中国农业大学学报 2006,11(3):98-100
Journal of China Agricultural University

基于 Logistic 映射的小波域图像加密技术

胡 梅 高万林
(中国农业大学 信息与电气工程学院,北京 100083)

摘 要 针对图像小波编码混沌加密技术中出现的边界效应问题,提出基于区间小波编码的混沌加密新技术。相对于传统的图像延拓方法,该方法在小波变换前后,不需要对图像进行特殊的延拓处理,可在对图像加密的同时,压缩图像文件规模,有效消除边界效应;此外,调整被逼近信号函数的 Hölder 连续指数 L 的大小,可满足对图像恢复精度的不同要求。实验结果表明,在 $L=1$ 时,信号恢复精度已满足要求。

关键词 区间小波;混沌加密;边界效应
中图分类号 TP 309.2;TN 911.73 **文章编号** 1007-4333(2006)03-0098-03 **文献标识码** A

Image encryption technology based on Logistic mapping in wavelet domain

Hu Mei, Gao Wanlin
(College of Information and Electrical Engineering, China Agricultural University, Beijing 100083, China)

Abstract To eliminate boundary effects in image a new image chaos encryption technology, the chaos encryption based on interval wavelet coding, is proposed. Compared with the traditional image extent method, the special extent processes is no longer necessary in this method before the wavelet transform (WT) to image and after the inverse wavelet transform (IWT) to chaos encryption serials. The test results shows that this method can be used to eliminate the boundary effect and compress the image file. Besides, the value of parameter L can be changed to meet various precision requirements for reconstruction of an image.

Key words interval wavelet; chaos encryption; boundary effect

小波变换和混沌理论是当今非线性科学领域的研究热点,将两者结合起来研究非线性问题具有其潜在的优势[1]。近年来,随着计算机网络技术的普及推广,网络信息传输的安全问题和传输速度已成为当前的研究热点。利用小波变换可实现数据的有效压缩,从而提高网络数据的传输速度,将混沌序列和现有的加密算法有机结合产生的混沌加密技术被认为是很有前途的加密新算法[2]。传统的图像混沌加密技术是基于离散余弦变换(DCT)的,即首先对图像进行离散余弦变换,然后用混沌序列对 DCT 变换系数进行置乱。目前基于小波编码的图像混沌加密研究只是简单用离散小波变换(DWT)代替 DCT[3-5],对该方法中出现的一些技术问题则未见讨论。本文中重点讨论了基于小波编码的图像混沌加密技术中小波变换引起的边界效应对加密图像的影响及其解决方法。区间小波[6]是解决边界效应的最好方法,但其构造复杂,计算工作量也比较大。笔者从区间小波构造方法中提取图像信号线性延拓技术,很好地解决了这一问题。

1 基于小波编码的图像混沌加密基本原理

常见的混沌映射方程有很多,如 Logistic、Henon、Ikeda、Quadratic、Mackey-Glass 等,本文中采用最常用的 Logistic 映射方程

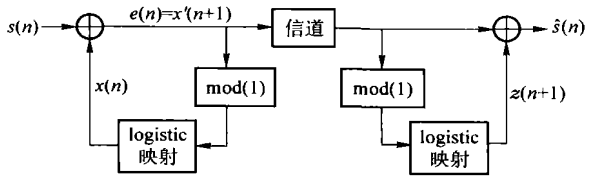
$$x_{n+1}=\mu x_n(1-x_n)$$

式中:$x_n\in(0,1)$,控制参数 $\mu\in(0,4)$。

混沌理论在数据传输领域的保密通信分为四大类:混沌扩频、混沌键控、混沌参数调制和混沌掩盖。

收稿日期:2005-07-01
基金项目:国家自然科学基金资助项目(10372036);中国农业大学科研启动基金资助项目(2005037)
作者简介:胡梅,高级实验师,E-mail:humei@cau.edu.cn

混沌参数调制技术因成熟且简单而得到广泛使用，利用调制技术和 Logistic 混沌映射方法可得到图像信号的混沌加密原理(图 1)。



$s(n)$ 为输入的原始信号的小波变换序列；$e(n)$ 为要传输到接收端的已加密的信息信号序列；$\hat{s}(n)$ 为最终的响应序列即恢复的信息信号序列；$z(n+1)$ 为从接收序列 $x'(n+1)$ 中恢复的混沌载波序列；$z(n+1)$ 为从接收序列 $x'(n+1)$ 中恢复的混沌载波序列

图 1　基于 Logistic 映射的图像信号加密原理

Fig. 1　Image signal encryption theory based on Logistic mapping

基于混沌映射的混沌加密系统的输出序列为：

$$x'(n+1) = 4x(n)(1 - x)(n)) + ks(n)$$

式中：k 为压缩系数，一般 $k < 1/50$。采用这种叠加调制的方法，显然有时会使得 $|x'(n+1)| > 1$，超出 logistic 混沌映射的工作区间。为了将 $x'(n+1)$ 限制在 0 与 1 之间，这里采用了取模运算，即

$$x(n+1) = [x'(n+1)]\bmod(1)$$

由此可知，通过将信息信号序列加入 Logistic 混沌映射序列实现了混沌载波调制。选择 $e(n) = x'(n+1)$ 作为通信信道中的传输信号序列，并且令 $x'(0) = x(0)$，$0 < x(0) < 1$。在接收端，用以下方法来恢复信息信号序列：

$$\begin{cases} y(n) = [x'(n)]\bmod(1) \\ z(n+1) = 4v(n)(1 - v(n)) = 4x(n)(1 - x(n)) \end{cases}$$

从下一个接收序列中减去从接收序列 $x'(n+1)$ 中恢复的混沌载波序列 $z(n+1)$，就可以恢复传输的信息信号序列，即

$$\hat{s}(n) = x'(n+1) - z(n+1) = ks(n)$$

式中 $\hat{s}(n)$ 表示混沌调制结果。最后对 $\hat{s}(n)$ 进行小波逆变换即可。

2　小波变换边界效应对混沌加密的影响及解决方法

尽管许多小波函数(如 Daubiches 小波)均具有紧支撑性，但紧支撑区间不能过小，因此对有限的图像信号进行变换必然会带来边界效应(图 2)。为解决该问题，可对原图像进行延拓，常见的延拓方法包括零延拓、对称延拓和周期延拓。零延拓其实就是不做任何延拓，边界效应无法得到改善；周期延拓只适合于周期信号，而大多数图像信号都不是周期的；对称延拓在有些情况下会恶化边界效应，应用范围较窄。

(a) 原图像　　(b) 用小波系数重构的图像

图 2　小波变换边界效应

Fig. 2　Boundary effect of wavlet tranformation

区间小波是为解决边界效应而提出的，但其构造方法复杂，计算量大，因此降低了图像处理速度，不适合用来进行图像加密。文献[7]基于广义变分原理提出了一种区间小波的构造方法，该方法得到的区间小波可表示为：

$$\omega_{j,k}(x) = w_{j,k}(x) + \sum_{n=-N+1}^{-1} a_{nk}\omega_{j,n}(x)$$

$$k = 0, \cdots, L$$

$$\omega_{j,k}(x) = w_{j,k}(x) \quad k = L+1, \cdots, 2^j - L - 1$$

$$\omega_{j,k}(x) = w_{j,k}(x) + \sum_{n=2^j+1}^{2^j+N-1} b_{nk}\omega_{j,n}(x)$$

$$k = 2^j - L, \cdots, 2^j \qquad (1)$$

其中

$$a_{nk} = l^1_{j,k}(x_{j,n}),\ b_{nk} = l^2_{j,k}(x_{j,n}) \qquad (2)$$

$$l^1_{j,k} = \prod_{\substack{i=0 \\ i\neq k}}^{L} \frac{x - x_{j,i}}{x_{j,k} - x_{j,i}},\ l^2_{j,k} = \prod_{\substack{i=2^j-L \\ i\neq k}}^{2^j} \frac{x - x_{j,i}}{x_{j,k} - x_{j,i}} \qquad (3)$$

$w_{j,k}(x)$ 为小波函数；L 为被逼近信号函数的 Hölder 连续指数；N 为小波函数的支撑区间，即 $\mathrm{supp}(w) = [-N, N]$。为减小计算工作量，可减小 L 的取值，当 $L = 1$ 时，相当于在图像边界处进行切线延拓。为便于对比，下面以一维信号 $y = \sin(x)$ 为例，并取 $L = 1$ 对比本文方法和对称延拓方法的效果。从图 3 可以看出，基于区间小波小波编码的混沌加密信号经解密后，与原始信号的误差比采用延拓方法的小得多，而延拓方法的误差主要体现在边界处，说明本文方法很好地解决了边界效应问题。

3　基于区间小波编码的图像混沌加密实验

二维区间小波可通过一维区间小波张量积运算得到，在实验中，取 Daubechies 小波为基小波，L =

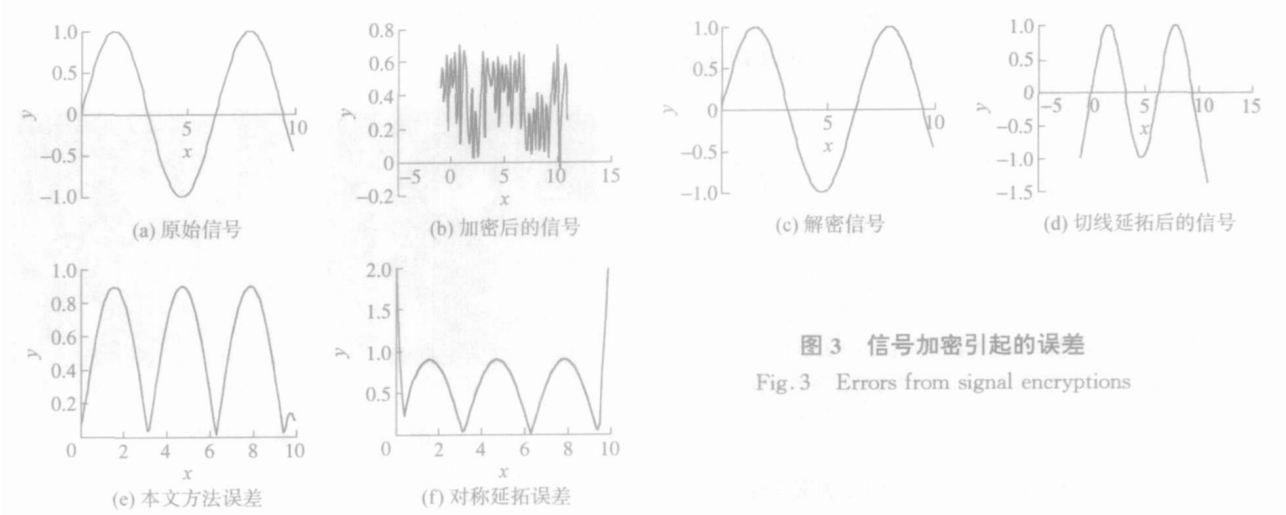


图 3 信号加密引起的误差

Fig. 3 Errors from signal encryptions

1。实验结果见图 4。不难看出,利用图像区间小波编码进行混沌加密,解密后的图像和加密前几乎没有差别,而其他延拓方法在边界处则存在非常明显的边界效应。

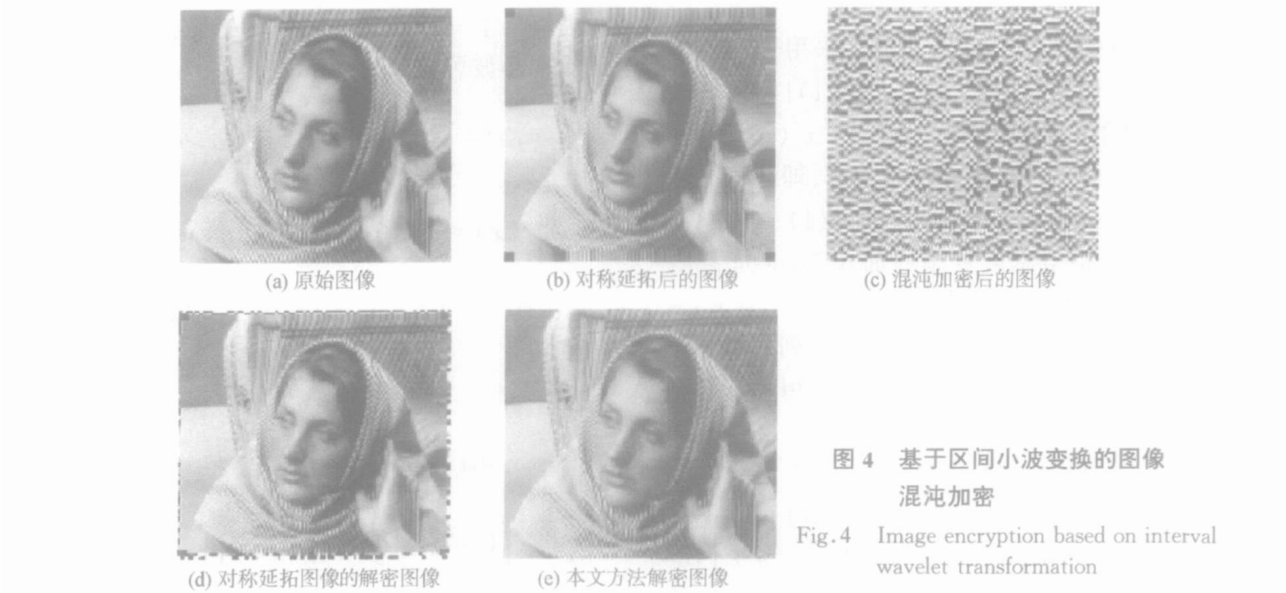


图 4 基于区间小波变换的图像混沌加密

Fig. 4 Image encryption based on interval wavelet transformation

4 结束语

混沌加密是一种新兴的图像信号加密技术,小波变换则是提高加密效率的需要。本文方法是为消除小波变换带来的边界效应而提出,其实质是将图像延拓运算映射到小波变换函数中,因此同样适合于图像的其他编码方法(如 Fourier 变换)。此外,从理论上来说,小波包编码应该比小波编码具有更好的保密性能,这也是笔者目前正在进行的研究。

参 考 文 献

[1] 游荣义, 陈忠, 徐慎初, 等. 基于小波变换的混沌信号相空间重构研究[J]. 物理学报, 2004, 53(9): 2882-2888

[2] Nikolaids, Athanasios. Asymptotically optimal detection for additive watermarking in the DCT and DWT domains [J]. IEEE Transaction Image Processing, 2003, 12(5): 563-571

[3] 陈文实, 曹光辉, 孟宪宇. 基于混沌和小波理论的图像加密技术实现[J]. 渤海大学学报:自然科学版, 2004, 25(3): 236-239

[4] 尹显东, 姚军, 唐丹, 等. 基于小波变换域的图像加密技术研究[J]. 信息与电子工程, 2005, 3(1): 1-5

[5] 赵健, 齐华, 田泽, 等. 改进的小波域混沌数字水印算法实现[J]. 光子学报, 2004, 33(10): 1236-1238

[6] Mei Shuli, Lu Qishao, Zhang Senwen, et al. Adaptive interval wavelet precise integration method for partial differential equations [J]. Applied Mathematics and Mechanics, 2005, 26(3): 364-371

[7] 梅树立. 小波数值方法及其在水土侵蚀模型分析中的应用[D]. 北京:北京航空航天大学, 2004