基于超混沌系统和密文交错扩散的图像加密新算法

朱从旭*① 胡玉平② 孙克辉③
①(中南大学信息科学与工程学院 长沙 410083)
②(广东省电子商务市场应用技术重点实验室 广州 510320)
③(中南大学物理与电子学院 长沙 410083)

摘 要：该文提出一种基于超混沌系统优化序列并结合密文交错扩散的并行图像加密策略。首先，对超混沌序列进行改造使得改进序列更适合图像加密；然后，利用改进的混沌序列产生与明文相关的最终密钥序列，使得算法对明文敏感。图像被分成两个子块，以并行方式对子块进行两轮像素加密，并引入密文交错扩散技术。对密钥空间和执行效率、像素分布特性、相关系数、抗差分攻击能力以及密钥敏感性进行了测试和分析，证明了方案的安全性和执行效率。结果表明，该算法安全高效，在图像保密通信中具有较大的应用潜力。

关键词：保密通信；图像加密；超混沌系统；密文扩散
中图分类号：TP309.7 **文献标识码**： A **文章编号**：1009-5896(2012)07-1735-09
DOI: 10.3724/SP.J.1146.2011.01004

New Image Encryption Algorithm Based on Hyperchaotic System and Ciphertext Diffusion in Crisscross Pattern

Zhu Cong-xu① Hu Yu-ping② Sun Ke-hui③
①(*School of Information Science and Engineering*, *Central South University*, *Changsha* 410083, *China*)
②(*Guangdong Key Lab of Electronic Commerce Market Application Technology*, *Guangzhou* 510320, *China*)
③(*School of Physics and Electronics*, *Central South University*, *Changsha* 410083, *China*)

Abstract: A new image parallel encryption strategy is proposed based on the improved hyperchaotic sequences and ciphertext diffusion in crisscross pattern. Firstly, the hyperchaotic sequences are modified to generate chaotic key stream that is more suitable for image encryption. Secondly, the final key stream is generated by correlating the chaotic key stream and plaintext which result in both key sensitivity and plaintext sensitivity. The plain-image is firstly divided into two sub-images, then sub-images are encrypted simultaneously in a parallel manner with two rounds. The technology of ciphertext diffusion in crisscross pattern is introduced. Performance test and security analysis are performed using key space analysis and algorithm efficiency test, the pixels distribution character, correlation coefficients, the ability to resist differential attack and key sensitivity test. Results suggest that the proposed image encryption scheme is secure and efficient, with high potential to be adopted for the secure image communication applications.

Key words: Secure communication; Image encryption; Hyperchaotic system; Ciphertext diffusion

1 引言

随着多媒体信息处理技术的广泛应用以及互联网、云计算技术的快速发展，多媒体数据日益广泛地在因特网或云计算节点间传播和存储。如何有效保护用户的秘密信息不被非法者使用，根本的措施是信息保密传输和存储。传统密码学作为一般数据加密手段却不太适合于图像数据加密，原因是图像类的信息具有数据量大、数据之间相关性高等特点。具有这种特点的数据用传统密码学加密会导致效率很低。在新的应用背景下，基于混沌的信息加密[1]和基于混沌同步的保密通信[2]已成为两种典型的非传统信息保密技术。混沌序列具有的内在伪随机性、非周期性和可确定的快速再生性，正与密码学所要求的特性天然相关；因此，混沌在信息加密中有着良好的应用前景，尤其在图像加密场合有许多独特优势等待开发。

但是，以往研究的混沌加密技术大多数基于低维离散混沌映射[3–8]，少数基于 3 维连续混沌系统[9,10]。虽然低维混沌系统由于形式简单而具有计算

2011-09-27 收到，2012-03-05 改回
国家自然科学基金(61073187, 61161006)，湖南省自然科学基金(10JJ6093)，广东省自然科学基金(S2011010001581)和湖南省科技计划工业支撑计划重点项目(2010GK2003)资助课题
*通信作者：朱从旭 zhucx@csu.edu.cn

时间开销小的优点[1]；但由于其密钥空间小，序列的复杂度不高，导致密码系统安全性不高。而高维混沌系统尤其是超混沌系统，由于具有 4 个以上的状态变量，因此密钥空间更大；另外，超混沌系统具有两个以上正的 Lyaponuv 指数，其非线性行为更复杂也更难以预测。这些特点使得超混沌系统用于图像加密无疑会提高系统的安全性。因此，随着现代计算机系统性能的不断提高，探索基于高维超混沌系统的图像加密算法将成为主流需求。文献[11]较先提出了一种基于超混沌系统的典型图像加密算法，该算法由图像像素位置置乱和像素值加密两个阶段组成。但是，文献[12]发现该算法存在安全缺陷，其主要原因是该算法的密钥与明文无关，导致无法抵御已知明文攻击；其次是该算法的置乱和替代加密独立，使置乱过程成为摆设。最近，文献[13]提出了一种基于新型超混沌系统的图像加密算法，该算法在加密过程考虑了密钥与明文的相关性，但总体上沿用了文献[11]的像素位置置乱和像素值加密的基本结构。调研发现，现有研究工作中对连续时间高维混沌序列的优化改造问题关注的不多；然而，混沌密码的安全性很大程度上依赖于混沌序列的分布特性、复杂性和随机性[14]。因此，对超混沌序列进行进一步改造无疑能提高密码的安全性。此外，如何提高超混沌图像加密算法的效率也值得研究。为了获得高安全与高效率的图像加密方案，本文提出了基于下列核心思想的超混沌图像加密算法：其一，对超混沌序列进行优化改进，提高其随机性和分布的均匀性。其二，建立密钥与明文的复杂相关性，增强密文对明文和密钥的敏感性。其三，省略像素置乱步骤，采取并行交错的加密策略，提高加密效率和算法的复杂性。

2 超混沌密码算法

2.1 超混沌系统模型及其序列改造

在本文的密码方案中，我们采用如下新型超混沌系统[15]：

$$\left.\begin{aligned}\dot{x}_1 &= a(x_2 - x_1)\\ \dot{x}_2 &= bx_1 + cx_2 - x_1x_3 + x_4\\ \dot{x}_3 &= x_2^2 - dx_3\\ \dot{x}_4 &= -ex_1\end{aligned}\right\} \tag{1}$$

这里，$\dot{x}_i = \mathrm{d}x_i / \mathrm{d}t$ 表示系统状态变量 $x_i(i = 1, 2, 3, 4)$随时间 t 的变化率。我们用 $\boldsymbol{x}=[x_1, x_2, x_3, x_4]$ 表示系统的状态向量。a, b, c, d, e 为系统参数，当 a=27.5, b=3, c=19.3, d =2.9, e=3 时，系统式(1)是超混沌的[15]；即，任意给定一组状态初值(x_{10}, x_{20}, x_{30}, x_{40})，理论上按式(1)随时间演化规律产生的 4 个实数序列是随机的无周期序列。但由于计算机有限精度的实现使这种序列特性有所退化。

原始的超混沌序列并不适合直接用于图像加密，其原因有二：一是实数序列的数值类型与数字图像的像素值类型不匹配；二是数字化原始超混沌序列的分布特性和伪随机特性并不很理想。基于以上原因，我们首先对原始超混沌序列进行改造，(1)使改进序列具有 Golomb 提出的理想伪随机序列所拥有的特性，即均匀的分布特性；自相关函数接近 δ 函数；互相关函数接近 0。(2)使改进序列的数据类型适合于图像数据加密。

将混沌序列进行改造，生成中间混沌密钥序列的步骤如下：

(1)设由系统生成的原始混沌序列表示为$\{x_j(i)$: i =1,2,$\cdots$,N_0+L/4; j =1,2,3,4$\}$。$\{x_j(i)\}$包括 4 个(j =1,2,3,4)长度为(N_0+L/4)的实数序列。其中，L 为待加密图像的像素点总数，N_0 为超混沌系统的预迭代次数。

(2)为了消除混沌序列暂态过程带来的有害效应，以便增强序列对初始条件的敏感性，去掉原始混沌序列的前 N_0 个值，得到 4 个长度分别为 L/4 的子序列$\{x_j(i)$: i =1,2,$\cdots$,L/4; j =1,2,3,4$\}$；再按照变换式(2)对序列$\{x_j(i)\}$进行改造，得到改进序列$\{y_j(i)\}$：

$$y_j(i) = [2 \times x_j(i) - (\max\_x_j + \min\_x_j)] / (\max\_x_j - \min\_x_j) \tag{2}$$

其中 $\max\_x_j$ 和 $\min\_x_j$ 分别是第j个序列中的最大值、最小值，j =1,2,3,4。然后由改进序列$\{y_j(i)\}$经二次改造，得到4个混沌密钥子序列$\{z_j(i)\}$：

$$z_j(i) = \mathrm{mod}((|y_j(i)| - \mathrm{floor}(|y_j(i)|)) \times 10^m, 256),\quad i = 1,2,\cdots,L/4;\ \ j = 1,2,3,4 \tag{3}$$

其中$|x|$取x的绝对值；floor(x)取小于或等于x的最大整数；m为正整数，在本文中取m=14。

(3)将改造后的4个子序列合并成长度为L的混沌密钥序列$\boldsymbol{K}$，合并方式如式(4)所示：

$$\boldsymbol{K} = [z_1(1), z_2(1), z_3(1), z_4(1), \cdots, z_1(L/4), z_2(L/4), z_3(L/4), z_4(L/4)] \tag{4}$$

下面通过实验证明：改进后的超混沌密钥序列具有更好的伪随机性和均匀分布特性。任取一组状态变量初值(x_{10}, x_{20}, x_{30}, x_{40})=(2.5, 5.2, 3.0, 7.3)，时间步长 t_1=0.001, 利用四阶五级 Runge- Kutta 法求解系统式(1)的状态方程组。以$\{z_1(i)\}$和$\{z_2(i)\}$两个子序列的前 2000 项为例，计算改造后序列$\{z_1(i)\}$, $\{z_2(i)\}$的自相关系数以及两个子序列$\{z_1(i)\}$与$\{z_2(i)\}$之间的互相关系数。计算前将序列值归一化到[–1,1]

范围：$Z_1(i)=(z_1(i)-127.5)/127.5$, $Z_2(i)=(z_2(i)-127.5)/127.5$；得到的相关系数结果分别如图 1(a), 1(b)和 1(c)所示。从图 1(a)和 1(b)看出，前两个改进序列的自相关函数都非常接近 δ 函数；而从图 1(c)也可以发现，前两个改进序列之间的互相关系数非常接近于 0。进一步的实验表明，其余几个改进子序列具有类似的结果。图 1(d)则给出了中间混沌密钥序列 $\boldsymbol{K}$ 的数值分布曲线，结果表明，生成的中间混沌密钥序列值分布均匀。

图 2 给出了改进前的 X 序列的对应结果。取前两个序列得到的相关系数结果分别如图 2(a), 2(b)和 2(c)所示。可见，原始序列的自相关函数并不是 δ 函数；前两个原始序列之间的互相关系数也不接近于 0。进一步的实验表明，其余几个原始子序列具有类似的结果。图 2(d)则给出了中间混沌密钥序列 $\boldsymbol{K}0$ 的数值分布曲线，$\boldsymbol{K}0$ 是将原始序列按线性转换公式 $xx_j(i)=[x_j(i)-\max(x_j)]\times 255/[\max(x_j)-\min(x_j)]$ 直接转换成[0,255]范围整数序列后，再连接起来所得到的中间密钥序列。结果表明，这样生成的中间混沌密钥序列值分布是不均匀的。

2.2 新的图像加密算法

本文提出的超混沌图像加密算法的主要思路是：采用超混沌系统的 4 个状态变量的初值作为原始密钥；首先由超混沌系统式(1)生成 4 个混沌实数序列；然后将混沌实数序列按 2.1 节所述方法进行优化改造，并得到性能优化的中间混沌密钥序列 $\boldsymbol{K}$。接下来，利用中间混沌密钥序列构造与加密图像有关的最终密钥序列 **Key**，并利用最终密钥序列 **Key** 对图像像素进行两个回合加密。在加密过程中，我们将图像划分成前后两个子块，同时对两子块进行并行加密；并引入密文交错扩散机制。

设原始图像像素大小为 M 行、N 列，总像素数为 $L=M\times N$，其矩阵表示形式为 $\boldsymbol{P}$

$$\boldsymbol{P}=\begin{pmatrix} P_1 & P_2 & \cdots & P_N \\ \vdots & \vdots & \ddots & \vdots \\ P_{(M-1)N+1} & \cdots & \cdots & P_L \end{pmatrix} \tag{5}$$

相应的加密图像矩阵用类似于式(5)的矩阵 $\boldsymbol{C}$ 表示，按逐行扫描顺序所得的密文像素序列为$\{C(i), i=1,2,\cdots,L\}$。明文图像的前半子块依次由像素序列$\{P(1), P(2),\cdots, P(L/2)\}$组成，后半子块依次由像素序列$\{P(L/2+1), P(L/2+2),\cdots, P(L)\}$组成。

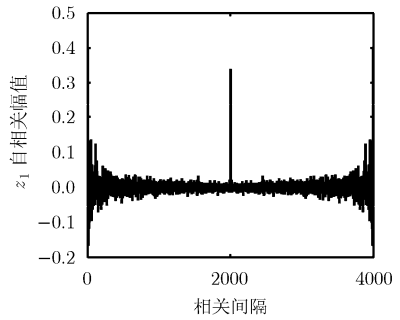
第 1 回合的加密操作由步骤 1 至步骤 3 描述。

步骤 1　$i\leftarrow 1$；并对前一子块的第 1 个像素分别采用式(6a)与式(6b)生成最终加密密钥并进行加密操作；同时对后一子块的第 1 个像素分别采用式(7a)与式(7b)生成最终加密密钥并进行加密操作。

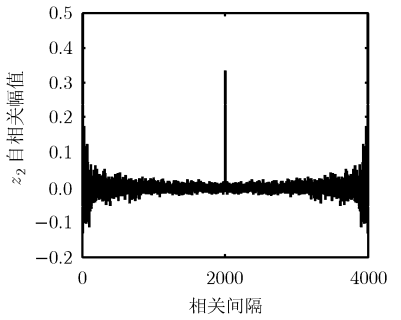
$$\mathrm{Key}(i)=\mathrm{mod}(C_0+K(i),256) \tag{6a}$$

$$C(i)=\mathrm{bitxor}(P(i),\mathrm{Key}(i)) \tag{6b}$$

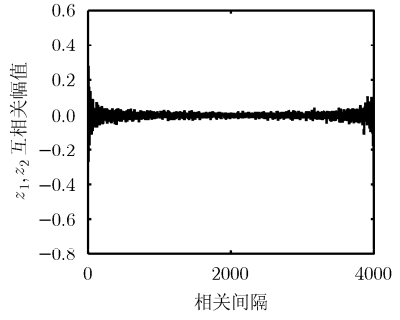
$$\mathrm{Key}(L/2+i)=\mathrm{mod}(C(i)+K(L/2+i),256) \tag{7a}$$



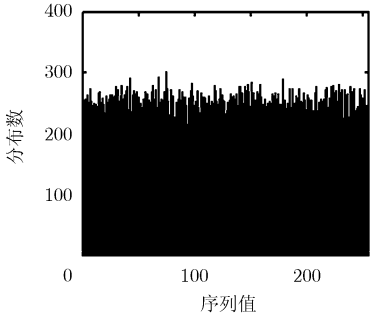
(a) Z_1 序列自相关系数曲线



(b) Z_2 序列的自相关系数曲线

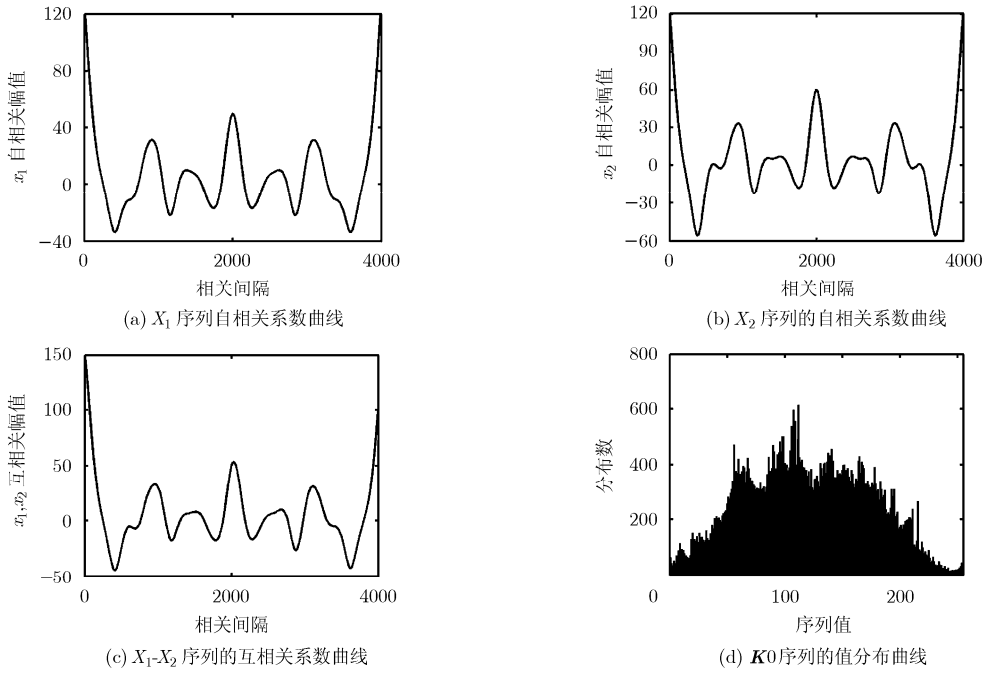


(c) Z_1-Z_2 序列的互相关系数曲线



(d) $\boldsymbol{K}$序列的值分布曲线

图 1 改进混沌序列的相关性和混沌密钥的值分布特征



(a) X_1 序列自相关系数曲线　(b) X_2 序列的自相关系数曲线

(c) X_1-X_2 序列的互相关系数曲线　(d) $\boldsymbol{K}0$序列的值分布曲线

图 2 原始混沌序列的相关性及生成的密钥序列值分布特征

$$C(L/2+i)=\mathrm{bitxor}(P(L/2+i),\mathrm{Key}(L/2+i)) \tag{7b}$$

在上述公式中，bitxor(x,y)将 x 和 y 按其二进制值进行比特位异或运算；mod(x,y)求 x 除以 y 得到整数商以后的余数。C_0 是一个预设的正整数，$C_0\in$[1,255]。$P(i)$，$C(i)$分别是原始图像和加密图像第 i 个像素的值。

步骤 2　$i\leftarrow i+1$；并对前一子块的第 i 个像素分别采用式(8a)与式(8b)生成最终加密密钥且进行加密操作；同时对后一子块的相应像素分别采用与式(7a)和式(7b)相同的公式生成最终加密密钥并进行加密操作。

$$\mathrm{Key}(i)=\mathrm{mod}(C(L/2+i-1)+K(i),256) \tag{8a}$$

$$C(i)=\mathrm{bitxor}(P(i),\mathrm{Key}(i)) \tag{8b}$$

步骤 3　重复步骤 2，直到 i=$L/2$，便完成了第 1 回合的加密操作。

第 2 回合加密操作由步骤 4 至步骤 6 描述。

步骤 4　$i\leftarrow 1$；并对前一子块的第 1 个像素分别采用式(9a)与式(9b)生成最终加密密钥且进行加密操作；同时对后一子块的第 1 个像素分别采用式(10a)与式(10b)生成最终加密密钥并进行加密操作。

$$\mathrm{Key}(i)=\mathrm{mod}(C(L)+K(i),256) \tag{9a}$$

$$C(i)=\mathrm{bitxor}(C(i),\mathrm{Key}(i)) \tag{9b}$$

$$\mathrm{Key}(L/2+i)=\mathrm{mod}(C(i)+K(L/2+i),256) \tag{10a}$$

$$C(L/2+i)=\mathrm{bitxor}(C(L/2+i),\mathrm{Key}(L/2+i)) \tag{10b}$$

步骤 5　$i\leftarrow i+1$，并对前一子块的第 i 个像素分别采用式(11a)与式(11b)生成最终加密密钥并进行加密操作；同时对后一子块的第 i 个像素分别采用与式(10a)和式(10b)相同的公式生成加密密钥并进行相应的加密操作。

$$\mathrm{Key}(i)=\mathrm{mod}(C(L/2+i-1)+K(i),256) \tag{11a}$$

$$C(i)=\mathrm{bitxor}(C(i),\mathrm{Key}(i)) \tag{11b}$$

步骤 6　重复步骤 5，直到 i=$L/2$，便完成了第 2 回合的加密操作，并得到密文图像 $\boldsymbol{C}$。

从上述加密过程可见，对图像像素加密所采用的最终加密密钥 Key(i)不仅与当前混沌密钥 $K(i)$有关，而且与另一子块前一个已经加密的密文像素值有关，即引入了密文交错扩散机制。因此，经过两个回合的加密后，任何像素值的变化都将影响到其余所有像素的密文值。

设解密图像用矩阵 $\boldsymbol{D}$ 表示，其像素值的表示形式类似于矩阵式(5)，按逐行扫描顺序所得的解密图像像素序列为$\{D(i),\ i$=$1,2,\cdots,L\}$，L 为图像像素总数。解密过程是加密过程的逆操作；但解密的像素顺序为逆序。2 个回合的解密操作共由 8 个步骤组成。

第 1 回合的解密操作由下列步骤 1 至步骤 4 描述。

步骤 1　$i\leftarrow L/2$。

步骤 2　对后半子块的第 i 个像素分别采用式(12a)和式(12b)生成解密密钥并进行解密：

$$\mathrm{Key}(L/2+i)=\mathrm{mod}(C(i)+K(L/2+i),256) \tag{12a}$$

$$C(L/2+i)=\text{bitxor}(C(L/2+i),\text{Key}(L/2+i)) \tag{12b}$$

对前半子块的第 i 个像素分别采用式(13a)和式(13b)生成解密密钥并进行解密操作：

$$\text{Key}(i)=\text{mod}(C(L/2+i-1)+K(i),256) \tag{13a}$$

$$C(i)=\text{bitxor}(C(i),\text{Key}(i)) \tag{13b}$$

步骤 3　$i\leftarrow i-1$, 并判断新的 i 值：如果 $i>1$，则执行步骤 2；否则，执行步骤 4。

步骤 4　对后半子块的第 1 个像素采用与式(12a)及式(12b)相同的计算公式生成密钥并进行解密操作；而对前半子块的第 1 个像素则分别采用式(14a)和式(14b)生成解密密钥并进行解密操作，于是完成了第 1 回合的解密。

$$\text{Key}(i)=\text{mod}(C(L)+K(i),256) \tag{14a}$$

$$C(i)=\text{bitxor}(C(i),\text{Key}(i)) \tag{14b}$$

第 2 回合的解密操作由下列步骤 5 至步骤 8 组成。

步骤 5　$i\leftarrow L/2$。

步骤 6　对后半子块的第 i 个像素分别采用式(15a)和式(15b)生成解密密钥并进行解密：

$$\text{Key}(L/2+i)=\text{mod}(C(i)+K(L/2+i),256) \tag{15a}$$

$$D(L/2+i)=\text{bitxor}(C(L/2+i),\text{Key}(L/2+i)) \tag{15b}$$

对前半子块的第 i 个像素则分别采用式(16a)和式(16b)生成解密密钥并进行解密：

$$\text{Key}(i)=\text{mod}(C(L/2+i-1)+K(i),256) \tag{16a}$$

$$D(i)=\text{bitxor}(C(i),\text{Key}(i)) \tag{16b}$$

步骤 7　$i\leftarrow i-1$, 并判断新的 i 值：如果 $i>1$，则执行步骤 6；否则，执行步骤 8。

步骤 8　对后半子块的第 1 个像素分别采用与式(15a)，式(15b)相同的公式生成解密密钥并进行解密操作；而对前半子块的第 1 个像素则分别采用式(17a)和式(17b)生成解密密钥并进行解密操作。

$$\text{Key}(i)=\text{mod}(C_0+K(i),256) \tag{17a}$$

$$D(i)=\text{bitxor}(C(i),\text{Key}(i)) \tag{17b}$$

完成步骤8的操作后，就得到了最终的解密图像 $\boldsymbol{D}$。

3　实验仿真与性能分析

实验中使用 256×256 的 8 位 Elaine 灰度图像和其它经典测试图像，在 Matlab7.1 下仿真。式(1)的系统参数取：a=27.5, b=3, c=19.3, d =2.9, e=3。这样，系统式(1)是超混沌的。取系统状态初值为(2.5,5.2,3.0,7.3)；微分方程组数值求解的时间步长取 0.001；其它参数为：N_0=1000, m=14, C_0=52。对原始 Elaine 图像进行 2 个回合的加密，加密前后的直观效果如图 3 所示。

(a) 原始 Elaine 图像　　(b) 加密 Elaine 图像

图 3 图像加密直观效果

3.1 密钥空间和执行效率分析

本文方案采用超混沌系统的 4 个状态变量初值作为原始密钥，用 15 位小数的双精度实数表示。因此，密钥空间可以达到 $10^{15}\times10^{15}\times10^{15}\times10^{15}=10^{60}\approx 2^{199}$，相当于 199 bit 的密钥长度。若将预迭代次数 N_0 和正整数 C_0 也作为原始密钥，则密钥空间更大。故本文算法具有抗穷举攻击的能力。实验硬件环境为 2.13 GHz Intel Celeron CPU, 2 GB 内存和 120 GB 硬盘的笔记本计算机；软件环境为 Windows XP+Matlab7.1 编译器。加密过程全部改用双字节整数运算，加密一幅 256×256 的灰度图像耗时约 0.047 s；比文献[13]的结果 0. 82 s 约快了 17 倍。效率提高的主要途径在于省去了置乱环节、采用整数运算且实行子图并行加密策略。

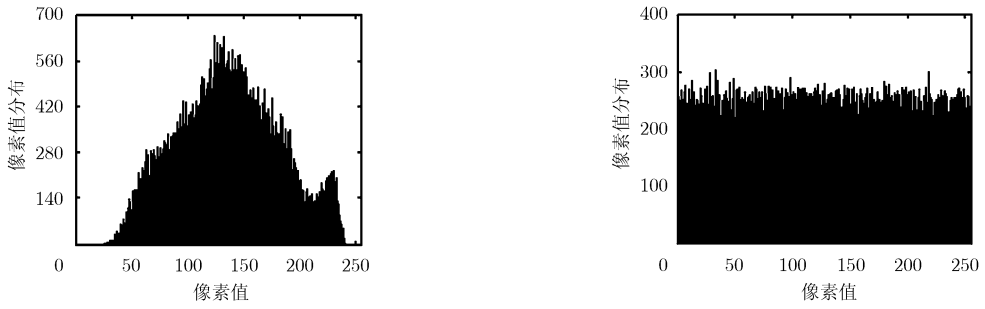
3.2 统计特性分析

(1)像素值分布特性　图 4 分别给出了 Elaine 明文图像和密文图像所对应的像素值分布直方图，由图 4(a)可见，原始图像的像素值分布是不均匀的；但图 4(b)表明，密文图像的像素值却呈现出平坦而均匀的分布特性，即加密图像的像素值在[0,255]范围内出现的概率几乎均等。因此，本文算法将能够有效地抵抗统计攻击。

(2)原始图像和加密图像的 2 维相关性　两个数据矩阵之间的 2 维相关系数定义为

$$C_{AB}=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(A_{ij}-\bar{A})(B_{ij}-\bar{B})}{\sqrt{\left(\sum_{i=1}^{M}\sum_{j=1}^{N}(A_{ij}-\bar{A})^2\right)\left(\sum_{i=1}^{M}\sum_{j=1}^{N}(B_{ij}-\bar{B})^2\right)}} \tag{18}$$

其中 A_{ij}, B_{ij} 分别代表明文、密文图像数据矩阵中位置(i, j)处的像素值。$\bar{A}$, $\bar{B}$ 分别代表明文、密文图



(a) 原始 Elaine 图像的像素值分布　　(b) 加密 Elaine 图像的像素值分布

图4 原始图像和加密图像的直方图

像的像素平均值。采用前述初始参数，对 4 幅标准测试图像进行加密实验，分别得到它们的密文图像和明文图像之间的 C_{AB}值，结果如表 1 所示。结果表明本文算法所得的加密图像和明文图像之间具有非常小的相关性(C_{AB}→0)。

(3)相邻像素之间的相关性分析　从图像中选取所有邻居像素对(包括水平、垂直和对角方向的 3 类邻居对)，用式(19)分别对每一类相邻像素之间的相关系数进行计算[11]：

$$r=\frac{\sum_{i=1}^{M_0}(x_i-\overline{x})(y_i-\overline{y})}{\sqrt{\left(\sum_{i=1}^{M_0}(x_i-\overline{x})^2\right)\left(\sum_{i=1}^{M_0}(y_i-\overline{y})^2\right)}} \tag{19}$$

其中 x_i和 y_i分别表示图像中第 i 组邻居像素的两个像素值；$\overline{x}$，$\overline{y}$ 分别为像素值 x_i 与 y_i的平均值；M_0 为邻居像素对的组数；r 即为相邻像素的相关系数。取与前所述相同的初始参数对 Lena 图像进行加密，计算加密前后图像 3 种方向的 r 系数，所得结果如表 2 第 2，第 3 列所示。尽管明文 Lena 图像的相邻像素存在高度相关性(r→1)；但对应密文图像的相邻像素已几乎不相关(r→0)。表 2 同时也给出了文献[11]和文献[13]同样基于超混沌的图像加密算法的相应结果。对比已有算法，本文算法所得的密文图像的 r 系数比文献[11]和文献[13]密文图像的所有 r 系数更低，表明本文算法对于打破相邻像素之间的相关性取得的效果更好。

表 1 4 种测试图像中密文与明文图像之间的相关系数

测试图像	Elaine	Lena	Cameraman	Barboon
相关系数	-9.77×10^{-5}	-3.24×10^{-4}	0.0037	0.0025

表 2 明文和密文 Lena 图像的相邻像素相关性

相邻方向	明文	密文	密文[11]	密文[13]
水平方向	0.9249	0.00210	−0.0142	0. 0064
垂直方向	0.9593	−0.00027	−0.0074	0. 0084
对角方向	0.9026	0.00093	−0.0183	0. 0107

3.3 抗差分攻击能力分析

对明文的敏感性越强，算法抵抗差分攻击的能力也就越强。可以用像素数改变率 NPCR (Number of Pixels Change Rate)指标度量加密算法对明文的敏感性；也可以用归一化像素值平均改变强度 UACI (Unified Average Changing Intensity)指标度量敏感性。当两个明文图像仅存在一个像素不同时，设它们的密文图像中第(*i*,*j*)点的像素值分别为 $C_1(i,j)$ 和 $C_2(i,j)$。若 $C_1(i,j)=C_2(i,j)$，定义 $D(i,j)=0$；若 $C_1(i,j)\neq C_2(i,j)$，定义 $D(i,j)=1$。则 NPCR 与 UACI 的计算公式分别为[1]

$$\mathrm{NPCR}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)\times100\% \tag{20}$$

$$\mathrm{UACI}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|c_1(i,j)-c_2(i,j)|}{255}\times100\% \tag{21}$$

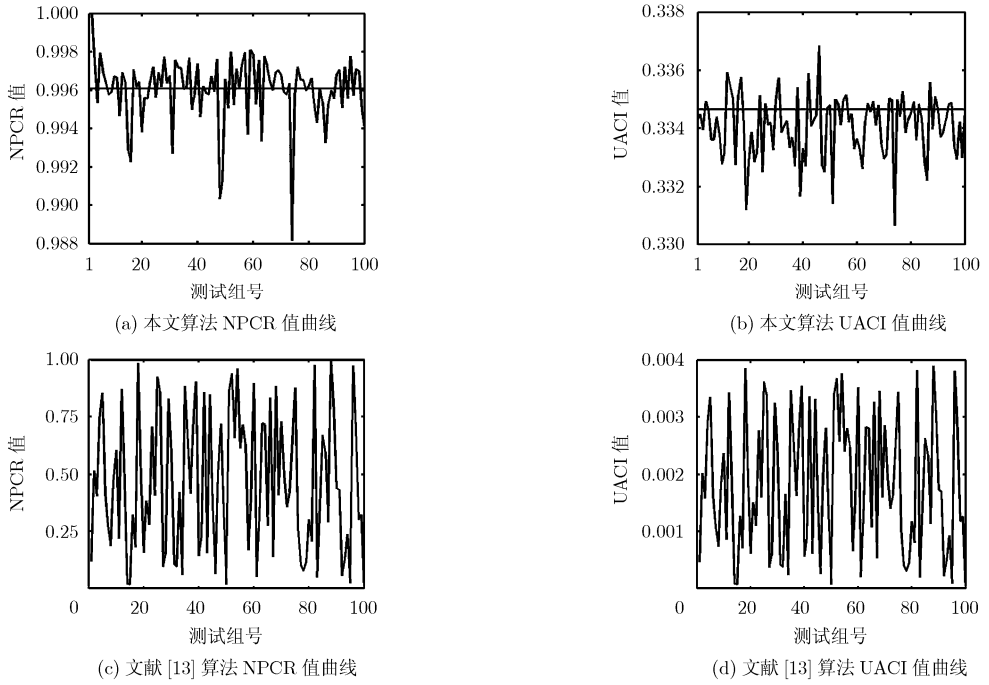
NPCR 与 UACI 的理想期望值可以用下列公式计算

$$\mathrm{NPCR}_E=(1-2^{-n})\times100\% \tag{22}$$

$$\mathrm{UACI}_E=\frac{1}{2^{2n}}\frac{\sum_{i=1}^{2^n-1}i(i+1)}{2^n-1}\times100\% \tag{23}$$

其中 M 和 N 分别是图像像素的行数与列数，n 为图像颜色位深。对于 8 位灰度图像(n=8)，NPCR 与 UACI 的理想期望值分别为 $\mathrm{NPCR}_E=99.6094\%$与 $\mathrm{UACI}_E=33.4635\%$。本文实验中，先后选取了 100 组 Lena 图像进行加密，每组 2 个图像，一个为原始图像，另一个则是对原始图像随机选择一个像素并使该像素的值改变 1(将最低比特位取反)，所得 100

组密文图像之间的NPCR与UACI值结果如图 5(a)和5(b)所示。图5(c)和5(d)同时给出了文献[13]算法加密结果。实验所得本文算法的NPCR与UACI值都分布在理想值(图中水平线)附近；并得到NPCR与UACI的平均值分别为$\overline{\text{NPCR}}$ =99.6057%和$\overline{\text{UACI}}$ =33.4049%，都非常接近相应的理想值。而文献[13]算法的NPCR与UACI的平均值分别为$\overline{\text{NPCR}}$ =46.1099%和$\overline{\text{UACI}}$ =0.1808%。可见，本文算法对明文的敏感性远远超过文献[13]算法对明文的敏感性。原因是文献[13]算法只在一轮像素替代操作过程中产生密文扩散效应，因此任何一个位置点的明文发生变化，仅仅只影响该点后面的密文发生变化。而本文算法设计了两轮替代操作，并进行交叉扩散，因此任何位置点的明文像素值发生变化，都将影响几乎所有点的密文发生变化。本文对图像加密 2 轮获得的$\overline{\text{NPCR}}$值高于文献[5]对图像加密 4 轮所得的平均值 99.5933533%，接近该文对图像加密 5 轮所得的平均值 99.6273041%；本文对图像加密 2 轮获得的$\overline{\text{UACI}}$值高于文献[5]加密 3 轮所得的平均值 33.3999634%，接近该文加密 5 轮所得的平均值 33.4815979%。因此，本文算法的抗查分攻击能力比文献[13]和文献[15]更强。



(a) 本文算法 NPCR 值曲线　(b) 本文算法 UACI 值曲线

(c) 文献 [13] 算法 NPCR 值曲线　(d) 文献 [13] 算法 UACI 值曲线

图 5 Lena 图像密文对明文的敏感性指标

3.4 对密钥敏感性的测试

一个好的加密算法应该对密钥具有强烈的敏感性，即密钥的微小变化，将导致密文截然不同。本文实验中先以$(x_{10}, x_{20}, x_{30}, x_{40})$=(2.5,5.2,3.0,7.3)为加密密钥，对 Cameraman 图像进行加密；然后用稍微不同的密钥对加密图像进行解密(解密密钥每次仅使其中 1 个初始变量改变10^{-10})，图 6 分别给出了正确密钥和 x_{10} 错误密钥的解密 Cameraman 图像。可见，密钥的微小差异导致不能正确解密。为了度量解密图像和原始图像的差别，引入均方误差MSE指标，设原始图像及其解密图像分别表示为 $\boldsymbol{P}=\{P(i,j)\}$和 $\boldsymbol{D}=\{D(i,j)\}$, i=1,2,…, M, j=1,2,…, N。则图像 $\boldsymbol{D}$ 与 $\boldsymbol{P}$ 之间的均方误差计算公式为

$$\text{MSE}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[D(i,j)-P(i,j)]^2 \qquad (24)$$

(a) 正确密钥 (2.5,5.2,3.0,7.3)　(b) 错误密钥(2.5000000001,5.2,3.0,7.3)

图 6 正确密钥和错误密钥的解密结果

对 Cameraman 图像，表 3 第 1 行给出了本文算法正确密钥及 4 组错误密钥所得解密图像分别与原始图像之间的均方误差值，结果表明，正确密钥可以实现完全精确解密；而具有微小错误的解密密

表 3 不同解密密钥的解密图像相对原始图像的均方误差

解密密钥	正确密钥	x_{10}误差 10^{-10}	x_{20}误差 10^{-10}	x_{30}误差 10^{-10}	x_{40}误差 10^{-10}
本文算法	0.00	9414.52	9419.76	9407.16	9302.89
文献[13]	0.00	9382.55	9418.81	9433.97	9418.45

钥所解密的图像将与原始图像相差巨大。这体现了算法对密钥的敏感性。表3第2行给出了文献[13]算法所得解密图像分别与原始图像之间的均方误差值。比较而言，本文算法对初始密钥x_{10}和x_{20}更敏感；而文献[13]算法对初始密钥x_{30}和x_{40}更敏感。这是由于两个超混沌系统的特性差异决定的。

3.5 信息熵分析

信息熵是反映信息的随机性的重要度量指标。设 s 代表一种信息源，则 s 的信息熵 $H(s)$可以用式(25)进行计算：

$$H(s)=-\sum_{i=0}^{2^n-1}P(s_i)\log_2[P(s_i)] \tag{25}$$

其中 $P(s_i)$表示符号 s_i 出现的概率，2^n 是信息源 s 的总状态数。对一个能发出 2^n 个符号的真随机信源，其信息熵就是 n。以一幅 256 级灰度图像作为信息源为例，其像素值有 2^8 种可能值，因此一幅 256 级灰度图像的理想信息熵应该是 8。如果一幅 256 级灰度图像的加密图像具有接近 8 的信息熵，则表明该密文图像接近随机分布。我们对标准 Lena 图像用本文算法加密，得到其密文图像信息熵为 7.9976，非常接近理想值 8。

3.6 混沌序列改进前后的加密性能对比

下面通过实验测试，对比本文改进混沌序列相对于原始混沌序列所得加密图像的性能差异。我们分别用图 1 的 $\boldsymbol{K}$ 序列与图 2 的 $\boldsymbol{K}0$ 序列得到中间混沌密钥，然后用本文相同的加密方法加密同样的 Lena 图像，对两种加密图像的主要统计指标(2 维相关性 C_{AB}，相邻像素的相关系数 r 及信息熵)进行计算，结果如表 4 所示。结果表明，用改进序列生成的密钥加密图像具有更小的相关系数但更大的信息熵，因此，得到的加密图像将具有更好的安全性。

表 4 混沌序列改进前后所得加密图像的统计结果对比

	C_{AB}	r(水平)	r(垂直)	r(对角)	信息熵
改进前	−0.0043	0.0033	0.0011	0.0014	7.9969
改进后	0.0019	0.0021	−0.0003	0.0009	7.9976

4 结束语

本文提出了改造新型超混沌系统混沌序列并结合密文交错扩散机制的并行加密思想，优化改造的超混沌序列具有更好的随机均匀分布特性。通过将待加密图像分块，以及对两个子块引入密文交错扩散和并行加密机制，提高了加密效率和密文对明文的敏感性。实验结果和分析表明，该算法具有如下特点：密钥空间大、加密效率高；加密图像像素具有均匀的统计分布特性；密文和明文以及相邻像素之间的相关性都非常趋近于零；算法具有较强的抗差分攻击能力和对密钥的高度敏感性。因此，本文提出的加密算法可以用于图像在因特网节点间、云计算核心与节点间的保密通信，以及图像信息保密存储等应用场合。

参 考 文 献

[1] Wang Y, Wong K W, Liao X, *et al*.. A new chaos-based fast image encryption algorithm[J]. *Applied Soft Computing*, 2011, 11(1): 514–522.

[2] 黄丽莲, 尹启天. 基于输出控制的混沌同步保密通信系统[J]. 电子与信息学报, 2009, 31(10): 2402–2405.
Huang Li-lian and Yin Qi-tian. A chaos synchronization secure communication system based on output control[J]. *Journal of Electronics & Information Technology*, 2009, 31(10): 2402–2405.

[3] Akhavan A, Samsudin A, and Akhshani A. A symmetric image encryption scheme based on combination of nonlinear chaotic maps [J]. *Journal of the Franklin Institute*, 2011, 348(8): 1797–1813.

[4] Yang H, Wong K W, Liao X, *et al*.. A fast image encryption and authentication scheme based on chaotic maps [J]. *Communications in Nonlinear Science and Numerical Simulation*, 2010, 15(11): 3507–3517.

[5] Zhu Z L, Zhang W, Wong K W, *et al*.. A chaos-based symmetric image encryption scheme using a bit-level permutation [J]. *Information Sciences*, 2011, 181(6): 1171–1186.

[6] Tong X and Cui M. Feedback image encryption algorithm with compound chaotic stream cipher based on perturbation[J]. *Science China Information Sciences*, 2010, 53(1): 191–202.

[7] Zhang G and Liu Q. A novel image encryption method based on total shuffling scheme[J]. *Optics Communications*, 2011, 284(12): 2775–2780.

[8] Wang X Y and Wang L L. A new perturbation method to the Tent map and its application[J]. *Chinese physics B*, 2011,

20(5): 500509.

[9] Guan Z H, Huang F J, and Guan W J. Chaos-based image encryption algorithm [J]. *Physics Letters A*, 2005, 346(1–3): 153–157.

[10] Özkaynak F and Özer A B. A method for designing strong S-Boxes based on chaotic Lorenz system[J]. *Physics Letters A*, 2010, 374(36): 3733–3738.

[11] Gao T and Chen Z. New image encryption algorithm based on hyper-chaos[J]. *Physics Letters A*, 2008, 372(4): 394–400.

[12] Rhouma Rhouma and Safya Belghith. Cryptanalysis of a new image encryption algorithm based on hyper-chaos[J]. *Physics Letters A*, 2008, 372(38): 5973–5978.

[13] 卢辉斌, 孙艳. 基于新的超混沌系统的图像加密方案[J]. 计算机科学, 2011, 38(6): 49–52.
Lu Hui-bin and Sun Yan. Image encryption scheme based on novel hyperchaotic system[J]. *Computer Science*, 2011, 38(6): 49–52.

[14] 陈小军, 李赞, 白宝明, 等. 一种基于模糊熵的混沌伪随机序列复杂度分析方法[J]. 电子与信息学报, 2011, 33(5): 1198–1203.
Chen Xiao-jun, Li Zan, Bai Bao-ming, *et al*.. A new complexity metric of chaotic pseudorandom sequences based on fuzzy entropy[J]. *Journal of Electronics & Information Technology*, 2011, 33(5): 1198–1203.

[15] Wang H X, Cai G L, Miao S, *et al*.. Nonlinear feedback control of a novel hyperchaotic system and its circuit implementation [J]. *Chines Physics B*, 2010, 19(3): 030509.

朱从旭： 男，1963 年生，教授，研究方向为网络信息安全、混沌密码学与混沌保密通信.

胡玉平： 男，1969 年生，教授，研究方向为信息隐藏、电子商务安全.

孙克辉： 男，1968 年生，教授，研究方向为混沌系统理论及其在信息安全中的应用.