基于可 Markov 分割混沌系统的图像加密算法

刘 泉*①② 李佩玥① 章明朝① 隋永新① 杨怀江①
①(中国科学院长春光学精密机械与物理研究所应用光学国家重点实验室 长春 130033)
②(中国科学院大学 北京 100039)

摘 要：为了设计复杂度高、安全性好而计算代价小的图像密码算法，该文从一类新的具有 Markov 分割性质的混沌系统出发构造了此算法。首先，通过控制此混沌系统的参数并配合时空混沌系统设计了一个密钥流发生器；然后，利用真随机数发生器产生的随机数来扰动系统的初始密钥，以动态生成图像的置换矩阵和加密密钥流；最后，通过利用不同群中的加法混合运算构造扩散函数以增加破译复杂度，以两轮迭代完成了图像加密过程。实验结果表明，此混沌系统产生的密钥流序列有比较好的统计特征，该算法可以破坏原始图像的特征，使得密文图像难以辨识。进一步分析可知，该算法可以很好地抵抗差分分析等其它已知攻击，效率高于一些基于超混沌系统设计的密码算法。此外，此算法计算简单，安全性高，易于实现，具有良好的应用前景。

关键词：图像加密；混沌；Markov 分割；时空混沌
中图分类号：TP309.7 **文献标识码**：A **文章编号**：1009-5896(2014)06-1271-07
DOI: 10.3724/SP.J.1146.2013.01246

Image Encryption Algorithm Based on Chaos System having Markov Portion

Liu Quan①② Li Pei-yue① Zhang Ming-chao① Sui Yong-xin① Yang Huai-jiang①
①(*State Key Laboratory of Applied Optics*, *Changchun Institute of Optics*, *Fine Mechanics and Physics*, *Chinese Academy of Sciences*, *Changchun* 130033, *China*)
②(*University of Chinese Academy of Sciences*, *Beijing* 100039, *China*)

Abstract: In order to construct a high complexity, secure and low cost image encryption algorithm, a class of chaos with Markov properties is studied and used to build the encryption algorithm. First, the key stream generator is designed by the Markov Chaos with changeable parameters and the improved spatiotemporal chaos. Then, a true uniform random number generator is used to disturb the original key of the algorithm, which can dynamically change the mixed matrix and the key stream. Finally, the diffusion function is built by two iterations of the round function which is composed of different kinds of additions in different groups to increase the complexity of decipher. The experiments indicate that the key stream possesses good statistical properties, and the characteristic of the original image is broken which makes the cipher image undistinguishable. The further analysis indicates that the proposed algorithm can resist some known attacks like differential attacks, and the proposed algorithm is more efficient than the existed algorithms based on super chaos. Additionally, the proposed algorithm is easy to realize and can satisfy the security and efficiency requirements, which indicates promising applications.

Key words: Image encryption; Chaos; Markov portion; Spatiotemporal chaos

1 引言

近年来，网络上保存和传输的图像数据量越来越大，图像信息的保密性成为一个突出问题，而加密算法可以保证仅授权用户才能获知图像信息，从而实现对图像信息的保密。传统的加密算法如数据加密标准 DES、高级加密标准 AES、国际数据加密算法 IDEA 等是基于文本设计的，将其用在图像加密上并不合适[1,2]，主要是因为 AES 等加密算法加密后的图像，其图像信息依然可以感知，这是由图像信息不同于文本信息，其相邻像素存在很强的相关性所致。

为解决这一问题，利用混沌的加密算法正吸引越来越多的注意[3–8]。Baptista[3]提出一种基于查找的混沌分组密码算法，此算法简单而受到了很多关

2013-08-19 收到，2013-11-21 改回
国家 973 规划项目(2007CB311201)，应用光学国家重点实验室开放基金(Y1Q03FQK02)和吉林省科技发展计划项目(20130522120JH)资助课题
*通信作者：刘泉 lovefirespread@gmail.com

注，但是因为它具有密文扩散且分布不均的缺点而没有得到广泛应用。Fridrich[4]提出了一种图像密码算法的结构模型，将整个密码算法分为两个阶段：置乱和扩散。置乱用于扰乱图像中像素的位置，可以改变图像的位置结构，消弱图像相邻像素的相关性；扩散用于替换掉图像的像素值，使得密文图像像素的分布特性与明文无关。现在设计的图像加密算法几乎都遵照该模型[3−9]。文献[10]破解了文献[4]所提出算法，主要原因是文献[4]中的扩散函数结构过于简单，难以抵抗选择明文攻击，文献[3–8]中的其它算法也存在类似的问题而存在被破解的可能。文献[11]总结了一些混沌图像加密算法存在的问题。文献[12]利用选择明文攻击 CPA 等多种攻击方式均破译了一种改进的混沌密码算法，并指出 Logistic 映射具有分布不均且密钥空间小的缺点不适合直接用于密码设计，并给出了算法设计的相关建议。通过对现有文献分析，我们认为混沌密码算法存在的问题主要有 3 方面：首先，混沌系统的极限分布不均匀而可能被破译者发现其特点，其抗差分攻击能力弱；其次是算法结构缺陷使其不能抵抗选择密文攻击 CCA 攻击或选择明文攻击 CPA 攻击等;最后，算法性能的优化问题，构造的算法结构过于复杂而造成加解密效率不高。

基于上述分析，本文采用了一类新的混沌系统[13]，该系统是一类具有 Markov 性质的分段线性映射。可以证明它产生的序列服从均匀分布，线性不相关，没有不动点，这比基于 Logistic 映射设计的混沌密码算法要好，通过参数的选取，它可以避免类似 Tent 映射的有限精度退化问题。文献[14]指出，Logistic 映射和 Tent 映射复杂度低，不适合用于设计密码算法，而本文所用混沌系统[13]是一种新型低维混沌系统，通过参数选取，产生的复杂度比 Logistic 和 Tent 映射大得多，这意味着其更接近真随机数[15]，显示其实用价值。为解决低维混沌系统密钥空间小的问题，采用时空混沌系统是一种不错的选择[16]，本文利用上述新的混沌改进了耦合格子映射，其产生的序列具有更好的统计性质。利用产生的序列构造置换矩阵，并用它来构造扩散阶段的密钥序列。通过对算法置乱和扩散阶段的函数进行优化，采用不同群中的加法混合运算构造的扩散函数可以更好地抵抗 CPA 和 CCA 攻击。本文设计的算法迭代两轮即可产生比较好的加密效果，而加解密效率并不低。

本文组织如下：第 2 节给出本文所用的混沌系统及其性质说明；第 3 节介绍本文所用的图像加密算法；第 4 节给出所用系统的各种测试；最后是本文内容的总结。

2 混沌系统构造

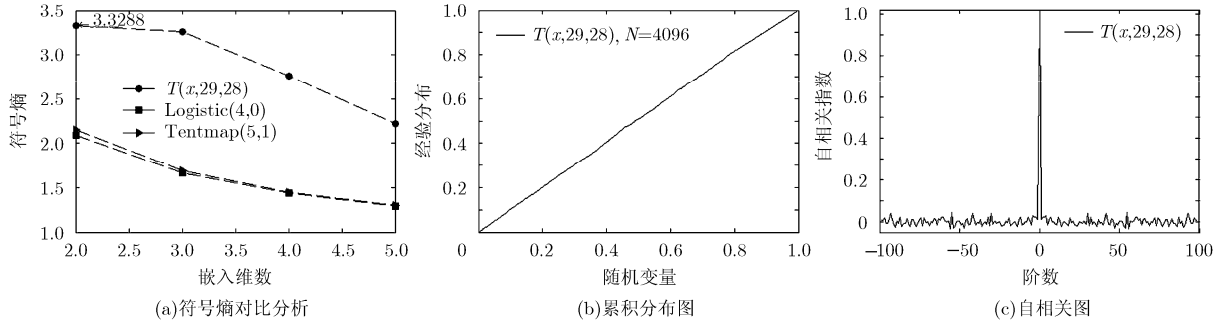
2.1 可 Markov 分割的混沌系统的特性

本文使用一种可 Markov 分割的混沌系统[13]，简单描述如下：选取参数 $p(p\ge 7)$ 是素数，将[0,1]区间 p 等分，构造映射 $T(x,p,\sigma)$ 如式(1)，其中 $\sigma\in Z^+$ 且 $2\le\sigma\le p-1$。

$$T(x,p,\sigma)=\begin{cases}\left[\sigma x+\dfrac{(i+1)-i\sigma}{p}\right]\bmod 1;\\ \quad x\in\left[\dfrac{i}{p},\dfrac{i+1}{p}\right),i=0,1,\cdots,p-2\\ \left[\sigma x+\dfrac{p-(p-1)\sigma}{p}\right]\bmod 1;\\ \quad x\in\left[\dfrac{p-1}{p},1\right]\end{cases}\tag{1}$$

其平均 Lyapunov 指数为 $\ln(\sigma)$，其 Markov 分割为 $I_1,I_2,\cdots,I_p$，其中 $I_k=[(k-1)/p,\ k/p]$，$k=1,2,\cdots,p$。

此系统产生的序列有着比较好的统计性质：其极限分布为均匀分布，自相关函数近似为 δ 函数，为一个理想的均匀伪随机序列。而通过对其复杂度分析可知，通过参数调整它具有比 Logistic 映射和帐篷映射高得多的复杂度，其符号熵对比分析结果如图 1(a)所示。



(a)符号熵对比分析 (b)累积分布图 (c)自相关图

图 1 序列的基本统计性质

随机选取初始点 $(x_0 = 1/23)$ 迭代 4096 次实验，其均匀性和相关性如图1(b)和图1(c)所示。从图 1(b)可知，其累计分布函数类似一条直线，这意味着其概率密度函数近似于常数，即为均匀分布。通过 Kolmogorov-Smirnov 统计检验得 p 值为 p1_KS=0.9590，通过 Chi-square 拟合优度检验得 p 值为 p1_CHI2=0.9597，可以认为此系统产生的序列服从均匀分布。而对序列的相关分析如图 3(c)所示，其接近于一个 δ 函数，为一个理想的伪随机序列。

2.2 改进时空混沌系统

低维的混沌系统因密钥空间限制和相空间结构简单而可能产生安全漏洞，这可以利用时空混沌系统来解决，其中最常用的是耦合格子映射。一个 K 阶的单向发展的耦合格子映射如式(2)，可掩盖系统的相空间结构，其常用于密码系统的设计，其结构表示如式(2)。

$$\left.\begin{aligned} &y_{n+1}(1) = (1-\varepsilon)f(y_n(1)+\varepsilon g_n)\\ &y_{n+1}(i) = (1-\varepsilon)f(y_n(i))+\varepsilon f(y_n(i+1))\\ &g_n = f(y_n(2));\ i = 2,3,\cdots,K,\ n = 0,\ 1,\ 2,\cdots \end{aligned}\right\} \quad (2)$$

边缘条件满足 $y_n(K+1) = y_n(1)$，g_n 表示耦合格子映射的输出，K 表示系统耦合的阶数，ε 表示为耦合轨道分配的权重。函数 f 为基本的混沌系统，在文献[16]中，$f(x) = 4x(1-x)$ 是 Logistic 映射，因其产生的序列非均匀分布，用于密码设计不够理想，这里用上述的混沌系统 $T(x,p,\sigma)$ 来代替。$(y_0(1), y_0(2),\cdots,y_0(K))$ 表示耦合格子系统的初始值，可用做混沌密码系统的初始密钥。

选取系统参数为K=6，权重 $\varepsilon = 0.99$ 初始值为 $(0.9/6, 1.9/6, 2.9/6, 3.9/6, 4.9/6, 5.9/6)$，迭代4096次后测试结果如图2所示。通过耦合格子映射变换后的混沌系统的相空间如图2(a)和图2(b)所示已无规律可循，由图中可以看出，原系统的相空间分布在边缘位置较稠密而中间偏稀疏，而改进后的系统其分布明显好于原系统。然后，对改进的系统测试其累积分布，与原系统的对比如图2(c)和图2(d)所示，可见改进系统其累积分布更接近均匀分布，因而更适合用于密码算法的设计。

3　图像密码算法构造

3.1 算法框架

分析了上述加耦合格子映射的混沌系统性质后，利用其产生的序列生成密钥流，根据密钥流生成动态置乱矩阵，对图像像素位置进行置乱，然后利用迭代加密模块对像素数值进行替换。该图像密码算法分为 3 个部分：密钥生成算法，加密算法和解密算法。其加密过程如图 3 所示。

3.2 密钥流生成算法

步骤 1　选择混沌系统参数 p(为素数)和 σ(sigma)，耦合格子系统阶数 K(dim)和耦合轨道分配的权重 e。

步骤 2　根据耦合格子系统阶数 K 选择迭代系统初始值为 $(X_1, X_2,\cdots, X_K)$，密钥为 $(x_1, x_2,\cdots, x_k)$，此处 $x_t(t = 1,\cdots, K)$ 仅表示与 $X_t(t = 1,\cdots, K)$ 区别，无特殊意义。然后通过[0,1]上均匀分布的真随机数 RND(其生成方式已有不少[17])扰动密钥，生成迭代初始值 $X_i = \overline{x_i + \mathrm{RND}}(i = 1,2,\cdots, K)$。引入真随机数可达到一次一密的效果。迭代过程中产生的密钥流需要量化为字节流 $k_n = \mathrm{floor}(g_n \times 256)$。

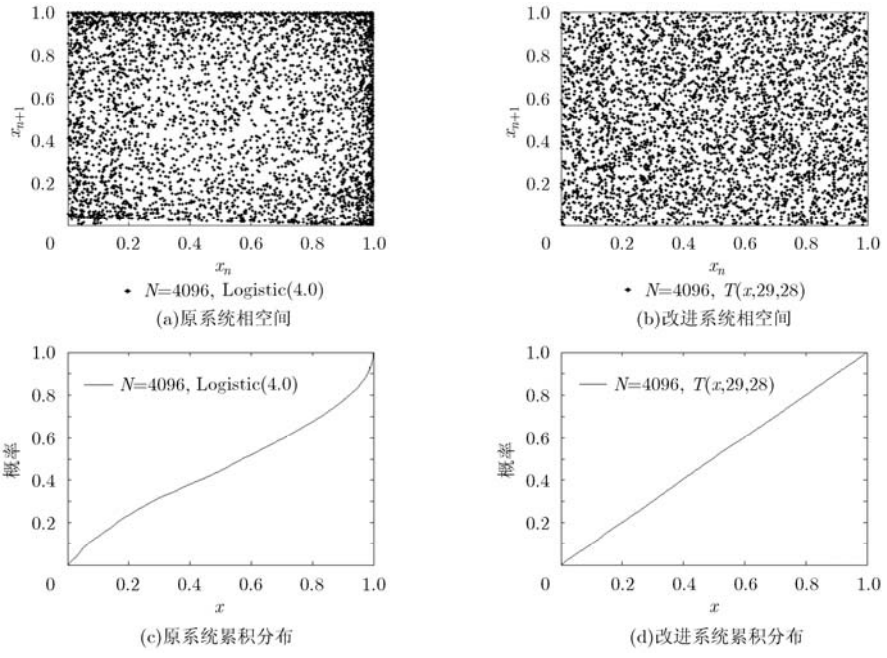


图 2 改进的时空混沌与原系统的特性对比

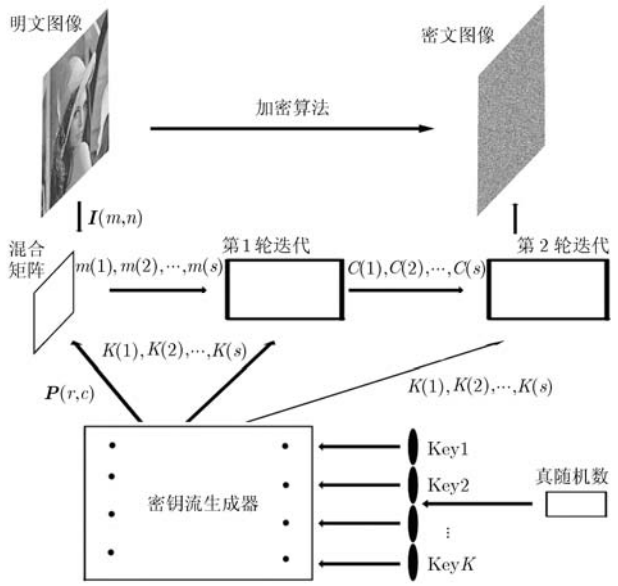


图 3 图像加密算法框架

步骤 3 根据输入的明文图像尺寸 $S(M\times N)$ 生成密钥流的长度 L=$2\times M\times N$，记为 $k_1,k_2,\cdots,k_L$。其中 $\boldsymbol{K}_{L_1}=(k_1,k_2,\cdots,k_{L_1})\triangleq(p_1,p_2,\cdots,p_{L_1})(L_1=M\times N-1)$ 用于消除系统初始迭代时的震荡和构造置换矩阵，舍弃前 16 个数值，然后依次产生 M 个和 N 个不同的整数序列构成两个置换 $\boldsymbol{P}_M$ 和 $\boldsymbol{P}_N$，将生成的置换矩阵记为 $\boldsymbol{P}^{rc}(I)=\boldsymbol{P}_M\circ\boldsymbol{P}_N(I)$。后半部分密钥记为 $\boldsymbol{K}_{L_2}=(k_{L_1+1},k_{L_1+2},\cdots,k_L)=(k_1,k_2,\cdots,k_{L_2})(L_2=L-L_1)$，直接用于加密图像的迭代操作。

3.3 加密步骤

步骤 1 初始明文图像记为 $\boldsymbol{I}=(I_{ij})_{M\times N}$，置换操作后的图像为 $\boldsymbol{P}=(p_{ij})_{M\times N}=\boldsymbol{P}^{rc}(I)$。将置换后的图像记为数据流的形式即为 $(m_1,m_2,\cdots,m_t,\cdots,m_s)$，其中 $m_t=p_{ij},t=(i-1)\times M+j,1\le t\le s$。

步骤 2 将生成的数据流依次输入两轮迭代系统表示如式(3)和式(4)，经过此两轮操作后产生的密文为 $(D_1,D_2,\cdots,D_t,\cdots,D_S)$。这里的 C_0 为迭代系统的启动参数，它作为密钥由密钥文件提供。

$$\text{Round1}:\begin{cases}C_1=\overline{(m_1+k_2)}\oplus\overline{(C_0+k_1)}\\C_2=\overline{(m_2+k_3)}\oplus\overline{(C_1+k_2)}\\\vdots\\C_S=\overline{(m_S+k_{S+1})}\oplus\overline{(C_{S-1}+k_S)}\end{cases}\tag{3}$$

$$\text{Round2}:\begin{cases}D_1=\overline{(C_1+k_2)}\oplus\overline{(C_S+k_1)}\\D_2=\overline{(C_2+k_3)}\oplus\overline{(D_1+k_2)}\\\vdots\\D_S=\overline{(C_S+k_{S+1})}\oplus\overline{(D_{S-1}+k_S)}\end{cases}\tag{4}$$

其中 $\oplus$ 表示异或运算，$\overline{(A+B)}$ 定义为 $(A+B)\bmod 1$。

3.4 解密步骤

该图像密码算法为对称密码算法，所用解密密钥同加密密钥一致，密钥生成算法同上，此处真随机数与加密过程所用保持一致。解密过程为加密过程的逆向操作，由 $(D_1,D_2,\cdots,D_S)$ 可先计算出 $(C_1,C_2,\cdots,C_S)$，然后再恢复出明文 $(m_1,m_2,\cdots,m_s)$，而图像的置乱操作是可逆的，利用置乱矩阵即可直接恢复出原图像。

3.5 密钥文件

上述算法所用的密钥文件如表所示，主要有 4 个部分构成，混沌系统参数、耦合格子映射参数，加密系统启动参数和真随机数。其中参数 $(p,\text{sigma},\dim,e)$ 这 4 个参数变动范围比较小，密钥空间的大小主要靠 $(X_1,X_2,\cdots,X_{\dim})$ 和 RND 来提高，以 dim=6 为例，在 32 位系统中，密钥长度即可达到 192 bit，再加上产生的真随机数 C 也是 32 bit，系统的密钥长度可达 224 bit。该图像加密算法对密钥的变化非常敏感，这可由后文的密钥敏感性测试看出。系统密钥文件的参数和功能如表 1 所示。

表 1 系统密钥文件

参数	功能
p, sigma	混沌系统参数
dim, e, X_1, X_2, $\cdots$,$X_{\dim}$	耦合格子映射参数
C	加密系统启动参数
RND	真随机数

4 系统测试

4.1 基本测试

为检验所设计混沌系统密码算法的安全性，选用以下参数进行验证：混沌系统为 $T(x,29,28)$，耦合格子映射的阶数为 K=6，权重 $\varepsilon=0.99$，初始值为(0.9/6, 1.9/6, 2.9/6, 3.9/6, 4.9/6, 5.9/6), RND=0.01/6, $C=29$。选择 Lena 图像，如图 4(a)所示，加密后的图像如图 4(c)所示。当密钥正确时，利用解密算法可以恢复出原始 Lena 图像，密钥错误时不能恢复。

由图 4 可知，加密后的图像没有明显的规律性，而且其灰度值大致均匀。对加密前后的图像像素值统计对比分析如图 5 所示。图 5(a)表示原始图像的灰度直方图，图 5(b)表示加密图像的灰度直方图，可见加密之后的图像灰度分布与原始图像相比有较大的改变，它近似为均匀分布。

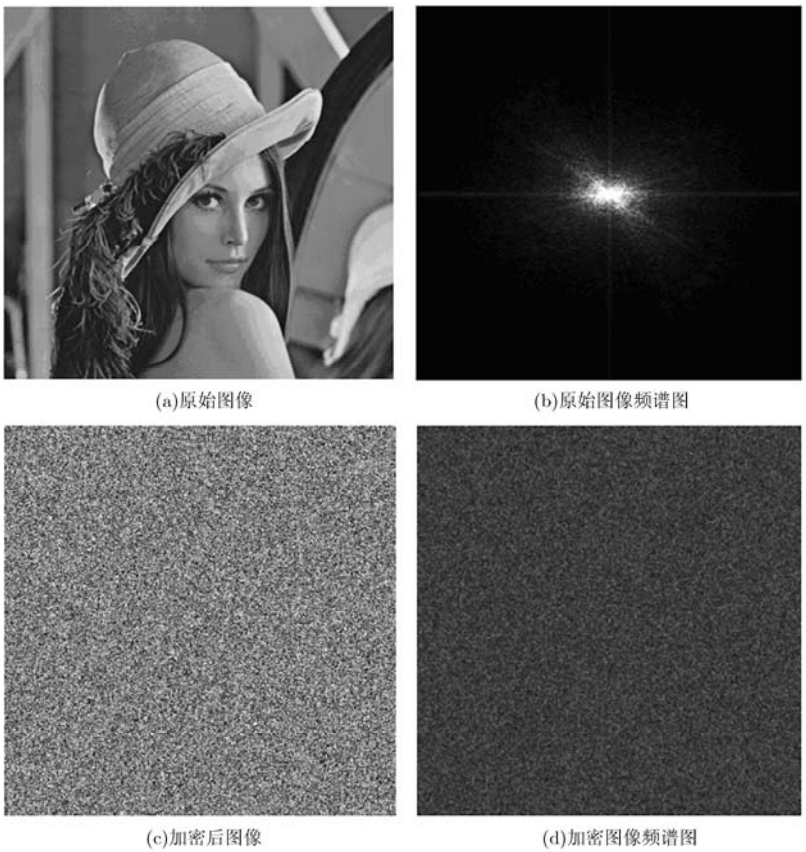


图 4 加密前后对比

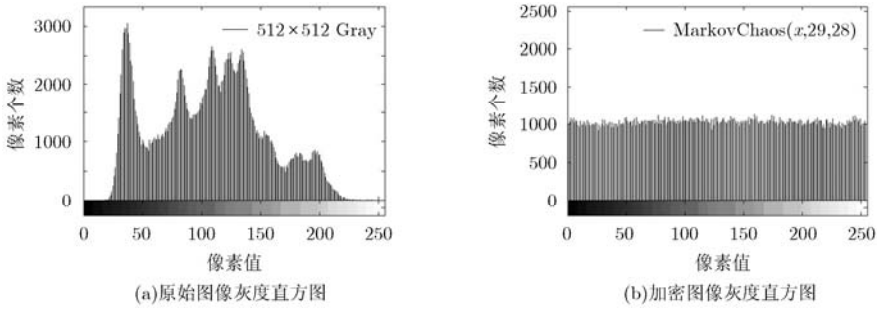


图 5 加密前后图像像素分布直方图对比

对图像进行 2 维傅里叶变换分析可知其原始图像的频谱中心化后如图 4(b)所示，加密后的图像做傅里叶变换如图 4(d)所示。通过比较可知，原图像在中心位置的能量较高。图像像素值可构成一个曲面，由图 4(b)可知此曲面的低频部分能量较高，而高频部分能量较低，而图 4(d)是加密后的图像，其高频和低频部分能量无明显差异，其能量分布整体上比较均匀。

4.2 安全性分析

(1)**相关分析**　对理想的图像加密算法来说，至少应保证其密文图像在水平、垂直和对角线方向的自相关函数近似为一个 δ 函数，而且 3 个方向的相邻像素几乎不线性相关。对其 3 个方向的自相关分析可知其自相关函数类似 δ 函数，对明文和密文相邻像素(在水平，垂直和对角线方向)的互相关分析对比如表 2 所示。

表 2 加密前后的相关系数对比

方向	原始图像	加密图像
水平	0.9704	−0.0601
垂直	0.9782	−0.0577
对角	0.9851	0.0092

由表 2 可知，原始图像在 3 个方向上的相关性

比较大，而加密图像却比较小。这主要是因为原始图像像素变化大致连续，相邻的像素值差别不太大，所以相关度比较高，而密文图像相邻像素变化剧烈，故其在 3 个方向的相关度都比较低。传统的分组密码算法(如 DES 和 AES 算法)在应用于图像加密时，密文图像的相关性比较强，这将导致图像相邻像素的关联信息泄露，而本文的密码算法相对来说更有优势。

(2)**差分分析** 由密码学原理，好的密码算法应该对明文变化敏感，敏感性与其抵抗差分攻击的能力密切相关。加密算法对明文的敏感性可以用图像像素数改变率(Number of Pixels Change Rate, NPCR)来衡量。定义其为两幅图像中不同像素的比例，设两幅密文图像中$(i,\ j)$值分别为$C_1(i,j)$和$C_2(i,j)$，则$D(i,j)=\begin{cases}1, C_1(i,j)\neq C_2(i,j)\\ 0, C_1(i,j)=C_2(i,j)\end{cases}$，那么$P_{\mathrm{NPCR}}$即为像素改变率。对 256 级灰度图像来说，$P_{\mathrm{NPCR}}$(定义如式(5)所示)其理想值为$P_{\mathrm{NPCR}}$=(1– 2– 8)×100% = 99.6094%。

$$P_{\mathrm{NPCR}}=\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{D(i,j)}{MN} \tag{5}$$

通过在原始图像中的起始部分，中间部分和末尾部分选取 100 个组对比实验，每次仅改变明文的一个比特，那么对应密文的 NPCR 值如图 6(a)所示，其变化率的均值接近于算法所能达到的理想值。与文献[16]等提出的算法相比，本文的算法对明文变化更敏感，且具有更强的抗差分攻击能力。

(3)**密钥敏感性测试** 一个好的密码算法需要对密钥非常敏感[18]，当密钥$(X_1, X_2, \cdots, X_{\mathrm{dim}})$或 RND 的一个比特发生变化时，密文将发生剧烈变化，其密文变化的理想值为 99.6094%，对图像算法测试可知，其 NPCR 值平均为 99.6103%。通过比较其密文的差值可知它们的变化是均匀随机的，图 6(b)以其前 200 个组的密文变化的情况为例进行验证，说明其在 0~255 间随机地变化。

4.3 算法效率

混沌密码算法所用混沌系统迥异，算法结构各不相同，安全性也有区别。本文先从密钥流生成的角度对它们进行分析。对基于微分方程的混沌系统来说，若采用四阶龙格库塔方法求解，每产生一个新的输出，Lorenz 系统需要 25 次加法，25 次乘法和 2 次除法操作，超混沌系统需要 36 次加法，44 次乘法和 2 次除法操作。Logisitc 映射需要 1 次加法和 2 次乘法操作。本文的混沌系统需要 3 次加法，2 次乘法，1 次除法和 1 次模 1 操作(复杂度小于加法)。加耦合格子后需要 30 次加法，18 次乘法，6 次除法和 6 次模 1 操作。故本文密钥流生成效率比文献[8,12]高，再从加解密操作来看，运算量与文献[8, 12]相当。故本文算法效率更高。若从并行计算角度来看本文的算法效率更容易提升，且耦合格子的使用效率可进一步提高。

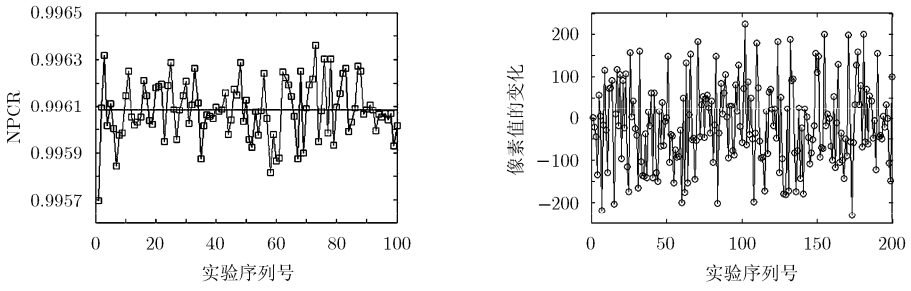
实验硬件环境为 Pentium(R) Dual-Core 2.6 GHz CPU, 2 G 内存的 PC 机，软件环境为 Windows XP 操作系统 Matlab 2009 平台。与基于连续映射的超混沌设计的密码算法[14]相比，在产生 4096 bit 长度密钥时，基于超混沌的算法需要 43.4375 s，基于 Lorenz 系统的混沌系统需要时间 10.8906 s，而本文算法仅需 0.1563 s。另外，基于耦合格子映射的系统有比较好的并行结构，在 FPGA 上实现时可达到更高的运算效率。由此可见，本文密码算法与建立在微分方程系统上的连续混沌系统相比有更大的速度优势。

4.4 与已有方案对比分析

首先，直接使用 Logistic 等映射构造密码算法时，其分布并不均匀，产生序列的极限分布特点会泄露所用混沌系统的参数信息，本文使用的混沌系统的极限分布是均匀分布的，不会泄露这部分信息。然后，由本文图 1(a)可知，本文所用的混沌映射比直接使用 Logistic 映射和 Tent 映射产生的序列的复杂度高，其随机性更好。其次，由 2.2 节可知，当直接使用低维的混沌系统构造密码算法时，因计算精度的限制，其密钥空间往往不够大而难以抵抗穷举攻击，利用本文提出的改进时空混沌可以简便地提升系统的密钥空间，还可以使密钥分布有更好的均匀性。另外，改进时空混沌采用周期边界约束，可以抵抗文献[19]提出的基于常数驱动的攻击。再次，通过采用不同群中的混合运算，可以抵抗文献[3~8]算法所面临的选择明文(CPA)和选择密文攻击(CCA)，与其相比具有更高的安全性。最后，通过引入随机数构造了一种概率密码，使得相同的明文可以产生不同的密文，从而达到一次一密的效果，这是目前诸多文献中未曾见到的。

5 结束语

本文应用一种新的混沌系统设计了一种新的混沌图像密码算法，分析可知此图像密码算法加密后的图像难以辨识，图像的统计分析表明其频谱图和像素直方图也没有可以分辨的特征。进一步的安全性分析可知，该算法破坏了原始图像相邻像素的相关性，有着比较理想的明文敏感性和密钥敏感性。与基于超混沌的密码算法相比，本文的密码算法在效率上更有优势。通过改进本文的图像密码算法可以达到更高的效率，表明本文的算法在实际应用中将有着不错的前景。



(a)图像微小变化　　(b)密钥微小变化

图 6 系统输入微小变化时的 NPCR 值

参 考 文 献

[1] Socek D, Magliveras S, C'ulibrk D, *et al.*. Digital video encryption algorithms based on correlation-preserving permutations[J] *EURASIP Journal on Information Security,* 2007, DOI.10.1155/2007/52965.

[2] Ji W Y and Hyoungshick K. An image encryption scheme with a pseudorandom permutation based on chaotic maps[J]. *Communications in Nonlinear Science and Numerical Simulation*, 2010, 15(12): 3998–4006.

[3] Baptista M S. Cryptography with chaos[J]. *Physics Letters A*, 1998, 240(1): 50–54.

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

[5] Tong Xiao-jun. Design of an image encryption scheme based on a multiple chaotic map[J]. *Communications in Nonlinear Science and Numerical Simulation*, 2013, 18(7): 1725–1733.

[6] 黄峰, 冯勇. 利用图像分割思想的二维混沌映射及图像加密算法[J]. 光学精密工程, 2007, 15(7): 1096–1103.
Huang Feng and Feng Yong. Novel 2D chaotic map based on image segmentation and image encryption approach[J]. *Optics and Precision Engineering*, 2007, 15(7): 1096–1103.

[7] 李娟, 冯勇, 杨旭强. 三维可逆混沌映射图像加密及其优化算法[J]. 光学精密工程, 2008, 16(9): 1738–1745.
Li Juan, Feng Yong, and Yang Xu-qiang. Invertible chaotic 3D map based image encryption and its optimized algorithm [J]. *Optics and Precision Engineering*, 2008, 16(9): 1738–1745.

[8] 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 Jing and Jiang Guo-ping. Cryptanalysis of a hyper-chaotic image encryption algorithm and its improved version[J]. *Acta Physica Sinica*, 2011, 60(6):060503.

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

[10] Ercan S, Cahit C, and Olcay T Y. Cryptanalysis of Fridrich's chaotic image encryption[J]. *International Journal of Bifurcation and Chaos*, 2010, 20(5): 1405–1413.

[11] Kanso A and Ghebleh M. A novel image encryption algorithm based on a 3D chaotic map[J]. *Communications in Nonlinear Science and Numerical Simulation,* 2012, 17(7): 2943–2959.

[12] Li Shu-jun, Li Cheng-qing, Chen Guan-rong, *et al.*. Cryptanalysis of the RCES/RSES image encryption scheme[J]. *The Journal of Systems and Software*, 2008, 81(7): 1130–1143.

[13] 刘泉, 李佩玥, 章明朝, 等. 一类具有 Markov 性质的混沌系统的构造[J]. 物理学报, 2013, 62(17): 170505.
Liu Quan, Li Pei-yue, Zhang Ming-chao, *et al.*. Construction of a class of chaos systems with Markov properties[J]. *Acta Physica Sinica,* 2013, 62(17): 170505.

[14] 朱从旭, 胡玉平, 孙克辉. 基于超混沌系统和密文交错扩散的图像加密新算法[J]. 电子与信息学报, 2012, 34(7): 1735–1743.
Zhu Cong-xu, Hu Yu-ping, and Sun Ke-hui. New image encryption algorithm based on hyperchaotic system and ciphertext diffusion in crisscross pattern[J]. *Journal of Electronics & Information Technology*, 2012, 34(7): 1735–1743.

[15] Azad R K, Rao J S, and Ramakrishna R. Information-entropic analysis of chaotic time series: determination of time delays and dynamical coupling[J]. *Chaos, Solitons & Fractals*, 2002, 14(4): 633–641.

[16] Garcia P, Paravano A, Cosenza M G, *et al.*. Coupled map networks as communication schemes[J]. *Physical Review E*, 2002, 65(4): 045201.

[17] 陈莎莎, 张建忠, 杨玲珍, 等. 基于混沌激光产生1 Gbit /s 的随机数[J]. 物理学报, 2011, 60(1): 010501.
Chen Sha-sha, Zhang Jian-zhong, and Yang Ling-zhen, *et al.*. One Gbit/s random bit generation based on chaotic laser[J]. *Acta Physica Sinica*, 2011, 60(1): 010501.

[18] Wang Xing-yuan and Xie Yi-xin. Cryptanalysis of a chaos-based cryptosystem with an embedded adaptive arithmetic coder[J]. *Chinese Physics B*, 2011, 20(8): 080504.

[19] 王开, 裴文江, 周建涛, 等. 一类时空混沌加解密系统的安全分析[J]. 物理学报, 2011, 60(7): 070503.
Wang Kai, Pei Wen-jiang, Zhou Jian-tao, *et al.*. Security of chaos-based secure communications in a large community[J]. *Acta Physica Sinica,* 2011, 60(7): 070503.

刘　泉：男，1985 年生，博士生，研究方向为混沌密码学、网络信息安全和嵌入式系统.

李佩玥：男，1985 年生，助理研究员，研究方向为网络信息安全、嵌入式系统、混沌密码和精密控制技术研究.

章明朝：男，1982 年生，副研究员，研究方向为光电探测、信息安全及信息融合研究.

隋永新：男，1970 年生，研究员，研究方向为网络信息安全、光学信息融合及深紫外光刻技术研究.

杨怀江：男，1966 年生，研究员，研究方向为网络信息安全、光学信息融合及深紫外光刻技术研究.