

一种混沌图像加密算法的研究与改进

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: 利用混沌序列的特性, 提出了一种新的混沌图像加密算法, 并进行改进. 首先由复合混沌映射生成混沌序列, 再结合灰度值替代和图像位置置乱方法对图像进行加密, 然后进行实验仿真和性能分析, 结果表明该算法具有一定的有效性和良好的加密性能.

关键词: 混沌序列; 图像加密; 密钥; 位置置乱

中图分类号: TP309.7; TP391

文献标识码: A

文章编号: 1000-7180(2010)10-0061-04

Study and Improvement of a Chaotic Image Encryption Algorithm

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 new image encryption algorithm is presented and improved based on chaotic sequence. At first, the chaotic sequences are generated by Logistic chaotic map. Then the image is encrypted combining the method of grey value substituting and position shuffling. The results of experiment simulation and performance analysis show that the algorithm is valid and has good performance.

Key words: chaotic sequence; image encryption; key; shuffle position

1 引言

在信息时代, 越来越多的信息在网络中传输, 由于 Internet 网传输图像数据方便快捷, 图像信息已成为人类进行信息交流的重要手段之一, 其安全问题也同时被提上了日程. 加密技术是保护信息安全最有效的手段, 已经成为一项非常实用又急需快速发展的关键技术.

近年来, 随着混沌动力学的发展, 人们已经逐渐认识到混沌的重要作用, 并开始研究和利用混沌. 混沌现象是非线性动力系统中出现的一种确定性的、内在随机过程的表现, 混沌系统产生的混沌信号具有类似白噪声, 结构复杂, 难以分析, 以及对初始条件和控制参数极端敏感等特性, 特别适用于数据加

密. 混沌系统用于数据加密最早由英国数学家 Matthews 提出^[1], 此后人们提出了多种基于混沌的图像加密算法^[2-3], 主要可分为灰度值替代或像素位置置乱, 以及两者的结合, 但其安全性和效率还有待进一步提高.

本文提出并改进了一种新的混沌图像加密算法, 进行实验仿真和性能分析, 结果表明改进后算法具有较好的性能.

本文采用一个 Cubic-Henon 复合混沌映射为例来进行图像加密, 其方程如下:

$$\begin{cases} x[k+1] = -3x[k] + 4x^3[k] \\ y[k+1] = 1 + 0.3z[k] - 1.4y^2[k] \\ z[k+1] = y[k] \end{cases} \quad (1)$$

式中, $x[k]$ 是 Cubic 混沌映射的状态; $y[k]$ 、 $z[k]$

收稿日期: 2009-08-03; 修回日期: 2009-10-08

基金项目: 国家自然科学基金项目(60474076); 江苏省“六大人才高峰”第三批高层次人才项目(06-E-029); 江苏省自然科学基金项目(BK2007061)

是 Henon 混沌映射的状态。

2 混沌图像加密算法研究

一幅灰度图像可以表示为 $M \times N$ 矩阵形式, 像素值 $\in [0, 255]$, 且相邻像素在空间域上具有很强的相关性。本文所采用的方法是利用混沌系统产生的混沌序列作用于原图像, 进行像素位置变换, 改变原图像中像素点的排列顺序, 从而使得原图像变成一幅杂乱无章的图像, 达到良好的加密效果。

2.1 加解密算法

加密过程如下:

第一步 给定初值 x, y, z (令初值为加密密钥), 由式(1)迭代 $N-1$ 次得 $\{x_1, x_2, \dots, x_n\}, \{y_1, y_2, \dots, y_n\}$ 序列, 分别升序排列得新的序列 $\{x'_1, x'_2, \dots, x'_n\}, \{y'_1, y'_2, \dots, y'_n\}$ 。

第二步 定位 x_i 在 x'_i 中的位置序数和 y_i 在 y'_i 中的位置序数, 得到位置序列分别记为: $r(t, :) = (r_1, r_2, \dots, r_n), s(t, :) = (s_1, s_2, \dots, s_n)$ 。并进行循环得到位置矩阵 r 和 s 。

第三步 以 r 为图像矩阵 A 的行地址置换码, 对图像矩阵 A 进行行地址变换; 以 s 为图像矩阵 A 的列地址置换码, 对图像矩阵 A 进行列地址变换。

第四步 再重复 1 次第三步, 变换后即可得到加密图像。

算法实现如下:

```
for t = 1:N;
    x(1) = key1; y(1) = key2; z(1) = key3;
    for n = 1:N-1;
        x(n+1) = -3 * x(n) + 4 * x(n) * x(n) * x(n);
        y(n+1) = 1 + 0.3 * z(n) - 1.4 * y(n) * y(n);
        z(n+1) = y(n);
    end; % 产生混沌序列
    [x_L, s(t, :)] = sort(x);
    [y_L, r(t, :)] = sort(y); % 产生位置序列
    key1 = x(n+1); key2 = y(n+1); key3 = z(n+1);
end;
```

解密过程是加密算法的逆运算, 先进行列地址变换, 再进行行地址变换, 从而恢复出原始图像。

2.2 实验仿真

本文对一幅尺寸大小为 512×512 的 Lena 图像进行加密, 其仿真结果如图 1 所示。仿真时取加密密钥与解密密钥相同, 分别为 $x = 0.655, y = 0.2, z = 1.2$ 。

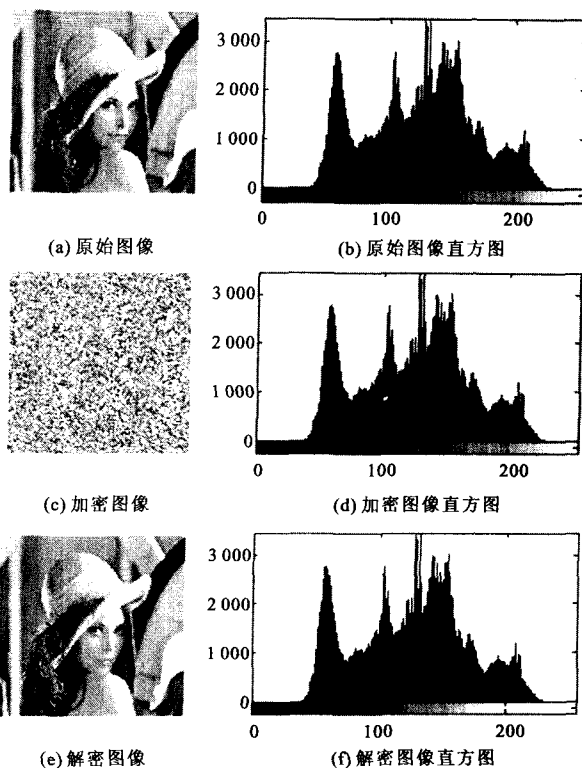


图 1 混沌图像加解密仿真图

由图 1 可知: 原始图像经加密后, 图像变得杂乱无章、不可识别, 而加密图像经正确的密钥解密后又能恢复出原始图像; 但密文直方图和原始图像直方图相同, 说明该算法没有改变图像的直方图分布, 抗统计攻击能力较差。

3 混沌图像加密算法的改进

目前大量文献研究表明^[4-6]: 很多图像加密方法仅仅是利用混沌序列产生置乱地址矩阵, 打乱了像素位置, 图像的灰度直方图并没有发生变化, 很容易被攻击者破译, 而对这些方案进行改进都是引入扩散函数。在加密方案中引入扩散函数可以将明文中的每一位的影响扩散到整个密文中, 从而弥补单纯像素置乱加密算法的不足, 同时可以有效地抵抗统计攻击。

通过研究发现, 利用灰度值替代的时候也可以改变图像的直方图分布情况, 且该算法比较简单, 能达到扩散函数相同的效果, 如将像素值替代引入到像素位置变换中, 正好能弥补像素位置变换不改变密文图像直方图分布这一缺点, 因此引出基于混沌的图像加密改进算法。

3.1 加解密算法

改进后的加密算法在像素位置变换前, 先进行

灰度值替代(如图 2 所示),步骤如下:

第一步 采用经典的 Logistic 映射生成混沌序列 $\{xx_1, xx_2, \cdots, xx_{M \times N}\}$, 将混沌序列中每个元素都取小数点后前三位, 再进行求余, 得到混沌矩阵.

第二步 将原始图像矩阵与混沌矩阵的对应元素相加, 再取余, 即得灰度值替代后的图像矩阵.

第三步 进行像素位置变换, 具体步骤与前一致, 从而得密文图像.

解密过程是加密算法的逆运算, 先进行列地址变换, 再进行行地址变换, 从而恢复出原始图像.

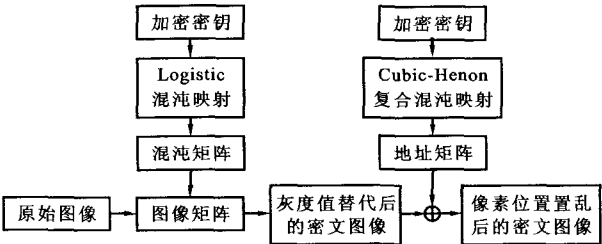


图 2 改进算法加密流程图

3.2 实验仿真

与前实验仿真类似, 同样对 Lena 图像进行加密, 仿真时取加密、解密密钥相同, 另取 Logistic 初值 $xx_1 = 0.3$. 由图 3 可看出: 该算法能改变图像的直方图分布, 使密文图像的抗统计攻击能力大大增加.

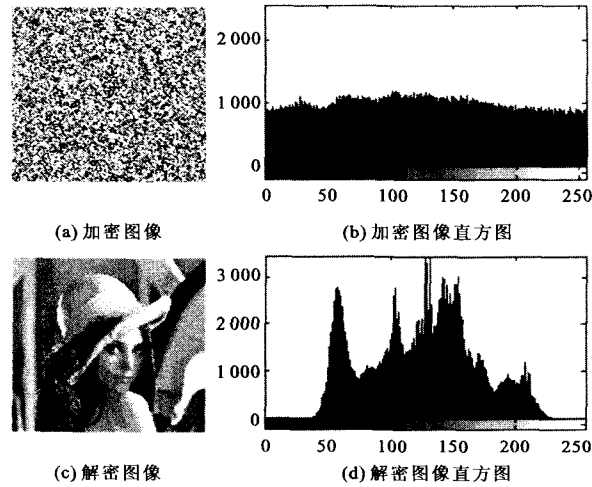


图 3 改进后的混沌图像加解密仿真图

4 性能分析

改进后的混沌图像加密算法密钥空间相对较大 (分别为 x, y, z, xx), 进行如下性能分析: 密钥敏感性、抗噪声性能、抗破损能力和相关统计特性, 并与改进前的混沌图像加密算法进行对比, 从而显示出该算法性能的优越性.

4.1 密钥敏感性

首先从密钥失配时的解密图像来定性考察密钥敏感性. 加密密钥分别取 $xx_1 = 0.3, x = 0.655, y = 0.2, z = 1.2$, 而解密密钥为 $x = 0.655 + 10^{-10}$ 或 $y = 0.2 + 10^{-10}$ (其余解密密钥参数不变) 时的解密图像见图 4 所示. 可见, 尽管加、解密密钥只有微小的偏差, 但解密后的图像已看不出任何原始图像的痕迹.

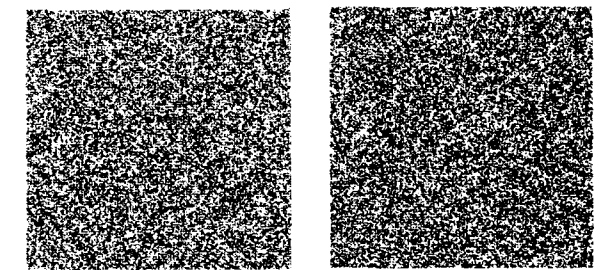


图 4 密钥发生微小变化后的解密效果图

下面由图像恢复性能指标 MSE 和 PSNR 来定量描述密钥敏感性. 当解密密钥 x 或 y 分别以 10^{-10} 的数量级失配时, 得到不同的解密图像, 测量其与原图像的 MSE 和 PSNR, 可得表 1、表 2.

表 1 当 y 不变 x 变化时, 图像恢复性能指标

Δx	改进前 PSNR/dB	改进后 PSNR/dB
10^{-10}	12.271	9.471 4
2×10^{-10}	12.285	9.473 6
3×10^{-10}	12.298	9.468 6
4×10^{-10}	12.291	9.466 4
5×10^{-10}	12.305	9.461 2
6×10^{-10}	12.274	9.471
7×10^{-10}	12.285	9.487 7
8×10^{-10}	12.282	9.474
9×10^{-10}	12.29	9.467 8

表 2 当 x 不变 y 变化时, 图像恢复性能指标

Δy	改进前 PSNR/dB	改进后 PSNR/dB
10^{-10}	12.45	9.518 9
2×10^{-10}	12.47	9.499 9
3×10^{-10}	12.459	9.482 4
4×10^{-10}	12.465	9.481 5
5×10^{-10}	12.446	9.509 6
6×10^{-10}	12.451	9.489 2
7×10^{-10}	12.436	9.498 9
8×10^{-10}	12.452	9.493 5
9×10^{-10}	12.458	9.503 2

其中:

均方误差 $MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (I'(i,j) - I(i,j))^2$ (2)

峰值信噪比 $PSNR = 10\lg\left(\frac{f_{max}^2}{MSE}\right)$ (3)

可见,密钥的微小变化可使改进算法的 PSNR 值较小,即密钥的微小变化,可以导致解密图像完全偏离原始图像,这意味着改进算法对密钥具有更大的敏感性.

4.2 抗噪声性能

图像数据在传输过程中难免会遇到各种噪声,下面在密文图像(如图 1 和图 3 的加密图像)中加入大约 10% 的椒盐噪声. 由图 5 可见,改进后算法的解密图像能更好地恢复出原始图像的样子,该算法具有较好的抗噪声攻击能力.

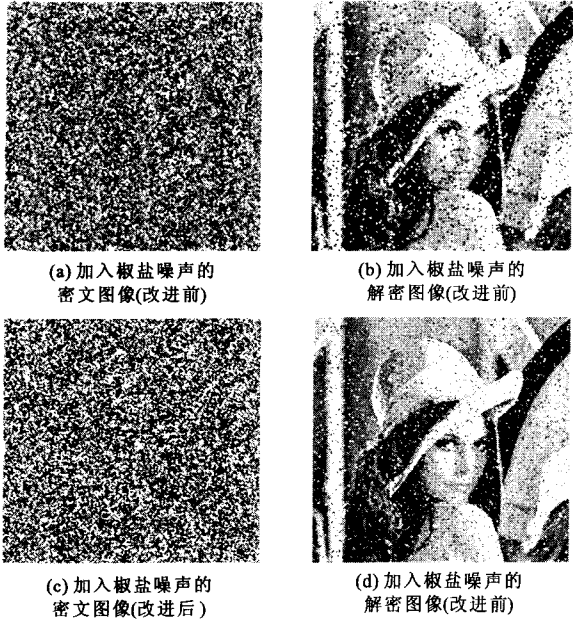


图 5 加入不同噪声的密文图像及其解密图像

4.3 抗破损能力

将密文图像裁剪掉 1/16, 然后进行解密,得到的效果仿真图如图 6 所示,进一步研究发现只要裁剪部位不超过密文图像的 20%, 就能够恢复出较为理想的图像.

4.4 相关性分析

通过下式计算相邻像素的水平、垂直和对角线方向的相关性:

$cov(x,y) = E((x - E(x))(y - E(y)))$ (4)

$R_{xy} = \frac{cov(x,y)}{\sqrt{D(x)} \cdot \sqrt{D(y)}}$ (5)

式中, x, y 是图像中两相邻像素的灰度值, $E(x)$ 是

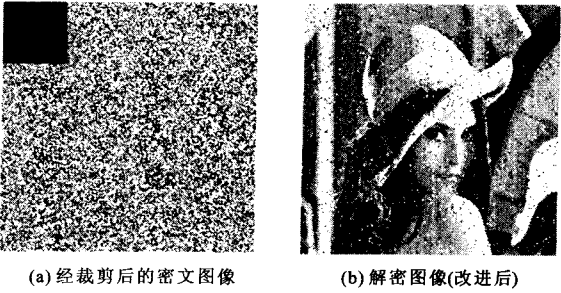


图 6 经裁剪的密文图像及其解密图像

x 的数学期望, $D(x)$ 是 x 的方差, $cov(x,y)$ 是 x, y 的协方差. 原始图像中相邻像素的相关性是很大的, 为了破坏统计攻击, 必须是相邻两个像素的相关性降低, 相关系数越小说明加密性能越好. 现从原始图像和密文图像中任取一行、一列以及对角线上的像素点进行相邻像素相关系数计算, 可得表 3.

表 3 相邻像素相关系数

像素关系	原始图像	加密图像 (改进前)	加密图像 (改进后)
水平相邻	0.985 73	0.041 218	0.004 991
垂直相邻	0.993 23	-0.013 266	0.005 209
对角相邻	0.954 92	-0.052 712	0.003 751

由实验结果可知,改进后算法的加密信号具有更好的扩散和混淆能力,加密效果好,因此该算法对统计分析具有较好的安全性.

5 结束语

混沌图像加密技术是计算机图像安全领域的一个研究方向. 本文提出并改进了一种基于混沌序列的图像加密方法, 利用混沌信号的优良特性, 结合灰度值替代和像素位置置乱方法, 在空间域内对图像进行加密. 该加密算法具有密钥空间大、不易破解等特点, 在抗破损、相关性统计攻击等方面也具有相对较好的性能, 实验结果验证了该算法的有效性.

参考文献:

[1] Matthews R. On the derivation of a chaotic encryption algorithm[J]. Cryptologia, 1989(1):29-42.
[2] Zhang Han, Wang Xiufeng. A new image encryption algorithm based on chaos system[J]. IEEE, 2003(10):778-782.
[3] Linhua Zhang, Xiaofeng Liao, Xuebing Wang. An image encryption approach based on chaotic maps[J]. Chaos, Solitons and Fractals, 2005(24):759-765.

(下转第 68 页)

很显然,逐渐求精的定位算法要求的网络连通度较高,这一点跟 Zhou 中所提算法类似^[5].原因在于,这些算法都是利用真实距离进行多边迭代,所以在各向异性条件下表现较好,但是为了得到真实距离,它们都需要利用节点密集的网络局部拓扑,并且在连通度较高的条件下,性能较好.

5 结束语

锚节点仅能在水面部署是水下传感网面临的一个现实问题,本文分析了此种三维水下场景中传感器节点自定位的困境,提出一种新的从水面向水底逐级定位,按级加权迭代求精的定位算法,并利用已知的节点深度信息来修正每次迭代结果,提高算法精度,仿真结果显示该算法各种表现良好,包含各向异性拓扑.

参考文献:

- [1] Jun-Hong C, Jiejun K, Gerla M, et al. The challenges of building mobile underwater wireless networks for aquatic applications[J]. Network, IEEE, 2006, 20(3):12-18.
- [2] Jiejun K, Jun-hong C, Dapeng W, et al. Building underwater ad-hoc networks and sensor networks for large scale real-time aquatic applications[C]//Military Communications Conference. New Jersey, IEEE, 2005:1535-1541.
- [3] 史庭俊,桑霞,徐力杰,等.一种基于信任度的 DV-Hop 改进定位算法[J]. 微电子学与计算机,2008,25(10):100-102.
- [4] 冯秀芳,曹美丽,孙超.无线传感器网络基于 Apit 的混合定位算法[J]. 微电子学与计算机,2009,26(6):58-62.
- [5] Yuecheng Z, Liang C. A distributed protocol for multi-hop underwater robot positioning[C]//Robotics and Biomimetics, IEEE International Conference. China: Shenyang, 2004:480-484.
- [6] Garcia J E. Ad hoc positioning for sensors in underwater acoustic networks [C]//OCEANS '04. MTS/IEEE TECHNO OCEAN '04. California, 2004:2338-2340.
- [7] Zhou Z, Cui J H, Zhou S. Localization for large-scale underwater sensor networks[C]//NETWORKING 2007. Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet. USA:Atlanta,2007.
- [8] Wei C, Teymorian A Y, Liran M, et al. Underwater localization in sparse 3D acoustic sensor networks[C]//INFOCOM 2008. The 27th Conference on Computer Communications. USA:Phoenix, IEEE, 2008:236-240.
- [9] Chris S, Jan M R, Koen L. Robust positioning algorithms for distributed Ad-Hoc wireless sensor networks[C]//Proceedings of the General Track of the annual conference on USENIX Annual Technical Conference: USENIX Association. USA:Boston,2002.
- [10] Ian F A, Dario P, Tommaso M. Challenges for efficient communication in underwater acoustic sensor networks [C]//ACM. USA:New York, 2004:3-8.

作者简介:

王 悒 女,(1979-),博士.研究方向为计算机网络.

(上接第 64 页)

- [4] 赵学峰.基于混沌映射的数字图像置乱方法[J]. 微电子学与计算机,2003,20(8):136-138.
- [5] 陈巧琳,廖晓峰,陈勇,等.改进的基于混沌序列的幻方变换图像加密[J]. 计算机工程与应用,2005(22):138-232.
- [6] 张燕,黄贤武,刘家胜.一种基于改进的混沌猫映射的图

像加密算法[J]. 计算机工程,2007,33(10):166-168.

作者简介:

盛苏英 女,(1979-),硕士,讲师.研究方向为混沌同步、混沌加密.

吴新华 男,(1980-),硕士.研究方向为计算机通信.