

## 基于二维 Logistic 混沌映射 DWT 脆弱数字水印算法\*

陈善学, 彭娟, 李方伟

(重庆邮电大学 移动通信安全研究所, 重庆 400065)

**摘要:** 提出一种基于二维 Logistic 混沌映射的 DWT 变换域脆弱数字水印算法。首先利用原始图像的特征信息结合密钥生成二维混沌映射的初值从而生成水印信息; 为了实现盲检测, 该算法结合小波变换后的特征信息将水印信息嵌入到经小波变换后的高频部分; 最后将修改后的小波系数与其他系数重组做离散小波反变换 IDWT, 从而得到含水印的图像。实验证明, 该算法不但能增强水印的安全性, 还有良好的不可见性和图像定位篡改能力。

**关键词:** 脆弱数字水印; 二维 Logistic 混沌; 离散小波变换

中图分类号: TN391.41

文献标识码: A

文章编号: 1674-7720(2013)06-0038-03

## DWT-domain fragile watermarking algorithm based on 2D Logistic maps

Chen Shanxue, Peng Juan, Li Fangwei

(Mobile Communication Security Lab, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

**Abstract:** The paper proposed the fragile watermarking algorithm of the DWT (Discrete Wavelet Transform). Firstly, take advantage of the characteristics of original image information produces the initial value of the 2D Logistic maps, so as to produce watermark information with key. Then put the watermark information embedded into the coefficients in the diagonal detail coefficients of  $-level$  DWT. Experiment results that the algorithm is not only strengthen the security of the watermark, but also invisibility and tamper localization ability.

**Key words:** fragile digital watermarking; 2D Logistic maps; DWT

随着计算机网络和通信技术的飞速发展, 数字媒体(图像、视频、音频)得到了广泛的应用, 与此同时, 数字媒体的信息安全、知识产权保护和完整性认证等问题也变得日益突出。传统的加密系统在数据传输过程中可以起到保密的作用, 但数据一旦被解密, 保护作用也随之消失。数字水印<sup>[1-3]</sup>作为传统加密方法的有效补充手段已经在各种多媒体的保护领域得到应用。鲁棒性数字水印用于数字产品的版权保护, 脆弱数字水印常用于数字产品的完整性认证和内容篡改的定位。

目前脆弱数字水印技术主要有空间域和变换域两种方法。空间域方法是基于像素的脆弱水印技术和基于分块的脆弱水印技术, 是最早的基于 LSB 的方法。参考文献[4]对原始图像的特征与一个有意义的二值水印图像经过异或操作后嵌入到图像中最低有效位, 该算法具有定位特性, 可以非常直观地看出被篡改的区域, 但其嵌入的水印信息量较小。变换域方法更容易对图像被篡

改的特征进行描绘, 因此更多的脆弱水印算法采用在变换域中。参考文献[5]对原始图像 DCT 低频系数进行二进制编码后的数据嵌入到图像的最低有效位, 这种方法对原始图像进行恢复。参考文献[6]介绍了一种图像小波父系数和子系数之间的水印算法, 该算法通过计算图像中隐藏的水印信息和基于接收到的图像构造的水印信息之间的相似度来描述图像变化的强度。

因为混沌系统对初值的极度敏感性, 很多研究都把混沌系统引入到水印的生成。参考文献[7]提出了一种基于混沌的 DCT 域脆弱数字水印算法, 该算法将图像 DCT 次高频系数和水印密钥合成为 Logistic 混沌映射初值从而生成水印, 再将水印嵌入到图像 DCT 变换后的高频系数中得到水印图像, 它可以精确检测到对水印图像的一个像数点的改变, 并具有良好的定位篡改能力。参考文献[8]提出基于混沌映射的小波域脆弱数字水印算法, 该算法在生成水印信息和检测水印时映射到每个小波系数, 并运用混沌理论在提取水印时实现盲检测, 它具有良好的验证功能。

\* 基金项目: 国家自然科学基金项目(61071116, 61102062); 重庆市发改委专项(渝发改投[2010]1455, 渝发改投[2009]1537); 重庆市自然科学基金项目(CSTC, 2010BB2407, CSTCJJA40002)

参考文献[9]抽取边缘纹理特征作为水印信息,并利用混沌加密后对小波系数进行量化调制来嵌入水印。为了提高水印的安全性,本文将二维 Logistic 混沌映射引入到脆弱数字水印中,将图像的特征信息和密钥产生混沌映射的初值,进而产生水印信息,并结合小波变换的特征信息将水印嵌入到小波变换后的高频部分。实验证明,该算法不但增强了水印的安全性,而且还具有良好的不可见性和篡改定位能力,符合脆弱数字水印必须要实现盲检测。

## 1 二维 logistic 混沌映射和 DWT 变换

### 1.1 二维 logistic 混沌映射

混沌指在确定性系统中出现的一种类似随机的现象,不收敛但有界,并且对初值具有极敏感的依赖性,因此利用混沌现象可以构造非常好的信息加密系统。

Logistic 混沌映射是一种常见的混沌动力系统,二维 Logistic 混沌映射系统为:

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

其中,  $g_1$  和  $g_2$  是耦合项,可以取两种情况,即  $g_1 = \gamma y_n, g_2 = \gamma x_n$  一次偶合项和  $g_1 = g_2 = \gamma x_n y_n$  对称一次耦合项,本算法采用一次耦合项;  $x_0$  和  $y_0$  为系统初值,  $x_0, y_0 \in (0, 1)$ ;  $\mu, \lambda_1, \lambda_2, \gamma$  为混沌系统控制参数。

### 1.2 DWT 变换

离散小波变换(DWT)应用于图像就是对图像进行多分辨率分解,将图像分解成不同空间、不同频率的子图像。图像进行 1 级小波分解,可以分解为低频 LL<sub>1</sub>、水平高频 LH<sub>1</sub>、垂直高频 HL<sub>1</sub> 和低频 HH<sub>1</sub>(1 表示 1 级小波分解)4 个子带分量。LL<sub>1</sub> 可以进行第 2 级小波分解,分成 4 个子带分量。图 1 为 3 级小波分解示意图,每个子带分辨率由低到高依次为: LL<sub>3</sub>、LH<sub>3</sub>、HL<sub>3</sub>、HH<sub>3</sub>、LH<sub>2</sub>、HL<sub>2</sub>、HH<sub>2</sub>、LH<sub>1</sub>、HL<sub>1</sub>、HH<sub>1</sub>。图像进行  $n$  级 DWT 后可生成  $3n+1$  个子带分量。

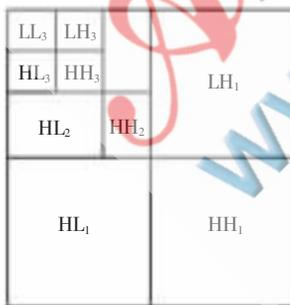


图 1 3 级小波分解示意图

分析图像小波变换可知,分辨率较小的小波系数有更重要的地位,小波分辨率最低时(LL<sub>N</sub>子带),集中了图像大部分能量,能够近似表示图像,是小波分解后最重要的部分;而小波分解后的高频部分含有图像边缘纹理信息,这部分对图像篡改敏感,为了提高脆弱数字水印对篡改的敏感性,将水印信息嵌入到高频子带中。

《微型机与应用》2013 年 第 32 卷 第 6 期

## 2 水印算法的实现

### 2.1 水印生成

在嵌入水印之前,为了确保水印信息的安全性,提出了用原始图像的特征信息结合二维 Logistic 混沌映射生成水印信息。用一幅  $N \times N$  原始图像  $I$  生成水印的步骤如下。

(1)将  $I$  做  $l(l=2,3)$  级 DWT,提取低频子带  $LL_l$  的系数,它的尺寸大小是  $N_0 \times N_0 (N_0 = N/2^l)$ ,然后将它分解成尺寸大小为  $4 \times 4$  的块,记作  $LL_l^{(m,n)}$ ,即:

$$LL_l^{(m,n)} = \begin{bmatrix} LL_l^{(1,1)}, LL_l^{(1,2)}, \dots, LL_l^{(1,M)} \\ LL_l^{(2,1)}, \dots, LL_l^{(2,M)} \\ \vdots \\ LL_l^{(m,1)}, \dots, LL_l^{(m,M)} \end{bmatrix} \quad (2)$$

其中,  $m, n \in \{1, 2, \dots, M\}, M = N_0/4$ 。

(2)计算  $LL_l^{(m,n)}$  绝对值的均值  $E^{(m,n)}$ ,并找出绝对值最大系数  $\text{Max}^{(m,n)}$  和绝对值最小系数  $\text{Min}^{(m,n)}$ ,计算  $a^{(m,n)}$  和  $b^{(m,n)}$ :

$$\begin{cases} a^{(m,n)} = \frac{E^{(m,n)}}{\text{abs}(\text{Max}^{(m,n)})} \\ b^{(m,n)} = \frac{\text{abs}(\text{Min}^{(m,n)})}{E^{(m,n)}} \end{cases} \quad (3)$$

由式(3)可知,  $a^{(m,n)}, b^{(m,n)} \in (0, 1)$ 。

(3)计算二维混沌映射的初值:

$$\begin{cases} x_0^{(m,n)} = a^{(m,n)} + \text{key}_1^{(m,n)} \\ y_0^{(m,n)} = b^{(m,n)} + \text{key}_2^{(m,n)} \end{cases} \quad (4)$$

其中,  $\text{key}_1, \text{key}_2$  是密钥,其取值范围为  $-a^{(m,n)} < \text{key}_1^{(m,n)} < 1 - a^{(m,n)}, -b^{(m,n)} < \text{key}_2^{(m,n)} < 1 - b^{(m,n)}$ 。

(4)将初值代入二维 Logistic 混沌映射产生长度为 16 的序列,然后将混沌序列量化成二值序列,并且把二值序列记作  $x_i^{(m,n)}, y_i^{(m,n)}, i \in \{1, 2, \dots, 16\}$ 。

(5)将  $x_i^{(m,n)}, y_i^{(m,n)}$  两个序列做异域操作,并将其结果转换成二维矩阵  $W^{(m,n)}$ ,并组合成水印信息  $W$ :

$$W = \begin{bmatrix} W^{(1,1)}, W^{(1,2)}, \dots, W^{(1,M)} \\ W^{(2,1)}, \dots, W^{(2,M)} \\ \vdots \\ W^{(M,1)}, \dots, W^{(M,M)} \end{bmatrix} \quad (5)$$

利用小波变换后低频子带中数据特征产生水印信息,在验证时不需要原始序列,降低了水印认证的风险。混沌映射对初值具有极端敏感性,可以实现内容篡改的准确检测,满足了脆弱水印对恶意篡改的脆弱性,采用二维混沌映射,有利于增强水印的安全性。

### 2.2 水印嵌入

图像经过  $l$  级 DWT 变换后的高频部分是图像感知中最不重要的分量,但它对图像的修改却是最为敏感的,因此将水印信息嵌入到原始图像的高频子带中,具体操作如下。

(1)计算  $\tau(i,j)$ :

$$\tau(i,j) = \text{abs}(\text{abs}(\text{HL}_l(i,j)) - \text{abs}(\text{LH}_l(i,j))) \quad (6)$$

(2)为了提高水印的不可见性,将  $\tau(i,j)$  量化:

欢迎网上投稿 www.pcachina.com 41

$$\begin{cases} \tau'(i,j)=\tau(i,j)*\alpha_1, 10 \leq \tau(i,j) \\ \tau'(i,j)=\tau(i,j)*\alpha_2, 5 \leq \tau(i,j) < 10 \\ \tau'(i,j)=\tau(i,j)*\alpha_3, \tau(i,j) < 5 \end{cases} \quad (7)$$

其中,  $\alpha_1, \alpha_2, \alpha_3 \in (0, 1)$ ,  $\alpha_1, \alpha_2, \alpha_3$  取值越小, 不可见性就越好, 但会影响水印的检测能力。实验证明,  $\alpha_1=0.05, \alpha_2=0.1, \alpha_3=0.15$  较好。

(3) 为了实现盲检测, 将水印信息嵌入到高频子带中:

$$HH_l'(i,j)=HH_l(i,j)+W(i,j)*(\tau'(i,j)-HH_l(i,j)) \quad (8)$$

当  $W(i,j)=1$  时,  $HH_l'(i,j)=\tau'(i,j)$ ; 当  $W(i,j)=0$  时,  $HH_l'(i,j)=HH_l(i,j)$ 。

(4) 将修改后的高频系数与其他系数组合后做离散小波反变换 IDWT, 即可得到含水印的图像  $I'$ 。

### 2.3 水印检测

为了使水印认证系统具有盲检测的能力, 设置了参考水印, 在水印提取前, 利用待测图像按照水印生成步骤生成参考水印  $W'$ 。因为水印是利用低频子带系数而产生的, 且水印是嵌入到高频子带中, 因而水印的嵌入不会影响参考水印的生成; 然后按照式(6)和式(7)计算  $\tau'(i,j)$ , 最后按照式(9)检测水印。

$$A(i,j)=\begin{cases} 1, & HH_l'(i,j)=\tau'(i,j) \\ 0, & HH_l'(i,j) \neq \tau'(i,j) \end{cases} \quad (9)$$

如果  $A(i,j)=W(i,j)$ , 则图像未被篡改; 如果  $A(i,j) \neq W(i,j)$ , 则图像被篡改。

## 3 实验结果

本实验采用 MATLAB 仿真来验证算法, 原始图像为  $512 \times 512$  的 Lena 和 Pepper, 为了使混沌系统工作稳定, 本实验中混沌系统的控制参数为:  $\mu=4.0, \gamma=0.1, \lambda_1=\lambda_2=0.89$ 。

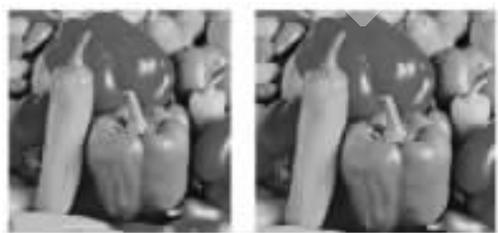
### 3.1 水印的不可见性

对 Lena 和 Pepper 图像加水印, 结果如图 2 和图 3 所示。从图中看出, 在视觉上原始图像与含水印图像没有



(a) 原始图像 (b) 含水印图像

图 2 Lena 加水印效果



(a) 原始图像 (b) 含水印图像

图 3 Pepper 中水印效果

差别。根据式(10)计算原始图像与含水印图像的峰值信噪比 PSNR (Peak Signal-to-Noise Ratio) 分别为 41.689 6 和 43.100 4, 由此可以得出该算法有很好的不可见性。

$$PSNR=10\log_{10} \frac{N \max[I^2]}{\sum_{i=1}^N \sum_{j=1}^N [I(i,j)-I'(i,j)]^2} \quad (10)$$

### 3.2 篡改定位能力

为了测试算法对图像篡改的敏感性和定位能力, 将 Lena 和 Pepper 剪切掉部分, 结果如图 4 和图 5 所示。实验证明该算法有良好的篡改定位能力。



(a) 篡改后的图像 (b) 篡改定位图像

图 4 Lena 剪切结果



(a) 篡改后的图像 (b) 篡改定位图像

图 5 Pepper 剪切结果

本文将二维 Logistic 混沌映射引入到脆弱数字水印中, 该算法首先将图像的特征信息结合密钥产生混沌映射的初值从而产生水印信息, 然后将水印信息嵌入到对篡改感知敏感的小波变换后的高频子带中, 最后根据小波变换后的系数特征实现水印盲检测。采用了二维混沌, 增强水印的安全性。实验证明, 该算法有良好的不可见性和图像篡改定位能力。

### 参考文献

- [1] 金聪. 数字水印理论与技术[M]. 北京: 清华大学出版社, 2008.
- [2] 龚岩琳. 基于混沌的数字图像加密与水印技术研究[D]. 重庆: 重庆邮电大学通信安全研究所, 2010.
- [3] 赵健, 周欣, 周明全. 非线性技术数字水印研究发展现状与展望[J]. 北京邮电大学学报, 2005, 10(25): 112-115.
- [4] WONG P W. A public key watermark for image verification and authentication[C]. Proceedings of the IEEE International Conference on Image Processing. Chicago, USA, 1998: 455-459.
- [5] FRIDRICH J, GOLJAN M. Image with self-correcting capabilities[C]. Proceedings of the IEEE International Conference on Image Processing, Kobe, Japan, 1999(3): 792-796.

《微型机与应用》2013年 第32卷 第6期

- [6] 邓承娟,杨百龙,林白露.基于图像的半脆弱数字水印技术研究[J].现代电子技术,2011,12,34(23):85-87.
- [7] 李赵红,候建军.基于 Logistic 混沌映射的 DCT 域脆弱数字水印算法[J].电子学报,2006(12):2134-2137.
- [8] 葛为卫,崔志明,吴健.基于混沌映射的小波域脆弱数字水印算法[J].计算机工程与设计,2008(8):2137-2139.
- [9] 赵娟,杨钊.一种用于图像内容认证的半脆弱数字水印[J].计算机技术与发展,2011,21(1):151-153.

(收稿日期:2013-01-02)

作者简介:

陈善学,男,1966年生,教授,研究生导师,主要研究方向:图像处理、数据压缩。

彭娟,女,1987年生,硕士研究生,主要研究方向:信息安全,数字水印。

李方伟,男,1960年生,博士,教授,主要研究方向:移动通信技术与理论、组网技术、信息安全技术、信号处理和智能天线技术。

