

基于耦合映象格子的混沌图像加密算法研究

盛苏英¹, 吴新华²

(1 南通大学 电气工程学院, 江苏 南通 226019; 2 南通纺织职业技术学院 现教中心, 江苏 南通 226007)

摘 要: 利用耦合映象格子的时空混沌特性, 研究提出了一种混沌图像加密算法. 首先由耦合映象格子产生随机数序列, 将明文图像划分为 8 幅位级图像并进行位级图像置乱; 然后选择对应的随机数序列组合, 采用逐位异或运算进行图像像素扩散; 测试结果表明所提算法比其它算法具有更好的加密性能和有效性.

关键词: 混沌; 图像加密; 耦合映象格子; 位级图像; 随机数序列

中图分类号: TP309.7; TP391

文献标识码: A

文章编号: 1000-7180(2014)01-0043-04

Research of Chaotic Image Encryption Algorithm Based on Coupled Map Lattices

SHENG Su-ying¹, WU Xin-hua²

(1 School of Electrical Engineering, Nantong University, Nantong 226019, China;

2 Modern Education Technology Center, Nantong Textile Vocational Technology College, Nantong 226007, China)

Abstract: A chaotic image encryption algorithm is presented with the spatiotemporal chaotic properties of coupled map lattices. With the random number sequences generated from coupled map lattices, 8 bit-level images divided from the plain image are permuted as a group. Then the image pixel-level diffusion is carried on bitwise XOR operation with selecting a corresponding combination of random number sequences. Simulation results show that the performance and security of the proposed algorithm is better than those of other existing algorithms.

Key words: chaos; image encryption; coupled map lattice; bit-level image; random number sequences

1 引言

大量数字图像信息传输于网络, 其安全性问题也同时被提上了日程. 传统的加密方式(如 DES, AES, IDEA 和 RSA 等)存在诸多问题, 近年来兴起的混沌加密方式为图像加密提供了一个新的有效途径.

混沌系统对初始条件和混沌参数非常敏感以及生成的混沌序列具有非周期性和伪随机性的特性, 混沌系统作为一种天然的密码系统, 已被引入到密码学领域. 自从英国数学家 Matthews 提出混沌数据加密的思想以来^[1], 人们提出了多种基于混沌的

图像加密算法, 主要有基于图像像素值的位置置乱^[2]、灰度值替代^[3], 以及位置置乱与灰度值替代相结合^[4-7]的三大类图像加密算法; 另外基于位级图像的加密研究相对较少, 且存在诸如混沌系统维数较低而造成的安全性不高、难以抵抗已知/选择明文攻击和差分攻击等局限性^[8-10], 而耦合映象格子(Coupled Map Lattice CML)作为时空非线性系统^[11]参与图像加密具有较强的安全性, 可一定程度上克服现有位级图像加密所存在的局限性.

本文利用具有混沌特性的耦合映象格子产生随机数序列, 采用位级图像置乱以及图像像素扩散的方法, 提出了一种新的混沌图像加密算法, 测试结果

收稿日期: 2013-03-16; **修回日期:** 2013-05-08

基金项目: 国家自然科学基金项目(61004027, 61174066); 江苏省自然科学基金项目(BK2010275); 2013 年中国纺织工业联合会科技指导性项目计划(2013062); 南通市应用研究计划项目(BK2012032); 江苏省高等学校大学生实践创新训练计划项目; 南通纺织职业技术学院自然科学研究项目(FYKY/2013/3)

表明所提算法在密钥空间、密钥敏感性、统计性、抗差分攻击性能和密文图像信息熵等方面具有一定的加密性能和有效性。

2 随机数序列生成

2.1 耦合映象格子

耦合映象格子^[11]是一种由具有空间和时间离散、但状态连续的低维动力系统组成的阵列,这些低维动力系统按照某些耦合规则进行相互耦合.当低维动力系统采用混沌系统时,由于其内在的非线性混沌动态性能以及其在空间耦合上的扩散,使得耦合映象格子在时间和空间方向上都具有混沌行为。

考虑采用如下的 CML 映射:

$$x_{n+1}(i) = (1 - \epsilon) \cdot f(x_n(i)) + \epsilon \cdot f(x_n(i-1)) \quad (1)$$

式中, n 表示演化时间, i 表示格子大小 ($i = 1, 2 \cdots L$), ϵ 为耦合系数 $\epsilon \in (0, 1)$, 边缘条件满足 $x_n(0) = x_n(L)$, 其中映射子函数 $f(x)$ 选用一维 Logistic 混沌系统:

$$f(x_n) = \alpha \cdot x_n \cdot (1 - x_n) \quad (2)$$

当取系统参数 $\alpha \in (3.569\ 945\ 6, 4)$ 、初值 $x_0 \in (0, 1)$ 时, CML 映射处于混沌状态。

2.2 随机数序列

上述耦合映象格子可产生双精度小数, 为了适

应图像加密, 将 CML 映射产生的混沌序列进行如下整数化变换, 生成属于 $[0, 255]$ 的随机数序列:

$$\text{mod}((x \cdot 10^{12} - \lfloor x \cdot 10^{12} \rfloor) \cdot 10^3, 256) \quad (3)$$

式中, $\lfloor x \rfloor$ 得到小于或等于 x 的整数, $\text{mod}(x, y)$ 返回余数. 取 $L = 3$, 对 CML 映射进行迭代, 可以得到三个混沌序列 $x(1) = \{x_n(1)\}$ 、 $x(2) = \{x_n(2)\}$ 和 $x(3) = \{x_n(3)\}$, 再进行整数化变换后得到对应的随机数序列 $X(1)$ 、 $X(2)$ 和 $X(3)$ 。

对于产生的随机数序列, 我们参考 FIPS 140-2 (Federal Information Processing Standard) 对其随机性进行测试, 主要包括单位测试 (mono bit test)、扑克测试 (poker test)、运行测试 (runs test) 和长时间运行测试 (long runs test) 四种. 测试中, 取密钥 $k = \{x_0(1), x_0(2), x_0(3), \epsilon, \alpha\} = \{0.123, 0.124, 0.125, 0.543\ 21, 3.99\}$ 进行式 (1)~式 (3) 的运算, 将产生的随机数序列分别进行二进制变换以形成比特位序列, 并以 20 000 位连续比特流为单位进行研究, 测试结果见表 1. 由表 1 可见, 对于任意一组比特流而言, 单位测试中出现比特 '0' 和 '1' 的个数大致相同; 扑克测试的计算值属于 (2.16, 46.17); 运行总次数大约为比特流位数的一半 (即 10 000), 而比特流中连续出现 26 个 '0' 或 '1' 的次数均为 0, 由此可见生成的随机数序列满足 FIPS 140-2 的测试标准, 具有较好的统计随机性能。

表 1 随机数序列测试

测试 序列	单位测试		扑克测试	运行测试	长时间运行测试	
	'0'	'1'			26 个连续 '0'	26 个连续 '1'
$x(1)$	10 125	9 875	14.362	10 032	0	0
$x(2)$	10 100	9 900	23.981	10 095	0	0
$x(3)$	10 098	9 902	12.627	10 060	0	0

3 混沌图像加密算法

3.1 位级图像置乱

假设明文灰度图像 I 的大小为 $M \times M$, 其位级图像的置乱算法如下:

(1) 按照图像像素由二进制表示的比特位置, 将明文图像 I 划分为 8 幅位级图像 (PiC8—PiC1, 大小为 $M \times M$, 以 Lena 灰度图像为例, 其 8 幅位级图像如图 1 所示), 然后将 8 幅位级图像组合为一个整体, 并将其转换为大小为 $2M \times 2M$ 的矩阵 (PI), 其表现形式如图 2 所示。

(2) 将 CML 映射 (见式 (1)) 先迭代 N 次, 以消

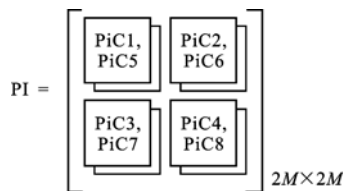


图 1 位级图像的置乱

除其瞬间作用的影响; 然后继续迭代 CML 映射, 得到三个混沌序列 $x(1) = \{x_n(1)\}$ 、 $x(2) = \{x_n(2)\}$ 和 $x(3) = \{x_n(3)\}$, 再进行整数化变换 (见式 (3)), 得到对应的随机数序列 $X(1)$ 、 $X(2)$ 和 $X(3)$ 。

(3) 采用 Arnold Cat Map 对矩阵 PI 进行置乱,

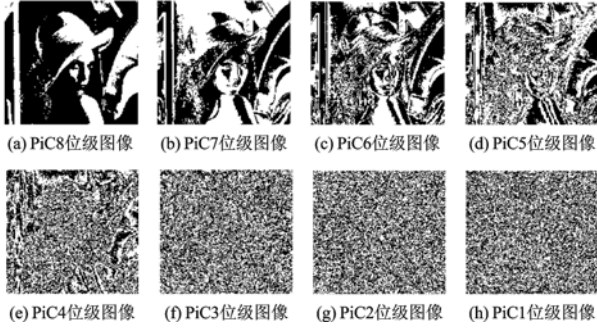


图 2 位级图像的划分

Arnold Cat Map 的数学表示如下:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & 1+pq \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod 2M \quad (4)$$

式中, $\begin{bmatrix} x \\ y \end{bmatrix}$ 和 $\begin{bmatrix} x' \\ y' \end{bmatrix}$ 分别表示图像像素置乱前和置乱后的坐标; 参数 p, q 和置乱轮数 n 与随机数序列有关,

$$\begin{cases} p = \text{mod}(X_{2M}(1) \cdot X_{2M+1}(2) + 1, 2 \cdot M) \\ q = \text{mod}(X_{3M}(2) \cdot X_{3M+1}(3) + 1, 2 \cdot M) \\ n = \text{mod}(X_{4M}(1), 5) + 1 \end{cases} \quad (5)$$

(4) 继续迭代 CML 映射, 重复进行 $n-1$ 轮置乱 (步骤 2 和 3)。

(5) 根据位级图像所在置乱矩阵中的位置, 得到置乱后的灰度图像。

3.2 图像像素扩散

首先将置乱图像矩阵进行 Z 字扫描形成一维序列 $P = \{P_1, P_2, P_3, \dots, P_{M \times M-1}, P_{M \times M}\}$, 像素按序进行如下操作:

$$\begin{aligned} C_{3i} &= P_{3i} \oplus C_{3i-1} \oplus d_i(1) \\ C_{3i+1} &= P_{3i+1} \oplus C_{3i} \oplus d_i(2) \\ C_{3i+2} &= P_{3i+2} \oplus C_{3i+1} \oplus d_i(3) \end{aligned} \quad (6)$$

式中, P_i 和 C_i 分别为扩散前、扩散后的图像像素值, C_0 为扩散初值密钥, $d_i(1), d_i(2)$ 和 $d_i(3)$ 为依赖扩散初值密钥而进行选择的随机数序列组合 (见表 2), 例如根据 $k = \text{mod}(C_0, 6) + 1$ 选择对应序号的随机数序列组合。

表 2 随机数序列组合选择

序号	1	2	3	4	5	6
序列						
$d_i(1)$	X(1)	X(1)	X(2)	X(2)	X(3)	X(3)
$d_i(2)$	X(2)	X(3)	X(1)	X(3)	X(1)	X(2)
$d_i(3)$	X(3)	X(2)	X(3)	X(1)	X(2)	X(1)

从式 (6) 中可看出, 图像像素扩散 C_i 不仅与 P_i 有关, 且与前一个扩散值 C_{i-1} 有关, 因此即使 1 bit

的小小改变, 也会使接下来的扩散值发生变化; 同时随机数序列组合选择与扩散初值密切相关, 增强了加密算法的安全性。

3.3 图像混沌解密

图像解密是“位级图像置乱-图像像素扩散”这一图像加密的逆过程, 即首先进行像素扩散, 再进行位级图像置乱 (其中 Arnold Cat Map 反变换见式 (7)). 图像加、解密过程中的密钥必须一致, 否则解密恢复图像的为无用信息。

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1+pq & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod 2M \quad (7)$$

4 性能分析

对所提混沌图像加密算法进行测试仿真和性能分析, 同时与其余图像加密算法进行比较, 包括: 位级图像置乱算法 (Bit-Level only Permutation, BLP) 和 Zhu 等人提出的位级图像置乱扩散算法^[12] (Zhu's Bit-Level Permutation and Diffusion, BLPD). 在算法仿真中, 设参数为 $\epsilon = 0.543\ 21, \alpha = 3.99$, 扩散初值为 $c_0 = 123$, CML 映射初值 $\{x_0(1), x_0(2), x_0(3)\}$ 与位级图像的 bit 分布有关。

4.1 密钥空间及密钥敏感性分析

所提算法的密钥主要包括 CML 映射的初值 $\{x_0(1), x_0(2), x_0(3)\}$ 、参数 (ϵ, α) 以及扩散初值为 (c_0) . 其中 CML 映射的任一初值和参数的敏感度均达到 10^{-14} 、扩散初值的取值有 256 种, 那么密钥空间至少达到 256×10^{70} ; 而对于 BLP 算法而言, 进行位级图像置乱时 p, q 和 n 的取值分别有 $2M, 2M$ 和 5 种, 密钥空间仅为 $20M^2$; Zhu's BLPD 算法的密钥空间达到 10^{42} , 可见所提算法的密钥空间较大且足以抵抗穷恶意举攻击. 仍以 Lena 图像为例 (见图 3a), 当仅改变加密密钥 α , 将其修改为 $\alpha = 3.990\ 000\ 000\ 000\ 01$, 分别进行混沌图像加密得到密文图像 (见图 3(b) 和 (c)), 两密文图像的差异图像为图 3(d), 可见算法对加密密钥的敏感性很高; 解密时, 当加、解密密钥一致时会恢复出原始图像, 如图 3(a) 所示, 当加、解密密钥不一致时, 即使细微的差别, 如仅仅改变解密密钥 $\tilde{\alpha} = 3.990\ 000\ 000\ 000\ 01$ (对应的加密密钥为 $\alpha = 3.99$), 解密图像如图 4(e) 所示, 为毫无价值的无用信息。

4.2 信息熵分析

在对称加密系统中, 信息熵是衡量加密效果的

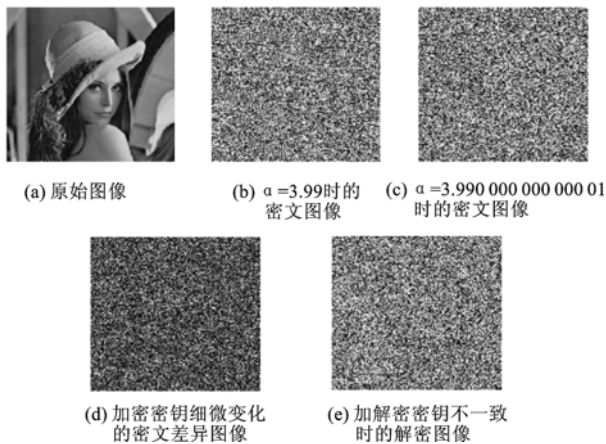


图 3 密钥敏感性分析图

标准之一,对于密文图像而言,8 bits 长度像素的信息熵理想值为 8. 以 Lena、Cameraman 和 Clock 图像为例,由式(10)可计算出信息源 m 的信息熵 $H(m)$,所提算法和对比算法(BLP 和 Zhu's BLPD)所得密文图像的信息熵分别见表 3,从中明显可见经所提算法加密的密文图像信息熵大于经其余算法加密的密文图像信息熵,且更接近于 8,由此可见该算法的加密效果优于其他对比算法.

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \log \frac{1}{p(m_i)} \quad (8)$$

表 3 密文图像的信息熵比较

Image	Proposed scheme	BLP	Zhu's BLPD
Lena	7.997 1	7.769 5	7.996 9
Cameraman	7.997 0	7.566 0	7.996 7
Clock	7.997 3	7.247 5	7.997 2

4.3 差分攻击分析

通过分析明文图像的细微变化而引起的密文图像误差,攻击者可以发现明文图像和密文图像之间的关系,理想情况下,希望明文图像的细微变化会引起密文图像“面目全非”,其效果可用像素变化率(NPCR)和平均变化强度(UACI)两个性能指标加以衡量,具体计算公式如下:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (9)$$

$$UACI = \frac{1}{M \times N} \sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255} \times 100\% \quad (10)$$

式中, C_1 和 C_2 为明文图像细微变化前后的密文图像像素值; $D(i, j)$ 为像素误差,当两像素值不相等时为 1,否则为 0. 仍以 Lena 图像为例,将明文图像右

下角像素值由“01001000”改为“01001001”,经所提算法分别加密(密钥相同),测得 NPCR 为 99.67%、UACI 为 33.56%,比较接近理想值;进一步测试发现经 BLP 和 Zhu's BLPD 算法加密后测得的 NPCR 和 UACI 均小于所提算法的测试值,由此可见此算法具有一定的抗差分攻击性能.

5 结束语

本文利用具有混沌特性的耦合映象格子(CML 映射)产生随机数序列,采用猫映射转换的位级图像置乱以及逐位异或运算的图像像素扩散方法,提出了一种新的混沌图像加密算法,测试结果表明所提算法在密钥空间、密钥敏感性、统计性、抗差分攻击性能和密文图像信息熵等方面比其它图像加密算法(如 BLP 和 Zhu's BLPD)具有更好的加密性能,以此验证所提算法具有较强的加密性能和有效性.

参考文献:

- [1] Matthews R. On the derivation of a chaotic encryption algorithm[J]. Cryptologia, 1989(1):29-42
- [2] 范延军, 孙燮华, 阎晓东, 等. 一种基于混合混沌序列的图像置乱加密算法[J]. 中国图象图形学报, 2006, 11(3): 387-393.
- [3] 刘家胜, 黄贤武, 朱灿焰, 等. 基于模运算与混沌映射的图像加密算法的研究[J]. 微电子学与计算机, 2006, 23(12): 206-209.
- [4] 吴新华, 刘同佩. 基于混沌的图像加密算法研究[J]. 微电子学与计算机, 2006, 27(9):73-75.
- [5] 王英, 郑德玲, 王振龙. 空域彩色图像混沌加密算法[J]. 计算机辅助设计与图形学学报, 2006, 18(16): 877-880.
- [6] Liao X F, Lai S Y, Zhou Q. A novel image encryption algorithm based on self-adaptive wave transmission[J]. Signal Processing, 2010(90):2714-2722.
- [7] Xiang T, Liao X F, Tang G P, et al. A novel block cryptosystem based on iterating a chaotic map[J]. Physics Letters A, 2006(349):109-115.
- [8] Fu C, Lin B B, Miao Y S, et al. A novel chaos-based bit-level permutation scheme for digital image encryption [J]. Optics Communications, 2011 (284): 5415- 5423.
- [9] Zhang W, Wong K W, Yu H, et al. A symmetric color image encryption algorithm using the intrinsic features of bit distributions[J]. Communications in Non-linear Science and Numerical Simulation, 2013,18(3): 584-600.

(下转第 51 页)

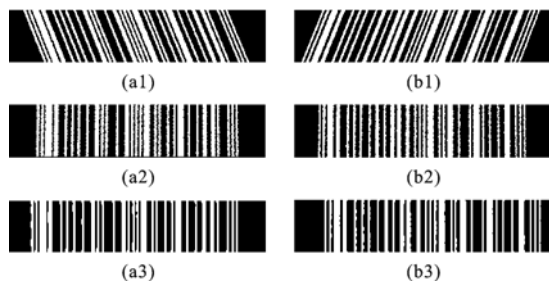


图5 几何校正图

((a1)(b1)分别为从条形码选取一等份并二值化的图像,(a2)(b2)分别为用 Hough 变换检测直线,然后用双线性插值进行旋转的图像,(a3)(b3)分别为用本文所提出的几何校正算法校正后的图像)

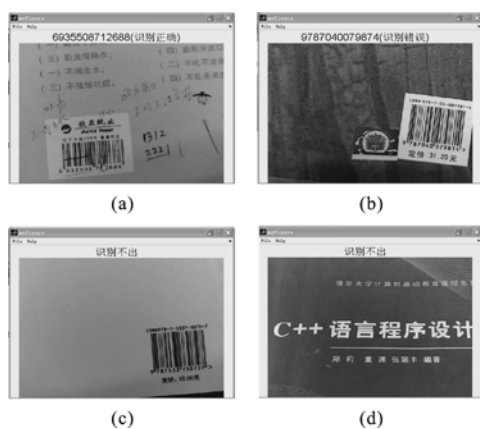


图6 识别结果

5 结束语

本文首先用 matlab 的图像采集工具箱(Image Acquisition Tool)控制 USB 摄像头采集图书条形码,然后进行进一步的识别.实验结果表明,本文所提出的 EAN-13 条形码识别算法,识别率高、鲁棒性强、而且处理速度快,满足工业自动化的要求.

参考文献:

- [1] 陈丹晖,刘红.条码技术与应用[M].北京:化学工业出版社,2006.
- [2] 马晓婷,程承恩.条码技术手册[M].北京:中国计量出版社,1991.
- [3] Jain A K, Chen Y. Barcode localization using texture analysis[C]// Proceedings of the 2nd International Conference on Document Analysis and Recognition. Tsukuba City, Japan, 1993:41-44.
- [4] Shellhammer S J, Goren D P, Pavlids T. Novel signal-processing techniques in barcode scanning[J]. IEEE Robot & Automation Magazine, 1996(6):57-65.
- [5] 徐益峰,金恒宏,戴曙光.基于 EAN-13 条形码识别的改进算法[J].计算机与数字工程,2011, 39(7):127-131.
- [6] 吴忻生,邓军.利用提取边缘线的方法定位条形码[J].计算机应用,2010, 30(5):1246-1250.
- [7] 范礼,高铁杠,杨群亭.基于小波提升与 Sobel 膨胀特征提取的零水印版权认证方案[J].计算机应用研究, 2010, 27(2):727-730.
- [8] 朱娟,刘艳滢,王延杰.一种基于 Hough 变换的新直线段检测算法[J].微电子学与计算机,2008, 25(12):60-63.
- [9] 吕晶晶,姚金杰.基于最小二乘法和牛顿迭代法的空中目标定位[J].微电子学与计算机,2011, 28(9):108-110.
- [10] 王雅静.基于图像处理的 EAN-13 条码识别算法[J].山东理工大学学报,2005, 19(4):14-18.

作者简介:

刘松男,(1987—),硕士研究生.研究方向为图像增强、图像匹配等.

卢一相男,(1980—),博士研究生,讲师.研究方向为图像增强、图像识别等.

孙冬男,(1982—),博士研究生,讲师.研究方向为图像增强、图像识别等.

(上接第46页)

- [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):4048-4054.
- [11] Pisarchik A N, Flores-Carmona N J, Carpio-Valadez M. Encryption and decryption of images with chaotic map lattices[J]. Chaos, 2006(16):033118-1-6.
- [12] 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.

作者简介:

盛苏英女,(1979—),硕士,讲师.研究方向为混沌加密、数码防伪.