

文章编号: 1001-0920(2006)09-1024-04

基于超混沌和小波变换的鲁棒性数字水印算法

殷虹^{1,2}, 陈增强¹, 袁著祉¹

(1. 南开大学自动化系, 天津 300071; 2 天津工程师范学院 计算机系, 天津 300222)

摘要: 提出一种基于二维超混沌序列和离散小波变换(DWT)相结合的鲁棒性数字水印算法。该算法利用形式简单的二维离散超混沌系统产生的超混沌序列生成密码对水印图像加密, 同时根据人类视觉系统的特性, 对宿主图像在YQ色彩空间中的Y分量进行多级离散小波变换后, 将加密后的水印图像嵌入到宿主图像Y分量的DWT中频子带中。实验结果表明算法同时具有良好的鲁棒性和不可见性。

关键词: 超混沌; 小波变换; 数字水印; 图像加密

中图分类号: TP391 **文献标识码:** A

Robust Digital Watermarking Algorithm Based on Hyperchaos and Wavelet Transform

YIN Hong^{1,2}, CHEN Zeng-qiang¹, YUAN Zhu-zhi¹

(1. Department of Automation, Nankai University, Tianjin 300071, China; 2 Department of Computer, Tianjin University of Technology and Education, Tianjin 300222, China Correspondent: CHEN Zeng-qiang, E-mail: chenzq@nankai.edu.cn)

Abstract: An algorithm of digital watermarking based on two-dimensional hyperchaos sequence and discrete wavelet transform is presented, which generates cipher sequence to encrypt the watermark using hyperchaos sequence generated by simple two-dimensional hyperchaos system. The characteristics of human visual system is used to embed the watermarks which is encrypted into mid-frequency subbands coefficients of Y branch of host image after Y branch of host image is transformed by the multilevel structures wavelet transform in the YQ pattern space. The experimental results show the robustness and invisibility of the proposed algorithm.

Key words: Hyperchaos; Wavelet transform; Digital watermarking; Image encryption

1 引言

近年来, 数字水印作为一种多媒体数据的版权保护和内容认证的新技术, 越来越受到国内外学者的重视, 并提出许多数字水印方案^[1,2], 而鲁棒水印应具备不可感知性、鲁棒性、安全性和实时操作性等特点^[3]。同时, 由于混沌系统在信息处理等方面展示了良好的应用前景, 对混沌控制及其应用的研究也受到了广泛的重视^[4]。目前, 混沌特性在图像处理领域得到了较广泛的认识, 因此提出了基于混沌序列的数字水印算法^[5], 但广泛应用于水印图像加密的混沌模型是一维离散系统(如Logistic映射), 具有

密钥空间太小的缺陷

本文利用超混沌随机性好、可确定再生且密钥空间较大的特性, 提出一种结合人类视觉系统^[6](HVS)的基于超混沌序列和离散小波变换(DWT)的鲁棒性数字水印算法。首先利用形式简单的二维离散超混沌系统产生超混沌序列, 然后利用阈值处理后的超混沌阵列为水印图像加密; 在兼顾嵌入水印不可见性和鲁棒性的情况下, 根据HVS特性, 采用二维DWT对宿主图像在YQ色彩空间中的Y分量进行4级分解, 并将加密后的水印图像嵌入到宿主图像Y分量的DWT域中。这样, 既保证水印有较

收稿日期: 2005-06-20; 修回日期: 2005-08-26

基金项目: 国家自然科学基金项目(60374037, 60574036); 教育部博士学科点基金项目(20050055013)。

作者简介: 殷虹(1973—), 女, 天津人, 博士生, 从事多媒体信息安全、智能网络管理等研究; 陈增强(1964—), 男, 天津人, 教授, 博士生导师, 从事智能预测控制、智能网络管理等研究。

好的不可见性又提高了水印的鲁棒性 仿真实验验证了算法的有效性

2 基于二维超混沌序列和DWT的鲁棒性数字水印算法

2.1 超混沌序列的产生

本文采用形式简单且具有超混沌特性的二维离散混沌系统产生超混沌序列 定义一种二维离散超混沌系统具有如下形式^[7]:

$$\begin{cases} x_{n+1} = a_1 y_n + a_2 y_n^2, \\ y_{n+1} = a_3 x_n + a_4 y_n. \end{cases} \quad (1)$$

当 $a_1 = 1.66, a_2 = -1.3, a_3 = -1.1, a_4 = 0.1$ 时, 系统进入超混沌状态 图 1 给出对应该组参数的超混沌吸引子.

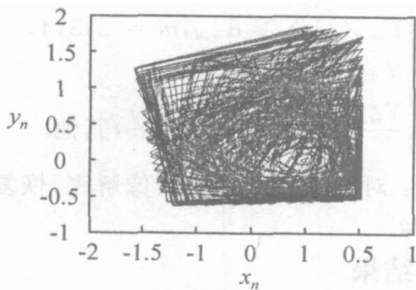


图 1 二维超混沌吸引子

由式(1)得到超混沌序列的方法如下:

1) 实数值超混沌序列: 即 $\{x_l, l = 0, 1, \dots\}$ 和 $\{y_s, s = 0, 1, \dots\}$. 混沌映射的轨迹点所形成的序列显然不宜直接应用于加密图像, 且理论研究表明这种无误差的平凡混沌加密方法是可破解的

2) 2^k 值超混沌序列: 可通过定义一个阈值函数 Γ , 如式(2)所示, 并由上述的实数值超混沌序列阈值化得到

二维超混沌系统的初始条件 x_0 和 y_0 作为密钥, 取初始值 $x_0 = 0.123, y_0 = 0.321$, 同时为了增加算法的随机性, 不使用该序列的初始段部分, 令

$$\Gamma(x) = \begin{cases} 00\dots00, 0 & x < \frac{1}{2^k}; \\ 00\dots01, \frac{1}{2^k} & x < \frac{2}{2^k}; \\ \vdots & \\ 11\dots10, \frac{2^k-2}{2^k} & x < \frac{2^k-1}{2^k}; \\ 11\dots11, \frac{2^k-1}{2^k} & x < 1. \end{cases} \quad (2)$$

实验结果表明, k 值越大, 加密效果越好. 考虑到数字图像特点和效率指标要求, 采用 8 位二进制序列作为加密因子序列 水印图像加密算法中应用的超混沌加密阵列可以通过式(2)形成的超混沌序列进行向量相乘得到, 即

$$C(i, j) = [x^\circ(i)]^T y^\circ(j). \quad (3)$$

其中: $x^\circ(i)$ 表示实数值超混沌序列 $\{x_l, l = 0, 1, \dots\}$ 阈值化后的行向量, $y^\circ(j)$ 表示实数值超混沌序列 $\{y_s, s = 0, 1, \dots\}$ 阈值化后的行向量, $C(i, j)$ 表示超混沌阵列

2.2 二维离散小波变换

Mallat 利用多分辨率分析的概念, 提出了离散小波变换的金字塔型算法 本文采用的二维 DWT 算法和二维逆离散小波变换 (IDWT) 算法是 Mallat 算法的推广. 具体描述如下:

1) 二维 DWT 算法

$$\begin{cases} C_{m,n}^{M+1} = f(m, n), \\ C_{k,l}^M = h(k-2m)h(l-2n)c_{k,l}^{M+1}, \\ \alpha_{k,l}^M = h(k-2m)g(l-2n)c_{k,l}^{M+1}, \\ \beta_{k,l}^M = g(k-2m)h(l-2n)c_{k,l}^{M+1}, \\ \gamma_{k,l}^M = g(k-2m)g(l-2n)c_{k,l}^{M+1}. \end{cases} \quad (4)$$

2) 二维 IDWT 算法

$$\begin{aligned} C_{m,n}^{M+1} = & c_{k,l}^M ih(m-2k)h(n-2l) + \\ & \alpha_{k,l}^M ih(m-2k)g(n-2l) + \\ & \beta_{k,l}^M ig(m-2k)h(n-2l) + \\ & \gamma_{k,l}^M ig(m-2k)g(n-2l). \end{aligned} \quad (5)$$

其中: $f(m, n)$ 为 $M+1$ 尺度层的图像信号; $\{h(k)\}$ 和 $\{g(k)\}$ 分别是标准正交尺度函数和小波函数的双尺度方程系数; $\{c_{m,n}^M\}$ 是 M 尺度层的图像信号, 它是 $M+1$ 尺度层图像信号 $\{c_{m,n}^{M+1}\}$ 的低频分量, 表现其粗略的概貌; $\{\alpha_{m,n}^M\}$ 表示 $\{c_{m,n}^{M+1}\}$ 在 x 方向的概貌和在 y 方向的高频细节信号; $\{\beta_{m,n}^M\}$ 表示 $\{c_{m,n}^{M+1}\}$ 在 y 方向的概貌和在 x 方向的高频细节信号; $\{\gamma_{m,n}^M\}$ 表示 $\{c_{m,n}^{M+1}\}$ 在 x 方向和 y 方向的高频分量, 同时也表明了沿对角线方向的细节信号

2.3 水印图像的加密与解密

设二值水印图像为 $W(i, j), i, j = 0, 1, \dots, R-1$, 对水印图像 $W(i, j)$ 加密如下:

$$W^*(i, j) = W(i, j)C(i, j). \quad (6)$$

其中: $W^*(i, j)$ 为加密后的水印图像阵列, $W(i, j)$ 为加密前的水印图像阵列, $C(i, j)$ 为超混沌阵列且满秩

解密过程进行如下:

$$\tilde{W}(i, j) = W^*(i, j)C^{-1}(i, j). \quad (7)$$

其中: $\tilde{W}(i, j)$ 为解密后的水印, $\tilde{W}^*(i, j)$ 为提取的水印, $C^{-1}(i, j)$ 为超混沌阵列 $C(i, j)$ 的逆矩阵

2.4 水印图像的嵌入

本文采用的宿主图像为 RGB 彩色图像, 根据 HVS 的特性, RGB 空间是颜色显示空间, 对目标物体的颜色模式描述复杂, 各个分量之间冗余信息多, 计算量大, 并不适合人的视觉特性. 而 YIQ 色彩表达系统由亮度信号 Y 和两个色差信号 I, Q 组成, 它利用人的可视系统对亮度变化比对色调和饱和度变换更敏感设计而成, 主要优点是去掉了亮度和颜色信息间的紧密联系, 能在不影响图像颜色的情况下处理图像的亮度成分. 本文提出的算法首先将 RGB 模式图像转换成 YIQ 表达模式, 将加密后的水印图像嵌入到其 Y 分量的 DWT 域中.

设 RGB 宿主图像为

$$P(i, j) = (R(i, j), G(i, j), B(i, j)), \quad i, j = 0, 1, \dots, M-1. \quad (8)$$

Step 1: 利用 RGB 模式转换 YIQ 模式的定义式, 将 RGB 宿主图像转换到 YIQ 模式

$$P(i, j) = (Y(i, j), I(i, j), Q(i, j)), \quad i, j = 0, 1, \dots, M-1, \quad (9)$$

然后提取出 Y 分量

Step 2: 采用式 (4) 对 YIQ 宿主图像的 Y 分量分别进行 4 级分解. $Y_{m,d}(i, j)$ 表示位于分辨率为 m , 方向为 d 的子带中 (i, j) 处的小波系数, 分解级数 $m = 1, 2, 3, 4, d = LL, HL, LH, HH$, 分别表示低频子带、水平、垂直、对角方向的高频子带图像信号.

Step 3: 由于隐藏于高频部分的信息在有损压缩等量化操作后容易丢失, 所以本文选择将水印嵌入到中频子带图像 $HH_2, HL_2, LH_2, HH_3, HL_3$ 和 LH_3 中. 将 $\tilde{W}^*(i, j)$ 嵌入到中频系数中, 即

$$Y_{m,d}^*(i, j) = \begin{cases} Y_{m,d}(i, j) + \mu T_{m,d}(i, j) \tilde{W}^*(i, j), \\ Y_{m,d}(i, j) & E_{m,d,m} = 2, 3, 4, \\ d = HH, HL, LH; \\ Y_{m,d}(i, j) + \lambda \tilde{W}^*(i, j), & \text{其他} \end{cases} \quad (10)$$

$$T_{m,d}(i, j) = (Y_{m,d}(i, j) - e_{m,LL}) / M_{m,d}^2, \quad (11)$$

$$E_{m,d} = \frac{1}{M_{m,d}^2} \sum_{i=0}^{M-1} \sum_{j=0}^{M-1} Y_{m,d}^2(i, j). \quad (12)$$

其中: μ, λ 为子带图像的调节因子, 分别取为 0.3 和 0.05; $T_{m,d}(i, j)$ 是视觉掩蔽函数, 表示第 m 级第 d 个子带图像 (i, j) 处的视觉掩蔽值; $E_{m,d}$ 表示第 m 级第 d 个子带图像的能量; $M_{m,d}^2$ 为第 m 级第 d 子带的大小; $e_{m,LL}$ 为第 m 级的低频子带 LL 的均值.

Step 4: $Y_{m,d}^*(i, j)$ 进行二维离散小波逆变换 (DWT) 后, 再将 YIQ 模式转换为 RGB 模式, 得到

嵌入加密水印图像的彩色图像

$$P^*(i, j) = (R^*(i, j), G^*(i, j), B^*(i, j)), \quad i, j = 0, 1, \dots, M-1. \quad (13)$$

2.5 水印图像的提取

水印的提取需要原始图像作参考, 水印提取方法是水印嵌入的逆过程.

Step 1: 分别将嵌入水印后图像 $P^*(i, j)$ 和原始图像 $P(i, j)$ 进行从 RGB 到 YIQ 的色彩空间转换;

Step 2: 分别提取转换后图像的 Y 分量, 并进行 DWT 变换;

Step 3: 提取加密水印图像如下:

$$\tilde{W}^*(i, j) = \begin{cases} \frac{Y_{m,d}^*(i, j) - Y_{m,d}(i, j)}{\mu T_{m,d}(i, j)}, \\ Y_{m,d}(i, j) & E_{m,d,m} = 2, 3, 4, \\ d = HH, HL, LH; \\ \frac{Y_{m,d}^*(i, j) - Y_{m,d}(i, j)}{\lambda}, & \text{其他} \end{cases} \quad (14)$$

Step 4: 对提取出的水印图像解密, 恢复出原始的水印图像.

3 实验结果

仿真试验采用 $256 \times 256 \times 8$ 标准 Lena 图像作为宿主图像, 水印为 "APLAB NK" 字样的黑白二值图像作为水印图像, 如图 2 所示. 图 3 所示为加密后的水印图像和嵌入水印后的图像. 为了考察算法的鲁棒性, 实验中对加水印的图像进行了 JPEG 压缩 (质量因子 50)、加入高斯噪声 (均值为 0, 方差为 0.002)、 3×3 中值滤波、剪裁等图像处理, 如图 4 所示. 经过处理后的图像仍能检测出水印, 如图 5 所示.



图2 实验中所用标准Lena图和水印图像



图3 加密后的水印图像和嵌入水印图像的Lena图

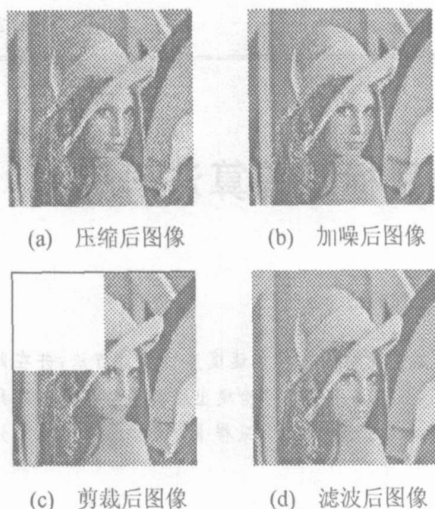


图4 图像经过压缩、加噪、剪裁、滤波后的效果

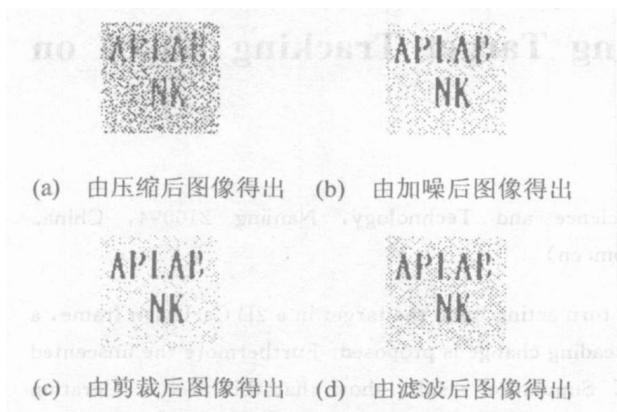


图5 抽取出的水印图像

4 结 语

本文提出了一种基于二维超混沌序列和DWT相结合的鲁棒性数字水印算法。针对HVS的特性折衷水印的鲁棒性和不可见性,选择YQ色彩模式的Y分量作为水印图像的隐藏空间,利用二维超混沌系统产生的超混沌序列对水印图像加密,将加密后

的水印图像嵌入到宿主图像Y分量的DWT中频子带系数中。实验结果表明算法具有良好的鲁棒性和不可见性。

参考文献 (References)

- [1] 刘春庆, 王执铨, 戴跃伟. 常用数字图像水印攻击方法及基本对策[J]. *控制与决策*, 2004, 19(6): 601-606
(Liu C Q, Wang Z Q, Dai Y W. Current Attacking Method to Digital Image Watermarking and Basic Countermeasures[J]. *Control and Decision*, 2004, 19(6): 601-606)
- [2] Cox IJ, Miller M L. The First 50 Years of Electronic Watermarking [J]. *Eurasip J of Applied Signal Processing*, 2002, 2(1): 126-132
- [3] Jiang J, Armstrong A. A Data Hiding Approach for Efficient Image Indexing[J]. *Electronics Letters*, 2002, 38(23): 1424-1425
- [4] 姚明海, 齐冬莲, 赵光宙. 基于李雅普诺夫指数的离散混沌系统的控制研究[J]. *控制与决策*, 2002, 17(2): 171-174
(Yao M H, Qi D L, Zhao G Z. On Control of Discrete-time Chaotic Systems Based on Lyapunov Exponents [J]. *Control and Decision*, 2002, 17(2): 171-174)
- [5] Sun T F, Wen Q, Wang S X. Based HVS Chaotic Array Image Watermarking Algorithm [J]. *Acta Electronica Sinica*, 2003, 31(1): 149-153
- [6] Watson A B. *Digital Images and Human Vision* [M]. Cambridge: The MIT Press, 1993: 163-178
- [7] 程丽, 陶路, 黄秋楠, 等. 构造具有超混沌特性的二维离散系统[J]. *东北师范大学学报*, 2002, 34(3): 47-52
(Cheng L, Tao L, Huang Q N, et al. Hyperchaotic System Generated by 2D Discrete System [J]. *J of Northeast Normal University*, 2002, 34(3): 47-52)

(上接第1023页)

- [8] Porter B. *Stability Criteria for Linear Dynamical Systems* [M]. New York: Academic Press, 1967.
- [9] Krall A M. On the Real Parts of Zeros of Exponential Polynomials[J]. *American Mathematical Society*, 1964, 70: 291-292
- [10] Liu G H, Chang C H, Han K W. Analysis of Robust

Control Systems Using Stability Equations[J]. *J of Control Systems and Technology*, 1993, 1: 83-89

- [11] Oliveira V A, Teixeira M C, Cossi L. Stabilizing a Class of Time Delay Systems Using the Hermite-biehler Theorem [J]. *Linear Algebra and Its Applications*, 2003, 369: 203-216