

基于提升小波变换的超混沌图像加密方案

张 欢, 蔡如华

(桂林电子科技大学 数学与计算科学学院, 广西 桂林 541004)

摘 要: 研究了一种基于提升小波变换与二维超混沌系统的图像加密方案. 首先将图像进行整数提升小波变换, 根据自适应排列置乱算法对提升小波变换后的低频子带系数进行调整置乱. 然后由两个二维超混沌系统生成混沌序列并进行预处理, 同时构造双混合反馈系统. 最后利用双混合反馈系统对小波重构后的图像进行像素灰度值替代加密. 仿真结果表明, 该加密方案弥补了图像经传统小波变换后不能无失真重构的缺陷, 并克服了单一的低维混沌系统保密性不高的缺点, 在密钥空间和抵抗各种攻击方法上均有较好的改进, 具有较高的安全性和实用性.

关键词: 超混沌系统; 提升小波变换; 图像加密; 自适应

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2011)07-0046-04

An Hyperchaotic Image Encryption Scheme Based on Lifting Wavelet Transformation

ZHANG Huan, CAI Ru-hua

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

Abstract: This paper proposes an image encryption scheme based on interger lifting wavelet transformation and 2D hyperchaotic system. Firstly, the low-frequency coefficients of the image integer lifting wavelet transformation are adjusted by self-adaptive permutation algorithm. Secondly, making use of the pretreated chaotic sequences which were generated by two 2D hyperchaotic systems, we construct dual hybrid feedback. Finally, the image after the wavelet reconstruction is encrypted by dual hybrid feedback systems. The experimental results demonstrate that the encryption scheme make up this deficiency which the image after the traditional wavelet reconstruction is distortion, and overcome this deficiency which the confidentiality of single low-dimensional chaotic system is not high, which has better improvement on both the key space and the resistance of various attacks than the other schemes and possesses high security and practicability.

Key words: hyperchaos system; the lifting wavelet transformation; image encryption; self-adaptive

1 引言

随着现代网络通信技术的飞速发展, 多媒体信息的安全问题越来越引起人们的关注, 图像加密技术作为对图像信息保护的手段之一, 已成为图像信息安全领域的一个研究热点. 其中基于混沌系统的加密算法在图像加密算法中研究最为广泛. 文献[1]提出了一种基于超混沌系统的图像加密算法, 难以抵抗已知明文攻击和选择明文攻击, 而文献[2]提出

的自适应图像加密算法, 可有效地抵抗已知明文攻击, 却不能有效抵抗选择明文攻击, 而且图像加密前后像素分布保持不变, 整体加密速度较慢. 但该自适应图像加密算法操作简单、敏感性高, 单轮加密速度快的优点值得保留.

近年来, 围绕小波变换的图像安全保密技术涌现了大量的工作, 与传统小波变换相比, 整数提升小波变换更能无失真快速重构图像信息. 文中基于自适应排列和整数提升小波变换, 研究了一种超混沌

收稿日期: 2010-11-24; 修回日期: 2010-12-20

基金项目: 广西区教育厅基金项目(200607LX010); 广西区科学基金项目(0731018)

图像加密系统.使用改进的高效自适应置乱算法,仅对小波低频系数置乱,以减少系数置乱所带来的对编码效率的影响.在确保加密过程简单高效的前提下,引入双密文输出混合反馈系统和多轮加密形式,进一步提高加密系统的安全性.实验结果表明,该图像加密算法效率高,并能有效实现对图像视觉内容的掩蔽和准确不失真解密.

2 超混沌动力系统模型

二维离散超混沌系统是一种具有两个正的Lyapunov指数的非线性动力系统.相对于更高维的连续超混沌系统,它输出超混沌序列的速度快,与一维混沌系统输出混沌序列速度更接近.而且从安全的角度考虑,由于超混沌系统比低维混沌系统具有更复杂的相空间^[3],用它设计图像加密系统不易被一类基于混沌同步的分析方法攻击.基于这些特点它更能满足现代保密通讯实时性的要求,因此二维离散超混沌系统更适合用于图像加密.

下面给出两种二维离散超混沌系统:Kawakami映射系统^[4]和Hopfield混沌网络模型^[4].

Kawakami映射系统描述如下

$$\begin{cases} x_{n+1} = y_n - ax_n \\ y_{n+1} = x_n^2 - b \end{cases} \quad (1)$$

其中 a 和 b 为参数,当 $a = 0.1, b = 1.6$ 时,式(1)存在混沌吸引子.

Hopfield混沌网络模型描述如下

$$\begin{cases} x_{n+1} = 10 \tanh(cy_n) \exp(-y_n) \\ y_{n+1} = 10 \tanh(x_n) \exp(-dx_n) \end{cases} \quad (2)$$

其中 c 和 d 为参数,当 $c = 1.2, d = 1.5$ 时,式(2)存在混沌吸引子.

3 基于超混沌的图像加密方案设计

3.1 加密过程

图像加密系统模型如图1(a)所示,假设原图像 I 的大小为 $m \times n, I(i, j)$ 为像素 (i, j) 处的灰度值,外部密钥串为 $\text{Key}_1 \text{Key}_2 \dots \text{Key}_6$,二维超混沌映射系统的初值为 x_{v0} 和 y_{v0} .从设计的角度进行分析,为了使图像加密系统不仅依赖于超混沌系统的初值和参数,而且极其敏感的依赖于明文,因此对Kawakami映射系统和Hopfield混沌网络模型的初值修正为:

$$\begin{aligned} x'_{v0} &= (x_{v0} + (B_1 \oplus T_1)/255) \bmod 1 \\ y'_{v0} &= (y_{v0} + (B_2 \oplus T_2)/255) \bmod 1 \end{aligned} \quad (3)$$

其中 $V_0 \in \{K0, H0\}$. B_1 表示图像 I 所有像素灰度

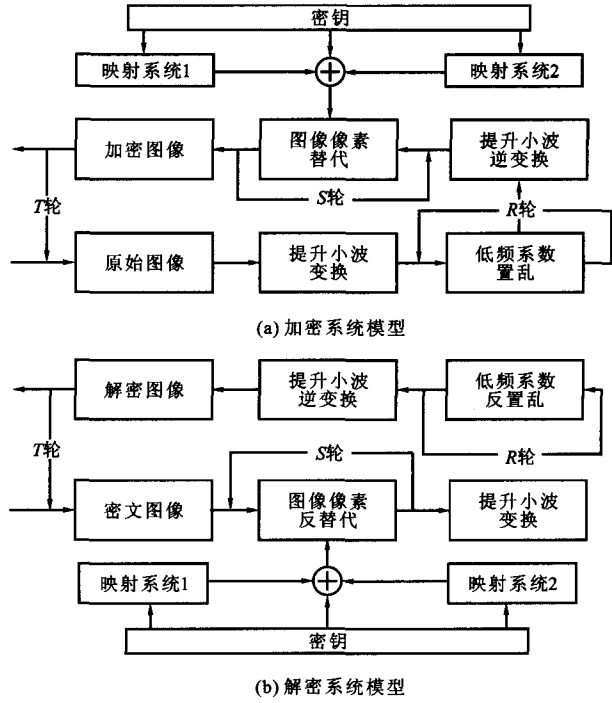


图1 图像加密和解密系统模型

值的异或, B_2 表示图像 I 的所有像素灰度值的和, T_1 表示所有外部密钥串的异或, T_2 表示所有外部密钥串的和, $\oplus$ 表示异或操作.

算法的具体过程描述如下

Step1: 输入密钥 $K_1 K_2 K_3 K_4 K_5 K_6, a, b, x_{K0}, y_{K0}, c, d, x_{H0}, y_{H0}, W, L, H, k, R, S, T$.

Step2: 输入图像.若图像大小 $m \neq n$,则对图像边界填充0,使其大小为 8×8 的整数倍.

Step3: 选择整数提升小波函数 W 对原始灰度图像 I 进行 L 级小波分解,产生 $3L+1$ 个不同小波子带的系数矩阵.其中, L 表示分解的级数.

Step4: 对低频子带系数矩阵采用改进的自适应排列算法进行 R 轮置乱.改进的自适应排列算法并不由密钥控制,而是每轮同时采用左右和上下排列模式.将调整后的低频子带系数与其余的中高频子带系数经过小波逆变换得到重构矩阵 I_1 .小波低频子带系数的置乱,重构图像时会出现溢出 $[0, 255]$ 的奇异值,对奇异值映射到 $[0, 255]$,进一步得到重构图像 I_2 .

Step5: 由二维超混沌系统生成混沌序列并进行预处理.输入Kawakami映射系统的控制参数 a, b 和初值 x_{K0}, y_{K0} ,再由式(1)构造 $(m \times n + 1024)$ 对混沌序列值,分别存储于数组 $\{x_K(i)\}$ 与 $\{y_K(i)\}$ 中, $i = 1, 2, \dots, m \times n$.同样输入Hopfield混沌网络模型的控制参数 c, d 和初值 x_{H0}, y_{H0} ,再由式(2)构造 $(m \times n + 1024)$ 对混沌序列值,分别存储于数组

$\{x_H(i)\}$ 与 $\{y_H(i)\}$ 中. 利用公式(4) 对混沌序列数组进行预处理, 得到序列 $t(i)$. 其中, k 为控制参数, ceil 表示超过 x 的最小整数.

$$t(i) = 10^k t(i) - \text{ceil}(10^k t(i)) \quad (4)$$

$$t \in \{x_K, y_K, x_H, y_H\}, i = 1, 2, \dots, m \times n$$

Step6: 构造混合反馈系统 C^1 和 C^2 . 分别输出混沌序列 C_i^1 和 C_i^2 . 令 $\text{key}_5 = C_0^1$, $\text{key}_6 = C_0^2$, 则混合反馈系统为:

$$C^1 : C_i^1 = \text{ceil}(\text{key}_1(x_K(i)^2 + y_K(i)^2)^{1/2} + \text{key}_2 C_{i-1}^1) \bmod 256 \quad (5)$$

$$C^2 : C_i^2 = \text{ceil}(\text{key}_3(x_H(i)^2 + y_H(i)^2)^{1/2} + \text{key}_4 C_{i-1}^2) \bmod 256 \quad (6)$$

Step7: 对图像像素灰度值输出反馈加密处理, 计算 $s_i = C_i^1 \oplus C_i^2$, $i = 1, 2, \dots, m \times n$.

第 1 轮加密: 对图像矩阵 I_2 第一个像素值单独加密

$$p(1) = [I_2(1) + C_1^2 C_2^2] \bmod 256$$

若 s_i 为奇数, 则加密算法为:

$$p(i+1) = p(i) \oplus C_{i+1}^1 \oplus \{[2C_{i+1}^2 + I_2(i+1)] \bmod 256\} \quad (7)$$

若 s_i 为偶数, 则加密算法为:

$$p(i+1) = p(i) \oplus C_{i+1}^2 \oplus \{[2C_{i+1}^1 + I_2(i+1)] \bmod 256\}, i = 1, 2, \dots, m \times n \quad (8)$$

第 $S(S > 1)$ 轮加密: 对第一个像素值单独加密

$$p(1) = [p(1) + p(m \times n) + C_1^2 C_2^2] \bmod 256.$$

将公式(7)和(8)中右端的 $I_2(i)$ 用上一轮得到的一维密文序列 $p(i)$ 替代, 继续重复类似上一轮的操作. 直到对图像进行 S 轮加密为止. 将 S 轮加密后生成的一维密文序列 p 按一定顺序排列成二维图像矩阵 I_3 .

Step8: 输出图像. 重复 Step3 到 Step7, 直到图像矩阵 I_3 进行 T 轮加密为止. 输出最终图像矩阵 I_4 .

3.2 解密过程

图像解密系统模型如图 1(b) 所示. 解密过程是加密过程的逆过程.

4 仿真结果与分析

在 Matlab 7.0 仿真环境下对一幅 256×256 的标准 Lena 灰度图像进行加解密实验, 选择 Haar 整数提升小波对图像进行小波分解, 分解级数为 $L = 1$, 采用光栅扫描方式, 自适应置乱轮数 $R = 4$, 控制参数为 $k = 5$, 灰度值替代加密处理轮数 $S = 1$. 给定 Kawakami 映射系统的参数 $a = 0.1, b = 1.6$ 以及初

值为 $x_{K0} = 0.1, y_{K0} = 0.2$. 给定 Hopfield 混沌网络模型的参数为 $c = 1.2, d = 1.5$ 以及初值为 $x_{H0} = 0.4, y_{H0} = 0.1$. 输入外部密钥 $(K_1, K_2, K_3, K_4, K_5, K_6) = (98, 57, 61, 123, 216, 84)$, 整个算法加密轮数 $T = 1$. 图 2(a) 为原图, 图 2(b) 为在上述密钥下加密后的图像.

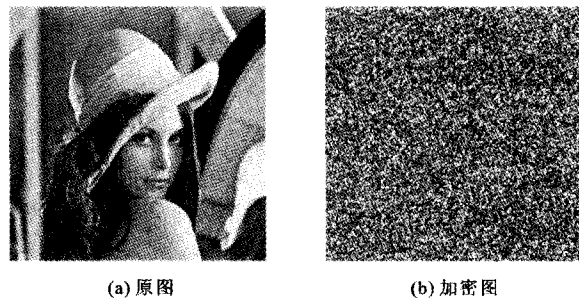


图 2 图像加密结果

4.1 密钥空间分析

本算法的密钥主要由两个超混沌系统的 4 个初值 $x_{K0}, y_{K0}, x_{H0}, y_{H0}$ 和外部密钥串 $K_1 K_2 K_3 K_4 K_5 K_6$ 组成. 假设采用 16 位的双精度小数作为系统的初值和长度为 48 bit 的字符作为外部密钥串, 则密钥空间可以达到 $(10^{16})^4 \times 2^{48} \approx 2^{260}$, 相当于 260 bit 的密钥长度. 若将提升小波函数类型 W , 小波分解级数 L , 系数扫描方式 H , 加密轮数 R, S, T 以及超混沌系统参数 a, b, c, d 和控制参数 k 作为原始密钥, 则密钥空间更大, 可以有效地对抗穷举攻击. 表 1 对比了不同加密方案的密钥空间, 可见本算法密钥空间最大.

表 1 密钥空间对比

加密方案	文献[5]	文献[1]	文中
密钥空间	2^{128}	2^{232}	2^{260}

4.2 差分攻击分析

测试明文一个像素的改变对整个密文的影响, 通常引入如下两个量: 像素数目改变率 NPCR 和整体平均改变强度 UACI^[5]. 从灰度图像中将最后一个灰度值修改为, 通过计算可以得到 $\text{NPCR} = 99.6185\%$ 和 $\text{UACI} = 33.4462\%$. 此结果表明, 对原始图像进行微小变动会导致加密图像很大的变化, 说明算法对明文相当敏感, 具有较强的抵抗差分攻击能力.

4.3 相邻像素的相关性分析

为测试明密文图像相邻像素的相关性, 从图像的水平, 垂直和对角方向随机选取 1000 对相邻像素, 由文献[5]定量计算其相邻像素相关系数. 加密

前后三个方向上的相关系数如表 2 所示. 从中可知, 密文的两相邻像素的相关系数接近于 0, 而且该项指标比文献[8]还要好一个数量级. 表明原图的统计特征已被很好地扩散到密图中.

表 2 明密文图像相邻像素的相关系数

方向	原图	密图	文献[6]
水平方向	0.95284	0.00148	-0.01589
垂直方向	0.97596	0.00113	-0.06538
对角方向	0.93736	0.00162	-0.03231

4.4 直方图分析

由图 3(b)可知密文的灰度直方图呈均匀分布, 很好的掩盖了明文图像的分布规律, 表明该算法能够有效抵御统计分析攻击和已知密文攻击.

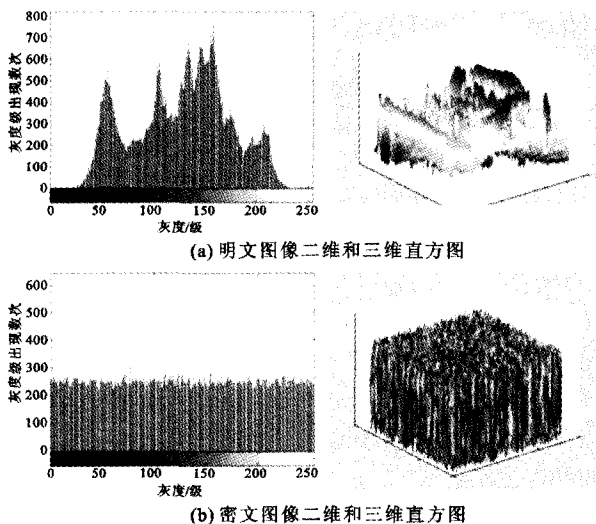


图 3 图像灰度直方图

4.5 密钥敏感性分析

图 4(a)为正确解密得到的图像, 图 4(b)为在其他解密密钥保持不变, 只解密密钥 y_{H0} 改变微小偏差 10^{-16} 时, 所获得的解密图像, 部分密钥敏感性测试如表 3, 可以看出算法对密钥相当敏感.

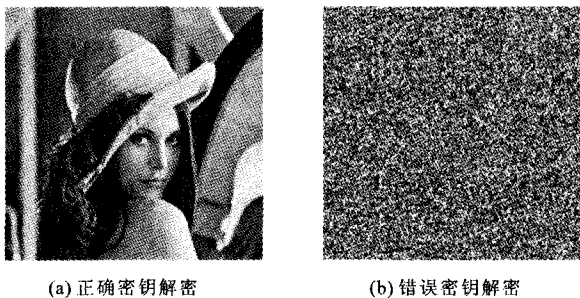


图 4 图像解密结果

4.6 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

$$H(m) = - \sum_{i=1}^{2N-1} P(m_i) \log_2 \frac{1}{P(m_i)} \quad (9)$$

表 3 密钥的微小偏差对两解密图像像素值的改变率

密钥	偏差	改变率 / %	密钥	偏差	改变率 / %
$x_{K0} = 0.1 + 10^{-16}$		99.5834	$K_2 = 57$	+1	99.5834
$y_{K0} = 0.2 + 10^{-16}$		99.5544	$K_3 = 61$	+1	99.5987
$x_{H0} = 0.4 + 10^{-16}$		99.5682	$K_4 = 123$	+1	99.5483
$y_{H0} = 0.1 + 10^{-16}$		99.6155	$K_5 = 216$	+1	99.5468
$K_1 = 98$	+1	99.5285	$K_6 = 84$	+1	99.5255

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 个符号以等概率出现的, 由文献[8]可知, 一个真正的随机信源的熵 $H(m) = 8$. 通过仿真分别与文献[7]、[8]相比较, 结果显示本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 4.

表 4 信息熵测试比较

加密方案	文献[7]	文献[8]	文中
$H(m)$	7.9338	7.9968	7.9979

4.7 峰值信噪比的分析

均方误差 MSE 或峰值信噪比 PSNR 是评价图像加密的一项重要指标, 图像矩阵大小为 $m \times n$, 量化级为 $0 \sim 255$ 的原图 $f(i, j)$, 密图为 $g(i, j)$.

$$MSE = \left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (f(i, j) - g(i, j))^2 \right) / m \times n \quad (10)$$

$$PSNR(dB) = 10 \log_{10} \frac{255^2}{MSE} \quad (11)$$

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为 PSNR 正无穷, 由此可见, 客观评价与主观评价结果一致, 图像可以无失真解密.

5 结束语

文中提出了一种基于提升小波变换和二维超混沌系统的图像加密方案, 该加密方案克服了单一的低维混沌系统保密性不高以及图像置乱加密计算量大的缺点. 方案中引入密文反馈和多轮加密机制, 使算法具有很好的扩散性和扰乱性. 同时混合反馈数据流的生成极其敏感地依赖于明文, 有效地提高了抵抗选择明文的能力. 仿真试验表明, 该加密方案密钥空间大, 对明文和密钥相当敏感, 能有效地抵抗多种攻击, 具有很高的安全性和良好的应用前景.

(下转第 53 页)

的有效性.该算法在通信信号的实时恢复中具有较好的实用价值.

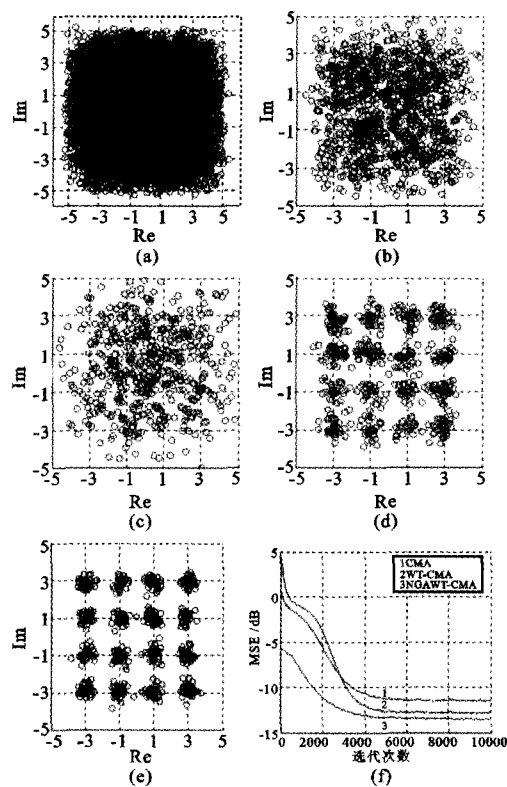


图3 仿真结果

参考文献:

- [1] 郭业才. 自适应盲均衡技术[M]. 合肥: 合肥工业大学

出版社, 2007.

- [2] 韩迎鸽, 郭业才, 吴造林, 等. 基于正交小波变换的多模盲均衡器设计与算法仿真研究[J]. 仪器仪表学报, 2008, 29(7): 1441—1445.
- [3] 李沉. 遗传神经网络盲均衡算法的研究[D]. 太原: 太原理工大学, 2006.
- [4] 韩迎鸽. 基于小波变换的盲均衡器设计与算法仿真研究[D]. 安徽: 安徽理工大学, 2007.
- [5] 谭艳艳, 许峰. 基于适应值共享的多生境排挤遗传算法[J]. 计算机工程与应用, 2009, 45(5): 46—49.
- [6] Zaouche A, Dayoub I, Rouvaen J M. Baud — spaced constant modulus blind equalization via hybrid genetic algorithm and generalized pattern search optimization. [J] Int J Electron Commun, 2008, 62: 122—131.
- [7] Luis M, San Jose Revuelta, Jesus Cid Sueiro. A neuro — evolutionary framework for Bayesian blind equalization in digital communications[J]. Signal Processing, 2003, 83: 325—338.
- [8] 王峰. 基于高阶统计量的水声信道盲均衡理论与算法[D]. 西安: 西北工业大学, 2003.

作者简介:

樊康 男, (1986—), 硕士研究生. 研究方向为通信信号处理.

郭业才 男, (1962—), 教授, 博士生导师. 研究方向为通信信号处理.

(上接第49页)

参考文献:

- [1] Gao T G, Chen Z Q. A new image encryption algorithm based on hyper — chaos[J]. Physics Letters A, 2008, 372(4): 394—400.
- [2] Chen G, Zhao X Y, Li J L. A self — adaptive algorithm on image encryption[J]. Journal of Software, 2005, 16(11): 1975—1982.
- [3] 彭飞, 丘水生, 龙敏. 基于二维超混沌映射的单向 Hash 函数构造[J]. 物理学报, 2005, 54(10): 4562—4568.
- [4] 何岱海, 徐健学, 陈永红. Kawakami 映射的超混沌行为研究[J]. 力学学报, 2000, 32(6): 750—754.
- [5] 张硕, 蔡如华, 陈光喜. 一种空频域结合的多维混沌系统图像加密方案[J]. 微电子学与计算机, 2010, 27(7): 60—64.
- [6] Gao H J, Zhang Y S. A new chaotic algorithm for image

encryption[J]. Chaos, Solitons & Fractals, 2006, 29(5): 393—399.

- [7] 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.
- [8] Behnia S, Akhshani A, Mahmodi H, et al. A novel algorithm for image encryption based on mixture of chaotic maps[J]. Chaos, Solitons & Fractals, 2008, 35(2): 408—419.

作者简介:

张欢 男, (1984—), 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.