doi:10.3969/j.issn.1000-436x.2014.03.025

像素位置与比特双重置乱的图像混沌加密算法

邓晓衡，廖春龙，朱从旭，陈志刚
(中南大学 信息科学与工程学院，湖南 长沙 410083)

摘 要：针对当前流行的一类具有置乱—扩散结构的混沌图像加密算法存在的安全缺陷问题，提出了一种能抵抗选择明(密)文攻击的图像加密算法。算法采用 Kent 混沌映射生成密钥序列，并根据明文像素值的特征和输入的密钥，分别产生混沌系统的参数和预迭代次数。首先，利用混沌序列实现图像像素位置的全局置乱；其次，根据另一个新生成的混沌序列，实现对图像像素值中 0 bit、1 bit 的置乱。实现了混沌映射产生的序列与图像本身内容的关联，从而实现了中间密钥随明文自适应变化，能有效抵抗选择明(密)文攻击。实验结果表明，该算法克服了以往算法不能抵抗选择明(密)文攻击的缺陷，同时具有加密算法简单、密钥空间大等加密性能，并能较好地抵抗统计特性分析、差分分析攻击。

关键词：图像加密；混沌系统；像素置乱；比特置乱
中图分类号：TP309.7 **文献标识码**：A **文章编号**：1000-436X(2014)03-0216-08

Image encryption algorithms based on chaos through dual scrambling of pixel position and bit

DENG Xiao-heng, LIAO Chun-long, ZHU Cong-xu, CHEN Zhi-gang
(School of Information Science and Engineering, Central South University, Changsha 410083, China)

Abstract: As the current popular chaos-based image encryption algorithms with the permutation–diffusion structure have security flaws of no immunity to attack. A new image encryption algorithm was proposed based on the analysis of current algorithms, which can well resist the chosen-plaintext and the chosen-ciphertext attacks. The algorithm uses Kent chaotic map to generate key streams, and produces the parameters of the chaotic system and the iteration times according to the characteristics of plaintext pixels and input key. Firstly, the positions of pixels were shuffled totally with the chaotic sequence. Secondly, the 0 and 1 bit positions of image pixels were scrambled by using another chaotic sequence generated by the input key. The experimental results show that the algorithm cannot only resist the chosen plaintext attack and chosen ciphertext attack but also achieve better cryptographic properties,such as key space, statistical analysis.

Key words: image encryption; chaotic system; pixels scrambling; bit scrambling

1 引言

随着互联网的发展，越来越多的信息以数字化的形式存储和传送，在数字化的信息中，图像信息因具有形象性、直观性和生动性等优点而被广泛使用。因此，图像信息的安全性越来越受到重视，各种不同的加密算法也应运而生[1~3]。由于图像信息具有数据量大、数据之间的相关性高等特点，使传统密码学对图像数据的加密遭遇了效率低的困难[4]；而混沌因其具有对初始条件的极端敏感性、无周期性、伪随机性、混沌序列的遍历性等密码学特性以及混沌序列能大量地快速产生和准确再生，使其特别适合于图像加密。于是，学者们先后提出了许多基于混沌系统的图像加密算法[5~10]。

根据现代密码学原理，安全性高的密码算法需具有如下几个基本特征：第一，应该具有足够大的

收稿日期：2012-07-24；**修回日期**：2013-11-01
基金项目：国家自然科学基金资助项目(61379058, 61379057,61350011, 60903058)；湖南省自然科学基金资助项目(10JJ6093)
Foundation Items: The National Natural Science Foundation of China (61379058, 61379057,61350011 60903058); The Natural Science Foundation of Hunan Province (10JJ6093)

密钥空间以抵抗穷举攻击；第二，应该对明文和密钥都极端敏感，能很好地抵抗差分攻击；第三，密文分布应该随机均匀且相邻数据不相关，以便抵抗统计分析。对于图像数据，由于像素位置置乱和像素值替代的思想很好地体现了香农对密码设计提出的 2 个基本原则：混淆、扩散，因此得到了混沌密码学界的推崇。

陈关荣[11]提出的一种典型“置乱—替代”结构的混沌加密方案,曾一度成为研究的热点。该算法首先利用三维的猫变换对图像进行置乱，然后通过 Logistic 混沌系统产生的中间密钥对像素的灰度值进行替代加密，具有形式简单、产生混沌序列时间短等优点, 但不能抵抗选择明文攻击。文献[12]对该算法提出了一种破译方方案：首先，选取像素值全部为 0 的明文（可以消除全局置乱效果）进行攻击，破译出算法替代加密过程的密钥序列；然后，选取唯一标识位置的明文，利用已经破译的替代加密过程的密钥序列，破译出该明文的置乱图像，并与明文进行对比，确定明文中各像素点置乱后的位置，即破获了算法置乱过程相应的密钥序列，所以，该算法不能抵抗选择明文攻击。针对这一问题，一些改进的算法被提了出来[13,14]。最近，张国基[15]提出了一种基于该结构的改进算法，其改进的策略是在替代加密阶段引入了密文反馈机制，该机制是通过控制混沌系统的迭代次数来实现对密文的影响。针对算法中新增的密文反馈机制，在文献[16]中又提出了一种基于选择明文和选择密文的综合攻击方案，该方案通过选择特殊的密文策略，使新增的密文反馈机制失效，再用类似于文献[12]的破译方法成功地破译了张国基的算法。通过对该类算法的深入分析后发现，该类算法存在一个共同的缺点就是用于像素位置置乱和像素值替代加密的 2 个混沌序列与明文无关，即只要初始密钥不变，对于任何图像进行加密，在置乱和替换阶段所使用的混沌序列都始终保持不变，从而给选择明文和选择密文攻击提供了机会，导致很多基于上述结构的算法在选择明文和选择密文的攻击下纷纷被破译[17~19]。

为避免加密算法出现上述的安全漏洞，本文提出一种利用明文自身特性来影响混沌序列的机制；同时将像素位置置乱和像素值变换相结合，提出一种新型“置乱—替代”结构的混沌加密方案。其核心思路如下。其一，对不同的待加密明文，将生成不同的混沌序列，从而生成不同的中间密钥序列，即避免不同的明文都采用相同中间密钥序列加密的缺陷；这样，就能使选择明文(密文)攻击的方法失效。因为即使攻击者用选择明文(密文)攻击法破获了针对选择明文(密文)适用的中间密钥序列，攻击者也不能用该中间密钥序列去解密其他待破解的密文（原因是两者的中间密钥不同所致）。因此，从一个方面提高了算法的安全性。其二，本文对像素值替代的方式不同于已有的一些方案。目前已有的像素值替代方式基本上可以分成 2 种类型，第一类方法是用一个整数密钥与一个像素的值进行某种运算(多数是异或运算)，从而改变该像素的值。第二类方法是基于图像全局的比特置乱，首先把一个含 $M\times N$ 个像素的 8 bit 灰度图像的每个像素值二进制化，使图像变成一个 $M\times N\times 8$ 的二值图像；然后对该二值图像进行全局性比特置乱；最后将置乱后的二值图像每 8 bit 为一组转化成十进制数，就得到加密图像。现有的这 2 种像素值替代方式都有其各自的不足之处。第一类方法由于是采用整数密钥与像素值的“运算”得到密文，因此攻击者易于用选择的像素值与对应密文进行相应的“逆运算”，从而破译出加密过程所用的整数密钥。而第二类方法相当于是对二值图像进行全局比特置乱，攻击者也可以采用选择的特殊二值图像来破解 0 bit、1 bit 置乱过程的密钥序列。基于以上理论分析，结合这两类方法的优点，提出了一种新的像素值替代加密结合像素位置置乱的加密方案，且置乱密钥不仅与混沌密钥有关，而且与明文相关。新方案对像素值替代加密是对每个像素值的二进制形式进行 0 bit、1 bit 的置乱，从而改变每个像素的值。与第一类方法相比，新方案不是用一个整数密钥对一个像素值进行变换，而是用一组包含 8 个元素的子序列的排序变换来间接实现图像像素值的变换；这样，攻击者要想利用选择的明文－密文对破译出加密一个像素所用的 8 元素子序列，比破译出加密一个像素所用的单个整数密钥，前者难度大得多。与第二类方法相比，由于新方案包含了 2 种置乱，选择明(密)文攻击法同时需要选择特殊的灰度图像和特殊的二值图像，因此破解难度也更大。所以本文方法又从抗选择明(密)文攻击的角度增强了算法的安全性。

2　算法基本原理

本文加密算法的整体原理如图 1 所示。

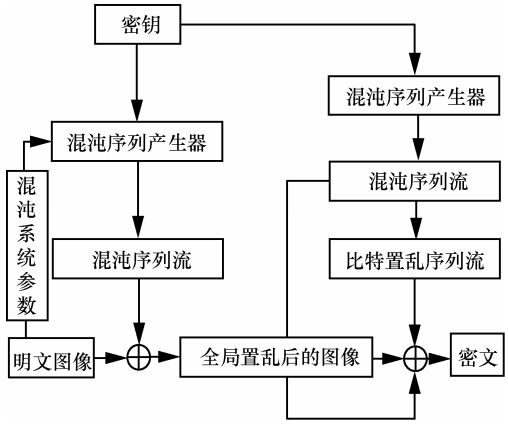


图 1 加密过程

解密过程为加密过程的逆过程，其原理如图 2 所示。图 2 中的混沌系统参数是由明文图像的所有像素值总和来确定，即根据像素值的总和计算出混沌系统的控制参数。

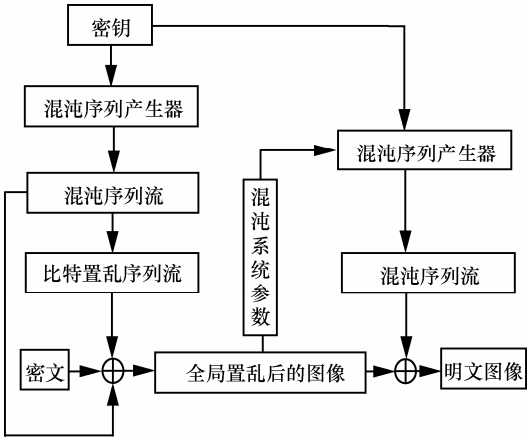


图 2 解密过程

2.1 混沌系统

本文选取的混沌系统为性能优良的 Kent 映射[20]，其映射关系为

$$F(x)=\begin{cases}x/S, x\in(0,S]\\(1-x)/(1-S), x\in(S,1)\end{cases} \tag{1}$$

当 $x\in(0,1)$，$S\in(0,1)$时，式(1)具有一个正的 Lyapunov 指数，表现为混沌运动。初始条件 x_0 在 Kent 映射作用下产生的序列具有很好的自相关性、互相关性和平衡性等优良伪随机性能，其中 S 为混沌系统的控制参数。

2.2 加密和解密原理

2.2.1 像素位置的全局置乱

像素位置置乱阶段的操作将实现对图像像素位置的全局置乱，以打破相邻像素的相关性。像素位置全局置乱的算法如下。

step1 将数字图像矩阵 $\boldsymbol{A}_{m\times n}$ 按行优先的顺序扫描，转换成长度为 $m\times n$ 的一维序列 $P=\{p_1,p_2,p_3,\cdots,p_{m\times n}\}$。

step2 计算所有像素值的和 *sum*，并利用式(2)和式(3)分别计算出混沌系统的控制参数 S 和混沌系统预迭代的次数 K。

$$S=sum/10^8 \tag{2}$$

$$K=1\,000+\mathrm{mod}(sum,1\ 000) \tag{3}$$

step3 根据 step2 的计算结果 S，设计式(1)的控制参数。输入初始密钥 x_0，预迭代 Kent 混沌映射 K 次以消除暂态效应的不良影响。

step4 继续迭代式(1) $m\times n$ 次，产生长度为 $m\times n$ 的混沌序列 $L=\{L_1, L_2, L_3, \cdots, L_{m\times n}\}$。将混沌序列 L 按照由小到大的顺序排序，得到有序序列 $L'=\{L'_1,L'_2,L'_3,\cdots,L'_{m\times n}\}$，并生成用于记录 L' 中各元素在原始序列 L 中位置的新序列 $T=\{t_1,t_2,t_3,\cdots,t_{m\times n}\}$。

step5 利用序列 T 置乱明文序列 P，得到置乱图像 $P'=\left\{p'_1,p'_2,p'_3\cdots p'_{m\times n}\right\}$，置乱原理如式(4)描述。

$$p'_i=p_{t_i}, i=1,2,3,\cdots,m\times n \tag{4}$$

2.2.2 基于比特置乱的像素值替代加密

本阶段操作将实现对像素位置全局置乱后的图像 P' 进行像素值替代加密，以混淆密文与明文之间的关系。现有算法大多采用异或运算，这种替代方法安全性低，可以通过选择一组特定的明文密文对，破译其用于像素值替代加密的混沌序列[16,17]。本文的像素值替代加密是在原有替代加密的基础上，增加了基于像素值内部比特置乱的操作，使选择明文攻击失效，增强算法的安全性。像素值替代加密算法的描述如下。

step1 设定混沌系统的控制参数 S 为另一个值 S_2。Kent 混沌系统迭代 K_2 次以消除初态效应，并继续迭代 $m\times n$ 次，产生长度为 $m\times n$ 的混沌序列 $d=\{d_1, d_2, d_3, \cdots, d_{m\times n}\}$；令 $i=0$。

step2 $i\leftarrow i+1$，d_i 为混沌序列 d 中第 i 个实数值，提取实数值 d_i 的小数点后 8 位数字，并由这 8 个数字组成序列 $W=\{W_1, W_2, W_3,\cdots, W_8\}$。例如，若混沌序列值 $d_i=0.568\ 972\ 344$，则生成的序列为 $W=\{5, 6, 8, 9, 7, 2, 3, 4\}$。

step3　将置乱图像 P' 中第 i 点的像素值 p_i' 转换成二进制形式，生成数组 $PBit$={Bit_1, Bit_2, Bit_3 ,…, Bit_8}。例如，假设 $p_i'=176$，则对应的数组为 $PBit$ = {1, 0, 1, 1, 0, 0, 0, 0}。

step4　对 step2 生成的序列 W 按照由小到大进行排序，得到有序序列 W'；然后利用数组 WT 保存 W' 各元素在 W 中的位置。例如，当 W={5, 6, 8, 9, 7, 2, 3, 4}时，得到的 W'={2, 3, 4, 5, 6, 7, 8, 9}。于是对应的 WT={6, 7, 8, 1, 2, 5, 3, 4}。

step5　利用 WT={ WT_1 , WT_1 , WT_1 , …, WT_1} 置乱 $PBit$={ Bit_1, Bit_2, Bit_3 ,…, Bit_8}，置乱原理类似 2.2.1 节的 step 5 操作方式，得到像素值比特置乱后重新排列的新形式：$PBit'$ ={ Bit'_1 , Bit'_2, Bit'_3, …, Bit'_8}。比如，若 $PBit$ = {1, 0, 1, 1, 0, 0, 0, 0}，WT={6, 7, 8, 1, 2, 5, 3, 4}，则该点经比特置乱后的二进制数位排列形式将变为 $PBit'$={0, 0, 0, 1, 0, 0, 1, 1}。

step6　经比特置乱后的二进制数 $PBit'$转换成十进制数，得到中间密文 C_i'。

step7　利用下面的式(5)和式(6)对中间密文 C_i' 再加密，得到第 i 点的最终密文 C_i。

$$D_i = \mathrm{mod}(d_i \times 2\text{^}48, 256) \tag{5}$$

$$C_i = \mathrm{mod}(D_i + C_i', 256) \oplus C_{i-1} \tag{6}$$

特别地，对于第一点(i=1)的加密需要用到 C_0，C_0 可以是一个常量，也可以作为密钥使用。

step8　重复 step2~step7，直到 i 值达到 $m \times n$，得到密文图像 C，加密过程结束。

2.2.3　解密原理

解密过程为加密过程的逆过程，先后对 2.2.2 节和 2.2.1 节进行逆向操作处理。

第一阶段处理：像素比特的反置乱操作。根据混沌系统产生的迭代值，首先由式(7)得到求解中间密文 C_i' 的计算公式

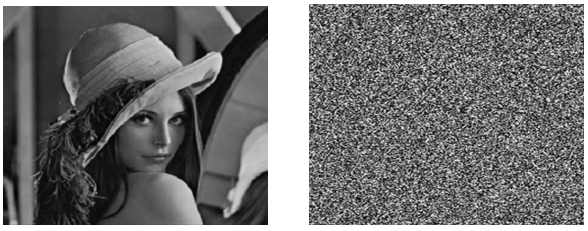
$$C_i' = \mathrm{mod}(C_i \oplus C_{i-1} + 256 - D_i, 256) \tag{7}$$

然后，把恢复的中间密文 C_i' 的二进制比特进行反置乱，得到原始的比特序列；再转换成十进制数，得到全局置乱后的图像像素值。

第二阶段处理：反全局像素置乱。计算原始明文图像的所有像素值的和，考虑到经全局置乱后的图像与原始明文图像之间仅仅是像素位置发生重排，所以其像素值的总和与原始明文图像的像素值总和是相同的。通过公式计算转换成混沌系统的控制参数和初始预迭代的次数，再结合初始密钥 x_0 就能获得生成图像像素位置反置乱的混沌序列。经过反置乱后得到像素在明文中的正确位置。最后将一维序列转换成二维矩阵，就得到恢复的解密图像。

3　实验仿真与分析

在本文算法的仿真过程中，选择 256×256 的 Lena 灰度图像进行实验，加密系统的初始密钥为(x_0, S_2)=(0.123 456 789 0, 0.23)。其他常量为 K_2=16, C_0 =20。图 3 是原始图像和对应的加密图像。由图 3(b)可见，加密图像已经与原始图像毫无关联。为了评估算法的总体性能，下面分别对算法的密钥空间、密文统计分布特性、抗差分攻击和抗选择明(密)文攻击等方面的性能进行分析。



(a) 原始图像　　(b) 加密图像

图 3　密钥为(x_0, S_2)=(0.123 456 789 0, 0.23)的加密效果

3.1　密钥空间分析

一个好的加密算法，密钥空间应该足够大以抵抗穷举攻击。本文选取混沌迭代的初始值 x_0 和第二阶段所需的混沌系统的参数 S_2 作为密钥。在 32 bit 计算机中双精度数据为 64 bit。则密钥空间为 $2^{64}\times 2^{64}=2^{128}$。即使攻击者以每秒一亿个密钥的速度进行攻击，穷举整个密钥空间需要 10^{14} 年。若把 K_2 和 C_0 也视为密钥，密钥空间将更大，需花费的时间也更多。所以本算法的密钥空间对穷举攻击是安全的。

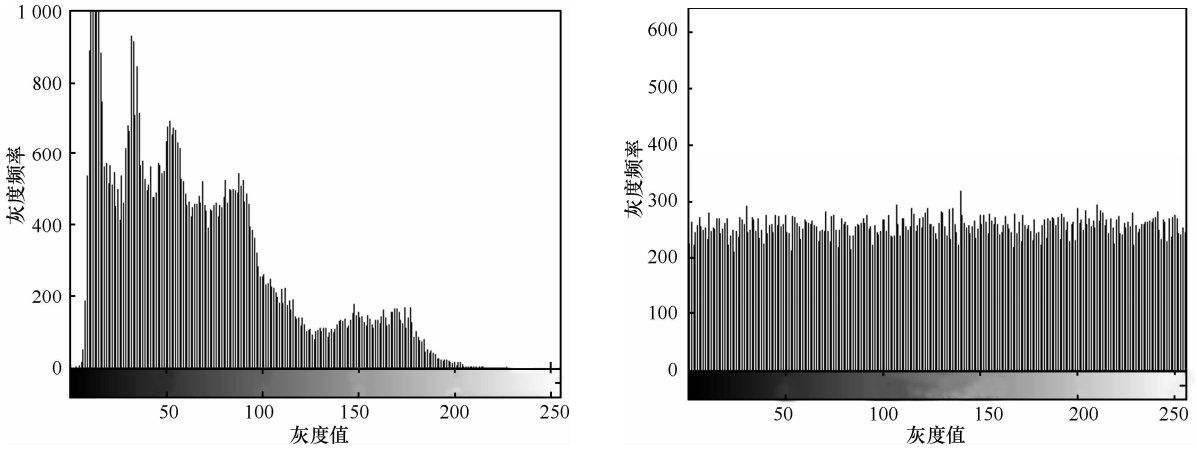
3.2　统计特性分析

图 4(a)与 4(b)分别给出了原始图像和加密图像的直方图。可见，加密过程已将原始图像像素值的不均匀分布变成了均匀分布，即明文图像的统计特性完全被打破，降低了明文与密文的相关性，隐藏了图像的统计特性。

3.3　抗差分攻击性能分析

3.3.1　明文敏感性分析

密文对明文的敏感性越好，算法抵抗差分攻击



(a) 明文图像直方图　　(b) 密文图像直方图

图 4　明文与密文图像直方图

的性能也就越好。本文引入像素数改变率(NPCR, number of pixels change rate)和归一化平均改变强度(UACI, unified average changing intensity)来度量加密算法对明文的敏感性。当 2 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

$$NPCR=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)\times 100\% \tag{8}$$

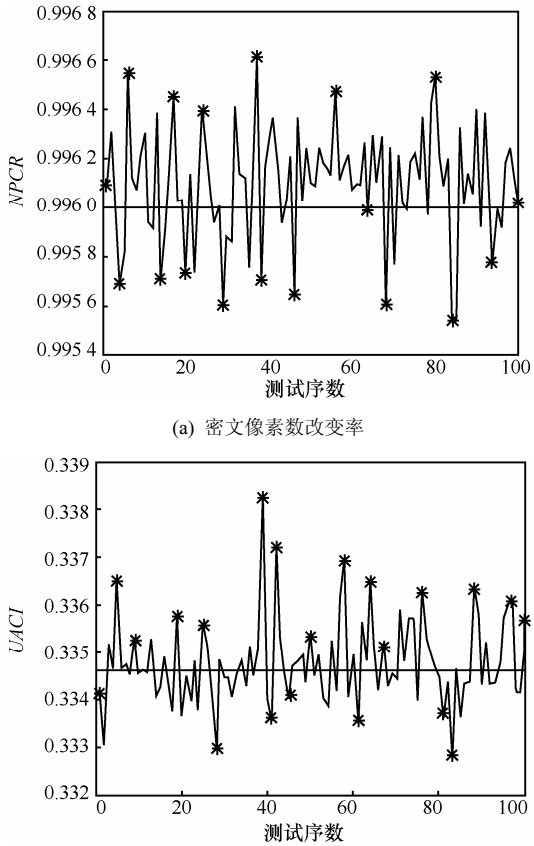
$$UACI=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|c_1(i,j)-c_2(i,j)\right|}{255}\times 100\% \tag{9}$$

NPCR 与 *UACI* 的理想期望值分别为

$$NPCR_E=(1-2^{-n})\times 100\% \tag{10}$$

$$UACI_E=\frac{1}{2^{2n}}\frac{\sum_{i=1}^{2^n-1}i(i+1)}{2^n-1}\times 100\% \tag{11}$$

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[21]：$NPCR_E$=99.6094%，$UACI_E$ =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改变该像素值的灰度值(加 1 再与 256 取摸)，所得 100 组密文图像之间的 *NPCR* 与 *UACI* 值，结果如图 5 所示。结果表明，实验所得 *NPCR* 与 *UACI* 值都分布在理想值(图中水平线)附近。



(a) 密文像素数改变率

(b) 归一化像素值平均变化强度

图 5　100 组 Lena 图像的 *NPCR* 与 *UACI* 值

3.3.2　相邻像素的相关性

为了检验明文图像和密文图像相邻像素的相关性，选取图像中 N 对相邻像素(水平方向，垂直方向和对角方向)，然后使用以下公式定量计算相邻像素的相关系数[11]

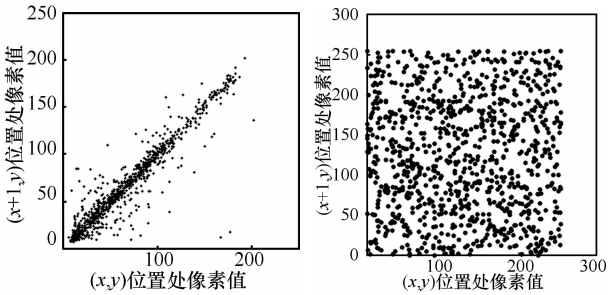
$$\bar{x}=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{12}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-\bar{x})^2 \tag{13}$$

$$Conv(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-\bar{x})(y_i-\bar{y}) \tag{14}$$

$$\gamma_{xy}=\frac{Conv(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{15}$$

其中，x 和 y 分别表示图像中 2 个相邻像素的灰度值，γ_{xy} 即为 2 个相邻像素的相关系数。图 6 是从明文图像和密文图像随机选取水平方向 1 000 组邻点作出的像素值关系图。图 6(a)表明明文图像中水平相邻点的像素值几乎相等；而图 6(b)表明密文图像中水平相邻点的像素值差别明显。



(a) 明文　　(b) 密文

图 6　明文和密文水平方向上的相邻像素的相关性

由表 1 可知，原始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，说明明文的统计特征已被扩散到随机的密文中。表 1 同时列出了最近基于混沌系统的图像加密算法对图像“Lena”仿真得到的相应参数，可见本文算法所得的密文图像具有更小的 γ 系数，能更好地达到破坏相邻像素相关性的目的，使密文具有更好的随机分布特性。

3.3.3　对密钥的敏感性分析

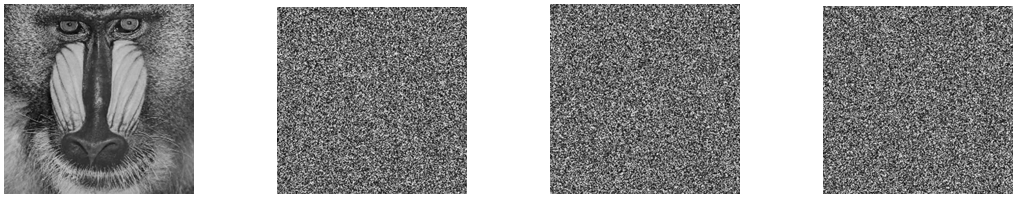
密钥敏感性是指 2 个具有微小差别的加密密钥，应该产生完全不同的密文图像；同样地，2 个具有微小差别的解密密钥，对同一密文的解密结果也应该截然不同。本阶段实验采用 256×256“baboon”图像，选取 $C_0=100$。图 7(a)是“baboon”原图；图 7(b)则是初始密钥为(x_0, S_2)=(0.123 456 789 0，0.23)的加密图像；图 7(c)是初始密钥为(x_1, S_{21})=(x_0+10^{-10}, 0.23)的加密图像；图 7(d)是初始密钥为(x_2, S_{22})=(x_0 , 0.23+10^{-10})的加密图像。为了更加准确地反应 2 幅密文图像的区别，分别计算密钥发生微小变化时，得到的密文与原始密文的 *NPCR* 和 *UACI*。从表 2 中可知，平均 *NPCR* 和 *UACI* 分别为 99.615%和 33.508%，即密钥发生微小变化时，所得的密文中 99%以上的点发生了改变。算法采用的是对称加密体制，加密和解密所使用的密钥相同，因此对于解密密钥同样可以得到类似的结论，所以算法对密钥非常敏感。

表 2　密钥为(x_0, S_2)的密文与密钥发生微小变化的密文之间的 *NPCR* 和 *UACI*

初始密钥	本文算法		文献[15]算法	
	NPCR	*UACI*	*NPCR*	*UACI*
(0.123 456 789 1, 0.23)	0.996 2	0.334 7	0.996 0	0.334 1
(0.123 456 789 2, 0.23)	0.996 4	0.335 3	0.996 2	0.334 8
(0.123 456 789 1, 0.23+10^{-10})	0.996 2	0.335 7	0.996 0	0.334 6
(0.123 456 789 1, 0.23+2×10^{-10})	0.995 8	0.334 6	0.996 2	0.334 7

表 1　　**“Lena”密文图像相邻像素的相关系数**

方向	原始图像	加密图像	文献[2]	文献[9]	文献[10]	文献[15]	文献[22]	文献[23]	文献[24]	文献[25]
水平	0.945 0	0.001 7	−0.014 2	0.020 4	0.024 2	0.000 8	0.081 5	0.011 7	0.012 7	−0.002 9
垂直	0.970 4	−0.000 3	−0.007 4	0.001 74	0.019 4	0.003 7	0.040 0	0.002 6	0.019 0	−0.015 0
对角	0.924 7	0.000 1	−0.018 3	−0.023 1	0.002 4	−0.000 2	0.004 7	0.001 0	0.001 2	0.012 9



(a) 原始图像　　(b) 密钥为(x_0, S_2)　　(c) 密钥为(x_1, S_{21})　　(d) 密钥为(x_1, S_{22})

图 7　密钥微小差异的加密效果

3.4 抗选择明(密)文攻击分析

选择明(密)文攻击的定义：攻击者有机会临时获得加(解)密机的使用机会，于是他(她)可以选择一些特殊的明(密)文，并得到相应的密(明)文；然后可以由这些明－密文对推导出等价的中间密钥。

基于“置乱—替代”结构的图像混沌加密，常用的攻击方法是选择明文和选择密文攻击[16,17]。通常采用的策略是选择一个与待解密文同样大小的像素值全部为 0 的图像以破译用于替代操作的中间密钥，再选取一个唯一标示位置的图像，根据对应的密文和像素值全部为 0 的图像替代操作中的中间密钥（由于一般的加密算法所用的混沌序列跟图像无关，所以像素值全部为 0 的图像和唯一标示位置的图像加密所使用的中间密钥相同），破译其置乱后的图像，再根据两者的关系，确定加密算法的置乱序列，从而破译算法[16,17]。下面以具体实例对现有加密算法安全缺陷作简单具体评估。

设算法在像素位置置乱阶段用到的中间密钥为 $T=\{t_1, t_1, \cdots, t_L\}$, L 为图像的像素数；在像素值替代变换阶段用到的另一种中间密钥为 $K=\{k_1, k_2, \cdots, k_L\}$。 其中，$T$ 与 K 的生成仅仅与混沌系统及其初始密钥有关，而与被加密图像内容无关；因此，T 与 K 成为初始密钥的等价密钥。设被加密图像明文为 $P=\{p(1), p(2), \cdots, p(L)\}$; 像素位置置乱后的图像为 $Q=\{q(1), q(2), \cdots, q(L)\}$;像素值替代变换后的最终密文图像为 $C=\{c(1), c(2),\cdots, c(L)\}$。2 种阶段的加密原理由式(16)和式(17)描述。

$$q(i)=p(t_i) \tag{16}$$

$$c(i)=f(q(i), k_i) \tag{17}$$

其中，$f(x,y)$代表某种加密变换函数，常见的是 $f(q(i), k_i)=q(i)\oplus k_i$。下面演示对这类算法的选择明文攻击方法，假设攻击者截获了一幅密文图像 $C=\{38, 9, 127, 0\}$，于是知道其大小 $L=4$;又根据公开算法知道替代变换函数 $f(q(i), k_i)=q(i)\oplus k_i$。攻击者先选择第一幅特殊明文图像如 $Pa=\{0, 0, 0, 0\}$, 经加密后假设得到对应密文为 $Ca=\{12, 7, 254, 32\}$；然后攻击者又选择第二幅特殊明文图像如 $Pb=\{45, 50, 70, 110\}$, 经加密后假设得到对应密文为 $Cb=\{98, 65, 204, 13\}$。1) 由 $Pa-Ca$ 对，可破获 K。因为，$Pa=Qa=\{0, 0, 0, 0\}$；又根据式(17), $k_i=ca(i)\oplus qa(i)$，所以，$K=\{12\oplus 0, 7\oplus 0, 254\oplus 0, 32\oplus 0\}=\{12, 7, 254, 32\}$；2) 由 $Pb-Cb$ 对，可破获 T。因为，$Qb=\{cb(1)\oplus k_1, cb(2)\oplus k_2, cb(3)\oplus k_3, cb(4)\oplus k_4\}=\{98\oplus 12, 65\oplus 7, 204\oplus 254, 13\oplus 32\}=\{110, 70, 50, 45\}$；又逐项对比 Qb 与 Pb 中的各像素值，即可得出 $T=\{4, 3, 2, 1\}$。由于等价密钥 K、T 与图像内容无关，因此攻击者即可利用所获得的密钥 K、T 去解密原密文图像 $C=\{38, 9, 127, 0\}$，得出其明文是 $P=\{32, 129, 14, 42\}$。

对于本文算法的抗选择明(密)文攻击性能，从如下两点来说明：第一，利用像素值全部为 0 的图像虽然可以破译出式(5)中的 D_i，但由 D_i 并不能推出 d_i，也就不能确定像素中的各个比特上的数字，所以用于替代操作的中间密钥不能破译；第二，即使穷举得到像素值全部为 0 的图像加密所使用的中间密钥，并用唯一标示位置的图像和其对应的密文破译出该图像的置乱序列。但此置乱序列也仅仅用于该特定的图像，因为待解密的图像的明文与此图像的像素值总和并不一定相等，经计算后得到的混沌控制参数也就不一样，所以 2 个图像加密所使用的置乱序列也就不一样，从而不能用于破译待解密的密文。所以，本文提出的算法能有效抵抗选择明(密)文攻击。

4 结束语

本文提出的算法是一种改进的基于像素位置置乱和像素值加密的混沌图像加密算法。改进的算法不仅保留了现有“置乱—替代”算法的优点，还克服了现有算法易受选择明(密)文攻击的缺点。本算法的主要特点如下。

1) 加密系统不再是一开始就设定为固定的系统，而是根据不同的明文产生对应的混沌系统控制参数，从而产生不同的混沌系统，使算法具有抗选择明(密)文攻击能力。

2) 与已有加密算法中常采用的异或运算相比，本文加密算法中采用了一种新的像素值加密思路，即通过置乱像素值中的比特来实现加密，提高算法的安全性。

3) 引入了像素值双重加密操作，使比特置乱后的像素值得到进一步加密，且引入密文输出反馈控制，增强了密文扩散效应，从而提高了算法的抗差分攻击的能力。

4) 密文在整个取值空间中分布均匀；相邻像素具有近似于零的相关性并优于已有文献报道的结果。

本文算法不仅克服了已有“置乱—替代”型加密系统不能抵抗选择明文和选择密文攻击的缺陷，同时强化了一些密码学性能，从而增加了密码系统的安全性和实用性。因此，本文算法在图像保密通

信等应用领域将具有更好的应用前景。

参考文献：

[1] PISARCHIK A N, ZANIN M. Image encryption with cha-otically coupled chaotic maps[J]. Physics Letters, 2008, 372: 2645-2652.

[2] GAO T G, CHEN Z Q. Image encryption base on a new total shuffling algorithm[J]. Chaos, Solitons & Fractals, 2008, 38: 213-220.

[3] GUAN Z H, HUANG F J, GUAN W J. Chaos based image encryption algorithm[J]. Physics Letters A, 2005, 346(1-3): 153-157.

[4] 廖晓峰, 陈勇, 肖迪等. 混沌密码学原理及应用[M]. 北京:科学出版社, 2009.
LIAO X F, CHEN Y, XIAO D, *et al*. Theory and Aapplication of Chaotic Cryptography[M]. Beijing: Science Press,2009.

[5] SEMPERE V, ALBERO T, SILVESTRE J. Analysis of communication alternatives in a heterogeneous network for a supervision and control system[J]. Computer Communications, 2006, 29(8): 1133-1145.

[6] TENNY R, TSIMRING L S, LARRY I, *et al*. Using distributed nonlinear dynamics for public key encryption[J]. Physical Review Letters, 2003, 90(4): 047903.

[7] KOCAREV L, TASEV Z. Public-key encryption based on Chebyshev maps[A]. Proceedings of the IEEE International Symposium on Circuits and Systems[C]. 2003, 1(3): 28-31.

[8] 曹建秋, 肖华荣, 蓝章礼. 像素位置与像素值双重置换的混沌加密算法[J]. 计算机工程与应用, 2010, 46(28): 192-195.
CAO J Q, XIAO H R, LAN Z L. Chaos encryption algorithm based on dual scrambling of pixel position and value[J]. Computer Engineering and Applications, 2010, 46(28): 192-195.

[9] WANG X Y, LEI Y. A novel chaotic image encryption algorithm based on water wave motion and water drop diffusion models[J]. Optics Communications, 2012, 285(20): 4033-4042.

[10] TENG L, WANG X Y. A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive[J]. Optics Communications, 2012, 285(20): 4048-4054.

[11] CHEN G R, MAO Y B, CHARLES K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons & Fractals, 2004, 3(21): 749-761.

[12] XIAO D, LIAO X F, WEI P C. Analysis and improvement of a chaos-based image encryption algorithm[J]. Chaos, Solitons and Fractals, 2009, 40 (5): 2191-2199.

[13] 朱从旭, 李力, 陈志刚. 基于多维混沌系统组合的图像加密新算法[J]. 计算机工程, 2007, 33(2): 142-144.
ZHU C X, LI L, CHEN Z G. A new image encryption algorithm based on Combined multidimensional chaotic systems[J]. Computer Engineering, 2007, 33(2): 142-144.

[14] ZHU Z L, ZHANG W, KWOK-WO W. A chaos-based symmetric image encryption scheme using a bit-level permutation[J]. Information Sciences, 2011, 181(2011): 1171-1186.

[15] ZHANG G J, LIU Q. A novel image encryption method based on total shuffling scheme[J]. Optics Communications, 2011, 284(12): 2775- 2780.

[16] ZHU C X, LIAO C L, DENG X H. Breaking and improving an image encryption scheme based on total shuffling scheme[J]. Nonlinear Dynamics, 2013,71(1-2): 25-34

[17] 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): 060503.
WANG J, JIANG G P. Cryptanalysis of a hyper-chaotic image encryption algorithm and its improved version[J]. Acta Physica Sinica, 2011, 60(6): 060503.

[18] WANG X Y, HE G X. Cryptanalysis on a novel image encryption method based on total shuffling scheme[J]. Optics Communications, 2012, 61(12): 120503.

[19] 朱从旭, 孙克辉. 对一类超混沌图像加密算法的密码分析与改进[J]. 物理学报, 2012, 61(12): 120503.
ZHU C X, SUN K H. Cryptanalysis and improvement of a class of hyperchaos based image encryption algorithms[J]. Acta Physica Sinica, 2012, 61 (12): 120503.

[20] 黄润生. 混沌及其应用[M]. 武汉:武汉大学出版社, 2000.
HUANG R S. Chaos and its application[M]. Wuhan: Wuhan University Press,2000.

[21] PATIDAR V, PAREEK N, SUD K. A new substitution-diffusion based image cipher using chaotic standard and logistic maps[J]. Communications in Nonlinear Science and Numerical Simulation, 2009,14 (7): 3056-3075.

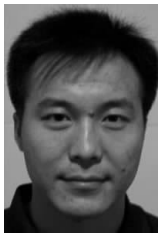
[22] ZHANG L H, LIAO X F, WANG X B. An image encryption approach based on chaotic maps[J]. Chaos, Solitons & Fractals, 2005, 24 (3): 759-765.

[23] LIU S B, SUN J, XU Z Q. An improved image encryption algorithm based on chaotic system[J]. Journal of Computers, 2009, 4(11): 1091-1100.

[24] LIAO X F, LAI S Y, ZHOU Q. A novel image encryption algorithm based on self-adaptive wave transmission[J]. Signal Processing, 2010, 90(9): 2714-2722.

[25] KANSO A, GHEBLEH M. A novel image encryption algorithm based on a 3D chaotic map[J]. Communications in Nonlinear Science and Numerical Simulation, 2012, 17(4): 2943-2959.

作者简介：



邓晓衡（1974-），男，湖南衡东人，博士，中南大学教授，主要研究方向为无线通信与网络、信息安全、分布式系统、大数据分析。

廖春龙（1985-），男，湖南永州人，中南大学硕士生，主要研究方向为信息安全、混沌保密通信。

朱从旭（1963-），男，湖南武冈人，博士，中南大学教授、硕士生导师，主要研究方向为信息安全、混沌密码学、混沌保密通信。

陈志刚（1964-），男，湖南益阳人，博士，中南大学教授，主要研究方向为分布式系统、网络通信。