基于物理随机位生成器与混沌像素交叉互换的图像加密算法

郭静博
（平顶山教育学院 计算机系，平顶山 467000）

摘要：目的 为了解决当前混沌图像加密技术忽略了随机序列产生的时间延迟现象，且难以克服其自身迭代的周期性，使其序列的自相关性不理想，导致密文安全性不佳等问题。**方法** 引入级联耦合混沌半导体环形激光器，设计基于物理随机位生成器与混沌像素交叉互换的图像加密算法。首先引入 SHA-256 散列函数，利用明文像素值，生成一个 256 位的密钥，并将其分割为一系列的 8 位子密钥；利用这些子密钥来计算 Logistic-Sine 复合映射的初始条件，以输出一组随机序列；根据混沌序列，定义像素交叉互换机制，对输入明文进行预处理，消除相邻像素之间的相关性；基于级联耦合混沌半导体环形激光器，充分利用其自身的时间延迟与交叉反馈的特性，设计物理随机位生成器，以同步输出考虑时间延迟的控制矩阵与随机位流；将 Logistic-Sine 复合映射输出的混沌序列转换为一个过渡矩阵，联合控制矩阵，定义像素混淆机制，彻底改变明文的像素位置；最后，利用随机位流，设计像素联系扩散函数，改变图像的像素值。**结果** 实验结果显示，与当前混沌加密技术相比，所提算法具有更高的安全性与鲁棒性，能够有效抗击明文攻击，相应的密文熵值约为 7.9958，且 NPCR（Number of Pixel Change Rate）、UACI（Unified Average Changing Intensity）分别为 99.50%、33.46%。**结论** 所提加密算法具有较高的安全性和抗攻击能力，能够安全保护图像在网络中传输，在信息防伪等领域具有较好的应用价值。

关键词：图像加密；物理随机位生成器；像素交叉互换；半导体环形激光器；控制矩阵；随机位流；像素混淆机制
中图分类号：TP391 **文献标识码：**A **文章编号：**1001-3563(2018)13-0222-11
DOI：10.19554/j.cnki.1001-3563.2018.13.036

Image Encryption Algorithm Based on Physical Random Bit Generator and Chaotic Pixel Cross Interchange

GUO Jing-bo
(Department of Computer, Pingdingshan Institute of Education, Pingdingshan 467000, China)

ABSTRACT: The work aims to solve the defects as unsatisfactory sequence autocorrelation that causes low cipher security induced by neglecting time delay generated by the random sequences in current chaotic image encryption technology and difficulty in overcoming the periodicity of its own iteration. The cascade-coupled chaotic semiconductor ring laser was introduced to design an image encryption algorithm based on physical random bit generator and chaotic pixel cross interchange. Firstly, the SHA-256 hash function was introduced and a 256-bit key was generated with the value of the plaintext pixels, and then the 256-bit key was divided into a series of 8-bit sub-keys. A group of chaotic sequences were outputted by calculating the initial conditions of Logistic-Sine composite map with these sub-keys. Then, the pixel cross interchange mechanism was defined according to the chaotic sequence and the input plaintext was preprocessed to eliminate the correlation between adjacent pixels. The physical random bit generator was designed based on the cascade-coupled chaotic semiconductor ring laser which made full use of its own time delay and cross feedback to synchronously output the control matrix and stochastic bit stream that considered the time delay. The pixel confusion mechanism

收稿日期：2018-01-14
基金项目：河南省科技计划重点项目(172400410498)；河南省科技厅计划(152400410323)
作者简介：郭静博(1982—)，女，硕士，平顶山教育学院讲师，主要研究方向为图像处理、信息安全。

was defined by transforming the chaotic sequence outputted by the Logistic-Sine composite map into a transition matrix and jointing the control matrix to completely change the location of plaintext pixels. Finally, the pixel diffusion function was designed with random bit stream to change the pixel value of the image. The experimental results showed that the proposed algorithm had higher security and robustness which could effectively resist against the plaintext attack compared with the current chaotic encryption technology, and its corresponding cipher entropy was about 7.9958, and the values of NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) were 99.50% and 33.46%, respectively. With higher security and anti-attack capability, the proposed encryption algorithm can protect the safe transmission of images in the network and it has better application value in the field of information security and anti-counterfeiting.

KEY WORDS: image encryption; physical random bit generator; pixel cross interchange; semiconductor ring laser; control matrix; random bit stream; pixel confusion mechanism

图像因其含有丰富的视觉表达信息，成为多媒体技术常用的介质，通常需要利用因特网进行传输，在此期间，易遭受各种非法攻击，使得图像信息被肆意窃取与篡改，给用户信息安全带来较大的隐患[1—2]。由此，如何保护图像信息在因特网中安全传输，防止其被攻击而导致外泄，已成为当今世界各国的研究热点[3]。

图像加密作为当前解决图像安全传输的重要技术，得到了各国学者的研究。近年来，随着混沌系统理论的日益完善，为图像加密提供了一种新的、有效的保护手段，当前混沌加密技术已成为一种较为主流的加密方案[4]。如 Ye 等人[5]提出了基于缠绕 Logistic 映射的图像加密方案，实验结果表明，此加密技术具有较高的加密速度和抗明文攻击能力。虽然缠绕 Logistic 映射在传统 Logistic 映射的基础上进行了改进，增大了其混沌窗口，但是其仍然属于低维混沌映射(≤3)，使其安全性不理想。王宏达[6]设计了一种基于混沌系统的新型图像加密算法，实验结果验证了其算法的合理性与有效性，由于此技术采用了四维 Chen 系统，复杂度较高，使得算法的加密效率较低。Xu 等人[7]提出了基于分块置乱与动态引擎扩散的图像加密方法，通过将输入明文分割为 2 个子块，利用混沌映射来构建 x 坐标、y 坐标与交换控制表，以置乱图像，并利用动态引擎扩散技术改变置乱密文的像素值，以获取密文。此加密技术忽略了混沌序列产生过程中的时间延迟现象，导致输出的随机序列自相关性较高，因此其密文安全性有待进一步提高。

已有研究表明[8—9]，若考虑混沌序列生成过程中的时间延迟现象，可使其自相关性达到较为理想的状态，具有更高的伪随机性，可提高密文安全性。对此，文中基于文献[9]的思想，并兼顾算法的加密效率与安全性，设计基于同步物理随机位生成器与混沌像素交叉互换的图像加密算法。利用明文像素值来计算复合混沌映射的初值，通过对其迭代，可获取随机序列，利用其来预处理明文；利用级联耦合混沌半导体环形激光器来同步生成控制矩阵与随机位流，将二者分别用于图像的置乱与扩散。并对所提算法的安全性进行验证。

1　级联耦合混沌半导体环形激光器

级联耦合混沌半导体环形激光器(CCSRL, cascade-coupled semiconductor ring lasers)的结构见图 1，它具有丰富的动态特征，所产生的混沌信号随机性更高，非常适合信号加密[10]，由一个主半导体环形激光器(M-SRL1)和一个独立的半导体环形激光器(S-SRL2 或者 S-SRL3)构成[11]。通常含有顺时针(CW, clockwise)和逆时针(CCW, conter-clockwise)模式。

对于一个单纵单横模式的半导体激光器 SRL，其速率方程可根据经过物质极化动力学的绝热消去处理后的 Maxwell Bloch 方程来推导[11]。在此，对于并行注入与交叉反馈的半导体激光器 SRL 而言，文中考虑采用双模速率方程[11]：

$$\frac{\mathrm{d}E_{1\mathrm{CW}}}{\mathrm{d}t}=k\left(1+i\alpha_1\right)\left(G_{1\mathrm{CW}}N_1-1\right)E_{1\mathrm{CW}}-\left(k_\mathrm{d}+ik_\mathrm{c}\right)E_{1\mathrm{CCW}}+kf_{1\mathrm{CCW}}E_{1\mathrm{CCW}}\left(t-\tau_{1\mathrm{CCW}}\right)\mathrm{e}^{-\mathrm{i}\left(\omega_1\tau_{1\mathrm{CCW}}\right)} \tag{1}$$

$$\frac{\mathrm{d}E_{1\mathrm{CCW}}}{\mathrm{d}t}=k\left(1+i\alpha_1\right)\left(G_{1\mathrm{CCW}}N_1-1\right)E_{1\mathrm{CCW}}-\left(k_\mathrm{d}+ik_\mathrm{c}\right)E_{1\mathrm{CW}}+kf_{1\mathrm{CW}}E_{1\mathrm{CW}}\left(t-\tau_{1\mathrm{CW}}\right)\mathrm{e}^{-\mathrm{i}\left(\omega_1\tau_{1\mathrm{CW}}\right)} \tag{2}$$

$$\frac{\mathrm{d}E_{2\mathrm{CW}}}{\mathrm{d}t}=k\left(1+i\alpha_2\right)\left(G_{2\mathrm{CW}}N_2-1\right)E_{2\mathrm{CW}}-\left(k_\mathrm{d}+ik_\mathrm{c}\right)E_{2\mathrm{CCW}}+kf_{12\mathrm{CW}}E_{1\mathrm{CW}}\left(t-\tau_{12\mathrm{CW}}\right)\mathrm{e}^{-\mathrm{i}\left(\omega_1\tau_{12\mathrm{CW}}+\Delta\omega_{12}T\right)} \tag{3}$$

$$\frac{\mathrm{d}E_{2\mathrm{CCW}}}{\mathrm{d}t}=k\left(1+i\alpha_2\right)\left(G_{1\mathrm{CCW}}N_2-1\right)E_{2\mathrm{CCW}}-\left(k_\mathrm{d}+ik_\mathrm{c}\right)E_{2\mathrm{CW}}+kf_{2\mathrm{CCW}}E_{1\mathrm{CCW}}\left(t-\tau_{12\mathrm{CCW}}\right)\mathrm{e}^{-\mathrm{i}\left(\omega_1\tau_{12\mathrm{CCW}}+\Delta\omega_{12}T\right)} \tag{4}$$

$$\frac{\mathrm{d}E_{3\mathrm{CW}}}{\mathrm{d}t}=k\left(1+i\alpha_3\right)\left(G_{3\mathrm{CW}}N_3-1\right)E_{3\mathrm{CW}}-\left(k_\mathrm{d}+ik_\mathrm{c}\right)E_{3\mathrm{CCW}}+kf_{13\mathrm{CW}}E_{1\mathrm{CW}}\left(t-\tau_{13\mathrm{CW}}\right)\mathrm{e}^{-\mathrm{i}\left(\omega_1\tau_{13\mathrm{CW}}+\Delta\omega_{13}T\right)} \tag{5}$$

$$\frac{\mathrm{d}E_{3\mathrm{CCW}}}{\mathrm{d}t}=k\left(1+i\alpha_3\right)\left(G_{3\mathrm{CCW}}N_3-1\right)E_{3\mathrm{CCW}}-\left(k_\mathrm{d}+ik_\mathrm{c}\right)E_{3\mathrm{CW}}+kf_{13\mathrm{CCW}}E_{1\mathrm{CCW}}\left(t-\tau_{13\mathrm{CCW}}\right)\mathrm{e}^{-i\left(\omega_1\tau_{13\mathrm{CCW}}+\Delta\omega_{13}T\right)} \tag{6}$$

$$\frac{\mathrm{d}N_j}{\mathrm{d}t}=\gamma\left[u_j-N_j-G_{j\mathrm{CW}}N_j\left|E_{j\mathrm{CW}}\right|^2-G_{j\mathrm{CCW}}N_j\left|E_{j\mathrm{CCW}}\right|^2\right] \tag{7}$$

$$\begin{cases} G_{j\mathrm{CW}} = 1 - s\left|E_{j\mathrm{CW}}\right|^2 - c\left|E_{j\mathrm{CCW}}\right|^2 \\ G_{j\mathrm{CCW}} = 1 - s\left|E_{j\mathrm{CCW}}\right|^2 - c\left|E_{j\mathrm{CW}}\right|^2 \end{cases} \tag{8}$$

式中：$j=1,2,3$ 分别表示主半导体环形激光器 M-SRL1，S-SRL2，S-SRL3；$E_{1\mathrm{CW}}, E_{1\mathrm{CCW}}$ 表示 M-SRL1 中的 CW 与 CCW 模式的平均场缓变振幅；$E_{2\mathrm{CW}}$，$E_{2\mathrm{CCW}}$ 表示 S-SRL2 中的 CW 与 CCW 模式的平均场缓变振幅；$E_{3\mathrm{CW}}, E_{3\mathrm{CCW}}$ 表示 S-SRL2 中的 CW 与 CCW 模式的平均场缓变振幅；N_j 为作用区的平均载流子密度；k 为光场衰减率；a_j 为线宽增强因子；γ 为载流子的衰减率；s 为自饱和系数；c 为交叉饱和系数；$k_\mathrm{d}, k_\mathrm{c}$ 为保守与耗散耦合系数；μ_j 为归一化注入电流；$kf_{1\mathrm{CW}}, kf_{1\mathrm{CCW}}$ 为反馈强度；$\tau_{1\mathrm{CW}}, \tau_{1\mathrm{CCW}}$ 为反馈时延；$k_{13\mathrm{CW}}, k_{13\mathrm{CCW}}, k_{12\mathrm{CW}}, k_{12\mathrm{CCW}}$ 为注入强度；$\tau_{13\mathrm{CW}}$，$\tau_{13\mathrm{CCW}}, \tau_{12\mathrm{CW}}, \tau_{12\mathrm{CCW}}$ 为注入时延；$\Delta\omega_{12}, \Delta\omega_{13}$ 为角频率失谐，其计算函数分别为 $\Delta\omega_{12}=\omega_1-\omega_2=2\pi(f_1-f_2)$，$\Delta\omega_{13}=\omega_1-\omega_3=2\pi(f_1-f_3)$，$f_1, f_2, f_3$ 分别为 M-SRL1，S-SRL2，S-SRL3 自由运行的光学频率。

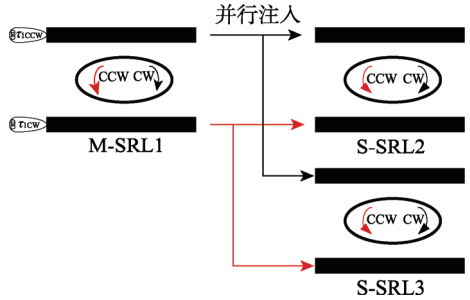


图 1　级联耦合混沌半导体环形激光器 CCSRL 的结构

Fig.1 Structure of cascaded-coupled chaotic semiconductor ring laser CCSRL

对于文中算法，在利用 CCSRL 系统生成混沌序列时，上述参数采用文献[10—11]的参数：s=0.005，c=0.01，$\Delta\omega T=0$，$\omega_1\tau_{1\mathrm{CW}}=\omega_1\tau_{1\mathrm{CCW}}=\omega_1\tau_{12\mathrm{CCW}}=\omega\tau_{12\mathrm{CW}}=\omega\tau_{13\mathrm{CCW}}=\omega\tau_{1\mathrm{CW}}=0$，$k_\mathrm{d}=0.033\ \mathrm{ns}^{-1}$，$k_\mathrm{c}=0.44\ \mathrm{ns}^{-1}$，$\gamma=0.2\ \mathrm{ns}^{-1}$，$\mu_1=\mu_2=\mu_3=1.75$，$kf_{1\mathrm{CW}}=2.5\ \mathrm{ns}^{-1}$，$kf_{1\mathrm{CCW}}=10\ \mathrm{ns}^{-1}$，$\tau_{1\mathrm{CW}}=0.7\mathrm{ns}$，$\tau_{1\mathrm{CCW}}=0.8\ \mathrm{ns}$，$k_{13\mathrm{CW}}=k_{13\mathrm{CCW}}=k_{12\mathrm{CW}}=k_{12\mathrm{CCW}}=50\ \mathrm{ns}^{-1}$，$\tau_{13\mathrm{CW}}=\tau_{13\mathrm{CCW}}=\tau_{12\mathrm{CW}}=\tau_{12\mathrm{CCW}}=5\ \mathrm{ns}$，$\mu_1=\mu_2=\mu_3=1.75$，$\alpha_1=\alpha_2=\alpha_3=8$。

为了直接量化半导体环形激光器 SRL 的混沌输出的同步程度，文中引用移位交叉相关函数[12]来进行评估：

$$\rho_{ij}(\Delta t)=\frac{<\left[I_i(t+\Delta t)-<I_i(t+\Delta t)>\right]\left[I_j(t)-<I_j(t)>\right]>}{\sqrt{<\left[I_i(t+\Delta t)-<I_i(t+\Delta t)>\right]^2><\left[I_j(t)-<I_j(t)>\right]^2>}} \tag{9}$$

式中：i，j=1,2,3，分别表示激光器 M-SRL1，S-SRL2，S-SRL3；< >为时间平均值；Δt 为滞后时间；$I_{i,j}$ 为输出强度，$I_{i,j}=\left|E_{i,j}\right|^2$。

2　物理随机位生成器的设计及混沌同步分析

根据 CCSRL 的特性，文中设计了一种物理随机位生成器，其结构见图 2。依图 2 可知，物理随机位生成器主要分为 2 个部分：作为物理熵源的混沌半导体环形激光器；用于量化的电子电路。首先，半导体环形激光器 S-SRL2 通过光隔离器，发射一个 50∶50 的光纤耦合器。对于其输出的信号，通过光电探测器，将其中一种进行转换并放大为电信号，再利用延迟光纤，将另外一种信号延迟 5.39 ns。然后，将 2 个电信号耦合到比较器中，通过对比各自比较器的相关输入差分来获得二进制位流。接下来，将二进制位流分为 2 个部分：一部分在进入逻辑异或 XOR 门之前，被发送到 1 个 215 位的寄存器；另外一部分则直接进入逻辑异或 XOR 门。最后，由混沌 CW、CCW 模式生成的 2 个随机二进制比特流通过一个 XOR 处理，即可输出一组随机性较高的随机位流。若其产生的混沌信号被记录在 25 ps 的采样周期内(采样率为 40 GHz)，则二进制位流的相关性可通过下采样和寄存器[13]消除。

根据上述描述可知，整个随机位流是通过级联耦合混沌半导体环形激光器 CCSRL 来生成的，而 CCSRL 考虑了时间延迟，避免了混沌系统反复迭代的周期性，且随机位流的相关性可在其生成过程中通过下采样和寄存器来消除，使其具备更为理想的伪随机性，可显著增强密文的安全性。

为了测试激光器 M-SRL1，S-SRL2，S-SRL3 的混沌同步程度，文中利用式(9)来量化，以最大的移位交叉相关系数为目标。在该次测试中，考虑耦合强度 $k_{13\mathrm{CW}}=k_{13\mathrm{CCW}}=k_{12\mathrm{CW}}=k_{12\mathrm{CCW}}$，则任意 2 个激光器之间的同步程度量化结果见图 3。依图 3 可知，当注入强

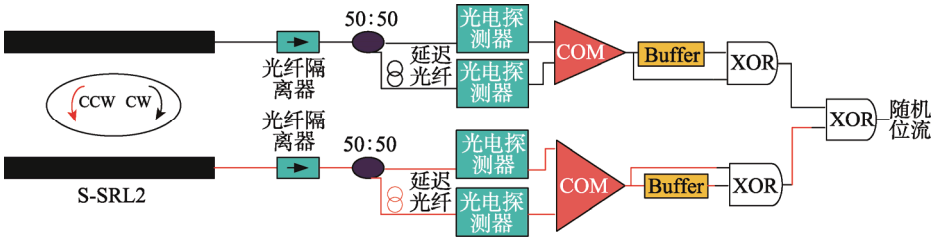


图 2　物理随机位生成器的结构

Fig.2 The structure of a physical random bit generator

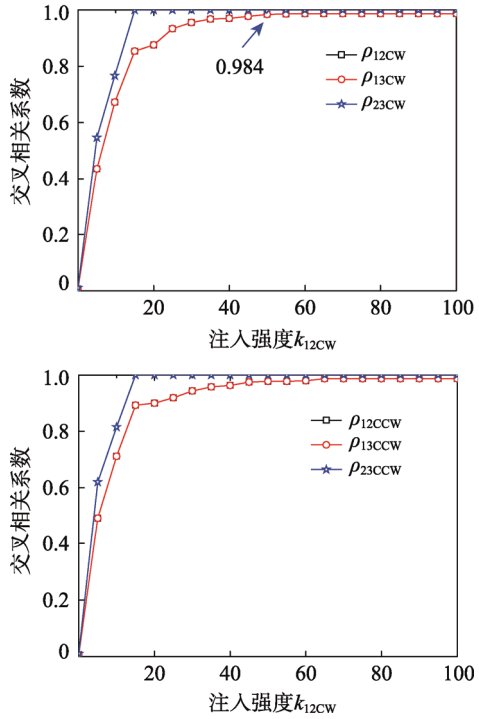


图 3　3 个激光器的混沌同步性测试

Fig.3 Chaotic synchronization test of three lasers

度增加到一个关键值时，S-SRL2 与 S-SRL3 之间的同步性达到理想值，与 1 接近。另外，当注入强度 $k_{12CW}=50\text{ns}^{-1}$时，M-SRL1 与 S-SRL2 之间的同步质量约为 0.984，这表明主半导体环形激光器 M-SRL1 与独立环形激光器 S-SRL 之间也具有理想的同步性。激光器 M-SRL1，S-SRL2，S-SRL3 的输出结果的时域特性见图 4。依图 4 可知，3 个半导体环形激光器都处于混沌状态，且任意 2 个激光器之间输出混沌信号的波形较为复杂，说明其具有较高的不可预测性；且在 S-SRL2 与 S-SRL3 之间的同步性能最好，交叉相关系数最大，约为 0.9998，非常接近理论值“1”。由此，可以使用从 S-SRL2 和 S-SRL3 等 2 种激光器中提取的物理随机位生成器来获取同步随机位生成器。

3　文中图像加密算法设计

文中设计的图像加密算法过程见图 5。可知，所提加密技术分为 3 个过程：基于像素交叉互换机制的明文预处理；基于物理随机位生成器的图像混淆；基于连续扩散函数的图像加密。

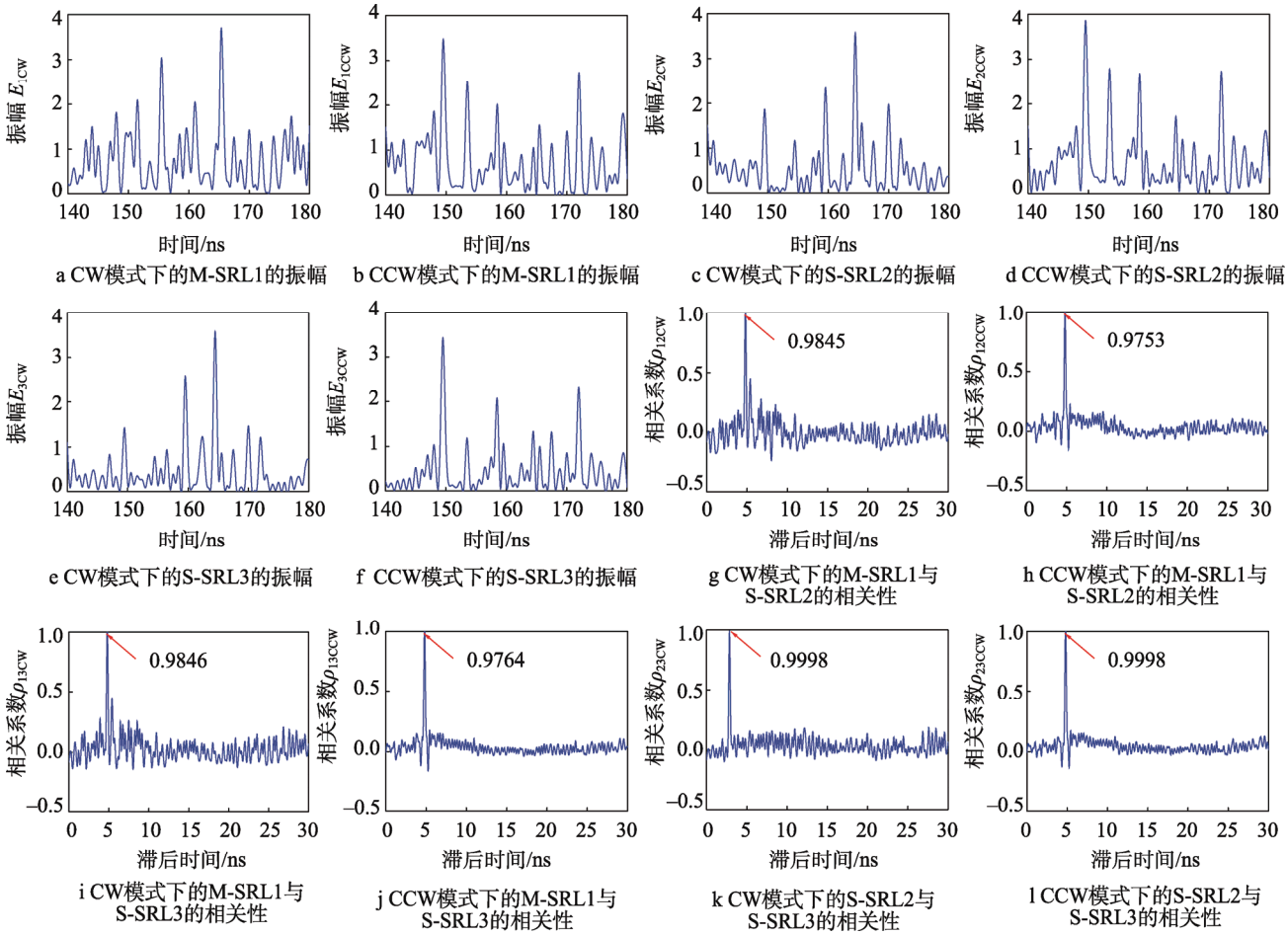


图 4　不同 SRL 在 CW 与 CCW 模式下的输出信号的时域特性测试

Fig.4 Time domain characteristics test of output signals of different SRLs in CW and CCW modes

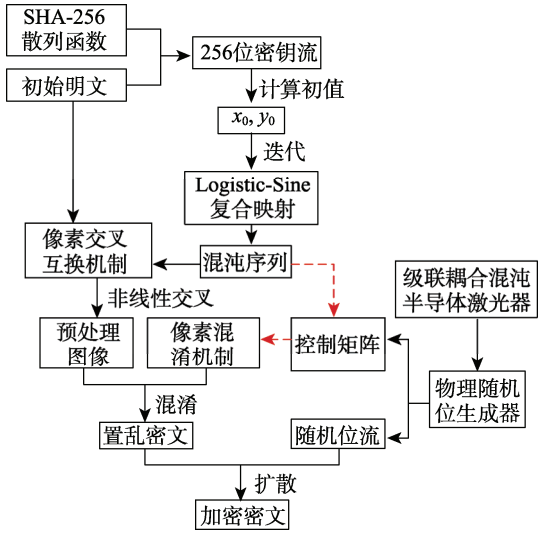


图 5　文中图像加密算法过程

Fig.5 The process of the proposed image encryption algorithm

3.1　基于像素交叉互换机制的明文预处理

为了消除图像相邻像素之间的强烈相关性[14]，文中设计了像素交叉互换机制，其过程如下所述。

1）引入 SHA-256 散列函数[15]，对尺寸为 $M\times N$ 的明文 $f(x,y)$ 进行处理，可获得一组 256 位的密钥流 K，使其与明文密切相关，提高算法对明文的敏感性，并将其分割为一系列不同的 8 位子密钥 k_i：

$$K=k_1k_2\cdots k_{32} \tag{10}$$

2）为了利用伪随机性较高的混沌序列来设计像素交叉互换机制，文中引入了 Logistic-Sine 复合映射[1−2]，以兼顾算法的效率与安全性，其函数如下：

$$\begin{cases} x_{i+1}=a\left(\sin\left(\pi y_i\right)+\mu\right)x_i\left(1-x_i\right) \\ y_{i+1}=a\left(\sin\left(\pi x_{i+1}\right)+\mu\right)y_i\left(1-y_i\right) \end{cases} \tag{11}$$

其中，$\alpha\in[0,1],\mu\in[0,3]$ 均为混沌控制参数。依据文献[2]可知，当 μ 接近或者等于 3 时，式(11)具有理想的混沌性能。为了提高加密算法的抗明文攻击能力，根据式(10)中与明文相关的子密钥 k_i 来计算式(11)中的初值 x_0，y_0：

$$x_0=\mathrm{mod}\left(\left(\left(k_2\oplus k_4\oplus k_6\oplus\cdots K_{32}\right)+\sum_{i=1}^{32}\left(k_i\right)\right)/2^8,4\right) \tag{12}$$

$$y_0=\mathrm{mod}\left(\left(\left(k_1\oplus k_3\oplus k_5\oplus\cdots K_{31}\right)+\sum_{i=1}^{32}\left(k_i\right)\right)/2^8,4\right) \tag{13}$$

再设置好 α,μ，联合 x_0，y_0 对式（11）完成迭代，可获取 2 组混沌序列 $\boldsymbol{X}=\{x_1,x_2....x_{M\times N}\}$，$\boldsymbol{Y}=\{y_1,y_2....y_{M\times N}\}$。

3）为了提高密文的随机性，从序列 $\boldsymbol{X}=\{x_1,x_2....x_{M\times N}\}$ 中提取排序为奇数的元素；从 $\boldsymbol{Y}=\{y_1,y_2....y_{M\times N}\}$ 中提取排序为奇数的元素，通过组合这些新元素，形成一个新的随机序列 $\boldsymbol{Z}=\{z_1,z_2....z_{M\times N}\}$。依据 $\boldsymbol{Z}=\{z_1,z_2....z_{M\times N}\}$，利用非线性交叉位交换算子，设计像素交叉互换机制：

$$a_i=i+\mathrm{mod}\left(\mathrm{floor}\left(z\left(i+1000\right)\times10^{10}\right),M\times N-1\right),\quad i\in[1,M\times N] \tag{14}$$

$$\left[P(i),P(a_i)\right]=swap\left\{P(i),P(a_i)\right\} \tag{15}$$

式中：a_i 为像素的新位置；$P(i)$ 是第 i 个像素的灰度值；floor( ) 为向下取整运算；$swap$ 为交叉互换函数。根据式(14)计算出任意位置 i 的像素所对应的新位置 a_i，然后，将 $P(i)$ 与 $P(a_i)$ 进行位置互换，从而降低相邻像素之间的相关性。利用上述过程处理所有像素，得到预处理图像 $I(x,y)$。以图 6a 为例，其相邻像素之间的相关性见图 6b；取 $\alpha=0.87,\mu=3$，经过上述过程预处理后，结果见图 6c，相应的相邻像素之间的相关性见图 6d。可知，明文经过像素交叉互换机制处理后，有效打乱了像素信息，使其呈现一幅与明文完全不同的图像。同时，明文的相邻像素之间的相关性非常高，见图 6c，所有像素堆积为“对角线”形状；经过预处理后，这种强烈的相关性被大幅剥削，见图 6d，像素分布均匀度较为理想。

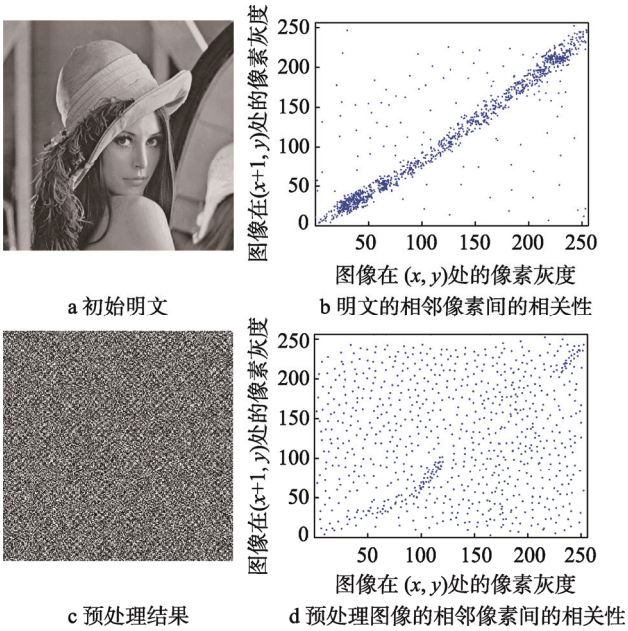


图 6　明文图像的预处理

Fig.6 Preprocessing of plaintext images

3.2　基于物理随机位生成器的图像混淆

虽然经过预处理后，图像的相关性被大幅削弱，但是其像素分布仍然还有部分堆积现象，而且信息冗余度较高。为此，文中设计了像素混淆机制，随机改变像素位置，充分破坏这相关性，有效抵御外来攻击。所设计的像素混淆过程如下所述。

1）首先，将预处理图像 $I(x,y)$ 按照从左到右、从上到下的顺序，对所有像素进行位置标记，得到一个对应的位置矩阵 $\boldsymbol{T}_{\text{posiotion}}$。

2）利用前文中的物理随机位生成器，输出一个控制矩阵 $\boldsymbol{T}_{\text{Control}}$：

$$\boldsymbol{T}_{\text{Control}} = RBG\left(N_0+1:2:N_0+2\times M\times N-1\right) \quad (16)$$

式中：RBG 为利用物理随机位生成器生成的随机位序列；N_0 为丢弃不稳定的 RBG 长度。

由于控制矩阵 P_{Control} 是一个位序列，因此其所有元素只有“0”或者“1”，代表向左或者向右。同时，依据 Logistic-Sine 复合映射输出的随机序列 $\boldsymbol{Z}=\{z_1,z_2....z_{M\times N}\}$，计算过渡矩阵 $\boldsymbol{T}_{\text{transition}}$：

$$\boldsymbol{T}_{\text{transition}} = \text{mod}\left(\text{floor}\left(z\left(501:X+500\right)\times 10^{10}\right),M\times N\right)+1 \quad (17)$$

式(17)输出的是一个实值矩阵，其元素值大小为 $[1,M\times N]$，每个元素值的大小代表沿着指定方向(向左或者向右)的移动距离。

3）联合控制矩阵 $\boldsymbol{T}_{\text{Control}}$、过渡矩阵 $\boldsymbol{T}_{\text{transition}}$ 以及位置矩阵 $\boldsymbol{T}_{\text{posiotion}}$，定义像素混淆函数，完成像素位置的置乱：

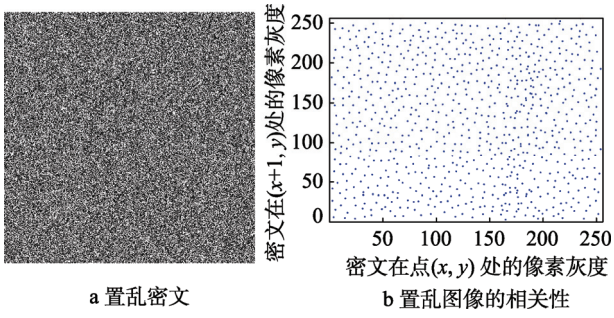
$$\boldsymbol{T}'_{\text{posiotion}} = v\left(\boldsymbol{T}_{\text{position}},\boldsymbol{T}_{\text{Control}},\boldsymbol{T}_{\text{transition}}\right) \quad (18)$$

式中：v 为表 1 中算法描述的函数；$\boldsymbol{T}'_{\text{posiotion}}$ 为由置乱像素位置所组成的矩阵。

表 1　像素混淆算法
Tab.1 Pixel confusion algorithm

1	Input: $T_{position}$, $T_{Control}$, $T_{transition}$ of size M × N.
2	Connect pixels in $T_{position}$ with locations 1 ,……,M × N into a circle.
3	for i = 1 to M × N do
4	if $T_{Control}$(i) > 0 do
5	if $T_{position}$(i) > 0 do
6	swap($T_{position}$(i), $T_{position}$(M × N - mod (($T_{position}$(i) − i) , M × N)));
7	else
8	swap($T_{position}$(i), $T_{position}$ (i − $T_{transition}$(i)));
9	end if
10	else
11	if $T_{transition}$(i)+I ≤ M × N do
12	swap($T_{position}$(i), $T_{position}$ (i + $T_{transition}$(i)));
13	else
14	swap($T_{position}$(i), $T_{position}$ (mod((i + $T_{transition}$(i)), M × N);
15	end if
16	end if
17	end for
18	output: T'$_{position}$ = swap (P(i) , P($T_{position}$(i)));

利用式(18)对预处理图像 $I(x,y)$ 的所有像素完成置乱，可输出一幅置乱密文 $I'(x,y)$。以图 6c 为例，利用上述过程对其进行置乱，结果见图 7a，相应的相邻像素间的相关性见图 7b。可知，经过所提像素混淆机制置乱后，明文信息被高度隐藏，呈现一幅重度噪声污染图像；且其相邻像素间的相关性被有效消除，所有像素分布非常均匀，无任何堆积现象，见图 7b。



a 置乱密文　　b 置乱图像的相关性

图 7　图像混淆测试
Fig.7 Image confusion test

3.3　基于连续扩散的图像加密

虽然明文图像经过预处理以及置乱后，其像素位置被充分打乱，相邻像素间的相关性被有效消除，但是像素值却没有发生变化。为此，文中利用物理随机位生成器输出的随机位流来构建扩散函数，对置乱密文进行加密，改变其像素值。为此，定义随机位流的生成函数如下：

$$\boldsymbol{T}_{\text{diffusion}} = RBG\left(N_0+2:2:N_0+2\times M\times N\times 8+2\right) \quad (19)$$

式中：$\boldsymbol{T}_{\text{diffusion}}$ 为由随机位流组成的矩阵；*RBG* 为利用物理随机位生成器生成的随机位序列；N_0 为丢弃不稳定的 *RBG* 长度。

再利用 $\boldsymbol{T}_{\text{diffusion}}$ 设计连续扩散函数，对置乱密文 $I'(x,y)$ 进行加密：

$$P''(i)=t_i\oplus P'(i)\oplus P''(i-1),i=1,2...M\times N \quad (20)$$

式中：$t(i)$代表矩阵 $\boldsymbol{T}_{\text{diffusion}}$ 中第 i 个位置的密钥；$P'(i)$ 为置乱图像 $\boldsymbol{T}'_{\text{posiotion}}$ 中第 i 个像素的像素值；$P''(i)$ 为加密后的像素值；$P''(i-1)$ 代表加密前一个像素的像素值，且初值 $P''(0)=100$。

依据式(20)可知，所设计连续扩散函数与前一个加密像素密切相关，有效增强了密文的随机性。以图 7a 为例，经过所提加密方法扩散后，输出的最终密文见图 8。

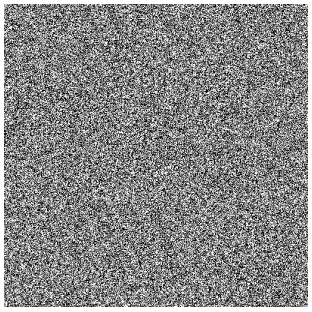


图 8 基于连续扩散的加密效果

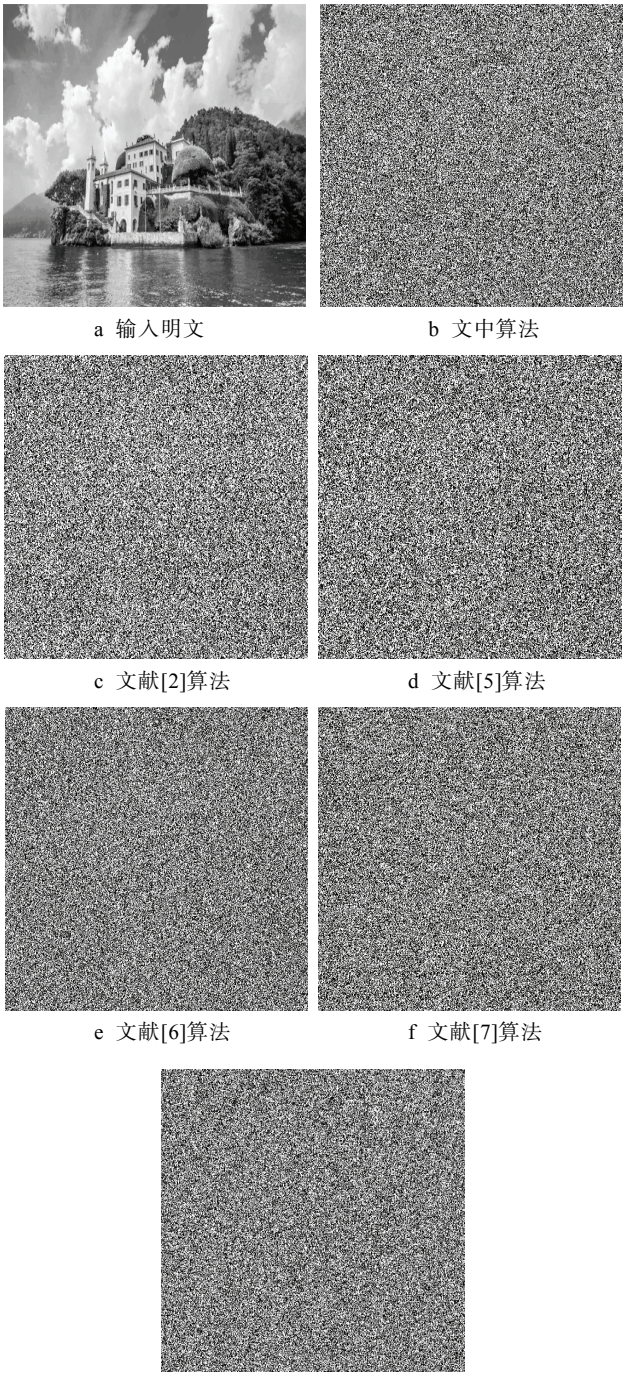
Fig.8 Encryption effect based on continuous diffusion

4 实验结果与分析

为了验证文中图像加密算法的有效性与优异性，利用 MATLAB 软件对其完成测试。另外，为了突出所提技术的优势，将当前安全性较高的混沌加密方法视为对照组：文献[2]、文献[5]、文献[6]、文献[7]、文献[9]。其中，文献[2]采用 Logistic-Sine 复合映射来完成图像加密，它在经典 Logistic 映射和 Sine 映射基础上进行了改进，具有很好的代表性和新颖性。文献[9]则是利用超混沌 Chen 系统与人为设置的时间延迟来完成图像加密，该技术考虑了时间延迟现象，且采用了经典的四维混沌系统，具有良好的代表性与先进性。级联耦合混沌半导体环形激光器的参数沿用文献[11]、文献[12]，见式(8)下面的参数设置。二维 Logistic-Sine 复合混沌映射的参数 $\alpha=0.87,\mu=3$；舍弃不稳定 RBG 的长度 $N_0=1000$。

4.1 加密效果与效率测试

以图 9a 为实验样本，借助文中算法、文献[2]、文献[5]、文献[6]、文献[7]和文献[9]对其进行加密处理，输出数据见图 9b—g。基于加密质量可知，依据人眼视觉特性，所提算法与 4 种对照组技术都可较好地对明文信息完成置乱与扩散处理，攻击者难以从中直接获得有关明文的任何线索，具有较好的隐秘性。为了客观评估文中算法与文献[2]、文献[5]、文献[6]、文献[7]和文献[9]加密安全性的差异，引入信息熵值[3]来量化，测试数据见表 2。根据测试数据可知，文献[9]的熵值最大，约为 7.9992，而所提算法的输出密文的熵值与文献[6]算法较为接近，且要显著高于文献[2]、文献[5]和文献[7]，分别为 7.9958，7.9979，7.9886，7.9934，7.9913。这表明所提算法的安全性与文献[6]具有同等的水平，而文献[2]、文献[5]和文献[7]的安全性有待进一步提升。原因是文献[9]不仅采用了 4 维超混沌系统的输出序列来完成像素的置乱与扩散，而且还考虑了混沌序列生成过程中的时间延迟现象，显著提高了混沌序列的伪随机性，使其具有最高的安全性，对应的密文熵值最大。文献[6]算法使用了四维 Chen 超混沌系统的输出序列来高度置乱明文像素，且联合 Chen 超混沌系统与 DNA 动态编码技术，对置乱图像完成扩散，充分利用了高维混沌系统极其复杂的混沌轨迹与相空间的特点，使其密文的安全性较高。相对于文献[9]而言，文献[6]算法没有考虑时间延迟现象，使其安全性要略低于文献[9]。文献[2]则是依赖二维复合混沌映射的随机序列来改变像素位置与像素值，这种低维混沌映射的结构仍然较为简单，存在显著的迭代周期性，使其安全性有待进一步提高。文献[5]则是利用明文像素来生成密钥流，充分利用缠绕 Logistic 映射的不可预测性，根据密钥流来迭代缠绕 Logistic 映射，从而完成图像加密，该技术考虑了明文特性，具有较强的抗明文攻击能力，虽然其改进了 Logistic 映射，但其实质仍是 1D 混沌映射，使其安全性不佳。文献[7]技术则是利用一维 Logistic 混沌映射与动态引擎扩散来完成图像加密，虽然动态引擎扩散具有较高的随机性与动态性，在一定程度上削弱了混沌周期性的不利影响，但是一维 Logistic 映射的结构简单，对应的混沌轨迹与窗口。以及算法密钥空间较小，且忽略了混沌序列产生过程中的时间延迟现象，使其输出的随机序列的自相关性不理想，导致其密文安全性不佳。文中算法则是利用 SHA-256 散列函数与明文像素值所生成的 256 位的密钥来迭代二维 Logistic-Sine 复合映射，利用其输出混沌序列对输入明文的像素位置进行非线性交叉互换，显著消除了相邻像素之间的相关性，并增强其对明文的敏感性，引入级联耦合混沌半导体环形激光器来设计物理随机位生成器，以同步输出控制矩阵与随机位流，联合相应的混淆机制与扩散方法来完成图像加密，充分考虑了自身的时间延迟与交叉反馈的特性，避免了混沌系统的迭代周期性，极大地增加了算法的密钥空间，使其安全性较为理想。



a 输入明文　b 文中算法　c 文献[2]算法　d 文献[5]算法　e 文献[6]算法　f 文献[7]算法　g 文献[9]算法

图 9　不同算法的加密效果测试

Fig.9 Encryption effect test of different algorithms

表 2　加密密文的熵值

Tab.2 Entropy of encrypted cipher

名称	密文
文中算法	7.9958
文献[2]算法	7.9886
文献[5]算法	7.9934
文献[6]算法	7.9979
文献[7]算法	7.9913
文献[9]算法	7.9992

加密技术除了拥有较高的安全性之外，还应具备较高的效率，能够快速实现图像的加密，因此，加密效率也是评估加密技术优异性的重要指标[17]。这里采用 DELL 2.5 GHz 双核 CPU，8 GB 的内存，以及 Windows XP 运行系统。以图 9a 为对象，基于文中算法、文献[2]、文献[5]、文献[6]、文献[7]和文献[9]等 5 种技术，对其完成加密，以密文达到稳定的 NPCR 值为标准，记录三者的时耗，见表 3。根据表 3 中的数据可知，文献[5]的加密效率最高，其时耗约为 47 ms；文中算法同样具有与文献[7]相近水平的效率，其加密耗时约为 83 ms。文献[9]技术的加密效率最低，耗时最为严重，约为 151 ms。原因是文献[7]技术采用了一维 Logistic 映射来实现图像加密，其结构较为简单，但是该技术为块加密机制，在一定程度上增加了算法复杂度，其加密耗时为 69 ms；文献[5]是利用一维缠绕 Logistic 映射来完成加密，该映射的结构简单，使其效率最高。文献[2]则是利用 2D 复合混沌系统，具有较高的加密效率，其时耗为 60 ms，但是相对于文献[5]的 1D 混沌映射，其效率要低。所提算法使用的是二维 Logistic-Sine 复合映射，也是低维混沌系统，且置乱与扩散密钥都是由文中算法的物理随机位生成器同步输出，显著改善了加密速度。文献[6]、文献[9]则是使用了四维超混沌系统，使得复杂度最高，相应的时耗最严重，要远高于文献[2]、文献[5]、文献[7]与文中算法。

表 3　3 种加密算法的效率测试

Tab.3 Efficiency test of three encryption algorithms

算法	NPCR	UACI	时耗/ms
文中算法	>0.953	>0.333	83
文献[6]	>0.953	>0.333	134
文献[7]	>0.953	>0.333	69
文献[2]	>0.950	>0.305	60
文献[5]	>0.953	>0.333	47
文献[9]	>0.953	>0.333	151

4.2　抗明文攻击能力测试

选择明文攻击是当前加密算法常遇到的攻击手段，未授权用户可利用明文攻击方法和大量的测试实验来解密密文，对算法的安全性威胁较大，因此，理想的加密算法应能充分抵御此类攻击[3]。根据文献[3]可知，NPCR 和 UACI 曲线是当前客观量化加密算法抵御选择明文攻击能力的常用指标。NPCR, UACI 的计算函数如下：

$$\mathrm{NPCR}=\frac{\sum_{i=1}^{W}\sum_{j=1}^{H}\mathrm{Difp}\left(I(i,j),I'(i,j)\right)}{W\times H}\times 100\% \qquad (21)$$

$$\mathrm{UACI}=\frac{1}{W\times H}\left[\sum_{ij}\frac{\left|I(i,j)-I'(i,j)\right|}{255}\right]\times 100\% \tag{22}$$

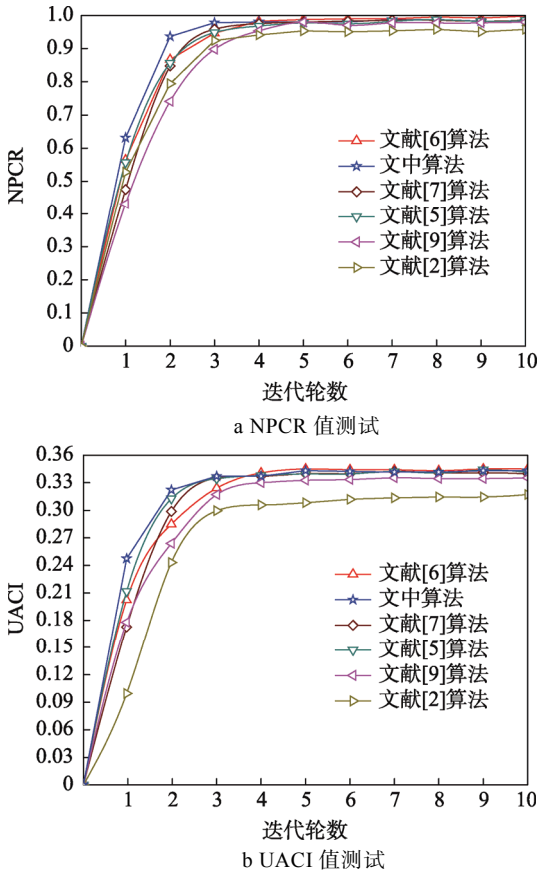
$$\mathrm{Difp}\left(I(i,j),I'(i,j)\right)=\begin{cases}0, & I(i,j)=I'(i,j)\\ 1, & I(i,j)\neq I'(i,j)\end{cases} \tag{23}$$

式中：$W\times H$ 为输入图像的尺寸；Difp 为量化函数，I,I' 分别为 2 个明文经加密处理后的 2 个密文，且二者只存在一个相异灰度值[3]。

以图 9a 为测试对象，把坐标(231, 154)的像素灰度值 172 修改成 76，以形成一个伪造明文；利用文中算法、文献[2]、文献[5]、文献[6]、文献[7]和文献[9]对初始明文，以及伪造后的明文完成置乱与扩散处理，输出 2 个密文；再根据式(21—23)，形成三者对应的 NPCR 与 UACI 曲线，见图 10。根据测试结果可知，文献[6]算法的抗明文攻击能力最强，所提算法与其非常接近，文献[5]也具有良好的抗明文攻击能力，而文献[2]、文献[7]和文献[9]的抵御选择明文攻击能力较弱，尤其是文献[2]技术，其性能最低。对于文献[6]，其稳定的 NPCR 和 UACI 值分别为 99.61%，33.52%，而文中算法的稳定的 NPCR 和 UACI 值分别为 99.50%，33.46%，文献[2]算法的 NPCR 和 UACI 值分别为 95.18%，30.54%。主要原因是文中算法利用 SHA-256 散列函数处理初始明文，形成了一组与明文密切相关的密钥，根据此密钥来迭代混沌映射，用于明文的预处理与置乱，使得整个算法与明文紧密相关，增强了算法对明文的敏感性，使其会随着明文的不同，而形成不同的密钥。若外来攻击者借助选择明文攻击方法和大量测试不同的明文来解密密文，因其解密密钥不正确，使其无法准确复原明文。同样，文献[6]技术也是采用了 SHA-256 散列函数来计算明文，利用其输出的密钥来迭代 Chen 超混沌系统，根据其输出随机序列对明文进行置乱与扩散，使其抗选择明文能力最强。文献[5]则是利用明文像素来生成一组密钥流，对缠绕 Logistic 映射进行迭代，使得整个算法与明文密切相关，具有较强的明文敏感性。文献[2]、文献[7]、文献[9]的加密算法在加密过程中，没有考虑明文信息，使其对明文的敏感性较低。由此，攻击者可以利用明文攻击方法和大量的测试实验来获取正确的解密密钥，使得二者的抗选择明文攻击能力不理想。

4.3 敏感性测试分析

密钥敏感性是评估当前加密算法安全性的常用手段，也就是满足严格的“雪崩效应”，当密钥发生微小波动时，所产生的解密图像差异是巨大的[4]。对此，文中测试了混沌参数 $\mu=3$ 的敏感性。基于扰动值 $\Delta=10^{-15}$ 来改变 μ 值，从而形成两组错误密钥：$(\mu-\Delta)$、$(\mu+\Delta)$。剩余密钥均不变。随后，利用正确的密钥，和这 2 组错误密钥对图 9b 进行解密，且获取了 μ 的 MSE(mean square error) 曲线，实验结果见图 11。基于图 11 的输出结果可知，即使密钥 μ 发生

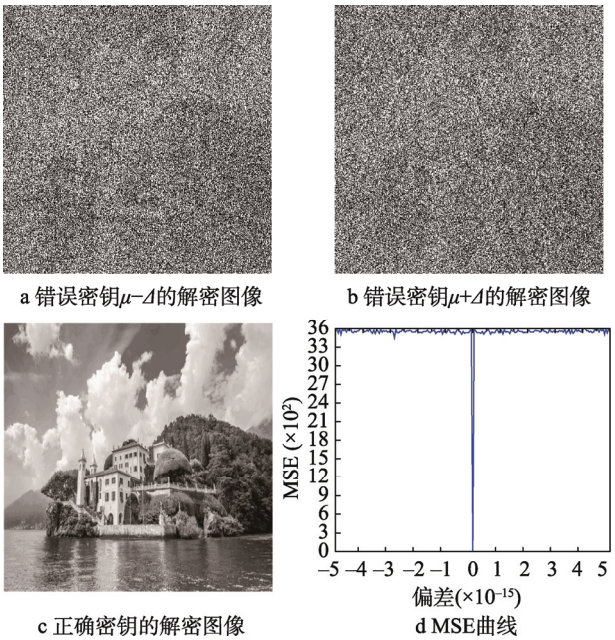


a NPCR 值测试

b UACI 值测试

图 10　3 种算法的抵御选择明文攻击能力测试

Fig.10 Resistance chosen plaintext attack ability test of three algorithms



a 错误密钥$\mu-\Delta$的解密图像　　b 错误密钥$\mu+\Delta$的解密图像

c 正确密钥的解密图像　　d MSE曲线

图 11　文中算法的密钥敏感性测试

Fig.11 Key sensitivity test of the proposed algorithm

了 10^{-15} 的微小偏差，攻击者仍然无法对密文完成正确解密，所得到的复原图像是一幅噪声干扰图像，无法清晰看到图像的信息，此时的 MSE 值都超过了 3500；只有解密参数都无偏差时，才能对其进行正确解密，获得清晰完整的初始图像，见图 11c；此刻的 MSE 曲线急剧下降，其 MSE 值趋于 0，图 11d。这表明文中加密技术满足严格的“雪崩效应”，具有理想的密钥敏感性。

4.4　抗剪切能力测试分析

剪切攻击是客观评估加密方案的安全性与鲁棒性的重要指标[16]。对此，文中以图 9b—g 为实验目标，对三者剪切 1/8，见图 12a，c，e，g，i，k，并进行复原，结果见图 12b，d，f，h，j，m。由图 12 可知，当密文在网络传输中遇到同等程度的剪切攻击时，所提算法具有更强的抗剪切攻击能力，复原结果清晰完整，保留了初始明文的绝大部分信息，与明文的视觉相似度最吻合，见图 12b，而文献[2]、文献[5]、文献[6]、文献[7]和文献[9]技术的抗剪切攻击能力不佳。即使能够复原密文，解密结果也不清晰，轮廓也不完整，会丢失较多的像素信息，见图 12d，f，h，j，m。原因是所提加密技术通过定义像素交叉互换机制，对输入明文进行预处理，消除了相邻像素之间的相关性，而且在此预处理基础上，利用级联耦合混沌半导体环形激光器所设计的物理随机位生成器来输出控制矩阵，对预处理图像进行置乱，避免了置乱周期性，使其像素位置的置乱度最高，像素分布更加均匀，从而使其抗剪切攻击能力最好。文献[2]、文献[5]、文献[6]、文献[7]和文献[9]算法则是依赖混沌系统的随机序列来对明文进行置乱，存在显著的置乱周期性，导致置乱像素在迭代过程中存在复原现象，使其置乱度不佳，以及像素分布均匀度不理想，从而削弱了二者的抗剪切攻击能力。

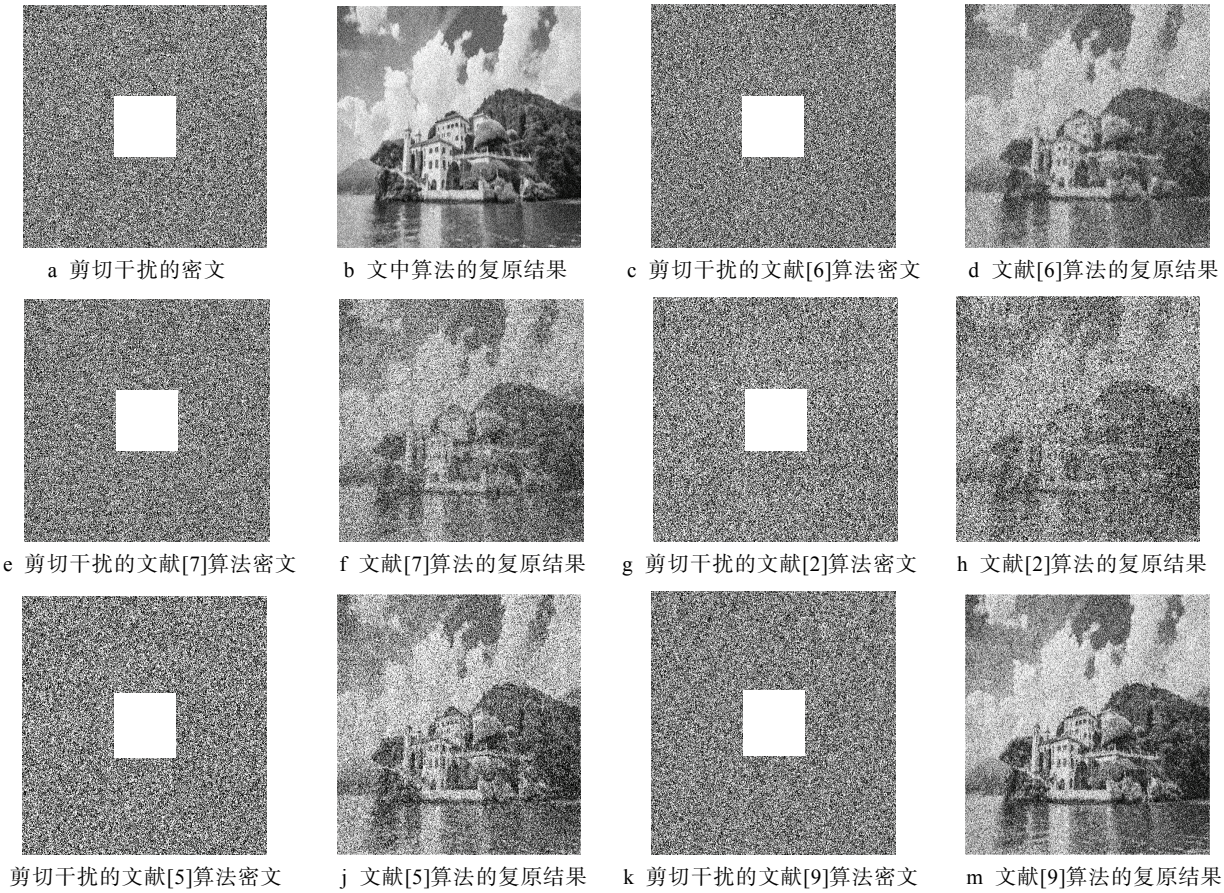


图 12　3 种算法的抗剪切攻击能力测试

Fig.12 Anti-shear ability test of three algorithms

5　结语

为了兼顾加密算法的安全性与效率，文中设计了基于物理随机位生成器与混沌像素交叉互换的图像加密算法。基于明文像素，利用 SHA-256 散列函数来获取一个 256 位的密钥，以计算 Logistic-Sine 复合映射的初值条件，从而输出一组混沌序列，通过定义像素交叉互换机制，对明文进行预处理，有效消除了相邻像素之间的相关性；利用级联耦合混沌半导体环形激光器来设计物理随机位生成器，以同步输出控制

矩阵与随机位流，分别设计了像素混淆机制与连续扩散函数，完成了明文的置乱与加密，使其输出密文的像素分布较为均匀。实验结果验证了所提加密技术的合理性与优异性。

参考文献：

[1] 郭静博, 王彦超, 周丽宴. 基于离散分数阶角变换与关联混沌映射的双图像加密算法[J]. 量子电子学报, 2017, 34(4): 420—431.
GUO Jing-bo, WANG Yan-chao, ZHOU Li-yan. Double Image Encryption Algorithm Based on Discrete Fractional Order Angle Transformation and Associated Chaotic Map[J]. Quantum Electronic Journal, 2017, 34(4): 420—431.

[2] HUA Zhong-yun, ZHOU Yi-cong. Image Encryption Using 2D Logistic-adjusted-Sine Map[J]. Information Sciences, 2016, 339(10): 237—253.

[3] 王涛涛, 张超. 基于 Diophantus 模型与动态 S 盒的图像加密算法[J]. 计算机工程与设计, 2017, 38(10): 2678—2685.
WANG Tao-tao, ZHANG Chao. Image Encryption Algorithm Based on Diophantus Model and Dynamic S-box[J]. Computer Engineering and Design, 2017, 38(10): 2678—2685.

[4] ZAHRA Parvin, HADI Seyedarab, MOUSA Shamsi. A New Secure and Sensitive Image Encryption Scheme Based on New Substitution with Chaotic Function[J]. Multimedia Tools and Applications, 2016, 75(17): 10631—10648.

[5] YE Guo-dong, HUANG Xiao-ling. An Efficient Symmetric Image Encryption Algorithm Based on an Intertwining Logistic Map[J]. Neurocomputing, 2017, 251(19): 45—53.

[6] 王宏达. 一种基于混沌系统的新型图像加密算法[J]. 光学技术, 2017, 43(3): 260—266.
WANG Hong-da. A New Image Encryption Algorithm Based on Chaotic System[J]. Optical Technology, 2017, 43(3): 260—266.

[7] XU Lu, GOU Xu, LI Zhi. A Novel Chaotic Image Encryption Algorithm Using Block Scrambling and Dynamic Index Based Diffusion[J]. Optics and Lasers in Engineering, 2017, 91(6): 41—52.

[8] 孙力, 黄正谦, 傅为民. 时间延迟与超混沌 Chen 系统相融合的图像加密算法研究[J]. 科学技术与工程, 2013, 36(35): 10523—10530.
SUN Li, HUANG Zheng-qian, FU Wei-min. Research on Image Encryption Algorithm Combined with Time Delay and Hyperchaotic Chen System[J]. Science and Technology and Engineering, 2013, 36(35): 10523—10530.

[9] YE Guo-dong, WONG Kwok-wo. An Image Encryption Scheme Based on Time-delay and Hyperchaotic System[J]. Nonlinear Dynamics, 2013, 71(1/2): 259—267.

[10] LI Nan-qi, PAN Wei, YAN Lian-shan. Hybrid Chaos-based Communication System Consisting of Three Chaotic Semiconductor Ring Lasers[J]. Applied Optics, 2013, 52(7): 1523—1530.

[11] LI Nan-qi, PAN Wei, YAN Lian-shan. Enhanced Chaos Synchronization and Communication in Cascade-coupled Semiconductor Ring Lasers[J]. Communications in Nonlinear Science and Numerical Simulation, 2014, 32(9): 19(6): 1874—1883.

[12] LI Jia-fu, XIANG Shui-ying, WEN Ai-jun. Role of Linewidth Enhancement Factor on Time-Delay Signature Concealment of Chaos in Mutually-Coupled Semiconductor Ring Lasers[J]. Wireless & Optical Communication, 2016, 32(7): 1—4.

[13] APOSTOLOS Argyris, EVANGELOS Pikasis, DIMITRIS Syvridis. Gb/s One-Time-Pad Data Encryption with Synchronized Chaos-Based True Random Bit Generators[J]. Journal of Lightwave Technology, 2016, 34(22): 5325—5331.

[14] 平萍, 李健华, 毛莺池. 混沌映射与比特重组的图像加密[J]. 中国图象图形学报, 2017, 22(10): 1348—1355.
PING Ping, LI Jian-hua, MAO Ying-chi. Image Encryption Algorithm Based on Chaotic Maps and Bit Reconstruction [J]. Journal of Image and Graphics, 2017, 22(10): 1348—1355.

[15] 杨康. 基于混沌系统的图像加密算法的设计与实现[D]. 开封：河南大学, 2016: 35—41.
YANG Kang. Design and Implementation of Image Encryption Algorithm Based on Chaotic System[D]. Kaifeng: Henan University, 2016: 35—41.

[16] LI Chang-qi, WANG Han. Image Encryption Algorithm Based on Chaotic Segmentation Projection Strategy and Gravity Model[J]. Packaging Engineering, 2017, 38(9): 1201—1209.

[17] CHAI Xiu-li, GAN Zhi-hua, ZHANG Miao-hui. A Fast Chaos-Based Image Encryption Scheme with a Novel Plain Image-related Swapping Block Permutation and Block Diffusion[J]. Multimedia Tools and Applications, 2017, 76(14): 15561—15585.