

一种基于小波变换和神经网络的数字水印算法

陈 军¹ 张 伟² 杨华千³ 何春筱⁴

(重庆教育学院教务处 重庆 400067)¹ (重庆教育学院院长办公室 重庆 400067)²

(重庆教育学院网络中心 重庆 400067)³ (重庆教育管理学校计算机教研室 重庆 400066)⁴

摘 要 提出了一种新的基于小波变换和神经网络的数字水印算法。该算法首先把原始图像分成 8×8 像素的小块, 根据 Logistic 映射产生的混沌序列选择相应的小块构造一个原始图像的子图, 接着把 DWT 变换作用在这个子图上, 得到两个子带 LH_1 和 HL_1 , 然后把水印信息嵌入在这两个子带上, 接着通过 IDWT 变换重构子图, 最后按构成子图的顺序把每一个 8×8 像素的小块放回到原图中相应位置, 从而得到一个嵌入了水印信息的图像。在水印的提取过程中使用了经典的 BP 神经网络。实验结果表明, 通过该算法嵌入的水印具有较好的鲁棒性、安全性和不可感知性。

关键词 数字水印, 神经网络, 小波变换, 混沌

Novel Digital Watermark Scheme Based on Wavelet Transform and Neural Network

CHEN Jun¹ ZHANG Wei² YANG Hua-qiang³ HE Chun-xiao⁴

(Studies Affairs Office, Chongqing Education College, Chongqing 400067, China)¹

(Dean's Office, Chongqing Education College, Chongqing 400067, China)²

(Network Center, Chongqing Education College, Chongqing 400067, China)³

(Teaching and Research Section of Computer, Chongqing Education Management School, Chongqing 400066, China)⁴

Abstract A novel digital watermark algorithm based on wavelet transform and neural network was proposed. Firstly, the original image was divided into some small blocks (8×8 pixels). The sub-image consists of some small blocks that are selected through logistic map. Two sub-bands LH_1 and HL_1 were generated by acting DWT on the sub-image. Secondly, the watermark was embedded into the sub-band's wavelet coefficients. The watermarked sub-image was reconstructed using IDWT. Finally, we put every small block (8×8 pixels) of the watermarked sub-image into the initial position of the original image. Thus, we got the watermarked image. Experiments show that the watermark embedded by this scheme has good robustness, imperceptibility and security.

Keywords Watermark, Neural network, Wavelet transform, Chaos

1 引言

随着信息的数字化及互联网的蓬勃发展, 如何在网络环境中实施有效的版权保护和信息安全手段, 成为一个迫在眉睫的现实问题。数字水印作为一种解决数字产品版权问题的有效手段^[1,2], 已经得到了人们的广泛关注, 并逐渐成为一个研究热点。近年来已经提出了一些基于神经网络的数字水印算法。文献[3,4]分别提出了两种不同的使用神经网络的方法来改善由 Kutter 等人提出的空域数字水印算法的鲁棒性。文献[5]提出了一种基于神经网络的易碎数字水印算法。本文在分析混沌系统和离散小波变换特性的基础上, 提出了一种新颖的数字水印算法, 把神经网络用于水印的检测过程, 较好地改善了水印算法的鲁棒性。

得到了 4 个子带——低频子带(LL_1 , 在图 2 中又把它进行了第二级分解)、高频子带(HH_1)、低-高频子带(LH_1)、高-低频子带(HL_1)。由于子带 LL_1 包含了图像的大部分重要信息, 根据人类视觉系统特性, 如果把水印嵌入在这个子带上, 水印的不可感知性较差^[6], 很可能降低图像的视觉质量。同样, 如果把水印嵌入在子带 HH_1 上, 嵌入水印的图像在进行低通滤波和有损压缩时, 水印的鲁棒性较差^[7,8]。所以, 本文的算法将把水印嵌入在 LH_1 和 HL_1 两个子带上。

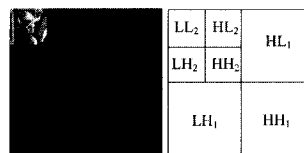


图 1 Lena 图的二级 DTW 分解

2 水印的嵌入

2.1 多级 DWT 变换

图 1 是对 Lena 图的二级 DWT 变换。第一级分解分别

2.2 水印序列的生成

本文使用一个二值水印序列 S , 由 P 和 W 两部分组成:

到稿日期: 2010-07-01 返修日期: 2010-11-05 本文受重庆市自然科学基金项目(CSTC, 2009BB2378)资助。

陈 军(1971-), 男, 硕士, 副教授, 主要研究方向为信息安全, E-mail: cj_cq@163.com; 张 伟(1970-), 男, 博士, 教授, 主要研究方向为信息安全、计算智能与数据挖掘; 杨华千(1972-), 男, 博士, 副教授, 主要研究方向为信息安全; 何春筱(1972-), 女, 高级讲师, 主要研究方向为信息安全与应用。

$$S=P+W=p_1+p_2,\dots,p_k,w_1,w_2,\dots,w_l=s_1,s_2,\dots,s_m \quad (1)$$

式中, $P=p_1,p_2,\dots,p_k$ 是一个长度为 k 的固定模式序列; $W=w_1,w_2,\dots,w_l$ 是图片版权所有者期望嵌入的信息; $m=k+l$ 。模式序列 P 用于训练神经网络。

2.3 水印的嵌入过程

由于即使对图像的局部区域进行攻击都会对图像的小波系数产生很大的影响^[9], 所以为了降低这种局部攻击所产生的影响, 本文的数字水印嵌入算法把小波变换作用在原始图像的局部区域上。算法的实现框图如图 2 所示。

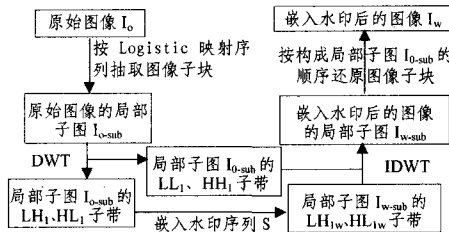


图 2 水印的嵌入框图

水印嵌入过程如下(为了叙述方便, 设原始图像的大小为 256×256 像素):

1) 构造原始图像 I_0 的局部子图 I_{0-sub} 。图 3 可视化了子图的构成过程。

其方法如下: 用 Logistic 映射产生一个包含 1024 个不同元素的混沌序列, 并对这 1024 个不同元素按其值在序列中的大小进行编号; 然后按行序把原始图像分成 8×8 像素、互不重叠的小块并按顺序编号, 共有 1024 个小块; 根据前面产生的混沌序列的前 256 个编号, 选出对应的小块构成 16×16 小块的子图 I_{0-sub} 。

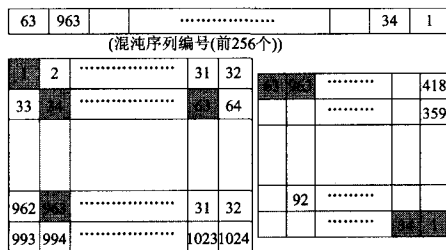


图 3 原始图像局部子图的构造过程

2) 对子图 I_{0-sub} 进行 DWT 变换, 得到用于嵌入水印的两个子带 LH_1 和 HL_1 。

3) 把水印 W 嵌入在两个子带 LH_1 和 HL_1 上, 得到嵌入水印后的子带 LH_{1w} 和 HL_{1w} 。

水印的嵌入规则如下:

$$\begin{cases} X_{LH_{1w}}(i) = X_{LH_1}(i) [1 + \alpha(2s_i - 1)] \\ X_{HL_{1w}}(i) = X_{HL_1}(i) [1 + \alpha(2s_i - 1)] \end{cases} \quad (2)$$

式中, $X_{LH_1}(i)$, $X_{HL_1}(i)$ 和 $X_{LH_{1w}}(i)$, $X_{HL_{1w}}(i)$ 分别是水印嵌入前后的小波变换系数, s_i 是水印信息, α 是水印嵌入强度因子, 用来调节水印嵌入强度, $i=1, 2, \dots, m$ 。

4) 进行 IDWT 变换, 得到嵌入水印后的子图 I_{w-sub} 。

5) 把子图 I_{w-sub} 按行序分成 8×8 像素、互不重叠的小块, 按构成子图 I_{w-sub} 的顺序把小块放回到原始图像原来的位置。这样就得到了已嵌入水印的图像 I_w 。

3 水印的提取

3.1 水印的提取过程

为了利用神经网络来检查给定的图像 (I') 中是否存在指定的水印信息, 本文的水印提取算法如下:

1) 构造给定图像 I' 的局部子图 I'_{sub} , 其构造过程中采用的混沌序列与水印嵌入过程中采用的序列相同。

2) 对子图 I'_{sub} 进行 DWT 变换, 得到两个子带 LH_1' 和 HL_1' 的小波系数 $D'_{LH_1} = \{u'_i, i=1, 2, \dots, m\}$ 和 $D'_{HL_1} = \{v'_i, i=1, 2, \dots, m\}$, $m=k+l$, 见 2.2 节。

3) 计算神经网络的样本集合 $C_i = \{d'_i, i=1, 2, \dots, m\}$, 其中的元素 d'_i 由式(3)计算得到:

$$\frac{\overline{d'_i} - \bar{d}}{\bar{d}} \quad (3)$$

$$\text{式中, } \bar{d} = \frac{\sum_{i=1}^m (u'_i + v'_i)}{2m}, \overline{d'_i} = \frac{u'_i + v'_i}{2}.$$

4) 检测水印信息。本文使用传统的 BP 神经网络, 并把集合 C_i 的前 k 个元素作为网络的训练集合。集合 C_i 的后 l 个元素作为神经网络的有效输入, 每一个被检测到的水印信息由神经网络的输出结果 $\hat{\beta}_j$ 确定, 定义如下:

$$\hat{w}_j = \begin{cases} 1, & \hat{\beta}_{k+j} \geq 0 \\ 0, & \hat{\beta}_{k+j} < 0 \end{cases} \quad j=1, 2, \dots, l \quad (4)$$

由此, 得出检测到的水印序列 $\hat{W} = \{\hat{w}_j, j=1, 2, \dots, l\}$ 。

3.2 水印的验证方法

为判定水印信息存在与否, 本文采用检测到的水印与原始水印的相关性作为衡量标准。相关系数 NC 定义如下:

$$NC = (\sum_{i=1}^l w_i \cdot \hat{w}_i) / \sqrt{\sum_{i=1}^l w_i^2 \cdot \sum_{i=1}^l \hat{w}_i^2} \quad (5)$$

根据事先制定的阈值 T_w , 来判断提取的水印是否为原始水印 W 。阈值 T_w 可以通过实验得到。

4 实验及其结果分析

在实验过程中, 采用 MATLAB 提供的 db4 进行 DWT 变换, 以得到各子带的小波系数。模式序列是 0101...01, 其长度 $k=200$, 有效水印信息序列长度 $l=1000$, 水印嵌入强度 $\alpha=0.1$ 。水印检测采用 BP 神经网络, 其结构是 9-5-1, 即输入层 9 个节点, 隐含层 5 个节点, 输出层 1 个节点, 学习参数 $lp=0.15$ 。实验结果如图 4 所示。从视觉效果上观察, 嵌入水印前后两图没有什么差别, 这说明本文算法嵌入水印具有良好的不可见性。

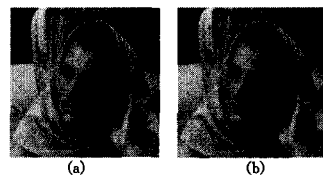


图 4 (a) 原始图像; (b) 嵌入水印后的图像

从式(2)可以看出, 嵌入水印后的局部子图, 其小波系数与强度因子 α 是线性相关的, 所以强度因子 α 直接影响了嵌入水印后图像的视觉质量。工程上通常使用 PSNR 来量化嵌入水印后图像的质量^[10]。为了评价本文提出的算法的一般

性能,实验针对不同的 α ,得到PSNR的值如表1所列。

表1 强度因子 α 与PSNR的关系

α	0.05	0.10	0.15	0.25	0.35
PSNR	42.85	41.34	39.80	38.91	38.00

实验结果表明,PSNR的值随着强度因子 α 的增大而减小。实验还发现,当 $\alpha \leq 0.05$ 时,很难检测到水印的存在;当 $\alpha \geq 0.35$ 时,图像嵌入水印后视觉质量较差。因此,在实际使用中应该选择一个较合理的水印强度因子,以便嵌入水印后获得较好的图像保真度。

从理论上讲,只要具有足够的知识,任何水印都可以去掉^[10]。但是如果只能得到部分信息,如水印在图像中的精确位置未知,那么破坏水印将导致图像质量的严重下降。

表2是针对不同的一些标准测试图像(512×512)进行的水印嵌入鲁棒性实验(α 表示水印嵌入强度因子)。实验结果证明了本文算法的有效性。

表2 一些标准灰度图的水印鲁棒性实验结果($\alpha=0.15$)

图像	Boat	Lena	Barbara	Mandrill	Facets
PSNR	38.70	39.80	39.08	38.99	39.47

表3是对嵌入水印的Lena图进行JPEG压缩后提取出的水印与原始水印的相关系数计算结果。可以看出,算法能经受一定的有损压缩攻击,同时随着压缩比的增加,水印的相关系数急剧减小(α 表示水印嵌入强度因子)。

表3 JPEG压缩后提取的水印与原始水印的相关系数($\alpha=0.15$)

质量因子	90	85	80	75	70	60
相关系数(r)	0.976	0.947	0.932	0.913	0.850	0.737

表4是对嵌入水印的Lena图加入各种噪声后提取出的水印与原始水印的相关系数计算结果(α 表示水印嵌入强度因子, n 表示叠加的噪声)。

表4 加入噪声后提取的水印与原始水印的相关系数($\alpha=0.15$,
 $n=0.05$)

噪声	Gaussian	Salt & pepper	Poisson	Speckle	Localvar
相关系数(r)	0.936	0.810	0.902	0.832	0.921

表5是对嵌入水印的Lena图进行各种剪切后(空出部分插入0值)提取出的水印与原始水印的相关系数计算结果(α 表示水印嵌入强度因子)。

表5 图像剪切15%后提取的水印与原始水印的相关系数
($\alpha=0.15$)

剪切方向	左	右	上	下
相关系数(r)	0.874	0.880	0.873	0.876

从上述实验结果可以看出,本文算法在对抗几种常见的水印攻击方式上都具有较好的鲁棒性和不可感知性。这主要有以下几个原因:首先,局部子图是通过混沌映射得到的,混沌映射产生的序列对初值非常敏感^[11],且初始条件任意小的改变,都会产生几乎完全不同的混沌序列^[12]。同时,Logistic映射轨迹在区间 $[0,1]$ 内是稠密的^[13]。其次,水印被嵌入在变换域上(DWT),这种变换是作用在原始图像的局部子图上。最后,水印被嵌入在DWT变换后的两个子带 LH_1 和 HL_1 ,使得嵌入的水印既具有比较随机的分布特性,又具有良

好的不可感知性与鲁棒性^[14]。

本文提出的水印嵌入算法存在4个参数:一个是混沌初始值 r ,它影响局部子图的构成,从而影响水印嵌入的位置;一个是模式序列的长度 k ,它影响神经网络的学习效果;一个是有效水印序列的长度 l ,它影响水印检测的响应情况;一个是水印嵌入的强度因子 α ,它影响嵌入水印后图像的视觉效果,其值不能太大也不能太小。

结束语 提出了一种新颖的基于小波变换和神经网络的数字水印算法。实验结果表明,算法具有较好的水印鲁棒性、安全性和不可感知性。从第2节的水印嵌入过程中,也发现整个嵌入过程中使用了一个全局的强度因子 α ,而没有考虑不同的小波系数应该嵌入不同强度的水印信息,使用不同的强度因子,这是以后需要进一步研究的问题。

参考文献

- [1] Petitcolas F A P, Anderson R J, Kuhn M G. Information Hiding-A Survey[J]. Proc. IEEE, 1999, 87: 1062-1078
- [2] Wu X Y, Guan Z H. A novel digital watermark algorithm based on chaotic maps[J]. Phys. Lett. A, 2007, 365: 403-406
- [3] Yu P T, Tsai H H, Lin J S. Digital Watermarking Based on Neural Networks for Color Images[J]. Signal Processing, 2001, 81: 663-671
- [4] Lu W, Lu H, Shen R. Color Image Watermarking Based on Neural Networks[J]. Advances in Neural Networks, 3174 of LNCS, 2004: 651-656
- [5] Zhang X P, Wang S Z. Statistical Fragile Watermarking Capable of Locating Individual Tampered Pixels[J]. Sign. Proc. Lett., IEEE, 2007, 14: 727-730
- [6] Mukherjee D P, Maitra S, Acton S T. Spatial domain digital watermarking of multimedia objects for buyer authentication[J]. Multimedia, IEEE Trans., 2004, 6: 1-15
- [7] Chu W C. DCT-based Image Watermarking Using Subsampling[J]. Multimedia, IEEE Trans., 2003, 5: 34-38
- [8] Liu S H, Yao H X, Gao W, et al. An image fragile watermark scheme based on chaotic image pattern and pixel-pairs[J]. Applied Mathematics and Computation, 2007, 185: 869-882
- [9] Potdar V M, Han S, Chang E. A survey of digital image watermarking techniques, Industrial Informatics[C]//3rd IEEE Inte. Conf(INDIN'05), 2005: 709-716
- [10] Zhao D W, Chen G R, Liu W B. A chaos-based robust wavelet-domain watermarking algorithm[J]. Chaos, Solitons and Fractals, 2004, 22: 47-54
- [11] Kuroda K, Nishigaki M, et al. A Digital Watermark Using Public-key Cryptography for Open Algorithm[C]//ICITA. 2002
- [12] 魏伟一. 基于小波对比度的自适应图像水印算法[J]. 计算机工程与应用, 2010, 46(26): 89-90, 141
- [13] Chang C Y, Su S J. A neural-network-based robust watermarking scheme[C]// Systems, Man and Cybernetics, 2005 IEEE Inte. Conf. 2005, 3: 2482-2487
- [14] Lee S, Yoo C D, Kalker T. Reversible Image Watermarking Based on Integer-to-Integer Wavelet Transform [J]. IEEE Transactions on Information Forensics and Security, 2007, 2: 321-330