基于 Logistic 和超混沌结合的加密算法

韩雪娟[1] 李国东[1] 王思秀[2]
(新疆财经大学应用数学学院 乌鲁木齐 830012)[1]
(新疆财经大学计算机科学与工程学院 乌鲁木齐 830012)[2]

摘 要 文中设计了一种置乱方案,同时改进了四维超混沌,基于该置乱方法和超混沌提出了双混沌图像的加密算法。该置乱方法先借助 Logistic 映射对图像进行两次置乱,再将经过置乱后的密文图像作为输入,结合改进的四维超混沌进行扩散,得到最终的密文图像。文中设计的算法将图像分块置乱和整体行列置乱结合起来,保证了像素的置乱率近为 100%。在扩散的过程中,通过改进的超混沌产生更具有伪随机性的密钥流进行多次加密,使得明文信息得到很好的隐藏。实验结果表明,该算法达到了比较好的加密效果,不仅敏感性强、密钥空间大,而且能够有效地抵御攻击,在图像信息安全方面具有一定的应用价值。

关键词 混沌,超混沌,图像加密,混沌加密
中图法分类号 TP309 **文献标识码** A

Cryptographic Algorithm Based on Combination of Logistic and Hyperchaos

HAN Xue-juan[1] LI Guo-dong[1] WANG Si-xiu[2]
(School of Applied Mathematics, Xinjiang University of Finance and Economics, Urumqi 830012, China)[1]
(School of Computer Science and Engineering, Xinjiang University of Finance and Economics, Urumqi 830012, China)[2]

Abstract In this paper, a scheme of scrambling was designed, and four-dimensional hyperchaos was improved. Based on the chaos method and hyperchaos, the algorithm of double chaos image encryption was proposed. The scrambled method uses Logistic map to scramble the image twice, then takes the scrambled ciphertext image as input, and diffuses it with the improved 4d hyperchaos to get the final ciphertext image. The algorithm designed in this paper combines the image block scrambling and the whole row and column scrambling to ensure the pixel scrambling rate of nearly 100%. In the process of diffusion, the key stream with more pseudo-randomness is generated through improved hyperchaos for multiple encryption, so that the plaintext information can be well hidden. The simulation results show that the algorithm has good encryption effect, not only has strong sensitivity and large key space, but also can resist attack effectively, and has certain application value in image information security.

Keywords Chaos, Super chaos, Image encryption, Chaos encryption

随着网络、科技的迅猛发展,越来越多的数字图像需要被更加保密的存储和传递,因此图像传递的保密性和安全性得到了广泛的关注。科学技术的发展在为生活带来很多便利的同时也在信息安全方面带来了不便之处:图像被窃取、保密文件在传输过程中被截取和解密、重要机密文件丢失。探索更加高效、安全的图像加密方法已经成为研究者的一个热点,近来年混沌研究已经成为学者的重点课题之一[1-5]。这些文章设计的加密方法主要利用某种混沌序列使图像点的位置或像素点灰度值的大小发生改变,以此来改变图像的整体布局。

超混沌是高维混沌,它和低维混沌对比来看:高维混沌序列拥有更好的伪随机性和更加复杂的动力学行为,而且如果使用能够破解低维混沌加密的方法,如相空间重构和非线性预测等,在破译经过超混沌加密的图像信息时都有一定的困难。所以,对于超混沌的研究越来越受学者的关注,成为研究热点之一[6-9]。许多学者在图像加密方面的文献中提到了各种不同类型的加密设计,张勋才等[10]针对 DNA 编码规则单一和混沌加密算法对密钥的灵敏度低等问题,提出了一种基于 DNA 编码和超混沌系统的图像加密方案。ZHANG 等[11]提出了一种基于混淆和扩散的图像加密方案,该方案具有效率性和有效性。Li 等[12]将混沌映射与分数阶 Fourier 变换相结合,实现了空间域和频域的置乱,使明文信息得到了隐藏。胡克亚等[13]解决了多图像加密系统数据量大的问题。

本文设计的加密算法将图像分块置乱和整体行列置乱相结合,对明文图像进行了两次置乱,明显提高了像素的置乱程度;在扩散的过程中通过改进的超混沌产生更具有伪随机性的密钥流进行多次加密,解决了密文容易破解的问题,具有一定的应用价值。

本文受国家自然科学基金(11461063),自治区自然科学基金(2017D01A24),自治区自然科学基金(2017D01A23),自治区高校科研计划青年项目(XJEDU2017S036)资助。

韩雪娟(1995-),女,硕士,主要研究方向为数据分析与图像处理,E-mail:1453545232@qq.com;**李国东**(1976-),男,博士,教授,主要研究方向为数据分析与图像处理,E-mail:lgdzhy@126.com(通信作者)。

1 加密算法的设计

1.1 加密原理

针对单一混沌系统的安全性不高等问题，本文设计了一种置乱方案，同时对四维超混沌进行了改进，结合该置乱方法和超混沌提出了一种双混沌图像加密算法。该算法不但避免了加密图像能够轻易被破解的问题，而且提高了加密图像的安全性。在置乱部分，先利用 Logistic 混沌映射迭代处理产生 2 个不同的混沌序列，分别截取不同的 $1/4*m*n$ 项得到序列 a_1'，a_2'，a_3'，a_4'对 $2*2$ 个子块进行像素置乱；将经过一次置乱后的分块矩阵合并成 $m*n$ 的大矩阵，对大矩阵分别进行行列置乱；具体的方法是根据 Logistic 产生的混沌序列落入 $m(n)$个区间的号码进行行列置乱。在扩散部分，利用改进的四维超混沌产生的伪随机序列设计密钥流，通过设计的密钥流将图像分为 3 部分，对两次置乱后的加密图像进行像素值异或，按照选取的序列进行多次加密处理。

1.2 置乱算法的设计

在图像置乱时，如果只使用一个混沌对图像进行置乱，密文图像较容易被破解。本文设计的置乱算法通过迭代 Logistic 混沌映射产生不同的混沌序列对图像进行了两种不同方法的置乱，既有分块置乱又有整体行列置乱，使明文信息的混乱程度加强，大大提高了图像信息的安全性。

1.2.1 混沌序列的分析

Logistic 映射是一种典型的动力系统，对 Logistic 映射的迭代操作会出现混沌的现象，Logistic 的动力学方程为：

$$x_{n+1}=\mu x_n(1-x_n),x\in[0,1],\mu\in(0,4] \tag{1}$$

Logistic 混沌映射的混沌行为受 μ 大小变化的影响，当取初始值 x 为 0.291 582 630 2 时，将混沌映射迭代 2 000 次，随着 μ 值变化，该模型由起初的倍分岔逐步演化为混沌状态。

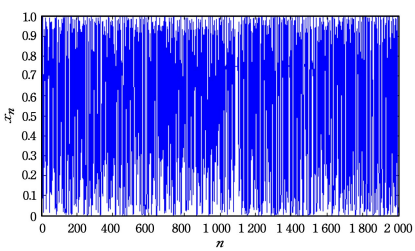


图 1 Logistic 映射时域图

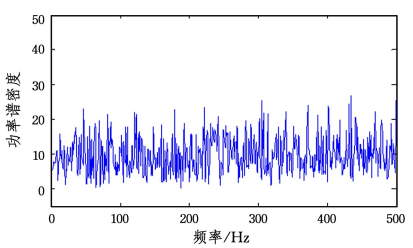


图 2 Logistic 映射频谱图

本文中，Logistic 混沌映射的初值：$a_1=0.291\,582\,630\,2$，$b_1=0.1$，参数 $u=4.0$。

1.2.2 置乱算法的描述

(1)一次置乱

设原始图像为 P，大小为 $s*t$，将原始图像填充成大小为 $m*n$ 的图像，填充元素为黑色，构成新的图像 P'。

将 P'平均分为 4 块 $1/2m*1/2n$ 的图像，记为 P'_1，P'_2，P'_3，P'_4，表示如下：

$$\begin{aligned}P_1'&=(P'_{11},P'_{12},P'_{13}\cdots P'_{1\,1/4*m*n})\\P_2'&=(P'_{21},P'_{22},P'_{23}\cdots P'_{2\,1/4*m*n})\\P_3'&=(P'_{31},P'_{32},P'_{33}\cdots P'_{3\,1/4*m*n})\\P_4'&=(P'_{41},P'_{42},P'_{43}\cdots P'_{4\,1/4*m*n})\end{aligned} \tag{2}$$

伪随机序列的构造过程是首先迭代 Logistic 混沌映射产生长度为 $1/3*m*n$ 的混沌序列：

$$a=(a_1,a_2,a_3\cdots a_{1/3*m*n}) \tag{3}$$

分别任意截取序列 a，得到长度为 $1/4*m*n$ 的 a_1'，a_2'，a_3'，a_4' 4 个序列，表示如下：

$$\begin{aligned}a_1'&=(a_{11},a_{12},a_{13}\cdots a_{1\,1/4*m*n})\\a_2'&=(a_{21},a_{22},a_{23}\cdots a_{2\,1/4*m*n})\\a_3'&=(a_{31},a_{32},a_{33}\cdots a_{3\,1/4*m*n})\\a_4'&=(a_{41},a_{42},a_{43}\cdots a_{4\,1/4*m*n})\end{aligned} \tag{4}$$

对序列 a_1'，a_2'，a_3'，a_4'做如下处理，目的是得到取值在[1，$1/4*m*n$]之间的整数序列 a_1''，a_2''，a_3''，a_4''：

$$\begin{aligned}a_1''&=ceil(\mathrm{mod}(a_1'*10^{14},1/4*m*n))\\a_2''&=ceil(\mathrm{mod}(a_2'*10^{14},1/4*m*n))\\a_3''&=ceil(\mathrm{mod}(a_3'*10^{14},1/4*m*n))\\a_4''&=ceil(\mathrm{mod}(a_4'*10^{14},1/4*m*n))\end{aligned} \tag{5}$$

位置置乱公式为：

$$\begin{aligned}P''_{1j}&=P'_{1a''_{1j}}\\P''_{2j}&=P'_{2a''_{3j}}\\P''_{3j}&=P'_{3a''_{4j}}\\P''_{4j}&=P'_{4a''_{2j}}\end{aligned},j=1,2,3,\cdots,1/4*m*n \tag{6}$$

将经过位置置乱后得到的序列 P_1''，P_2''，P_3''，P_4''合成大小为 $m*n$ 的矩阵 $\boldsymbol{Q}$，$\boldsymbol{Q}$ 即为一次置乱矩阵。

(2)二次置乱

首先把 Logistic 混沌序列的取值范围 $\theta\in(0,1)$平均分成 m 个小区间，并对这 m 个小区间按照区间均值的大小进行排序，记为：

$$W=(W_1,W_2,W_3,\cdots,W_m) \tag{7}$$

利用 Logistic 映射产生长度为 $1/2m*1/2n$ 的混沌序列：

$$\boldsymbol{b}=(b_1,b_2,b_3\cdots b_{\frac{1}{2}*m*n}) \tag{8}$$

任意截取 $\boldsymbol{b}$ 中长度为 m 的序列 $\boldsymbol{b}'=(b_1',b_1',b_3',\cdots,b_m')$对矩阵 $\boldsymbol{Q}$ 进行行置乱，置乱公式为：

$$\begin{aligned}&Q'(i,:)=Q(k,:),b_i'\in W_k,i=1,2,3,\cdots,m,\\&k=1,2,3,\cdots,m\end{aligned} \tag{9}$$

同理，把 $\theta\in(0,1)$区间平均分成 n 个小区间，对这 n 个区间按照均值大小排序，记为：

$$W'=(W_1',W_2',W_3',\cdots,W_n') \tag{10}$$

迭代 Logistic 映射产生混沌序列 $\boldsymbol{b}$，任意截取 $\boldsymbol{b}$ 中长度为 n 的序列 $\boldsymbol{b}''=(b_1'',b_1'',b_3'',\cdots,b_n'')$对行置乱后的矩阵进行列置乱，置乱公式为：

$$\begin{aligned}&Q''(:,j)=Q'(:,l),b_i''\in W_l',j=1,2,3,\cdots,n,\\&l=1,2,3,\cdots,n\end{aligned} \tag{11}$$

将经过两次置乱的矩阵记为 Q''，大小为 $m*n$。

1.3 扩散算法的设计

结合超混沌系统应用于图像加密的优点，本文对超混沌系统进行了改进。因此扩散算法具有以下几个优点：产生了更加理想的混沌序列；在进行扩散操作时将图像平均分成了 3 部分，对这 3 部分分别采用不同的密钥流进行异或处理，增加了解密的难度；利用产生的密钥流对图像进行了 3 次加密，更好地隐藏了明文信息。

1.3.1　超混沌序列的分析及改进

本文采用的是超混沌系统[14]，其动力学方程如下：

$$\begin{aligned} x_1 &= a(x_2 - x_1) + x_4 \\ x_2 &= dx_2 - x_1 x_3 + cx_2 \\ x_3 &= x_1 x_2 - bx_3 \\ x_4 &= x_2 x_3 + rx_4 \end{aligned} \tag{12}$$

其中，$a=35$，$b=3$，$c=12$，$d=7$，$r=0.6$，在混沌迭代了 $m*n+200$ 次的条件下，系统有 3 个正的 Lyapunov 指数 5.5765，7.2346 和 0.5904，呈现超混沌行为，表现出了比一般混沌系统更加复杂的特性，图 3 是超混沌的 Lyapunov 指数频谱图和超混沌吸引子在平面上的投影图。

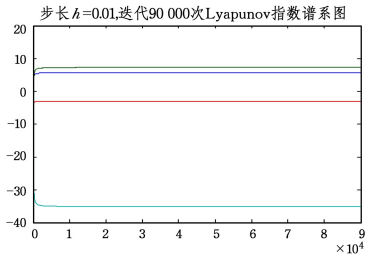
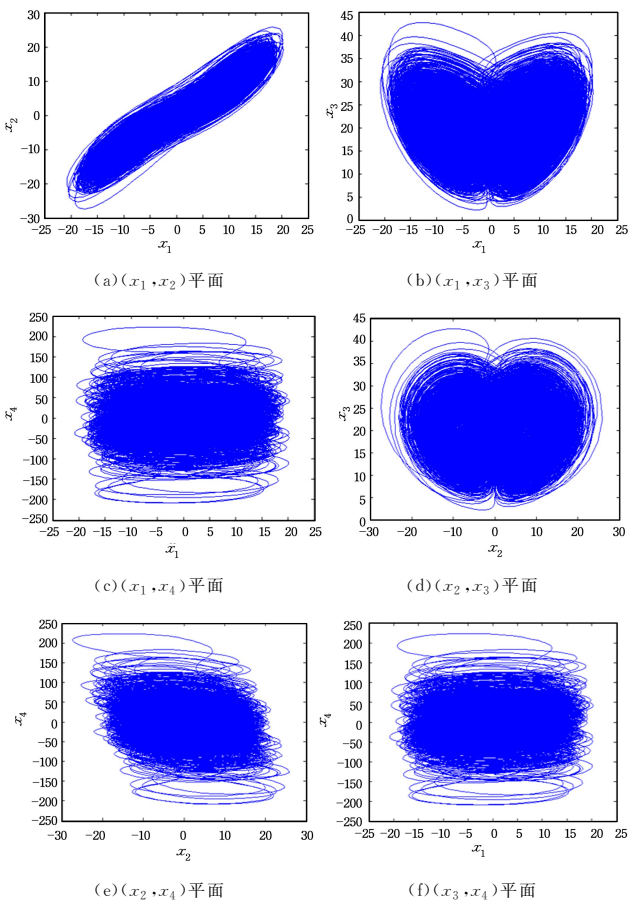


图 3　Lyapunov 指数频谱图



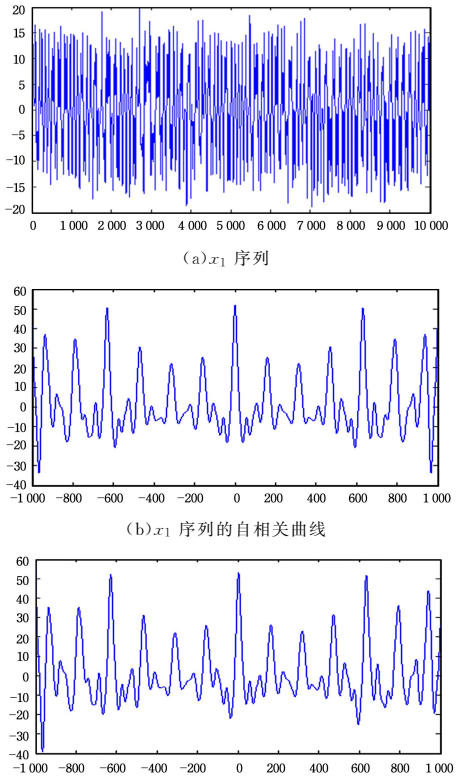
(a)(x_1，x_2)平面　(b)(x_1，x_3)平面

(c)(x_1，x_4)平面　(d)(x_2，x_3)平面

(e)(x_2，x_4)平面　(f)(x_3，x_4)平面

图 4　系统的超混沌吸引子在平面上的投影

理想的混沌序列应该具有如下特性：1）服从均匀分布；2）自相关是冲激函数；3）互相关为零。当 a，b，c，d，r 取值保持不变时，在初值 $x_{10}=0.5$，$x_{20}=0.008$，$x_{30}=0.02$，$x_{40}=0.3$ 的条件下，采用 Runge-Kutta 法求解混沌序列，结果如图 5 所示（以 x_1 序列为例）。通过分析可以发现，这些序列并不是很理想的伪随机序列。



(a)x_1 序列

(b)x_1 序列的自相关曲线

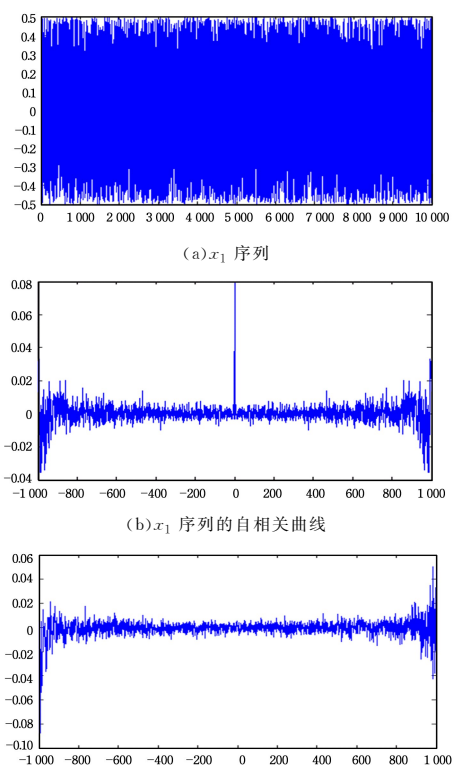
(c)x_1 的互自相关曲线

图 5　混沌序列 x_1 的自相关和互自相关特性

对混沌序列通过式(13)进行改进：

$$x_i = 10^4 * x_i - round(10^4 * x_i) \tag{13}$$

图 6 给出了改进之后的混沌序列 x_1 的统计特性，对混沌序列 x_2，x_3，x_4 也进行同样的改进。



(a)x_1 序列

(b)x_1 序列的自相关曲线

(c)x_1 的互自相关曲线

图 6　改进后混沌序列 x_1 的自相关和互自相关特性

由图 6 可以看出，x_1 序列经过处理之后，值域范围由原来的 $-20<x_1(i)<25$ 变为 $-0.5<x_1(i)<0.5$，明显变小；自

相关也呈冲击状，互自相关特性明显变好，说明改进之后的混沌序列比改进之前的混沌序列具有更强的为随机性。

1.3.2 扩散算法的描述

超混沌系统迭代 $m*n+200$ 次，舍弃前 200 次迭代产生的数据，得到改进后的序列为：

$$\begin{aligned} x_1&=\{x_{1k}\mid k=1,2,\cdots,m*n\}\\ x_2&=\{x_{2k}\mid k=1,2,\cdots,m*n\}\\ x_3&=\{x_{3k}\mid k=1,2,\cdots,m*n\}\\ x_4&=\{x_{4k}\mid k=1,2,\cdots,m*n\} \end{aligned} \tag{14}$$

计算如下变量：

$$x_i=\mathrm{mod}((abs(x_i)-floor(abs(x_i)))*10^{14},256),i=1,2,3,4,x_i\in[0,255] \tag{15}$$

$$y=\mathrm{mod}((a+b)*10^{14},3) \tag{16}$$

任意截取 y 中的 3 个数得到序列 $\boldsymbol{y}'=\{y_k'\mid k=1,2,3\}$，根据 $y'\in[0,2]$ 的取值，在表 1 中选择相对应的密钥对最终置乱后的矩阵进行加密，具体加密过程如下：

$$\begin{aligned} C_{3*(i-1)+1}&=P^{\pi}_{3*(I-1)+1}\oplus D_{x1}\\ C_{3*(i-1)+2}&=P^{\pi}_{3*(I-1)+2}\oplus D_{x2}\\ C_{3*(i-1)+3}&=P^{\pi}_{3*(I-1)+3}\oplus D_{x3} \end{aligned} \tag{17}$$

其中，D_{x1}，D_{x2}，D_{x3} 如式(18)所示：

$$\begin{aligned} D_{x1}&=\mathrm{mod}((B_{x1}\oplus C_{3*(i-1)}),256)\\ D_{x2}&=\mathrm{mod}((B_{x2}\oplus C_{3*(i-1)+1}),256)\\ D_{x3}&=\mathrm{mod}((B_{x3}\oplus C_{3*(i-1)+2}),256) \end{aligned} \tag{18}$$

其中，$D_x\in[0,255]$，C_0 由设计者自行决定，$i=1,2,\cdots$ 表示第 i 次超混沌迭代。

表 1 超混沌序列的不同组合

y'	对应组合
0	(x_1,x_3,x_4)
1	(x_1,x_2,x_3)
2	(x_2,x_3,x_4)

2 本文算法的原理与实现

加密过程流程图如图 7 所示。

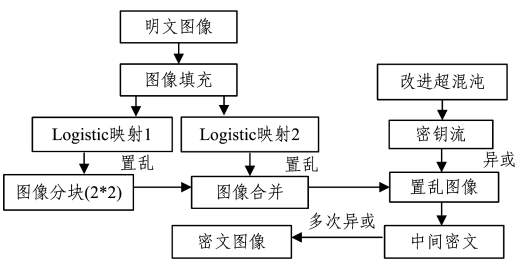


图 7 加密过程流程图

本文算法的主要步骤如下：

(1)获取样本图像的像素数字矩阵 $\boldsymbol{P}$，将原始图像填充成长和宽均为偶数的图像(用黑色填充)，处理后的图像大小为 $m*n$。

(2)通过对 Logistic 混沌映射进行迭代，产生混沌序列：$a=\{a_k\mid k=1,2,\cdots,1/2*m*n\}$，分别截取序列 a 的前 $1/4*m*n$ 项，后 $1/4*m*n$ 项以及任意取长度为 $1/4*m*n$ 两项，得到序列 a_1'，a_2'，a_3'，a_4'。

(3)对明文图像进行 $2*2$ 分块，利用处理后的序列 a_1''，a_2''，a_3''，a_4'' 对 4 个分块序列进行位置置乱。具体的方法是：分别用 a_1'' 和 a_2'' 对主对角线上的 2 个分块进行置乱，分别用 a_3'' 和 a_4'' 对副对角线上的 2 个分块进行置乱。

(4)将 4 个矩阵子块合并成 $m*n$ 的大矩阵 $\boldsymbol{Q}$，然后利用 Logistic 混沌映射迭代产生混沌序列 $b=\{b_k\mid k=1,2,\cdots,1/2*m*n\}$。将 $\theta\in(0,1)$ 划分成 m 个小区间并且对小区间进行从 1 到 m 的编号，任意截取 b 序列中长度为 m 的序列，得到序列 b'，判断序列 b' 中的值落入 m 个小区间中的几号区间，就对矩阵 $\boldsymbol{Q}$ 的第几行进行置乱，直到判断完序列 b' 中的所有值，得到矩阵 $\boldsymbol{Q}'$。同理，将 $\theta\in(0,1)$ 划分成 n 个小区间并且对小区间进行从 1 到 n 的编号，任意截取 b 序列中长度为 n 的序列，得到序列 b''，判断序列 b'' 中的值落入 n 个小区间中的几号区间，就对矩阵的第几列进行置乱，直到判断完序列 b'' 中所有值，得到矩阵 $\boldsymbol{Q}''$。

(5)利用 Runge-Kutta 算法解超混沌，产生超混沌序列，为了防止过渡效应，本文将舍弃前 200 次迭代产生的数据。

(6)对改进后的超混沌系统进行迭代，产生随机序列 x_1，x_2，x_3，x_4，利用式(4)计算 $x_i(i=1,2,3,4)$，然后按照式(5)计算 y。

(7)任意截取 y 中的 3 个数，根据 $y'=(0,1,2)$，从表 1 中选取相应组合，根据式(17)和式(18)对置乱后的矩阵进行加密。

(8)按照序列 y' 对图像分别进行 3 次扩散，得到最终的密文图像。

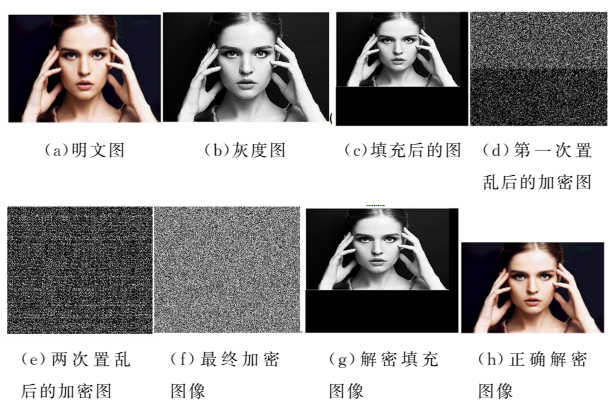
(9)解密过程是加密过程的逆过程，只需要在公式中稍作改变。首先使用改进后的超混沌产生相同的混沌序列，再将式(17)改为：

$$\begin{aligned} P^{\pi}_{3*(I-1)+1}&=C_{3*(i-1)+1}\oplus D_{x1}\\ P^{\pi}_{3*(I-1)+2}&=C_{3*(i-1)+2}\oplus D_{x2}\\ P^{\pi}_{3*(I-1)+3}&=C_{3*(i-1)+3}\oplus D_{x3} \end{aligned} \tag{19}$$

然后，进行加密过程的逆过程即可。

3 仿真实验

通过本文设计的加密算法对图 8(a)进行加密，将明文图像转化为灰度图 8(b)，对灰度图进行填充得到图 8(c)，利用 Logistic 混沌映射对填充后的图进行分块置乱从而得到第一次置乱图 8(d)，从图中可以看出，第一次置乱加密图呈现出上下两部分的明暗分块；再次使用 Logistic 混沌映射对图像进行第二次置乱，经过两次置乱后得到最终置乱的加密图像 8(e)，置乱后的图像已经很难看出具体的信息。



(a)明文图 (b)灰度图 (c)填充后的图 (d)第一次置乱后的加密图

(e)两次置乱后的加密图 (f)最终加密图像 (g)解密填充图像 (h)正确解密图像

图 8 加密效果图

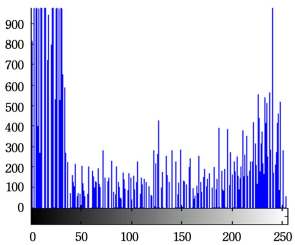
利用超混沌对两次置乱后的图进行扩散加密，在经过多次的加密过程处理后，从最终的密文图像中去分辨原图的图

像特征是相当困难的,从加密的仿真结果来看,最终的加密图像杂乱无章,完全看不出原图像的样子,因此可知加密效果较好。

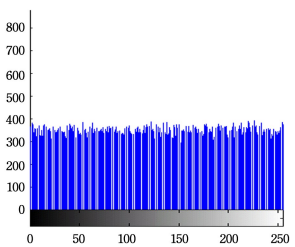
4　结果检验——性能分析

4.1　直方图统计特性分析

如果直方图越平稳,则密文图像的安全性就越高。由图 9 可知,能量分布有很大的不同,灰度值出现的概率有明显的差异,加密后的图像像素出现的频率基本相同,较为平滑,随着序列次数的增进,密文直方图像素的能量的分布越均匀;密文图像的直方图更加平稳,波动程度小,可以有效地抵抗攻击。



(a)明文直方图

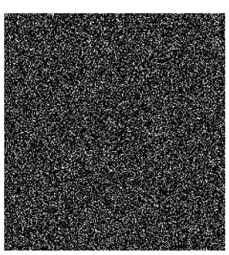


(b)密文图像

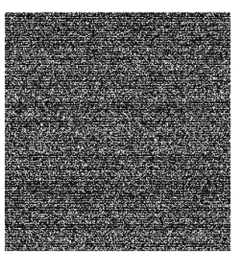
图 9　对实验样本图像进行直方图分析

4.2　密钥敏感性分析

(1)Logistic 映射具有复杂动态性能,微弱的数字差就会得出完全不同的密文,也还原不出明文;将 Logistic 的密钥增加 0.000000000000001,利用相同的算法解密将会发生错误,如图 10(a)所示。



(a)Logistic 的 Key 发生错误的解密图



(b)超混沌的 Key 发生错误的解密图

图 10　发生错误的解密图像

(2)对于超混沌的密钥敏感性,本文将超混沌的参数 r=0.6 改为 r=0.600000001 时对图像进行解密,如图 10(b)所示。

根据图 10 可以看出:即使使用与正确密钥相差极小的密钥进行解密,得到的解密图与原始图像相差很大,说明了本文算法对密钥具有高度的敏感性。

4.3　抗差分攻击能力分析

NPCR(像素改变率):当明文中任意像素值发生微小变化时,密文发生明显的改变,其像素值发生变化的比率。NPCR 的理论期望值为 99.6094%。UACI(归一化平均改变强度):不仅比较相应位置的像素点的值'不同'外,还计算了'不同'的程度。UACI 的理论期望值为 33.4635%。

$$NPCR=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)}{M\times N}\times 100\% \tag{20}$$

$$UACI=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|D_1(i,j)-D_2(i,j)|}{255}\times 100\% \tag{21}$$

其中,D_1 为密文图像,D_2 表示明文图像像素值发生改变时的密文。任取明文图像中的坐标,对该坐标进行微小的改变,如像素点(10,159)转化为(10,159)得到 NPCR 和 UACI 值。

表 2　NPCR 与 UACI

(单位:%)

	明文	本文算法	文献[7]算法
NPCR	99.89	99.70	99.72
UACI	38.80	33.47	33.74

从表 2 可以发现:本文算法的 NPCR 和 UACI 值更加接近于理想值,因此本文算法的抗差分攻击能力较强。

4.4　信息熵分析

信息熵反应图像信息的不确定性,信息熵越大,可视信息就越少,如式(22)所示:

$$H=-\sum_{i=0}^{L}p(i)\log_2 p(i) \tag{22}$$

其中,L 表示图像的灰度等级数,$p(i)$为灰度值 i 出现的概率。当 L=256 时,信息熵 H 的理论值为 8。文献[7]算法的信息熵为 7.99667,本文算法计算的信息熵 H=7.9980,更加接近 8,因此本文的加密算法能够较好的抵抗统计攻击。

4.5　相邻像素的相关性分析

在明文图像和密文图像中随机地选取 N 对像素值,计算在水平、垂直和对角方向上的相关系数。

$$r_{xy}=\frac{\mathrm{cov}(\boldsymbol{u},\boldsymbol{v})}{\sqrt{D(\boldsymbol{u})}\sqrt{D(\boldsymbol{v})}} \tag{23}$$

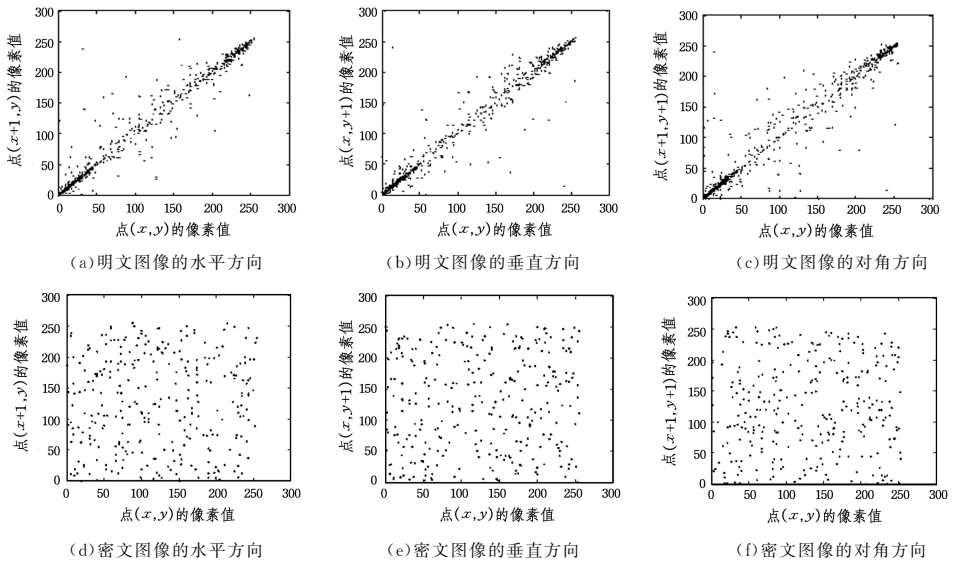
$$cov(\boldsymbol{u},\boldsymbol{v})=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(\boldsymbol{u}))(y_i-E(\boldsymbol{v})) \tag{24}$$

$$D(\boldsymbol{u})=\frac{1}{N}\sum_{i=1}^{N}(u_i-E(\boldsymbol{u}))^2 \tag{25}$$

$$E(\boldsymbol{u})=\frac{1}{N}\sum_{i=1}^{N}u_i \tag{26}$$

设 u_i 的坐标为(x_i,y_i),当 v_i 的坐标为(x_i+1,y_i)时,表示水平方向上的相关系数;当 v_i 的坐标为(x_i,y_i+1)时,表示垂直方向上的相关系数;当 v_i 的坐标为(x_i+1,y_i+1)时,表示正对角上的相关系数;当 v_i 的坐标为(x_i-1,y_i+1)时,表示反对角上的相关系数。

由图 11 可以看出:明文图像在各个方向上具有明显的线性关系,密文图像在各个方向上的相邻点几乎没有任何关系。从表 3 中的数据可以得到:密文的相关系数几乎为零,并且相关性低于文献[7]算法计算的相关性,说明本文算法的抗统计能力很强,按照此法加密的效果较好。



(a)明文图像的水平方向 (b)明文图像的垂直方向 (c)明文图像的对角方向

(d)密文图像的水平方向 (e)密文图像的垂直方向 (f)密文图像的对角方向

图 11 明文与密文的相邻像素相关性散点图

表 3 相关系数

方向	明文图像	密文图像	文献[7]算法
水平方向	0.9782	0.0022	−0.0032
垂直方向	0.9581	−0.0018	−0.0063
对角方向	0.9433	−0.0028	0.0086

4.6 密钥空间分析

本文算法采用了双混沌映射的初值及参数作为初始条件的密钥,参数选择至少达到 10^{80},为算法提供了相当大的密钥空间,因此想要破解此密文图像很难实现。

结束语 本文设计的双混沌图像加密算法是在 Windows 8 操作系统上,以 Matlab 2017 作为实验平台进行实验的。本文设计的置乱算法首先通过 Logistic 混沌映射产生的序列对图像进行两次像素位置的置乱:第一次是分块置乱,对 4 个分块矩阵的每个像素位置进行置乱;第二次是在第一次分块置乱基础上进行合并置乱,判断混沌序列的数值进入的区间编号进行整体行列置乱;最后运用改进的超混沌产生的随机序列对最终置乱后的图像进行扩散处理。该算法解决了传统系统在单一领域内使用某一方法而削减了参量导致系统结构简单、易被攻击、安全性低的问题。该算法具有更大的密钥空间,密钥的敏感性强,安全性级别高,综合上述内容,该算法不仅有很好的加密效果,而且有非常强的抗破译能力。

参 考 文 献

[1] 徐潇,马峻,赵飞乐,等. Arnold 变换和混沌映射的计算全息多图像同步加密[J]. 激光杂志,2018,39(6):57-60.

[2] LIU C,LIU Y,ZHANG L Y,et al. Cryptanalyzing a class of image encryption schemes based on Chinese remainder theorem [J]. Signal Process-image,2014,29:914-920.

[3] 徐兵,袁立. 基于改进 Logistic 混沌映射的数字图像加密算法研究[J]. 计算机测量与控制,2014(7):165-167.

[4] RAMADAN N,AHMED H,ELDIN H,et al. Permutation-substitution image encryption scheme based on a modified chaotic map in transform domain[J]. Journal of Central South University,2017,24(9):2049-2057.

[5] 张颖,杨玥. Arnold 双置乱图像加密算法[J]. 辽宁工程技术大学学报(自然科学版),2013,32(10):1429-1432.

[6] 朱淑芹,王文宏,孙忠贵. 对一种基于比特置乱的超混沌图像加密算法的选择明文攻击[J]. 计算机科学,2017,44(11):273-278.

[7] 林青,王延江,王珺. 基于超混沌系统的图像加密算法[J]. 中国科学:技术科学,2016,46(9):910-918.

[8] 杨志宏,屈双惠,张彩霞,等. 一个四翼超混沌系统在图像加密技术中的应用[J]. 西南大学学报(自然科学版),2018,40(5):170-177.

[9] VASILEIOS B,CHRIS G. Antonopoulos. Hyperchaos & labyrinth chaos: revisiting Thomas-Rössler systems[J]. Journal of Theoretical Biology,2018.

[10] 张勋才,刘奕杉,崔光照. 基于 DNA 编码和超混沌系统的图像加密算法[J]. 计算机应用研究,2019(4):1-6.

[11] ZHANG S,YANG L,ZHANG Y,et al. A Bit Level Encryption Scheme Based on Hyper-chaotic System Combing with the Ideology of Central Dogma[J]. Chinese Journal of Electronics,2018,27(3):595-602.

[12] LI G D,WANG L L. Double chaotic image encryption algorithm based on optimal sequence solution and fractional transform [J]. Visual Computer,2018,1(1):1-11.

[13] 胡克亚,王君,王莹. 基于分块压缩感知和改进幻方变换的图像加密[J]. 激光技术,2018:1-11.

[14] 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[J]. 物理学报,2011,60(6):83-93.