# 一种基于混沌的代换-置换结构图像加密算法

蔡 俊[1] 陈 昕[1] 向旭东[2]
(北京信息科技大学计算机学院 北京 100101)[1] (北京科技大学计算机与通信工程学院 北京 100083)[2]

**摘 要** 近年来,随着多媒体技术的发展,互联网上数字图像相关内容和应用的比例越来越高,其安全性也日益受到人们的关注。图像的安全性,一般通过加密方法来保证。图像加密算法中,基于置乱-扩散结构的加密算法因其充分考虑图像数据二维分布的特点,特别适合图像数据的加密。然而,该加密算法存在安全性不高、扩散效率低,以及密钥扩展计算复杂度高等问题。通过引入分组密码学中的代换-置换(SP,Substitution-Permutation)结构,提出了一种基于混沌的SP结构图像加密算法SPCME,该算法采取3种策略:(1)通过混沌映射进行置换和扩散,采用AES算法的S盒进行字节代换,以增强算法安全性;(2)使用双向的置乱-扩散策略,加快扩散速度;(3)运用简单的异或和移位操作,提高密钥扩展效率。为评价该算法的性能,文中做了密钥空间分析、密钥敏感性分析、统计直方图分析、相邻像素相关性分析、信息熵分析、差分攻击分析等大量的性能分析实验。实验结果表明,该算法仅通过3轮迭代就可达到与以前提出的图像加密算法相同的安全级别,加密效率明显提高。

**关键词** SP结构,图像加密,混沌,三维Arnold映射,Logistic映射
**中图法分类号** TP309.7 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.09.030

## Substitution-Permutation Network Structured Image Encryption Algorithm Based on Chaotic Map

CAI Jun[1] CHEN Xin[1] XIANG Xu-dong[2]
(School of Computer, Beijing Information Science & Technology University, Beijing 100101, China)[1]
(School of Computer & Communications Engineering, University of Science and Technology Beijing, Beijing 100083, China)[2]

**Abstract** Various image encryption algorithms based on the permutation-diffusion structure have been proposed in the past few years. However, permutation and diffusion are considered as two separate stages, making image encryption vulnerable to attacks. Moreover, the algorithms, in general, have low diffusion efficiency and high computational complexity in key scheming. To solve these problems, this paper proposed a SP(Substitution-Permutation) network image encryption algorithm based on chaotic map. The proposed algorithm adopts the following three strategies: (1) To further enhance the security of the cryptosystem, XOR and S-box operations are introduced in the beginning of each encryption round; (2) An bidirectional permutation-diffusion strategy is proposed to accelerate the spreading process; (3) Simple circular bit shift and XOR operations are used to improve the efficiency of key scheming. We conducted a rich set of cryptanalyses on the proposed algorithm, e.g., key space analysis, key sensitivity analysis, various statistical analyses and differential analysis. Analytical results demonstrate that the proposed algorithm reaches the same security level of previously proposed counterparts in merely three iterations with high efficiency, and is thus applicable for secure image encryption.

**Keywords** SP network, Image encryption, Chaos, 3D arnold map, Logistic map

## 1 引言

近年来,图像数据的应用与安全已经受到学术界和业界的广泛关注。图像数据可能涉及国家安全、商业利益和个人隐私,因此许多应用领域需要对其进行加密保护。传统的加密方法,如AES、IDEA、三重DES等,因其将图像看作二进制流进行加密,未考察二维图像的空间二维分布、视觉冗余性和相邻像素相关性等特性。在对图像文件加密时,存在耗费时间较长,可能会泄露原始图像的几何分布信息等缺陷。

混沌系统具有对初值及控制参数的极度敏感特性、遍历特性和伪随机特性,本质上与加密系统相似[1],较适用于数据加密。例如,混沌系统中的Logistic映射、Chebyshev映射和分段线性映射常被用作流加密[2-5],而Logistic映射、分段线性映射、Baker映射和Arnold映射常用于分组加密[6-10]。这些加密系统的核心部件由一个或者多个混沌映射组成。

基于混沌系统的加密算法已成为图像加密算法研究领域

到稿日期:2013-09-05 返修日期:2013-12-08 本文受国家自然科学基金面上项目(61370065)资助。
蔡 俊(1986-),男,硕士生,主要研究方向为网络安全与系统性能评价,E-mail:caijun0213@163.com;陈 昕(1965-),男,教授,硕士生导师,CCF高级会员,主要研究方向为计算机网络及其性能评价、航电网络与网络安全;向旭东(1986-),男,博士生,主要研究方向为网络性能评价与优化控制。

的热点。Fridrich 于 1998 年提出基于置乱-扩散结构的图像加密算法[7]，该加密算法结合图像数据二维分布的特点，加密过程不需要图像的预处理，因而加密效率高。文献[8]提出用三维的 Arnold 映射对像素进行置乱，相对二维映射，三维映射的混沌动力学特性更复杂，像素置乱的效果更好。佟晓筠[11]提出了一种基于多混沌映射的图像加密方案，该方案设计了一个分块 Arnold 映射，用于图像不同部分的像素置乱，解决了 Arnold 映射密钥空间较小的问题。文献[12,13]在图像加密中用高维的混沌系统来代替一维的混沌系统，克服了一维混沌系统密钥空间小、安全性低等问题。文献[14]提出了用双非线性混沌映射来克服一维混沌系统的缺陷。王永等人[15]提出了可调整控制参数的图像加密算法，以避免置乱的周期性以及提高算法抵御已知明文或者选择明文攻击的能力。张伟等人[16]提出一种置乱与扩散合并的图像加密方案，进一步提高了基于置乱-扩散结构图像加密算法的加密效率。文献[17]提出了一种基于混沌的图像加密算法，该算法采用双向扩散策略，加快了扩散速度，提高了加密效率。

上述基于混沌的图像加密算法，在安全性和效率等方面考虑较少，无法满足当前图像数据加密的实际需求。这里，安全性是指置乱与扩散阶段相互独立可能会产生分割攻击；而效率是指扩散阶段涉及实数的算术运算耗时较长，密钥扩展阶段采用高维的混沌系统，使得系统方程的求解会耗费大量的计算时间。

围绕基于混沌的图像加密的安全性和效率问题，文中提出一种基于混沌的 SP 结构图像加密方案。SP 结构采用代换-置换网络体系，属于一类特殊的迭代分组密码。代换-置换网络的轮函数通过变换实现，其中变换包括 3 种：代换、置换和密钥混合。交替使用代换和置换，可以破坏对密码系统进行的各种统计分析。因而，SP 成为设计现代分组密码的基础。基于上述分析，文中提出了 SP 结构的图像加密方案，该方案采用 3 种策略：(1)引入混沌映射异或加密和 AES 算法的 S 盒字节代换，提高了基于置乱-扩散结构算法的混淆特性和安全性；(2)采用双向置乱-扩散的策略，加快扩散速度，减少加密轮数，提高加密效率；(3)采用基于异或和移位操作的密钥扩展算法，密钥扩展的效率得到了提高，且算法具有良好的密钥敏感性。

## 2 Arnold 映射和 Logistic 映射的混沌特性

加密系统应具有对密钥的敏感性，能够将明文充分置乱，并改变其统计特性[18]，而这与混沌的混迭特性相一致。混沌系统和加密系统二者之间存在许多共性，具体表现为：(1)混沌对初值和控制参数的敏感特性对应密码对密钥的敏感性；(2)混沌的混迭与拓扑传递特性类似于密码的混淆与扩散特性；(3)混沌映射通过多轮迭代将一个确定性系统变成一个具有遍历性的随机信源，密码变换则通过迭代与混合的方法将明文信息随机置乱。文中所提出的图像加密算法，利用了混沌良好的密码特性，引入了两种经典的混沌映射：Arnold 映射和 Logistic 映射。

### 2.1 Arnold 映射

在混沌图像加密中，Arnold 映射通常用于像素点位置的变换，其方程定义如式(1)所示：

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1 = C \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1 \tag{1}$$

其中，mod 1 表示对 1 取模运算，结果取小数部分，即 $x \bmod 1 = x - \lfloor x \rfloor$，$\lfloor x \rfloor$ 表示不大于 $x$ 的最大整数，坐标值 $(x_n, y_n)$ 的相空间被限制在一个单位正方形内。

Arnold 映射的 Lyapunov 指数[8]为：

$$\lambda_1 = \ln\left(\frac{3+\sqrt{5}}{2}\right) > 0, \lambda_2 = \ln\left(\frac{3-\sqrt{5}}{2}\right) < 0 \tag{2}$$

依据混沌的判断准则，该映射有一个 Lyapunov 指数 $\lambda_1$ 为正，即为混沌映射。

Arnold 映射不仅具有混沌的一般属性，还具备两个重要的特性：(1)Arnold 映射中矩阵 $C$ 的行列式满足 $|C|=1$，该映射是一个保面积映射；(2)该映射为一一映射，即单位矩阵内任意一点的坐标，存在唯一一个单位矩阵内的点的坐标，通过该变换与之对应。

式(1)描述了实数范围内的 Arnold 映射，通过引入两个控制参数 $a$ 和 $b$，二维 Arnold 映射可以表示为更一般的形式，如式(3)所示：

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1 \tag{3}$$

为提高混沌系统的安全性，式(3)需要扩展到三维，如式(4)所示：

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \bmod 1 \tag{4}$$

其中，

$$A = \begin{bmatrix} 1+a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{bmatrix}$$

矩阵 $A$ 中的 $a_x$、$a_y$、$a_z$、$b_x$、$b_y$ 和 $b_z$ 为扩展后的三维 Arnold 映射的控制参数。假定 $a_x = a_y = a_z = b_x = b_y = b_z = 1$，则得到矩阵 $A$ 的一个特例：

$$A = \begin{bmatrix} 2 & 1 & 3 \\ 3 & 2 & 5 \\ 2 & 1 & 4 \end{bmatrix}$$

通过数值计算，可得该特例下混沌方程的 Lyapunov 指数[8]分别为 7.1842、0.2430 和 0.5728。与二维 Arnold 映射相比，三维 Arnold 映射的 Lyapunov 指数值更大。因此，扩展到高维的 Arnold 映射具有更好的混沌特性，并且控制参数增加到 6 个，这意味着加密系统密钥更多，密钥空间大，保密性高。

### 2.2 Logistic 映射

Logistic 映射是典型的一维混沌映射，它具有对初值敏感、混沌序列生成速度快等优势，其方程定义如式(5)所示：

$$x(n+1) = \mu x(n)[1 - x(n)] \tag{5}$$

式中，$x \in (0,1)$，$\mu \in [0,4]$。当 $\mu \in [3.5699, 4]$ 时，整个系统处于混沌状态。

对于一个离散混沌映射 $F: X \to X, X \subseteq \mathbb{R}^N$，其迭代轨迹 $\{x, F(x), F^2(x), \cdots\}$ 在相空间会呈现一定的分布。由混沌映

射的拓扑传递性，可以得到其遍历特性。混沌轨迹会落在 $X$ 中的每一点的邻域内，但在 $X$ 上的分布并不均匀。如 Logistic 映射在区间(0,1)上的分布如式(6)所示：

$$v(x)=\frac{1}{\pi\sqrt{x(1-x)}} \tag{6}$$

显然，此分布不是均匀分布，在分布曲线两端出现奇异性，如图 1 所示。

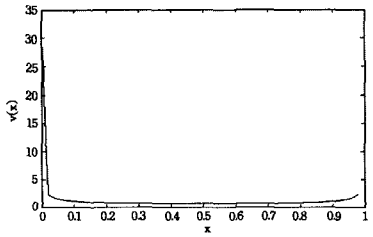


图 1　Logistic 映射的分布图

对于一个混沌映射，如果它的轨迹的分布具有均匀性，则可以保证明文经过一定次数的迭代后，能获得分布均匀的密文。因此，用 Logistic 映射迭代产生密钥流时，密钥流的取值 $x\in(0.2,0.8)$。在这个区间内，密钥流的分布是均匀的。

## 3　基于混沌的 SP 结构图像加密算法

SP 结构为图像加密算法的设计提供了代换和置换两种重要方法，文中提出了基于混沌的 SP 结构图像加密算法 SPCME。该图像加密算法分 3 部分：混淆变换、扩散变换和密钥扩展。

### 3.1　混淆变换

混淆变换 XORSP(Xor-Substitute-Permutation)分 3 个步骤：异或加密、字节代替和像素置乱。

第 1 步(异或加密)：首先，用 Logistic 映射迭代产生密钥序列。在(0,1)区间中随机选取一个数 $x(0)$作为 Logistic 映射迭代的初值，控制参数取 $\mu\in[3.9,4]$；迭代 Logistic 映射，当迭代值 $x(k)$落在区间(0.2,0.8)时，经过适当比例的量化得到一个整数值 $\phi(k)$，量化公式如式(7)所示：

$$\phi(k)=\mathrm{mod}\ (floor(x(k)\times 10^{12}),256) \tag{7}$$

式中，$floor(x)$表示取不超过 $x$ 的最大整数。否则，继续迭代，直到满足条件。按照这样的迭代规则，迭代结束，将会产生一个与明文序列等长的密钥序列。

这里需要注意的是，迭代值 0.5 被称为一个“坏”点。因迭代值为 0.5 时，经过几轮迭代，迭代值将会陷入固定值 0。为避免“坏”点出现，需对迭代值 0.5 施加一个细微的干扰 $x(k)=0.5+0.000001$。

然后，使用提取的整数值 $\phi(k)$对明文进行异或加密，相应计算公式如式(8)所示：

$$E(k)=m(k)\oplus\phi(k) \tag{8}$$

式中，$k=1,2,\cdots,N$，$N$ 为图像像素总个数。$m(k)$为当前明文像素值，$E(k)$为异或加密后的密文。经过几轮异或加密迭代之后，密文像素分布趋于均匀。

第 2 步(字节代替)：采用 AES 算法的 S 盒进行字节代替，能以较少的轮数操作达到更好的混淆效果。

第 3 步(像素置乱)：置乱操作采用三维的 Arnold 映射，由于图像加密是在有限域上进行操作，为了将其应用于图像加密，需要依据式(9)对式(4)中的 Arnold 映射进行离散化：

$$\begin{bmatrix}x_{n+1}\\y_{n+1}\\z_{n+1}\end{bmatrix}=A\begin{bmatrix}x_n\\y_n\\z_n\end{bmatrix}\bmod N \tag{9}$$

离散化后的 Arnold 映射保留了混沌的混淆特性，以及对初值和控制参数的敏感特性。

然而，混沌映射离散化后的混沌特性有可能会改变。文献[8]中非周期的二维 Anornd 映射离散化后，会呈现周期性，图像经过若干轮的置乱会自动恢复原图像。三维 Anornd 映射离散化后，也存在同样的问题。为防止对置乱过程的单独攻击，可采取两种措施进行防范，具体为：(1)每一轮置乱操作采取不同控制参数 $a_x$、$a_y$、$a_z$、$b_x$、$b_y$ 和 $b_z$；(2)采用双向置乱，即前后两轮置乱的方向相反，若前一轮置乱方向从左到右、从上到下，则后一轮置乱采用从右到左、从下到上。

### 3.2　扩散变换

扩散变换通过修改像素值来扰乱明文图像与密文图像之间的关系。在扩散过程中，Logistic 映射用于产生扩散过程中的密钥流，扩散变换产生新的像素值。这里，所得到的像素值不仅与当前像素有关，还与之前像素相关。其计算如式(10)和(11)所示：

$$c(n)=\{[p(n)+k(n)]\bmod N\}\oplus c(n-1) \tag{10}$$

$$c(1)=\{[p(1)+k(1)]\bmod N\}\oplus R_0 \tag{11}$$

式中，$n$ 为像素序号，$p(n)$、$k(n)$和 $c(n)$分别表示当前明文像素、密钥流和输出密文像素，$c(n-1)$为前一个密文像素，$N$ 为图像的灰度级，$R_0$ 为扩散过程的控制参数，每一轮 $R_0$ 取值不同。若 $n=1$，则用式(11)进行扩散；否则，用式(10)进行扩散。

扩散变换是可逆变换，在解密时，其逆变换计算公式如式(12)和式(13)所示：

$$p(n)=[c(n)\oplus c(n-1)+N-k(n)]\bmod N \tag{12}$$

$$p(1)=[c(1)\oplus R_0+N-k(1)]\bmod N \tag{13}$$

上述扩散变换主要用来加强密码系统抗差分攻击的能力。一般情况下，攻击者可对明文进行一个微小的调整，并对原明文图像和调整后的明文图像进行加密，通过比较两幅密文图像，确定明文图像与密文图像之间的某种关系。如果明文图像中的一个微小变动扩散到整个密文图像中，差分攻击就会变得无效。文献[8,15,19]中扩散策略采取的扩散方向为从左到右、从上到下，文献[17]指出了这种扩散耗时且低效，并提出一种双向扩散的方案。文中引入了双向扩散的方案，即前后两轮扩散方向相反，该扩散方案使得明文一个微小变动在经过三轮加密之后就能影响到整个像素空间。

### 3.3　密钥扩展

密钥扩展是指由密码密钥得到指定长度的扩展密钥。由于所提出的图像加密算法 SPCME 要求每轮使用不同的轮密钥，用于混沌映射和扩散变换的控制参数，因此，扩展密钥中的字节数等于控制参数个数乘以轮数。

算法 1 密钥扩展算法的基本要素包括：(1)输入：16 个字节；(2)输出：一个由 27 个字节组成的一维数组，为加密算法提供三轮的密钥，每一轮需要 9 个字节的密钥。算法 1 描述了密钥扩展的过程。

**算法 1**　密钥扩展

输入：密码密钥 user_key[16]

输出：扩展密钥 key[27]

```
1. for i=0 to 2 do
2. key[i]=user_key[i]
3.   end for
4. for i=3 to 15 do
5.     if i mod 3==0 then
6.       key[i]=S(circshift(user_key[i-1]))⊕ key[i-3]⊕ user_
             key[i]⊕ Rcon[(i-1)/3];
7.     else
8.       key[i]=key[i-1]⊕ key[i-3];
9.   end if
10. end for
11. for i=16 to i=26 do
12.   if i mod 3==0 then
13.   key[i]=S(circshift(key[i-1]))⊕ key[i-3]⊕ Rcon[(i-1)/3];
14.   else
15.     key[i]=key[i-1]⊕ key[i-3];
16. end if
17. end for
```

输入密钥的前 3 个字节直接复制到扩展密钥数组的前 3 个字节。然后，每次向扩展密钥数组填充一个字节。在扩展密钥数组中，每一个新增的字节 $key[i]$ 的值依赖于 $key[i-1]$ 和 $key[k-3]$。当数组下标为 3 的倍数时，采用更复杂的函数来计算。

该函数具有 3 种功能：

(1)字节循环移位功能

字节循环功能使一个字节循环移位若干位。扩展密钥数组前 16 个字节，字节循环移位位数为 mod ($user\_key[i-1]$ ⊕ $user\_key[i-2]$,8)，移位方向使用规则：若 mod ($user\_key[i]$,2)=1，则向左移位；否则，向右移位。剩余字节循环移位的位数为 mod ($k(i-2)$⊕$k(i-1)$,8)，移位方向使用规则：若 mod ($k(i-1)$,2)=1，则向左移位；否则，向右移位。

(2)字节代换

字节代换功能利用 AES 算法的 S 盒对输入字节进行字节代换，以增强算法的混淆特性。

(3)消除对称性

将(1)和(2)的结果再与轮常量相异或 $Rcon[j]$，以消除算法的对称性。其中 $Rcon$ 的十进制数组为 $Rcon$=[1 2 4 8 16 32 64 128 27]。

### 3.4 SPCME 算法

SPCME 加密过程可归结为 5 个步骤，如图 2 所示。

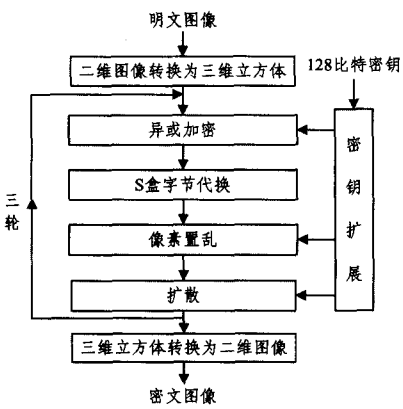


图 2 加密算法流程图

步骤 1(密钥扩展) 输入一个 128bits/16B 的密钥，经过密钥扩展算法，扩展为 216bits/27B 的密钥。按顺序每 9 个字节一组作为加密算法每轮的控制参数 $\mu, x_0, a_x, a_y, a_z, b_x, b_y, b_z, R_0$。具体的扩展算法见 3.3 节。

步骤 2(图像预处理) 将二维的图像数组分割并堆叠成若干个立方体。假定图像大小为 $W\times H$，可分割成若干个立方体 $N_1, N_2, \cdots, N_i$，这些立方体满足条件式(14)：

$$W\times H=N_1^3+N_2^3+\cdots+N_i^3+R \tag{14}$$

其中，$N_i\in\{2,3,\cdots,N\}$ 为立方体的边长，$N$ 为立方体边长最大值，$R\in\{0,1,2,\cdots,7\}$ 为余数。

步骤 3(混淆变换) 按照 3.1 节的规则对立方体进行混淆变换。

步骤 4(扩散变换) 按照 3.2 节的规则对混淆变换后的各像素值进行扩散变换。

步骤 5(图像二维转换) 将一系列立方体转换成二维图像。

考虑到安全性，步骤 3 和步骤 4 交替执行三轮。轮数越多，安全性越高，但加密计算所消耗的时间就越长。

解密过程是加密过程的逆过程，仅需对步骤 3 和步骤 4 的执行顺序进行交换。解密算法和加密算法结构类似，因此，它们的计算复杂度和消耗的时间基本相同。

## 4 性能分析

评价加密系统性能的基本方法是检验该系统能否阻止未授权者获取明文信息。一个好的加密系统应该能抵御所有已知的攻击，如已知明文攻击、选择明文攻击、唯密文攻击、统计分析攻击、差分攻击以及各种暴力破解攻击。SPCME 算法主要进行了 4 种安全性分析，具体包括：密钥空间分析、密钥敏感性分析、统计分析和差分攻击分析。

### 4.1 密钥空间分析

密钥空间大小是衡量密码系统安全性的一个重要指标，空间越大，系统抵抗暴力破解的能力越强。SPCME 算法的密钥长度为 128 比特，密钥空间大小为 $2^{128}\approx 3.4028\times 10^{38}$。从安全的角度来讲，密钥空间$\geqslant 2^{100}\approx 10^{30}$[20]就能满足较高的安全级别。由于该算法充分利用了混沌映射，攻击者可能会绕过密钥猜测，直接对混沌映射的控制参数进行猜测攻击[21,22]。

加密系统的参数密钥由 3 部分组成：异或密钥($\mu, x_0$)、置乱密钥($a_x, a_y, a_z, b_x, b_y, b_z$)和扩散密钥 $R_0$。异或阶段，使用 Logistic 映射，控制参数包括：$\mu\in[3.9,4]$和 $x_0\in(0,1)$。置乱阶段，采用 3D Arnold 映射，控制参数包括：$a_x$、$a_y$、$a_z$、$b_x$、$b_y$和 $b_z$ 等 6 个，每个控制参数均在区间[0,19]之内。扩散阶段的控制参数为 $R_0\in[0,255]$。参数密钥的这 3 个部分相互独立，并且每一轮的控制参数均不同，整个加密系统密钥空间如式(15)所示：

$$H=(10^6\times 10^6\times 20^6\times 256)^3\approx 4.398\times 10^{66} \tag{15}$$

显然，其足以抵抗控制参数密钥的暴力破解攻击。

### 4.2 密钥敏感性分析

密钥敏感性分析测试通过对密钥的微小调整，来考察 SPCME 算法加密系统的扩散特性。这种分析测试较为重要，因为攻击者可能会利用正确猜测的部分密钥对明文进行加密，在仔细观察密文图像的基础上，可能会重构部分明文图像。

密钥的敏感性分析采用两种方式：(1)利用两组具有微小差别的密钥加密同一幅图像，考察两个密文图像的差异；(2)解密密钥与加密密钥取微小差别，考察密文图像的解密效果。

具体实验步骤如下：

步骤 1　选择 6 组有 1 比特差别的密钥对，对同一幅256×256 的图像进行加密；

步骤 2　选择密钥“bsdfghjklm123456”对用“asdfghjklm123456”加密的密文图像进行解密。

实验结果 1：只有 1 比特差别的密钥对，分别加密同一幅图像，两个密文图像像素灰度值的差异度均在 99.60%以上，如表 1 所列。

表 1　密钥敏感性测试

| 密钥对(k1,k2) | 差异(%) |
|---|---|
| k1=asdfghjklm123456<br>k2=bsdfghjklm123456 | 99.62 |
| k1=asd fghjklm123456<br>k2=asd gghjklm123456 | 99.60 |
| k1=asdfgh jklm123456<br>k2=asdfgh iklm123456 | 99.63 |
| k1=asdfghjkl m123456<br>k2=asdfghjkl n123456 | 99.60 |
| k1=asdfghjklm12 3456<br>k2=asdfghjklm12 4456 | 99.64 |
| k1=asdfghjklm12345 6<br>k2=asdfghjklm12345 7 | 99.61 |

实验结果 2：如图 3 所示，若使用密钥“asdfghjklm123456”对图像进行加密，则该密钥能够正确解密密文图像，而使用具有 1 比特差别的密钥“bsdfghjklm123456”对图像解密失败。实验结果证明，该算法具有良好的密钥敏感性。

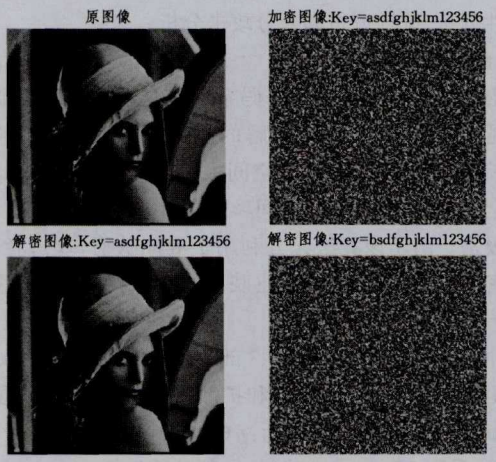


图 3　密钥敏感性测试

### 4.3　统计分析

攻击者可以利用统计分析工具，破译加密后的图像文件。因此，一种有效的加密系统应该能够抵御各种统计分析攻击。为了证明 SPCME 算法加密方案的鲁棒性，对密文做了以下 3 种常用的统计分析：统计直方图对比分析、相邻像素相关性分析和信息熵分析。

#### 4.3.1　统计直方图对比分析

图像的直方图通过统计图像中每一个灰度级的像素个数，揭示图像像素的分布规律。密文像素分布规律对整个密码的安全性起着至关重要的作用。具体来说，密文像素分布规律应能够隐藏明文的冗余度，不能泄露明文的任何信息以及明文与密文之间的关系。

明文图像(见图 4(a))和密文图像(见图 4(c))的直方图分别如图 4(b)和图 4(d)所示。从图 4 中可以看出，密文图像的直方图几乎是均匀分布的，与明文图像的直方图有较大区别。因此，密文图像直方图对于统计攻击无法提供任何攻击的线索。

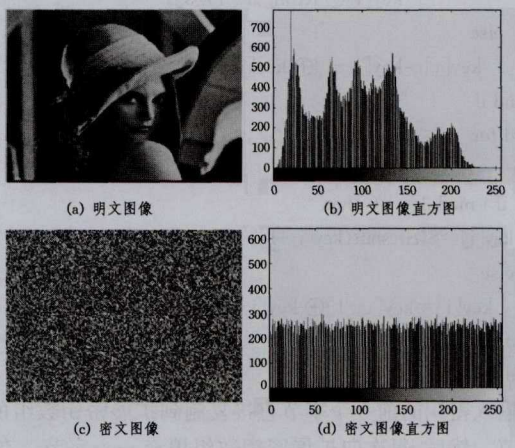


图 4　明文图像与密文图像的直方图

#### 4.3.2　相邻像素相关性分析

在普通的明文图像中，每一个像素与在水平、垂直和对角线方向上的相邻像素都有较强的相关性。因此，一个有效的图像加密系统应该使密文图像相邻像素相关系数趋于 0。

为了量化和比较明文图像和密文图像相邻像素相关性，分析测试采取以下两个步骤。首先，分别在明文图像和密文图像的每一个方向上随机选取 2000 对相邻像素值。其次，通过式(16)－式(19)计算相关性，进行比较分析。

$$\mathrm{cov}(x,y)=E\{(x-E(x))(y-E(y))\} \tag{16}$$

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{17}$$

$$E(x)=(\sum_{i=1}^{N}x_i)/N \tag{18}$$

$$D(x)=\{\sum_{i=1}^{N}(x_i-E(x))^2\}/N \tag{19}$$

其中，$x_i$ 和 $y_i$ 为图像第 $i$ 对相邻像素的灰度值，$N$ 表示随机挑选像素对的个数。

明文图像和密文图像相邻像素相关系数的计算结果如表 2 所列。明文图像与密文图像在水平方向、垂直方向和对角线方向相邻像素的相关性分析测试结果分别如图 5－图 7 所示。

表 2　明文图像和密文图像相邻两像素相关系数

| | 明文图像 | 密文图像 |
|---|---|---|
| 水平方向 | 0.9503 | −0.015 |
| 垂直方向 | 0.9148 | −0.0118 |
| 对角方向 | 0.9173 | 0.0129 |

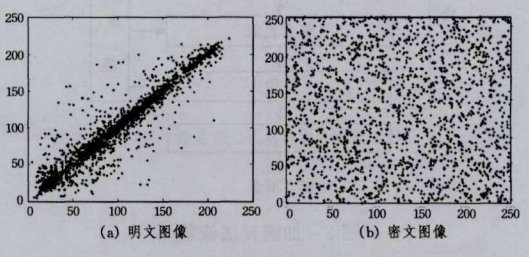


图 5　水平方向相邻像素的相关性

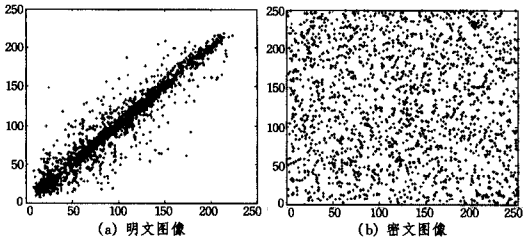


图 6　垂直方向相邻像素的相关性

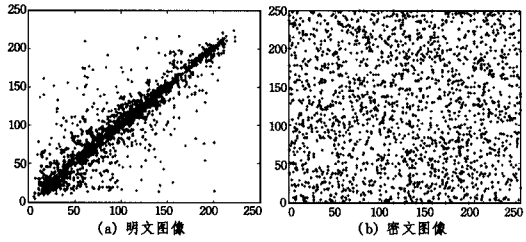


图 7　对角方向相邻像素的相关性

图 5—图 7 和表 2 显示：明文图像相邻像素相关性较大，而经过 SPCME 算法加密之后，密文图像相邻像素相关性趋近于零。

4.3.3　信息熵分析

在信息论中，信息熵是系统有序化程度的一个度量。信源 $S$ 的熵 $H(S)$可用式(20)进行计算：

$$H(S)=-\sum_{i=0}^{2^N-1}P(s_i)\log_2 P(s_i) \tag{20}$$

其中，$S=\{s_0,s_1,\cdots,s_i,\cdots,s_{255}\}$，$N$ 为符号 $s_i$ 二进制表示时的位数，$P(s_i)$为信源取第 $i$ 个符号 $s_i$ 的概率，$H(S)$的单位为比特。

一个完全随机的信源 $S$，输出 $2^N$ 个随机变量，其信息熵 $H(S)=N$。因此，密文图像的灰度级为 256 时，理想的熵 $H(S)=8$。若密文输出变量的熵小于 8，则表明密文存在一定程度的可预测性，密文的安全性较低。

用 SPCME 算法加密图像，分别统计明文和密文图像每一个像素 $s_i$ 出现的次数，并计算 $s_i$ 出现的概率。明文和密文图像的信息熵分别为 $H(S)=7.5534$ 和 $H(S)=7.9969$。密文图像的信息熵接近理论值 8，说明加密过程的信息泄露可以忽略，整个加密系统能够抵御熵攻击。

### 4.4　差分攻击分析

差分攻击通过对明文进行微小调整，比较原明文和微小调整之后密文之间的差别实施的攻击。通常采用像素变化比率(NPCR，Number of Pixel Change Rate)和统一平均变化程度(UACI，Unified Average Changing Intensity)两个指标对 SPCME 算法抵抗差分攻击性能进行评价。NPCR 表示明文图像发生一个像素值的变化时，加密后的图像发生变化的像素点个数占总像素点个数的比率，计算公式如式(21)所示。UACI 表示明文图像发生一个像素点变化时，所得密文图像与原图像相比，像素值发生的变化占整体灰度级的比率，计算公式如式(22)所示。

$$NPCR=\frac{\sum_{i,j}D(i,j)}{W\times H}\times 100\% \tag{21}$$

$$UACI=\frac{1}{W\times H}\left[\sum_{i,j}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right]\times 100\% \tag{22}$$

其中，$C_1$ 和 $C_2$ 为两个密文图像，与其所对应的明文图像仅有一个像素不同。$C_1(i,j)$和 $C_2(i,j)$分别为 $C_1$ 和 $C_2$ 在坐标 $(i,j)$处的像素值。$D$ 的值由 $C_1(i,j)$和 $C_2(i,j)$确定，当 $C_1(i,j)=C_2(i,j)$时，$D(i,j)=0$；否则，$D(i,j)=1$。

为了测试 SPCME 算法的 NPCR 和 UACI，加密一幅256×256 的图像，不同加密轮数时的 NPCR 和 UACI 值如表 3 所列。测试结果表明：随着加密轮数的增加，改变一个像素对整个密文的影响会变大，当加密轮数大于 3 时，NPCR 和 UACI 的值趋于稳定，分别维持在 99.60%和 33.50%左右。测试结果表明 SPCME 算法具有较好的抵抗差分攻击的能力。

表 3　SPCME 算法在不同加密轮数下的 NPCR 和 UACI 值

| 轮数 | NPCR(%) | UACI(%) |
|---|---|---|
| 1 | 47.81 | 23.99 |
| 2 | 97.36 | 32.55 |
| 3 | 99.61 | 33.51 |
| 4 | 99.61 | 33.40 |
| 5 | 99.59 | 33.50 |

### 4.5　加密效率分析

加密系统不仅要考虑安全问题，同时也要考虑加密效率问题，尤其是一些对实时性要求比较高的互联网应用。以 NPCR 和 UACI 同时接近理想值为标准($NPCR>0.996$，$UACI>0.333$)，比较 SPCME 算法与文献[8,23]中的算法所需置乱和扩散的次数，如表 4 所列，在保障安全的条件下，SPCME 算法具有较高的加密效率。

表 4　算法所需置乱/扩散次数对比

| | NPCR(%) | UACI(%) | 置乱 | 扩散 |
|---|---|---|---|---|
| 文献[8] | 50.23 | 25.23 | >5 | >5 |
| 文献[23] | >99.60 | >33.30 | 18 | 6 |
| SPCME 算法 | >99.60 | >33.30 | 3 | 3 |

**结束语**　本文提出一种基于混沌的 SP 结构图像加密算法 SPCME，用于提高基于置乱-扩散结构的图像加密算法的安全性和效率。SPCME 算法首先引入了现代分组密码设计所遵循的 SP 结构，利用混沌映射异或加密和 AES 算法的 S 盒进行字节代换，增强了算法的安全性。其次，SPCME 采用双向的置乱-扩散策略，增强了算法的混淆特性，加快了扩散速度。第三，SPCME 密钥扩展过程采用简单的循环移位和异或操作，降低了计算复杂度，提高了密钥扩展效率。最后，针对 SPCME 算法的安全性和效率，分别进行了密钥空间分析、密钥敏感性分析、统计分析以及差分攻击分析等性能分析。结果表明，相较于基于置乱-扩散结构的图像加密算法，基于混沌的 SP 结构图像加密算法 SPCME 具有两方面优势：(1)安全性好，能够抵抗典型密码分析攻击；(2)效率高，经过较少轮数加密就能达到同类算法的安全级别。

## 参 考 文 献

[1]　Alvarez G, Li S. Some basic cryptographic requirements for chaos based cryptosystems[J]. International Journal of Bifurcation and Chaos, 2006, 16(08): 2129-2151

[2] 黄伟琦,陈志刚,梁涤青,等.基于多混沌系统的医学图像加密算法[J].计算机科学,2012,39(12):261-263,299

[3] Li Shu-jun, Mou Xuan-qin, Cai Yuan-long. Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography[M]// Progress in Cryptology-INDOCRYPT 2001. Springer Berlin Heidelberg,2001:316-329

[4] Liu Nian-sheng. Pseudo-randomness and complexity of binary sequences generated by the chaotic system[J]. Communications in Nonlinear Science and Numerical Simulation, 2011, 16(2): 761-768

[5] Chee C Y, Xu D. Chaotic encryption using discrete-time synchronous chaos[J]. Physics Letters A,2006,348(3):284-292

[6] Kocarev L,Jakimoski G. Logistic map as a block encryption algorithm [J]. Physics Letters A,2001,289(4):199-206

[7] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps[J]. International Journal of Bifurcation and Chaos,1998,8(6):1259-1284

[8] Chen Guan-rong, Mao Yao-bin, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons & Fractals,2004,21(3):749-761

[9] Zhu Zhi-liang, Zhang Wei, Wong K, et al. A chaos-based symmetric image encryption scheme using a bit-level permutation [J]. Information Sciences,2011,181(6):1171-1186

[10] Tong Xiao-jun, Cui Ming-gen. Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator[J]. Signal Processing,2009,89(4):480-491

[11] Tong Xiao-jun. Design of an image encryption scheme based on a multiple chaotic map[J]. Communications in Nonlinear Science and Numerical Simulation,2012,18(7):1725-1733

[12] Rhouma R, Meherzi S, Belghith S. OCML-based colour image encryption[J]. Chaos, Solitons & Fractals,2009,40(1):309-318

[13] Xu Shu-jiang, Chen Xiu-bo, Zhang Ru, et al. An improved chaotic cryptosystem based on circular bit shift and XOR operations [J]. Physics Letters A,2012,376(10):1003-1010

[14] Mazloom S,Eftekhari-Moghadam A M. Color image encrypttion based on coupled nonlinear chaotic map[J]. Chaos, Solitons & Fractals,2009,42(3):1745-1754

[15] Wang Yong, Wong K, Liao Xiao-feng, et al. A chaos-based image encryption algorithm with variable control parameters[J]. Chaos, Solitons & Fractals,2009,41(4):1773-1783

[16] Zhang Wei, Wong K, Yu Hai, et al. An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion [J]. Communications in Nonlinear Science and Numerical Simulation,2013,18(8):2066-2080

[17] Fu Chong, Chen Jun-jie, Zou Hao, et al. A chaos-based digital image encryption scheme with an improved diffusion strategy [J]. Optics Express,2012,20(3):2363-2378

[18] Shannon C E. Communication theory of secrecy systems [J]. Bell system technical journal,1949,28(4):656-715

[19] Wang Yong, Wong K, Liao Xiao-feng, et al. A new chaos-based fast image encryption algorithm[J]. Applied soft computing, 2011,11(1):514-522

[20] Schneier B. Applied cryptography: protocols, algorithms, and source code in C[M]. John Wiley & Sons,2007

[21] 郭建胜,张锋.一种图像加密算法的等效密钥攻击方案[J].电子学报,2010,38(4):781-785

[22] Solak E,Cokal C, Yildiz O T, et al. Cryptanalysis of Fridrich's chaotic image encryption[J]. International Journal of Bifurcation and Chaos,2010,20(05):1405-1413

[23] Lian S,Sun J, Wang Z. A block cipher based on a suitable use of the chaotic standard map[J]. Chaos, Solitons & Fractals, 2005, 26(1):117-129

(上接第 136 页)

[10] Van den Bergh F. A new locally convergent particle swarmoptimizer[C]//Proc of the IEEE Int Conf on Systems, Man and Cybernetics. Tunisia: IEEE,2002:94-99

[11] Sun J, Feng B, Xu W B. Particle swarm optimization with particles having quantum behavior[C]// Proc of 2004 Congress on Evolutionary Computation. Portland: IEEE,2004:325-331

[12] 龙海侠,须文波,王小根,等.基于选择操作的量子粒子群算法[J].控制与决策,2010,25(10):1499-1506

[13] 章国勇,伍永刚,顾巍.基于精英学习的量子行为粒子群算法[J].控制与决策,2013,28(9):1341-1348

[14] 刘军名,高岳林.混沌粒子群优化算法[J].计算机应用,2008,28(2):322-325

[15] Chen D B, Wang J T. An improved group search optimizer with operation of quantum-behaved swarm and its application[J]. Applied Soft Computing,2012,12(2):712-725

[16] 逄珊,杨欣毅,张小峰.混沌映射的多种群量子粒子群优化算法[J].计算机工程与应用,2012,48(33):56-62

[17] 武晓今,朱仲英.遗传算法多样性测度问题研究[J].信息与控制,2005,34(4):416-422

[18] Wieselthier J E, Nguyen G D, Ephremides A. On the construction of energy-efficient broadcast and multicast trees in wireless networks[C] // Proceedings of IEEE INFOCOM' 2000. Tel Aviv, Israel,2000:585-594

[19] 朱晓建,沈军.基于粒子群优化的 ad hoc 网络最小能耗多播路由算法[J].通信学报,2012,33(3):52-58

[20] 李渊,杨立波.基于最优能耗多播树构造的 Ad hoc 网络节点路由算法研究[J].计算机科学,2013,40(4):115-118

[21] Wieselthier J E, Nguyen G D, Ephremides A. Energy-aware wireless networking with directional antennas: the case of session-based broadcasting and multicasting[J]. IEEE Transactions on Mobile Computing,2002,1(3):176-191