

# 基于混沌加密和离散小波变换的数字图像水印算法

郑建云

(湖南邮电职业技术学院,湖南长沙 410015)

**【摘要】**数字水印是保护数字产品版权的有效办法。首先阐述了一种传统的数字水印算法,该算法将数字水印小波分解后,嵌入到原始载体图像第三级小波子带,实现水印的嵌入;然后详细介绍了混沌加密以及离散小波变换的原理;最后,设计了一种结合混沌加密和水印嵌入的图像水印算法。仿真验证结果表明,该算法对于水印的嵌入和提取有较好的效果,能够从嵌入水印的原始图像中获得正确的图像内容,并且满足了不可见水印的要求。

**【关键词】**数字水印;离散小波变换;混沌加密;图像水印算法

**【doi:10.3969/j.issn.2095-7661.2019.03.008】**

**【中图分类号】**TP309.7

**【文献标识码】**A

**【文章编号】**2095-7661(2019)03-0029-03

## Digital image watermarking algorithm based on chaotic encryption and DWT

ZHENG Jian-yun

(Hunan Post and Telecommunication College, Changsha, Hunan, China 410015)

**Abstract:** Digital watermarking is an effective method to protect the copyright of digital products. This paper introduces a kind of traditional digital watermarking algorithm which divides the digital watermark wavelet and embeds it into the third level wavelet of the original carrier image to realize the embedding of watermark. This paper also introduces in detail the principle of the chaos encryption and discrete wavelet transform. Finally, an image watermarking algorithm is designed, which combines chaos encryption with watermark embedding. The simulation results show that this algorithm has better effect for the watermark embedding and extraction. The algorithm can obtain the correct image content from the original image watermark embedding and meet the requirements of the invisible watermark.

**Keywords:** digital watermarking; discrete wavelet transform; chaotic encryption; image watermarking algorithm

随着信息技术的迅猛发展,数字图像、视频等多媒体信息的流通越来越普及,版权保护成为重要的问题之一。数字水印主要是向数字作品(图像、声音、视频信号)中添加某些数字信息以求达到信息保密的作用,作为信息隐藏技术研究领域的重要分支,数字水印技术为版权保护提供了一种有效途径。目前,数字水印技术面临着较多尚待深入研究解决的问题<sup>[1-4]</sup>。

本文研究了离散小波变换和混沌加密技术,提出了一种新的基于小波变换的数字图像水印算法,采用混沌映射产生一个混沌序列来实现水印加密。

### 1 混沌加密

混沌是一种具有特殊性质的复杂动力学行为,混沌系统有些不符合概率统计学原理,如初始状态复杂

的动力学行为、高度的敏感性等方面,这样在混沌系统中让我们难以预测和重构。但在实际中解密者即使了解了产生混沌序列的方法,也较难确定混沌序列的初始值和混沌序列的系数参数。

文章通过混沌映射生成一个混沌序列,并将其转化为二值矩阵,该矩阵的大小与水印大小相同,同时与水印进行异或运算,对水印进行加密。在这个过程中,我们还可以对水印进行置乱运算以增强水印的安全性。其加密算法如下:

1)输入加密初始值。

2)利用混沌映射公式产生一个与水印相同大小的混沌序列。采用的混沌公式如下,其中 key 为初始密钥,  $m \times n$  为水印图像的大小。

**【收稿日期】**2019-06-11

**【作者简介】**郑建云(1980-),女,湖南湘阴人,湖南邮电职业技术学院讲师,硕士,研究方向:图像处理、智能控制。

$$L(1) = \text{key} \quad \text{key} \in (0,1)$$

$$L(i) = 1 - 2 \times L(i-1) \times L(i-1) \quad i = 2, 3, \dots, m \times n \quad (1)$$

3) 将产生的混沌序列转换成 0,1 序列。

$$\begin{cases} L'(i) = 1 & L(i) \geq 0 \\ L'(i) = 0 & L(i) < 0 \end{cases} \quad (2)$$

4) 将产生的 0,1 序列与水印进行异或。

解密是加密的逆过程<sup>[5-8]</sup>,解密过程中需要知道密钥、混沌公式以及加密后的水印图像。通过混沌公式和密钥得到混沌序列,将混沌序列转化为 0,1 序列,然后与经过加密的水印图像进行异或,就可以得到解密后的图像。如果使用的密钥错误,将不能得到解密后的水印图像。

## 2 图像的离散小波变换

离散小波变换 (Discrete Wavelet Transform, DWT) 是离散化连续小波基函数中的伸缩因子  $a$  和平移因子  $b$  离散<sup>[7]</sup>,即:

$$a = a_0^m (a_0 > 1), \quad b = nb_0 a_0^m, (b_0 \in R, (m, n) \in Z^2) \quad (3)$$

则有:

$$\varphi_{m,n}(t) = a_0^{m/2} \varphi(a_0^m t - nb_0) \quad (4)$$

通常情况下,取  $a_0 = 2, b_0 = 1$  得到:

$$\varphi_{m,n}(t) = 2^{m/2} \varphi(2^m t - nb) \quad (5)$$

对于任意函数  $\varphi(t) \in L^2(R)$  的离散小波变换为:

$$W_f(m, n) = \langle f, \varphi_{m,n} \rangle = \int_{-\infty}^{+\infty} f(t) \times \varphi_{m,n}(k) \quad (6)$$

如果  $f(t)$  也是离散的,记为  $f(k)$ ,则有

$$W_f(m, n) = \sum_k f(k) \times \varphi_{m,n}(k) \quad (7)$$

数字图像是二维信号,离散小波变换采用 Mallat 算法及二维分离的方式来实现,即通过对数字图像数据进行行和列的一维分离离散小波变换来实现<sup>[8]</sup>。从图像信号的小波变换多分辨率的特征来看,离散小波变换的原理是通过倍频程来分离出频谱信号,从而得到一个低频子带与几个高频子带的多分辨率信息。离散小波变换采用 Mallat 算法及二维分离的方式来实现,如图 1 所示,从变换的分解图可以看出,经过几次离散小波变换后的图像信号,产生多个子带。其中, L 为低通滤波器, H 为高通滤波器。

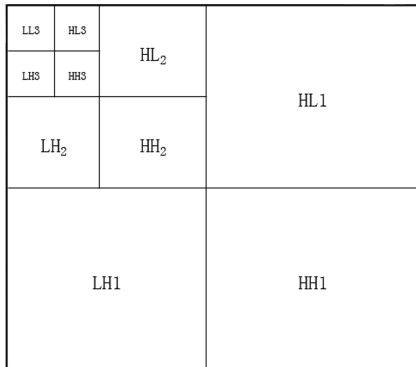


图 1 基于离散小波变换的分解图  
将图像进行三级小波变换后,LL3 频带为低频子

带,HHk、LHk、HLk(k=1,2,3)等频带为高频子带。HHk 频带是对角线子带,HHk 频带为图像中对角线上的高频信息的展现。HLk 频带是水平细节子带,其是在行方向上通过低通滤波在列方向上通过高通滤波得到的子带。因此该子带垂直方向上的信息融入到了水平方向上的细节信号中。LHk 频带是垂直细节子带,其原理同 HLk 频带一样,那么该子带水平方向上的信息融入到了垂直方向上的细节信号中。在第三层小波变换分解中,低频子带 LL3 含有原始图像的最低分辨率信息,HL3、LH3、HH3 为 LL3 的精细信息数据,并且 HL3、LH3、HH3 包含第二层分解的频带 HL2、LH2、HH2 的粗糙信息数据,第二层分解的频带 HL2、LH2、HH2 包含第一层分解的频带 HL1、LH1、HH1 的粗糙信息。根据小波分析多分辨率具有分解的特性情况,其图像的小波分析多分辨率中方向的选择性较好,人类视觉系统能与其较好结合在一起。

## 3 利用小波变换的水印算法

水印算法运用特别广泛,该技术具有较好的不可知性和鲁棒性,基于该性能,本文采用水印算法。下面着重介绍该算法的嵌入与提取流程,如图 2 所示。

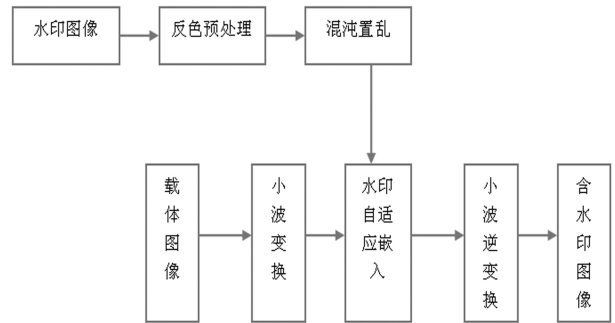


图 2 水印算法的嵌入和提取流程图

### 3.1 水印的嵌入算法

水印的主要嵌入步骤如下:

- 1) 首先利用混沌加密方法得到水印图像 D。
- 2) 将通过混沌加密后的水印图像 D 扩充得到原始图像大小 D1。
- 3) 对 QR 码图像 I(MxM) 进行 3-DWT 变换,得到小波三层系数 LL1, LL2, LL3, 将 LL3 作为水印嵌入。
- 4) 根据水印嵌入公式,将水印分别嵌入到三层 DWT 的逼近子带 LL3 中,其中, key 为嵌入强度,取值为 10。wm、wn 为水印图像的大小。
$$LL3w(i, j) = LL3(i, j) + key \times w(\text{mod}(i-1, wm)+1, \text{mod}(j-1, wn)+1) \quad (8)$$
- 5) 逆小波变换得到后就可以得到嵌入水印后的图像。

### 3.2 水印的提取算法

水印的提取算法具体步骤如下:

- 1) 将原始图像和待提取图像通过 3-DWT 分解,得到 wLL1, wLL2, wLL3 和 LL1, LL2, LL3。

2)利用公式  $w_e(i, j) = w_{LL3} - LL3$  得到水印信息  $w_e(i, j)$ 。

3)利用水印嵌入公式的逆运算公式得到混沌加密后的水印信息。

$$ow((\text{mod}((i-1), wm)+1), (\text{mod}((j-1), wn)+1)) = ow((\text{mod}((i-1), wm)+1), (\text{mod}((j-1), wn)+1)) + w_e(i, j) \quad (9)$$

4)将得到混沌加密后的水印信息进行解密,即可以得到解密后的水印信息。

#### 4 仿真实验

实验中原始图像为  $512 \times 512$  像素的图像,水印图像为  $64 \times 64$  像素的二值图像,工具软件为 Matlab7.8,如图3所示。运行程序,选取原始图像和水印图像,得到如图4所示的仿真结果。该结果满足了水印信息的不可见性,并且可以正确提取。



图3 原始图像和水印图像图



图4 嵌入水印后的图像和提取出来的水印图像图

#### 5 结语

本文研究了离散小波变换和混沌加密技术,提出了一种新的基于小波变换的数字图像水印算法,该算法加密是采用混沌异或算法,在这个过程中,我们还对水印进行置乱运算并对其原始图像进行三次小波分解以增强水印的安全性。实验结果表明,该算法对于水印的嵌入和提取产生较好的效果,可以从嵌入水印的原始图像中获取正确的图像信息,还能够满足不可见水印的要求。

#### 【参考文献】

- [1]李豪.基于DWT和混沌原理的图像数字水印算法研究[D].杭州:浙江大学,2014.
- [2]薛胜男,陈秀宏.基于混沌加密和SVD的数字图像水印算法[J].计算机工程,2012(19):107-110.
- [3]Zhang K B, Tao D C, Gao X B, et al. Learning multiple linear mappings for efficient single image super-resolution[J]. IEEE Transactions on Image Processing, 2015(3):846-861.
- [4]陈雪松,申美玲.基于Lorenz混沌加密的DWT音频水印算法[J].科学技术与工程,2011(7):1590-1595.
- [5]张新,张帆,李雪梅,汤煜春,张彩明.特征约束的多实例图像超分辨率方法[J].计算机辅助设计与图形学学报,2016(4):579-588.
- [6]谢荣生,赵欢喜,陈玉明.基于QR码的防伪电子票数字水印方法[J].厦门大学学报,2013(3):338-342.
- [7]蔡卫红,孔凡凤,何亮.TD-LTE移动系统下行容量影响因素研究[J].湖南邮电职业技术学院学报,2017(2):1-3.
- [8]LIU Jian-ming, LI Xiao-jun, Chaos watermarking algorithm based on fuzzy wavelet domain[J]. Computer Engineering, 2011(8):132-134.

(上接第19页)

环形组网下W网  $E_c/I_0$  指标和LTE网 SINR 指标良好,改造不会抬升底噪和产生干扰。无论何种方式中断尾纤,均不产生小区退服告警。单边链路中断,只产生光模块收发异常告警,提示光口出现异常。

#### 3 总结

环形组网通过实验验证可以提升网络的安全性,对单点中断业务有较好的保护能力。中断主用链路的CPRI光纤时,小区业务短暂中断后自行恢复(W网语音业务在30秒以内,LTE数据业务在5秒以内);中断备用链路的CPRI光纤时,业务未受影响。无论哪个单边CPRI光纤中断,均无RRU中断。可避免重要小区产生退服告警,对降低投诉率和提升客户NPS有积极作用。尤其在重要小区,如高铁、工业园区等站点,能给予运维人员充足的修复时间。因此,该组网方式有良好的应用和推广价值。

#### 【参考文献】

- [1]张子萃.基于RoF的前传技术在全频谱无线接入网中的应用研究[D].北京:北京邮电大学,2018.
- [2]李崇鞅,胡国安.无线城市建设策略与组网研究[J].湖南邮电职业技术学院学报,2014(3):25-27.
- [3]张敏.利用BBU+RRU技术实现对别墅小区的无线覆盖[J].湖南师范大学自然科学学报,2010(3):42-45,72.
- [4]王永贵,张国俊,崔晓俊.RRU关键技术及创新[J].中兴通讯技术,2018(3):48-53.
- [5]黄耿,郭鸿.BBU+RRU分布式基站组网模型探讨[J].通信技术,2010(11):129-133.
- [6]赵捷,徐梅香.BBU集中部署下RRU组网方案的应用研究[J].电信快报,2018(6):10-14.
- [7]斯强.RRU设备故障导致VoLTE接通率低的案例研究[J].通讯世界,2018(2):42-43.
- [8]何宏智,刘占军,李云鹏,陈前斌.一种C-RAN架构无线网络中的干扰抑制方法[J].重庆邮电大学学报(自然科学版),2015(4):493-498.