

一种空频域结合的多维混沌系统图像加密方案

张 硕, 蔡如华, 陈光喜

(桂林电子科技大学 数学与计算科学学院, 广西 桂林 541004)

摘 要: 研究了一种基于二维 Logistic 映射和三维混沌的图像加密系统. 首先利用二维 Logistic 映射产生加密模板对小波分解的低频系数进行调整, 接着由 Chen 系统对小波重构之后的图像进行异或操作, 进一步使加密性能得到了很大的提高. 通过试验比较分析, 该方案不但密钥空间大, 而且对密钥和明文相当敏感, 具有更优良的扩散性和扰乱性能, 并能抵抗各种攻击.

关键词: 二维 Logistic 映射; Chen 系统; 小波变换; 图像加密

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2010)07-0060-05

An Image Encryption Algorithm Based on Multidimensional Chaotic Systems in Spatial and Frequency Domain

ZHANG Shuo, CAI Ru-hua, CHEN Guang-xi

(School of Mathematics and Computational Science, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract: This paper proposes an image encryption algorithm based on coupled Logistic chaotic map and Chen's chaotic attractor. Firstly, the low-frequency coefficients of the image wavelet decomposition are adjusted by the Logistic chaotic sequence. Secondly, the image after the wavelet reconstruction is encrypted by the Chen's chaotic system. To further enhance the encryption performance. The experimental results demonstrate that the encryption algorithm not only has a large key space but also has a very sensitivity with respect to the secret key and the original image. The encryption algorithm proposed in this paper possesses perfect diffusion and confusion properties and it can resist the various attacks.

Key words: coupled Logistic chaotic map; Chen system; wavelet transform; image encryption

1 引言

由于图像信息安全逐渐成为关注的焦点, 其中图像加密技术成为图像信息安全领域中的研究热点. 图像加密具体可分为空间域加密和变换域加密, 空间域加密实现容易但图像信息冗余巨大, 容易被攻击. 变换域加密是考虑到数字图像信息冗余大, 数据高度相关, 且人类的视觉系统允许图像内容有一定程度缺损的特点而提出的一种有效加密方法, 因此结合变换域^[1-2]加密更符合现代流行的图像加密编码方案. 目前低维混沌所产生的混沌的序列虽然具有形式简单和时间短的优点, 但密钥空间太小, 很

难有效的抵御穷举攻击. 因此有必要探索基于高维混沌系统和超维混合混沌系统的图像加密算法^[2].

本文根据混沌系统具有伪随机性、确定性、对初始条件和系统参数的极端敏感性, 提出了一种基于二维 Logistic 映射和 Chen 系统所生成的混沌序列对图像进行小波域和空域上的加密, 从而加密性能得到进一步的提高.

2 混沌动力系统模型

2.1 二维 Logistic 混沌映射

由一维 Logistic 映射, 可以定义二维 Logistic 混沌映射^[3]如:

收稿日期: 2009-06-08; 修回日期: 2009-08-08

基金项目: 国家自然科学基金项目(10871217); 广西区教育厅基金资助项目(200607LX010, 200807LX112); 广西区科学基金资助项目(0731018)

$$\begin{cases} x_{n+1} = 4\mu_1 x_n(1 - x_n) + g_1(x_n, y_n) \\ y_{n+1} = 4\mu_2 y_n(1 - y_n) + g_2(x_n, y_n) \end{cases} \quad (1)$$

式中, g_1 和 g_2 是耦合项, 可以取两种情况: 即 $g_1 = \gamma y_n$ 和 $g_2 = \gamma x_n$ 的一次耦合项, 或者 $g_1 = g_2 = \lambda x_n y_n$ 的对称二次耦合项. 采用一次耦合项形式的二维 Logistic 映射产生混沌序列, 映射的形式为

$$\begin{cases} x_{n+1} = 4\mu_1 x_n(1 - x_n) + \gamma y_n \\ y_{n+1} = 4\mu_2 y_n(1 - y_n) + \gamma x_n \end{cases} \quad (2)$$

混沌序列的产生可以由控制参数 μ_1 、 μ_2 和 γ 决定. 当 $\gamma = 0.1$, $\mu_1 = \mu_2 = 0.9$ 时, 经计算得到的二维 Logistic 映射的最大 Lyapunov 指数: $\lambda = 0.11 > 0$, 表明此时处于混沌状态, 与计算机模拟的系统相图是一致的.

2.2 三维 Chen 系统

该系统为三维自治系统^[4], 其动力学方程分别为

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x - xz + cy \\ \dot{z} = xy - bz \end{cases} \quad (3)$$

对于该系统, 当参数取值为 $a = 35$, $b = 3$, $c = 28$ 时, 系统有一个混沌吸引子, 如图 1 所示.

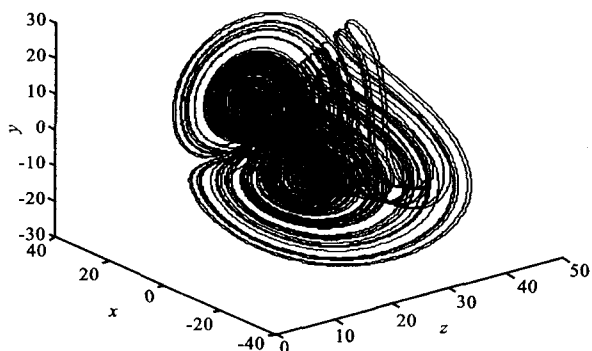


图 1 Chen 系统的吸引子

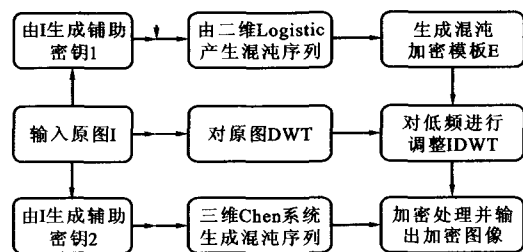
由初始条件, 通过四阶 Rung-Kutta 迭代作用产生的三维混沌序列是非周期且对初值非常敏感. 由该混沌系统生成的混沌序列具有以下优点: 一是系统结构较低维系统复杂, 系统变量的实数值序列更不可测; 二是对系统输出的实数值混沌序列进行处理, 可以产生单变量或多变量组合的加密混沌序列, 使得加密序列的设计非常灵活; 三是系统的初值和系统参数均可以作为生成加密混沌的种子密钥, 若设计过程中再加入部分控制变量, 加密算法的密钥空间将大大高于低维混沌系统.

3 加密方案设计

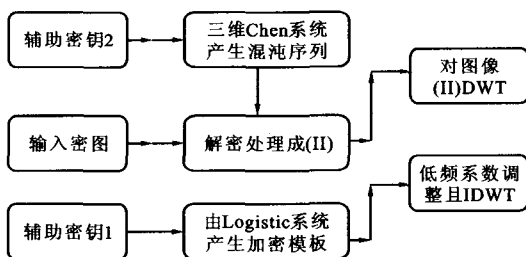
图 2(a) 所示为加密流程图. 设原图像 I 的大小为 $m \times n$, $I(i, j)$ 为像素 (i, j) 处的灰度值,

$$B = \bigoplus_{i=1}^m \bigoplus_{j=1}^n I(i, j) \quad (4)$$

式中, B 表示图像所有像素灰度值的异或.



(a) 加密过程



(b) 解密过程

图 2 图像加密与解密流程

3.1 加密过程

具体步骤如下:

Step1: 确定二维 Logistic 混沌的初值, 再由 B 进一步对其修改, 生成混沌序列, 选择加密模板 $E(n)$ 的生成方式如下:

$$E(n) = \begin{cases} 4 & 0 < x(i) \leq 0.5, 0 < y(i) \leq 0.5 \\ 1 & 0 < x(i) \leq 0.5, 0.5 < y(i) \leq 1 \\ -1 & 0.5 < x(i) \leq 1, 0 < y(i) \leq 0.5 \\ 2 & 0.5 < x(i) \leq 1, 0.5 < y(i) \leq 1 \end{cases} \quad (5)$$

Step2: 选择小波函数 W 对原图像 I 进行 R 级小波分解, 由加密模板 $E(n)$ 和小波低频系数矩阵点乘, 完成了对其系数的调整;

Step3: 将调整后低频系数再与其余的中高频系数经过小波逆变换重构图像 I' , 此时需要对重构图像的矩阵做进一步的调整(归一化处理之后每个像素再乘以 255, 假设原图的灰度级为 $0 \sim 255$);

Step4: 给出三维 Chen 混沌系统初值 $\{x_1, y_1, z_1\}$, 产生三组混沌序列 ($m \times n + 1000$), 各组分别舍去前 1000 个值, 每组分别取第 1001 至第 ($m \times n + 1000$) 的共 $m \times n$ 值, 分别存储于数组 $\{x(i)\}$ 、 $\{y(i)\}$ 和 $\{z(i)\}$ 中, $i = 1, 2, 3, \dots, m \times n$;

Step5:混沌序列 $p(i)$ 的生成,顺序取图像 I' 中的一点(设点的序号为 i),具体方案如表 1 所示.

表 1 混沌序列的生成

$\text{mod}(i,3)$	$p(i)$
0	$\text{mod}(\text{floor}(x(i) * 10 \cdot 10), 256)$
1	$\text{mod}(\text{floor}(y(i) * 10 \cdot 10), 256)$
2	$\text{mod}(\text{floor}(z(i) * 10 \cdot 10), 256)$

Step6:用图像 I' 中的第 i 个像素点的灰度值与产生的混沌序列 $p(i)$ 值进行按二进制位异或操作,得到加密后的像素值,重复上述操作,直到所有的像素点加密完毕,即得到加密图像 I'' ;

从设计加密方案的角度进行分析,该加密系统对密钥是敏感的,对于明文虽然在 Step1 中也能起到一定的敏感性,但缺少较强的敏感性.为克服这一缺点,对算法进行局部修改.记

$$C = \sum_{i=1}^m \sum_{j=1}^n \text{round}(I(i,j)^2 + B_2)^{1/2}) \text{mod} 256 \tag{6}$$

$$\bar{C} = \text{mod}(C, 256) / 256 \tag{7}$$

分别对混沌系统的初值 $\{x_1, y_1, z_1\}$ 进行修改,使得 $\{x_{11} = x_1 + \bar{C}, y_{11} = y_1 + \bar{C}, z_{11} = z_1 + \bar{C}\}$,为 Chen 系统修改后的初值,这样对图像做细微的变动就会得到不同的混沌系统初值,其效果相当于对密钥进行了局部修改,而由于算法对密钥是敏感的,因此最终导致算法对明文也是敏感的.

3.2 解密过程

由图 2(b) 可知解密过程:首先由密钥 2 生成三维混沌序列对加密图像序列进行异或解密处理,接着对解密之后的 II 进行小波分解,此时根据密钥 1 生成二维 Logistic 混沌序列生成解密模板 $D(n)$:

$$D(n) = \begin{cases} 1/4 & 0 < x(i) \leq 0.5, 0 < y(i) \leq 0.5 \\ 1 & 0 < x(i) \leq 0.5, 0.5 < y(i) \leq 1 \\ -1 & 0.5 < x(i) \leq 1, 0 < y(i) \leq 0.5 \\ 1/2 & 0.5 < x(i) \leq 1, 0.5 < y(i) \leq 1 \end{cases} \tag{8}$$

再由 $D(n)$ 对低频系数进行调整,最后经过小波逆变换重构出原图.具体解密程序是加密程序的逆过程,可参考加密中的具体步骤,这样就可以实现信息的解密,输出原图像.

本算法不仅适合对 8 位灰度图像加密,若加密图像为 RGB 图像,则要对像素点的 R、G、B 三个分量分别进行加密,稍微修改即可对真彩色图像加密.

4 仿真试验结果及其分析

下面利用一幅 256×256 的标准 Lena 图像作为

试验图像,采用上述方案对原图像进行加密,该方案选择 Haar 小波对原图像进行小波分解,由于低频系数对图像视觉的影响起主要作用,故选择二维 Logistic 映射对低频系数进行调整也是合理的.图像加密的安全性是评价一个图像加密系统的最核心的标准.现从以下几方面进行安全性的分析.

4.1 峰值信噪比的分析

在变换域的图像加密中,均方误差 MSE 或者峰值信噪比 PSNR 是评价图像加密的一项重要指标,图像的矩阵大小为 $m \times n$,量化级为 $0 \sim 255$ 的原图 $f(i,j)$,密图为 $g(i,j)$.其中:

$$\text{MSE} = (\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (f(i,j) - g(i,j))^2) / m \times n \tag{9}$$

$$\text{PSNR}(\text{dB}) = 10 \lg \frac{255^2}{\text{MSE}} \tag{10}$$

若用峰值信噪比对解密图像和原图的一致性进行客观评价,则可得到解密图像与原图的峰值信噪比 $\text{PSNR} = 99.1029$,由此可以看出,客观评价与主观评价结果一致,且性能很好.

4.2 密钥 / 明文敏感性分析

图 3(a) 为原图,图 3(b) 和 (c) 分别对应原图只有一个像素只差时的加密图像, (d) 为两密图的不同, (e) 为正确解密的图像, (f) 是在密钥发生微小偏差情况下,即当 $x_0 = -3.000\ 000\ 000\ 000\ 1, y_0 = 2, z_0 = 10$ 时,获得的解密图像,可以看出密图对密钥和明文均具有高度的敏感性.

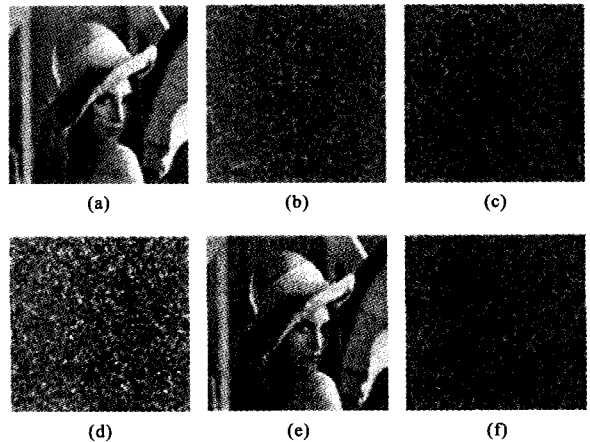


图 3 图像加密和解密结果

4.3 信息熵的分析

信息熵 $H(m)$ 是反映信源的平均信息量,公式为

$$H(m) = \sum_{i=1}^{2^N-1} P(m_i) \log_2 \frac{1}{P(m_i)} \tag{11}$$

此处的 $P(m_i)$ 表示符号 m_i 的概率.假设一个

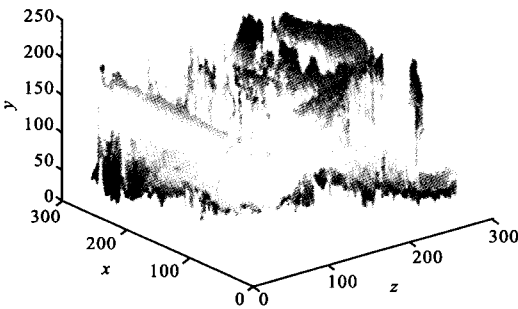
信源是所含 2^8 个符号是以等概率出现的,由文献[5-6]可知,该信源的熵 $H(m) = 8$,即是对应于一个真正的随机信源。

通过仿真分别与文献[5-6]相比较,结果显示本文方案密图的信息熵更接近理论值 8,即上述加密方案效果更好且更能有效抵御熵的攻击,见表 2。

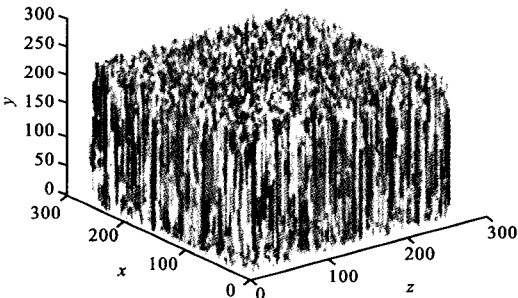
表 2 信息熵测试比较			
测试方案	文献[5]	文献[6]	本文
$H(m)$	7.933 8	7.996 8	7.997 7

4.4 密文分布特性分析

由图 4 可知密文的灰度三维图几乎趋于均匀分布,很好地掩盖了明文的分布规律,可见明文像素的统计信息在密文中没有体现,明密文之间统计上的



(a) 原图灰度三维图



(b) 密图灰度三维图

图 4 明文和密文的灰度三维图

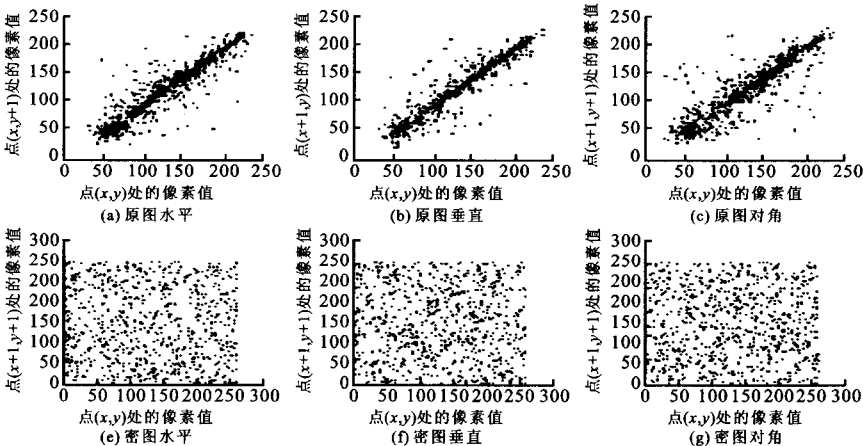


图 5 图像相邻像素的相关性

相关性非常小,表明方案能够有效抵御基于像素统计的攻击。

4.5 差分攻击分析

检测一个像素的改变对密文的影响通常采用像素数目的改变率 NPCR 和整体平均改变强度 UACI^[7]。记两密文图像 C_1 和 C_2 分别对应着仅有一个像素不同的两明文,定义矩阵 D 与 C_1 和 C_2 具有相同大小,当 $C_1(i, j) = C_2(i, j)$ 时, $D(i, j) = 1$; 反之, $D(i, j) = 0$

$$NPCR = \frac{1}{W \times H} \times \sum_{i,j} D(i, j) \times 100\% \tag{12}$$

$$UACI = \frac{1}{W \times H} \left[\sum_{i,j} \frac{|C_1(i, j) - C_2(i, j)|}{255} \right] \times 100\% \tag{13}$$

式中, W 和 H 分别为矩阵 D 的长和宽。以 Lena 图像的加密结果为 C_1 , 以经过修改后(改变第一个像素的灰度值)的 Lena 图像的加密结果为 C_2 , 通过计算得到 $NPCR = 0.402\ 83\%$, $UACI = 33.513\%$, 这一结果表明对原始图像进行微小的改变会导致加密图像有很大的变化,故加密方案具有较强的抵抗差分攻击能力。

4.6 相邻像素的相关性

为检验密图和原图相邻像素的相关性,现随机从图像中抽取 1024 对相邻像素(水平,垂直或对角)。根据文献[7]中的公式计算相邻像素相关系数:

$$\gamma_{xy} = cov(x, y) / (\sqrt{D(x)} \sqrt{D(y)}) \tag{14}$$

式中, x 和 y 分别代表相邻像素的灰度值, $cov(x, y)$ 为 x 与 y 的协方差, $D(x)$ 、 $D(y)$ 分别为 x 、 y 的标准差。

图 5 分别表示了原图和密图的水平、垂直和对角方向相邻像素的相关性。

表 3 则分别列出了按照三种方向计算所得到的相关系数. 密图的两相邻像素的相关系数接近于 0, 相邻像素已基本不相关, 说明原图的统计特征已被扩散到随机的密图中. 同时由表 3 的比较可知本文加密方案在某种程度上优于文献[8].

表 3 原图和密图的两相邻像素的相关性

方向	原图	密图	文献[8]
水平方向	0.951 7	- 0.001 2	- 0.015 89
垂直方向	0.968 0	- 0.005 0	- 0.065 38
对角方向	0.924 4	- 0.002 2	- 0.032 31

4.7 密钥空间分析

关于此算法的破解, 由于算法的密钥为 $K = (W, R, B, x'_0, y'_0, \gamma, \mu_1, \mu_2, x_1, y_1, z_1, C)$, W 为选用的小波, 为小波分解级数, 和为二维 Logistic 映射的初值. 现直接对图像数据流进行解密, 解密的过程根本无法实现; 并且两混沌系统的初值均精确到小数点后 14 位; 况且此算法首先采用了由二维 Logistic 映射产生的混沌序列, 对原图进行小波域上的加密, 由于混沌系统具有较高的安全保密性能, 密钥空间为 $(0,1)$ 之间的全体实数, 由此可见该算法的密钥空间非常大, 可以有效地抵御对密钥的攻击.

5 结束语

根据混沌系统初始条件与系统参数的极端敏感性以及伪随机性和确定性, 现结合二维 Logistic 映射和 Chen 系统, 由此生成混沌序列, 对图像进行小波和空域上的加密, 克服了低维混沌系统有可能退化为周期以及图像置乱加密计算量大的缺点, 采用了小波系数的混沌调整加密, 同时在空频域上进行了混沌序列异或加密, 仿真试验表明解密图像与原图像有很高的峰值信噪比, 以及加密图像的灰度三维图几乎接近均匀分布, 此算法具有良好的扩散和

扰乱性, 符合现代密码学的特点, 而且还能抵御一些攻击. 由分析可知具有相当高的加密强度, 且算法简单, 易于实现, 密钥空间大, 不易破解等特点且具有良好的实用性.

参考文献:

[1] 刘家胜, 黄贤武, 朱灿焰, 等. 基于混沌与小波变换的图像加密算法[J]. 微电子学与计算机, 2007, 24(12): 6-8.

[2] Gao T, Chen Z. A new image encryption algorithm based on hyper-chaos[J]. Physics Letters, 2008(a372): 394-400.

[3] 王兴元, 朱伟勇. 二维 Logistic 映射中混沌与分形的研究[J]. 中国图像图形学报, 1999(4): 340-344.

[4] Chen G, Ueta T. Yet another chaotic attractor[J]. Int. J. of Bifur. Chaos, 1999(9): 1465-1466.

[5] 李鹏, 田东平. 基于超混沌序列的数字图像加密算法[J]. 微电子学与计算机, 2008, 25(3): 4-7.

[6] Behnia S. A novel algorithm for image encryption based on mixture of chaotic maps[J]. Chaos, Solitons & Fractals, 2008, 35(2): 408-419.

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

[8] Gao H J, Zhang Y S, Liang S Y, et al. A new chaotic algorithm for image encryption[J]. Chaos, Solitons & Fractals, 2006, 29(5): 393-399.

作者简介:

张 硕 男, (1983-), 硕士研究生. 研究方向为小波分析及其应用、图像信息安全.

蔡如华 男, (1971-), 副教授, 硕士生导师. 研究方向为小波分析及其应用.

陈光喜 男, (1971-), 博士, 副教授, 硕士生导师. 研究方向为计算机软件与理论、信息安全.