	0.0047

图 6(c) 和(d) 分别为明文图像及加密图像的统计直方图. 由图可见，加密图像的直方图分布均匀，掩盖了原始图像的分布规律，能够抵抗攻击者的已知明文或选择明文攻击.

3.2.5　计算时间比较

在加密速度方面，分别对同样大小的图像使用本方案的一般方法(8.11 s) 及快速算法(4.03 s) 所需时间进行了比较. 实验基于 Win XP 操作系统，1 GB 内存，Matlab2007，对 1024 × 651 像素图像上加密.

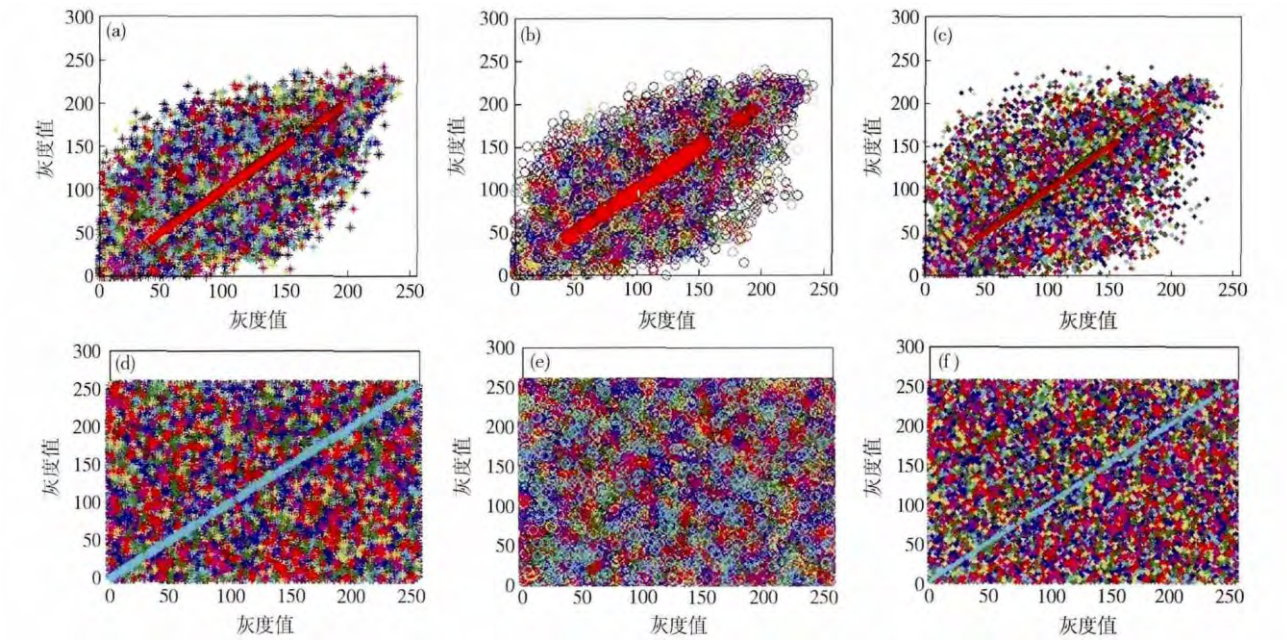

图 5　图像相邻像素相关性. (a) 原始图像水平方向相邻像素相关性; (b) 原始图像垂直方向相邻像素相关性; (c) 原始图像对角线相邻像素相关性; (d) 加密图像水平方向相邻像素相关性; (e) 加密图像垂直方向相邻像素相关性; (f) 加密图像对角线方向相邻像素相关性

Fig. 5　Image correlation of adjacent pixels: (a) correlation plot of two adjacent plain-image pixels in the horizontal; (b) correlation plot of two adjacent plain-image pixels in the vertical; (c) correlation plot of two adjacent plain-image pixels in the diagonal directions; (d) correlation plot of two adjacent pixels in the cipher-image in the horizontal; (e) correlation plot of two adjacent pixels in the cipher-image in the vertical; (f) correlation plot of two adjacent pixels in the cipher-image in the diagonal directions

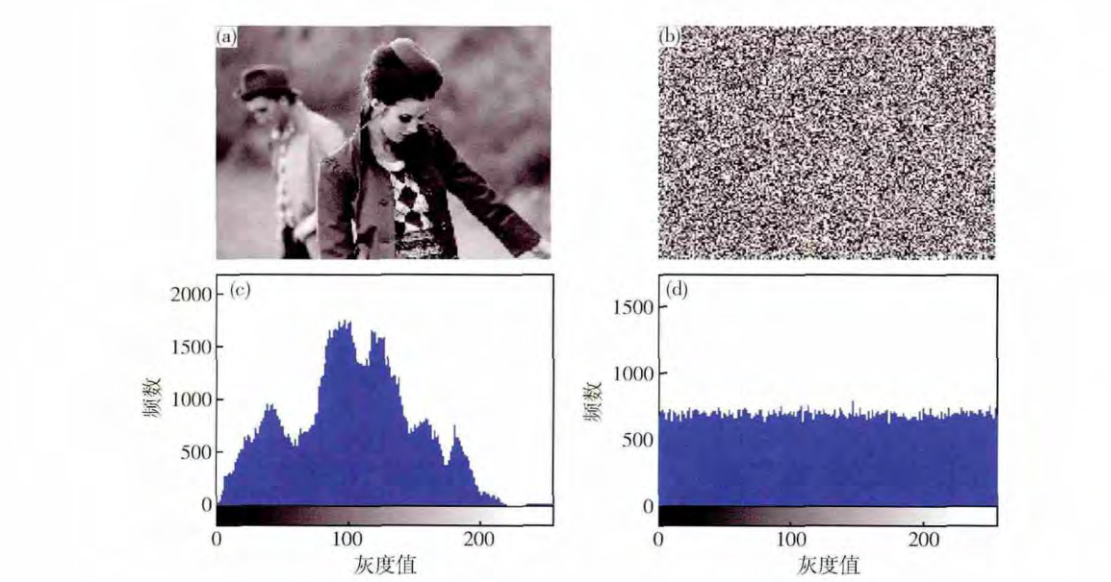

图 6　直方图分析结果. (a) 原始图像; (b) 加密图像; (c) 原始图像直方图; (d) 加密图像直方图

Fig. 6　Histogram analysis results: (a) plain image; (b) cipher-image; (c) histogram of the plain-image; (d) histogram of the cipher-image

4　结论

本文提出了基于独立同分布密钥流的混沌流加密方案. 该算法具有的优点是: (1) 构造的新系统为低维的混沌系统，具有低纬混沌系统运算速度快的优点; (2) 使用独立同分布的密钥流，密钥流具有很好的随机性，不需要多轮迭代即可获得很好的加密效果; (3) 混沌系统每次随机产生的密钥不同，具有一次一密的特性; (4) 密文具有在整个取值空间均匀分布的特性，相邻像素具有近似于零的相关性; (5) 使用密钥流产生的快速算法的时间开销小; (6) 使用公钥算法仅加密密钥，具有安全性高的特点.

实验结果验证了此加密方案的安全性，满足密码学对安全性和效率问题的要求，加密方案具有很高的安全性和实际可用性.

参　考　文　献

[1] Xü Z G, Tian Q, Tian L. Theorem to generate independently and uniformly distributed chaotic key stream via topologically conjugated maps of Tent map. *Math Probl Eng*, 2012, 2012: 619257

[2] Xü Z G, Tian Q, Tian L. A new theorem to generate independently and uniformly distributed chaotic key stream via topologically conjugated maps of Tent map. *Acta Phys Sin*, 2013, 62(12): 120501
(徐正光，田清，田立. 一类可以产生独立同分布密钥流的混沌系统. 物理学报，2013，62(12): 120501)

[3] Li P, Li Z, Halang W A, Chen G. A stream cipher based on a spatiotemporal chaotic system. *Chaos Solitons Fractals*, 2007, 32(5), 1867

[4] Chen T M, Jiang R R. New hybrid stream cipher based on chaos and neural networks. *Acta Phys Sin*, 2013, 62(4): 040301
(陈铁明，蒋融融. 混沌映射和神经网络互扰的新型复合流密码. 物理学报，2013，62(4): 40301)

[5] Xiang F, Qiu S S. Stream cipher design based on inter-perturbations of chaotic systems. *Acta Phys Sin*, 2008, 57(10): 6132
(向菲，丘水生. 基于混沌系统互扰的流密码设计. 物理学报. 2008，57(10): 6132)

[6] Riad D, Alaa E, Elminir H K, et al. Security evaluation and encryption efficiency analysis of RC4 stream cipher for converged network applications. *J Electr Eng*, 2013, 64(3): 196

[7] Zheng F, Tian X J, Fan W H, et al. Image encryption based on Henon map. *J Beijing Univ Posts Telecommun*, 2008, 31(1): 66
(郑凡，田小建，范文华，等. 基于 Henon 映射的数字图像加密. 北京邮电大学学报，2008，31(1): 66)

[8] Pareek N K, Patidar V, Sud K K. Diffusion-substitution based gray image encryption scheme. *Digital Signal Process*, 2013, 23(3): 894

[9] Huang X. Image encryption algorithm using chaotic Chebyshev generator. *Nonlinear Dyn*, 2012, 67(4): 2411

[10] Ye G, Wong K W. An efficient chaotic image encryption algorithm based on a generalized Arnold map. *Nonlinear Dyn*, 2012, 69(4): 2079

[11] Li C Q, Li S J, Lu G D. Breaking a modified substitution-diffusion image cipher based on chaotic standard and logistic maps. *Commun Nonlinear Sci Numer Simul*, 2011, 16(2): 837

[12] Elshamy A M, Rashed A N Z, Mohamed A E N A, et al. Optical image encryption based on chaotic baker map and double random phase encoding. *J Lightwave Technol*, 2013, 31(15): 2533

[13] Fu C, Chen J, Zou H, et al. A chaos-based digital image encryption scheme with an improved diffusion strategy. *Opt Express*, 2012, 20(3): 2363

[14] Zang H Y, Min L Q, Wu C X, et al. An image encryption scheme based on generalized synchronization theorem for discrete chaos system. *J Univ Sci Technol Beijing*, 2007, 29(1): 96
(臧鸿雁，闵乐泉，吴春雪，等. 基于离散混沌系统广义同步定理的数字图像加密方案. 北京科技大学学报，2007，29

(1): 96)

[15] Xü G, Zhang Y D, Zhang X X, et al. Digital image encryption algorithm based on an alternating iterative chaotic system. *J Univ Sci Technol Beijing*, 2012, 34(4): 464
(徐刚, 张亚东, 张新祥, 等. 基于交替迭代混沌系统的图像加密算法. 北京科技大学学报, 2012, 34(4): 464)

[16] Wen C C, Wang Q, Liu X H, et al. An encryption algorithm for image based on affine and composed chaos. *J Comput Res Dev*, 2013, 50(2): 319
(文昌辞,王沁,刘向宏, 等. 基于仿射和复合混沌的图像加密新算法. 计算机研究与发展, 2013, 50(2): 319)

[17] Chen Y F, Li Y F. Image encryption algorithm based on reciprocally-disordered diploid chaotic sequences alternated in subsection. *J South China Univ Technol Nat Sci*, 2010, 38(5): 27
(陈艳峰, 李义方. 交替分段相互置乱的双混沌序列图像加密算法. 华南理工大学学报: 自然科学版, 2010, 38(5): 27)

[18] Wang J, Jiang G P. Cryptanalysis of a hyper-chaotic image encryption algorithm and its improved version. *Acta Phys Sin*, 2011, 60(6): 060503
(王静, 蒋国平. 一种超混沌图像加密算法的安全性分析及其改进. 物理学报, 2011, 60(6): 060503)

[19] Mohammad Seyedzadeh S, Mirzakuchaki S. A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. *Signal Process*, 2012, 92(5): 1202

[20] Kanso A, Ghebleh M. A novel image encryption algorithm based on a 3D chaotic map. *Commun Nonlinear Sci Numer Simul*, 2012, 17(7): 2943

[21] Zhu C X. A novel image encryption scheme based on improved hyperchaotic sequences. *Opt Commun*, 2012, 285(1): 29

[22] Wang X Y, Teng L. An image blocks encryption algorithm based on spatiotemporal chaos. *Nonlinear Dyn*, 2012, 67(1): 365

[23] Patidar V, Pareek N K, Sud K K. A new substitution-diffusion based image cipher using chaotic standard and logistic maps. *Commun Nonlinear Sci Numer Simul*, 2009, 14(7): 3056

[24] Xü Z G, Tian Q, Tian L. An image encryption method based on independently and uniformly distributed chaotic key stream. *J Inf Comput Sci*, 2013, 10(18): 5971

[25] Hu H P, Liu S H, Wang Z X, et al. A method for generating chaotic key stream. *Chin J Comput*, 2004, 27(3): 408
(胡汉平, 刘双红, 王祖喜, 等. 一种混沌密钥流产生方法. 计算机学报, 2004, 27(3): 408)