解决所有权死锁的一种数字水印算法

宋劲松[1]，周激流[1]，李振华[1]，张晓阳[2]

(1. 四川大学电子信息学院 成都 610065; 2. 成都市无线电监测站 成都 610031)

【摘要】为解决数字水印技术中广泛存在的所有权死锁问题，提出一种可靠的水印算法。通过引入Chebyshev和Henon混沌系统，结合非盲水印策略，得到密钥 k_1 和 k_2，其中 k_1 与混沌系统初值有关，容易获取；k_2 与原始图像有关，必须通过原始图像获取相应信息，即 k_2 的获得具有唯一性，非版权人在一般情况下不可能获得 k_2，从而起到作品版权保护的目的。实验测试分析所提出的算法表明，该算法具有较高的鲁棒性和可靠性，完全能达到理论分析中所提到的作品版权保护目的。

关 键 词 混沌系统； 版权死锁； 数字水印； 小波变换

中图分类号 TP391.41 **文献标识码** A doi:10.3969/j.issn.1001-0548.2011.05.029

Authentic Watermarking Algorithm Based on Resolving Copyright Deadlock

SONG Jin-song[1], ZHOU Ji-liu[1], LI Zhen-hua[1], and ZHANG Xiao-yang[2]

(1. School of Electronics and Information Engineering, Sichuan University Chengdu 610065; 2. Chengdu Radio Monitoring Station Chengdu 610031)

Abstract Based on an application of the digital image watermarking of the wavelet and chaotic theory, an watermarking method is proposed to resolve copyright deadlock. By using Chebyshev and Henon chaose system with non-blind watermarking, Keys K_1 and K_2 are obtained, where K_1 correlates with the initial value of chaose system, and K_2 with the initial image. Experiments indicate that the proposed algorithm is effective and superior to the traditional algorithms.

Key words chaotic system; copyright deadlock; digital watermark; wavelet transform

随着数字技术和网络技术的迅速发展，图像、音频及视频等数字产品的传播和获取变得快捷和方便，也使复制及传播未经授权的数字产品内容变得非常简单。因此，数字产品的版权保护越来越引起人们的关注，成为一个亟待解决的问题[1-5]。

目前的一些基于密钥的混沌数字水印技术主要采取对嵌入水印进行加密，从原始图像中获取密钥，由于种种原因没有或考虑得较少。文献[6]指出，如果攻击者在已有水印的作品中添加自己的水印，并且与原创者一样拥有相同的水印检测结果时，将会出现作品版权之争(版权死锁)，即版权死锁问题。针对该问题，本文引入混沌系统及混沌系列，通过非盲水印有效地解决版权的死锁。

1 混沌系统与混沌序列

混沌现象是指一种貌似无规则的运动。在非线性动力系统中，该运动既非周期又不收敛，但却是一种确定性的、类似随机的过程。利用混沌信号的特殊特性对水印信号进行加密，可以增强水印信号的安全性。一个一维混沌系统可以定义为：

$$x_{k+1} = f(x_k, \mu) \tag{1}$$

式中，$x_k \in V$ 为状态，k=0,1,2,…； $f: V \to V$ 是一个非线性映射，可将当前状态 x_k 映射到另一状态 x_{k+1}。

混沌序列的主要优点有：1) 初值敏感性，通过改变初始值或系统参数，可以得到众多的混沌序列；2) 有确定性的、类似随机的过程，具有很好的安全性，保密程度比较高；3) 白噪声的统计特性，可以用于需要噪声调制的应用场合。由此可见，可以方便地把水印的初始值作为序列的密钥，在水印提取时通过密钥重新得到水印序列。因此，利用混沌序列作为水印信号具有简单易行、安全可靠的特点。

下面对Chebyshev和Henon混沌系统分别进行介绍。

1) Chebyshev混沌系统[2]。

n阶Chebyshev映射定义为：

$$x_{n+1} = \cos(n(\arccos x_n)) \qquad x_n \in (-1,1) \tag{2}$$

收稿日期：2009－12－28； 修回日期：2010－07－06

基金项目：国家自然科学基金(60572033)；教育部博士点基金(60773168)

作者简介：宋劲松 (1967－)，男，博士生，主要从事通信与信息处理方面的研究.

式中，x_n 为映射变量，以初始值 x_0 代入方程开始迭代，就可以得到混沌序列 x_n，本文取n=4。

2) Henon混沌系统。

Henon映射定义为：

$$x_k = 1 + p(x_{k-2} - x_{k-3}) - qx_{k-1}^2 \quad (3)$$

式中，在 $p = 0.3$，$1.07 \leqslant q \leqslant 1.09$，本文取 $p = 0.3$、$q = 1.08$。

为了提高系统对初值的敏感性和拉长输出序列的周期，将迭代中的Henon映射替换[7]为：

$$x_{\mathrm{k}} = f(x_k, I_k) =$$
$$(1 + 0.3(x_{k-2} - 1.08) - 379x_{k-1}^2 + t\mathrm{Idct}_k) \bmod 3 \quad (4)$$

式中，t=1 001；Idct_k 是原始图像经过DCT变换后随机选取的系数值；密钥 k_1 由 x_k 的初值 x_0 产生；密钥 k_2 是 x_k 经过二值化操作后的取值。

根据DCT变换的特点，原始图像任意像素值的改变与DCT系数的变化有关；此外，根据混沌系统具有遍历性、初值敏感性的特性，Idct_k 的变化与 x_k 的变化有关。所以，密钥 k_2 的取得与原始图像紧密相关。

2 水印的置乱加密

从安全角度考虑，将混沌实值序列进行二值化[6]，使其丧失部分信息难于破译，可以增强其保密性。因此，要保证数字水印信号的不可逆性，在水印嵌入之前，对混沌实值序列进行二值化，并且，混沌二值序列仍具有良好的自相关及互相关特性，对数字水印的应用过程意义重大。

下面对式(2)产生的非周期且长度无限的实数混沌序列进行二值化，生成二值序列作为数字水印信号，以实现水印的加密。此外，为进一步提高水印的保密度，增加攻击难度，保证水印由原作者有效地提取使用，本文对水印进行了二次加密，其步骤如下。

输入参数：经过DCT变换的原始图像、二值图像水印 $w_{m\times n}$、初值密钥 k_1。

输出参数：二次加密水印 $w_{m\times n}^2$。

1) 参数计算。

(1) 对Chebyshev映射产生混沌序列进行二值化操作，该过程记为 H^1；

(2) 对原始图像进行DCT变换，选取N个DCT变换系数作为 Idct_k 值，其中$1 \leqslant k \leqslant N$。

(3) 在密钥 k_1 及参数 Idct_k 的基础上，对Henon映射生成的混沌序列进行二值化，得到密钥 k_2，该过程记为 H^2；

2) 置乱加密操作(如图1所示)。

(1) 对产生的二值水印图像进行扫描，得到序列 L_k，$1 \leqslant k \leqslant N$，通过 $D = L \oplus H^1$ 进行一次加密，即一次加密水印 $w_{m\times n}^1$；

(2) 通过 $W = D \oplus H^2$ 实现二次加密结果，即得到二次加密水印 $w_{m\times n}^2$。

经过二次加密后，各次加密的水印图像与原始水印图像的比较如图2所示。

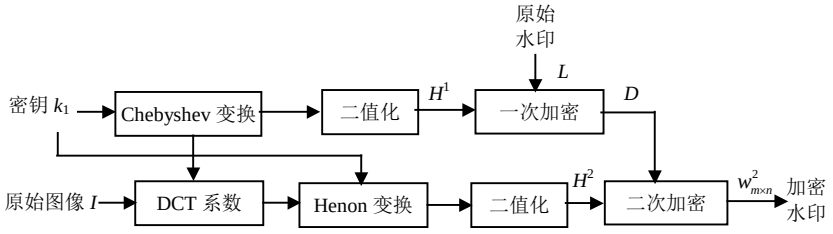

图1 水印加密过程

a. 原始水印图像 $w_{m\times n}$ b. 一次加密结果 $w_{m\times n}^1$ c. 二次加密结果 $w_{m\times n}^2$

图2 二次加密后各次加密的水印图像与原始水印图像的比较

3 水印的嵌入和提取(检测)

水印的嵌入和提取(检测)[8-14]是水印技术的重要环节，不同的水印嵌入提取方式决定了水印的不同效果。

水印嵌入是在小波域中进行的，小波域中高频部分代表图像的边缘及纹理部分，人眼不易发觉的嵌入水印容易在图像经过有损压缩处理后丢失。而

低频部分集中了图像的大部分能量，该部分的改变容易影响图像的质量。因此，结合人类视觉系统HVS的亮度掩蔽特性、边界掩蔽特性和纹理掩蔽特性等，本文将宿主图像 $I(i,j)(1\leqslant i,j<M)$ 进行3级小波分解，选择将水印嵌入到第3级中频子带图像即HH_3、HL_3和LH_3中。

二次加密水印的嵌入过程如下：

1) 选择水印嵌入块。对原始图像进行小波分解，得到几个不同频带的子图，选择小波分解的第3级细节子图的中频块HH_3、HL_3和LH_3作为水印的嵌入块；

2) 确定嵌入位。由密钥 k_1 通过Chebyshev映射产生随机序列，固定嵌入水印的位置。

3) 确定所选系数的邻域均值。设 $c_{i,j}$ 为系数值，$\text{mean}_{i,j}$ 为邻域均值，则有：

$$\text{mean}_{i,j}=\text{mean}(c_{i,j-1},c_{i-1,j},c_{i+1,j},c_{i,j+1}) \tag{5}$$

4) 生成一个嵌入标记位 $f_{i,j}$，并嵌入水印。在水印 $w^2_{m\times n}=1$ 且 $c_{i,j}$ 大于 $\text{mean}_{i,j}$ 值时，用 $c'_{i,j}$ 替代 $c_{i,j}$ 值，并使嵌入标记位 $f_{i,j}$ 值为0，其中 α 取0.01，即：

$$\text{if } (c_{i,j}>\text{mean}_{i,j} \text{ and } w^2_{i,j}=1), \text{ then}$$
$$c'_{i,j}=c_{i,j}(1-\alpha w^2_{i,j})$$
$$f_{i,j}=0$$

同理，可以得到嵌入水印时其他嵌入标记位 $f_{i,j}$ 的值。

5) 水印图像的获得。通过对嵌入后的小波变换图像进行小波反变换，能够获取已添加了水印的图像 I^*。

水印的提取过程与水印的嵌入过程是两个互逆的过程。在水印的提取过程中，水印的置乱规则以及产生水印序列的密钥是水印嵌入者和检测者都必须预先知道的。因此，本文的算法通过密钥 k_1 和水印的置乱规则，确定了嵌入标记位 $f_{i,j}$，能够进行水印的提取。其提取过程描述如下：

1) 利用小波变换，将已添加了水印的图像 I^* 进行3级多分辨率小波变换；

2) 由混沌系统初值所生成的密钥 k_1 确定所嵌入水印的具体位置；

3) 通过标记位 $f_{i,j}$ 和邻域均值 $\text{mean}_{i,j}$，用与水印嵌入过程相反的过程重建水印 W^*。

此外，还可以采用如下的水印检测方法检验：

$$H_0: E=F^*-F=N \qquad \text{无水印}$$
$$H_1: E=F^*-F=W^*+N \qquad \text{有水印}$$

式中，W^* 为待测试水印序列；F^* 为待测试图像；F 为原始图像；N为噪声。

将重构的水印 W^* 与嵌入水印 W 进行比较，可以判断提取的水印正确与否，达到识别数字产品真伪的目的。此外，还可以通过归一化相似度 NC (normalized correlation)进行客观评价，因有：

$$\text{NC}=\sum_{i=1}^{N}w(i)w^*(i)\Big/\sqrt{\sum_{i=1}^{N}w^2(i)}\sqrt{\sum_{i=1}^{N}w^{*2}(i)} \tag{7}$$

将结果 NC 和门限 T_s 比较，大于门限说明待测信号中含有水印；反之则不含水印。$\text{NC}\in[0,1]$，NC越接近1，表明获得的水印效果越好。

4　实验结果分析

4.1　无失真情况测试

由图3可知，对于嵌入水印的Lena图像(图3c的PSNR=72.23)与Lena原图像3a，人眼无法感知水印的存在；对于提取出的水印(图3d的NC=0.997)与原始水印图像3b，人眼无法感知水印的区别。因此，水印嵌入状态良好，无失真情况。


a. Lena原图


b. 原始水印


c. 嵌入水印后的图像


d. 提取的水印

图3　算法无失真测试图例分析

4.2　安全性测试

Lena图像在密钥 k_1 分别正确与错误(混沌序列的初值改变10^{-12})时提取水印的情况分别如图4a和图4b所示。Lena图像在密钥 k_1 正确，密钥 k_2 分别正确与错误(原始图像某一像素值改变10^{-12})时提取出的水印的情况分别如图4c和图4d所示。由图4可知，密钥 k_1 与混沌系统的初值有关，密钥 k_2 与原始图像有关，密钥 k_1 和 k_2 共同提供安全保护。


a. k_1 正确时解密水印


b. k_1 错误时解密水印


c. k_1、k_2 正确时解密水印


d. k_1 正确、k_2 错误时解密水印

图4　算法安全性测试图例分析

5 结 论

为了解决所有权死锁问题，本文引入Chebyshev和Henon混沌系统，通过非盲水印方法，得到2个密钥 k_1 和 k_2，其中，k_1 与混沌系统初值有关，k_2 与原始图像有关。从某种意义上讲，尽管 k_1 的获得比较容易，但 k_2 的获得必须通过原始图像，即 k_2 的获得具有唯一性。因此，非版权人一般情况下不能获得 k_2，从而起到了保护作品版权的目的。

参 考 文 献

[1] CRAVER S, MEMON N B L M, YEUNG M. Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implication[J]. IEEE Journal on Selected Areas in Communications, 1998, 16(4): 573-586.

[2] FLORENT A V, PATRICK L C. A robust image watermarking chnique based on quantization noise visibility thresholds[J]. Signal Processing, 2007, 87(6):1363-1383.

[3] 高铁杠，莫然. 一种基于小波系数动态量化的鲁棒数字水印算法[J]. 武汉大学学报(理学版), 2011, 57(5): 449-454.
GAO Tie-gang, MO Ran. A robust watermarking scheme based wavelet coefficient dynamical quantization[J]. J Wuhan Univ (Nat Sci Ed), 2011, 57(5): 449-454.

[4] 李明, 廖晓峰. 结合混沌的小波变换数字水印技术[J]. 计算机科学, 2007, 34(8): 245-247.
LI Ming, LIAO Xiao-feng. A new method for digital watermarking of wavelet transform combined chaos[J]. Computer Science, 2007, 34(8): 245-247.

[5] 李赵红, 侯建军. 基于Logistci混沌映射的DCT域脆弱数字水印算法[J]. 电子学报, 2006, 34(12): 2134-2137.
LI Zhao-hong, HOU Jian-jun. DCT-domain fragile watermarking algorithm based on logistic maps[J]. Acta Electronical Sinca, 2006, 34(12): 2134-2137.

[6] 朱从旭, 陈志刚. 一种基于混沌映射的空域数字水印新算法[J]. 中南大学学报(自然科学版), 2005, 36(2): 272-276.
ZHU Cong-xu, CHEN Zhi-gang. A novel spatial domain digital watermarking algorithm based on chaotic map[J]. J Cent South Univ (Science and Technology), 2005, 36(2): 272-276.

[7] LIU Nian-sheng, YANG Guo-hao. A new wavelet watermark scheme of color image based on chaotic sequences[C]//International Conference on Intelligent Information Hiding and Multimedia Signal Processing. [S.l.]: [s.n.], 2008.

[8] 焦占亚, 王蕊. 时空二维混沌的JPEG2000数字水印算法研究[J]. 计算机与数字工程, 2008, 12(36): 108-110.
JIAO Zhang-ya, WANG Rui. A digital image watermarking algorithm based on spatiotemporal chaos and JPEG2000[J]. Computer and Digital Engineering, 2008, 12(36): 108-110.

[9] 吴涛, 毕笃彦. JPEG2000图像压缩算法研究[J]. 计算机应用与软件, 2007, 24(9): 155-157.
WU Tao, BI Du-yan. Study of wavelet-based JPEG 2000 image Compression Algorithm[J]. Computer Applications and Software, 2007, 24(9): 155-157.

[10] 彭军, 李学明, 张伟, 等. 基于偶合映像格子模型的时空混沌二值序列及其分析[J]. 计算机科学, 2005, 32(2): 196-199.
PENG Jun, LI Xue-ming, ZHANG Wei, et al. A spatiotemporal chaotic binary sequence based on coupled map lattices model and its performance analysis[J]. Computer Science, 2005, 32(2): 196-199.

[11] 杨恒伏, 孙光, 田祖伟. 一种基于双混沌映射的DCT域图像加密算法[J]. 科学技术与工程, 2008, 21(8): 5838-5840.
YANG Heng-fu, SUN Guang, TIAN Zu-wei. DCT domain image encryption scheme based on dual chaotic maps[J]. Science Technology and Engineering, 2008, 21(8): 5838-5840.

[12] 朱兴力, 张家树. 基于小波系数块能量分析的自适应数字水印算法[J]. 计算机应用, 2006, 26(4): 830-832.
ZHU Xing-li, ZHANG Jia-shu. Adaptive digital watermarking algorithm based on energy analysis of wavelet coefficients block[J]. Journal of Computer Applications, 2006, 26(4): 830-832.

[13] 欧珊瑚. 基于混沌特性和视觉模型的小波数字水印算法研究[J]. 中国图象图形学报, 2004, 9(3): 345-351.
OU Shan-hu. Research on wavelete digithal watermarking algorithm based on chaotic property and visual model[J]. Journal of Image and Graphics, 2004, 9(3): 345-351.

[14] 记震, 李慧慧, 肖薇薇, 等. 基于混沌序列的数字水印信号研究[J]. 电子学报, 2004, 32(7): 1132-1134.
JI Zhen, LI Hui-hui, XIAO Wei-wei, et al. The research of digital watermarking signal based on chaotic sequences[J]. Acta Electronical Sinca, 2004, 32(7): 1132-1134.

编 辑 黄 莘