文章编号:1000-5862(2013)01-0042-04

一种基于边缘检测和正负量化的盲水印算法

赵晓花,张贵仓*
(西北师范大学计算机科学与工程学院,甘肃 兰州 730070)

摘要:提出了一种基于 DCT 域边缘检测和正负量化的盲水印算法:先用 Arnold 置乱方法对水印图像进行加密,并对其进行正负变换,然后用边缘检测算子对载体图像进行边缘提取,再根据阈值的设定选择不同的量化值将水印嵌入,提取水印时不需要原始图像的参与,实现了盲提取. 实验结果表明:该算法对于裁剪、压缩、噪声、滤波、缩放等攻击都具有较好的鲁棒性和不可见性.

关键词:水印;离散余弦变换;正负量化;鲁棒性
中图分类号:TP 309 **文献标志码**:A

0 引言

为了解决随着计算机技术的发展而引发的版权保护问题,各种数字水印技术相继被提出. 数字水印技术[1] 是一种信息隐藏技术,即在数字产品中嵌入一些秘密信息来保护产品的版权和可靠性. 它的嵌入算法主要有 2 种:空域算法和变换域算法. 用空域算法嵌入水印时,对外来攻击的抗攻击能力比较差,而变换域则可以将水印信息分散开来,保证了水印的不可见性,所以算法采用变换域算法中的离散余弦变换[2-6] 来嵌入水印. 粟伟峰等[7] 和贾伟等[8] 分别提出了基于边缘检测的图像水印算法,它们都是将水印按照载体图像的不同边缘设定不同的嵌入强度嵌入到载体图像的低频系数中,这样受到某些攻击后水印的鲁棒性较高,但是对于有些攻击水印的鲁棒性却较低. 何选森等[9] 和李昊等[10] 提出奇偶和正负量化 DCT 系数实现信息隐藏,保证了受到攻击后嵌入信息的载体不受很大的影响,但是水印的鲁棒性却稍微弱一些. 因此本文提出了一种将边缘和正负量化结合的水印算法.

1 算法用到的技术

1.1 Arnold 置乱

对水印图像进行置乱[11] 可以加密,文中根据 Arnold 置乱的定义,对于一幅 $N \times N$ 图像,变换过程可表示为

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\mathrm{mod}\ N) \qquad (1)$$

其中 x,y 为变换前图像的像素位置,x',y' 是变换后图像像素位置,N 是图像阶数,mod 是模运算.

Arnold 置乱有 2 个优点:(ⅰ)它将图像的像素位置次序打乱重新排列,从得到的这个新图像的色彩和纹理中根本就不能辨别出任何跟原图像有关的信息.(ⅱ)它把置乱度作为密钥进行加密,不同的置乱度会产生不同的置乱图像,所以如果不知道密钥也就不能提取出原本的水印图像,即使知道了密钥,但如果不知道该水印图像是使用什么方法置乱的,也是无法提取出原始的水印图像的,这样就在一定程度上增加了水印图像的安全性.

1.2 离散余弦变换

离散余弦变换是数字信号处理技术中常用的线性变换之一,它具有较好的能量压缩能力和去相关能力,而且在 2 维离散余弦变换的基础上还建立了数字图像的 JPEG 压缩标准,它的定义为

$$C(u,v) = a(u)\,a(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cdot \cos\left[\frac{(2x+1)u\pi}{2N}\right] \cos\left[\frac{(2y+1)v\pi}{2N}\right], \qquad (2)$$

其中 $u,v = 0,1,\cdots,N-1$. $C(u,v)$ 为图像变换后的 DCT 系数,$a(u)$ 和 $a(v)$ 的值是相同的,式子如下:

收稿日期:2012-10-16
基金项目:甘肃省自然科学基金(0803RJZA109)和甘肃省科技攻关课题(2GS035-A052-011)资助项目.
作者简介:张贵仓(1964-),男,甘肃天水人,教授,博士,主要从事计算机辅助几何设计、图形学、数字水印等方面的研究.

$$a(u) = \begin{cases} \sqrt{1/N}, u = 0, \\ \sqrt{2/N}, u = 1,2,\cdots,N-1. \end{cases}$$

相应的逆变换定义为

$$f(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} a(u)\,a(v)\,C(u,v) \cdot \cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2x+1)v\pi}{2N}\right], \quad (3)$$

其中 $x,y = 0,1,\cdots,N-1$.

2　水印的嵌入和提取

2.1　水印的嵌入算法

(ⅰ) 根据水印图像 S 的大小 N 设定置乱周期，用公式(1) 对其进行置乱，得到置乱后的图像 S'，再将经过置乱后的水印图像 S' 转换成 1 维数组 $\{x_i; i = 1,2,\cdots,N\times N\}$，然后将数组的值根据一定的规则转换成正负序列.

(ⅱ) 用 prewitt 算子提取原始载体图像的边缘图 L，然后将载体图像 I 进行 8×8，记为 $I_n = f_n(x,y)$，$n = 0,1,2,\cdots,M-1$.

(ⅲ) 对边缘图像 L 进行 8×8 分块，得到的边界值 T 跟设定的阈值 T_1 比较，如果 $T > T_1$，也就是说是边缘值时设定量化值为 a_1; 反之，当 $T < T_1$ 时设定量化值为 a_2.

(ⅳ) 将分块后的载体图像进行 DCT 变换，并对载体图像的中频系数(12,13) 根据步骤(ⅲ) 中选择的量化值进行更改，公式为

$$\begin{cases} dct\_I_n(i,j) = a_1 \times message(k), T > T_1, \\ dct\_I_n(i,j) = a_2 \times message(k), T < T_1, \end{cases}$$

其中 T_1 为设定的阈值，T 为边缘值.

(Ⅴ) 最后对嵌入水印后图像的各个子块再进行 DCT 的逆变换:

$$f'(x,y) = \cup\, DCT^{-1}(dct\_I_n(x,y)), 0 \leqslant x,y \leqslant 7,$$

由此得到含水印的图像.

2.2　水印提取算法

水印提取算法是嵌入算法的逆过程，步骤为

(ⅰ) 把嵌入水印后的载体图像 I' 分成 8×8 互不覆盖的子块，对它的各个子块进行 DCT 变换后，得到 $dct\_I'_n$.

(ⅱ) 根据选定的中频系数值的正负来提取水印，如果是正数，则提取出的信息为 1，否则为 0.

(ⅲ) 将步骤(ⅰ) 中得到的信息从中提取出嵌入的置乱水印信息，将其转换成 2 维数组，然后根据 Arnold 置乱周期进行反置乱，得到最终的水印提取图像.

3　实验结果及分析

算法采用的原始载体图像是 256×256 大小的，二值水印图像为 32×32 大小的，采用的量化值 $a_1 = 87$，$a_2 = 78$. 通过计算原始载体图像 I 和受到以下各种攻击后的含水印的载体图像 I' 的峰值信噪比(PSNR) 以及原始水印图像和提取出的水印图像的相关系数 $sim(NC)$ 来验证算法性能的好坏. 算法中根据不同的边缘值采用不同的量化值，使提取出的水印相似度更高一些.

相关系数(sim) 比较的计算公式为

$$sim(d,d') = \frac{\sum_{i=1}^{N-1}\sum_{j=1}^{M-1} d(i,j)\,d'(i,j)}{\sqrt{\sum_{i=1}^{N-1}\sum_{j=1}^{M-1} d^2(i,j)}\sqrt{\sum_{i=1}^{N-1}\sum_{j=1}^{M-1} d^2(i,j)}}, \quad (4)$$

其中 d 和 d' 在算法中分别是原始载体图像和嵌入水印后的图像.

峰值信噪比($PSNR$) 的计算公式为

$$PSNR = 10\times \lg\left(\frac{255^2}{MSE}\right), \quad (5)$$

$$MSE = \frac{1}{M\times N}\sum_{i=1}^{N}\sum_{j=1}^{M}[f(i,j) - f'(i,j)]^2, \quad (6)$$

其中 M,N 为图像的长和宽.

图 1 为原始载体图像和原始水印图像.

(a) 原始载体图像

(b) 水印图像

图 1　原始载体图像和水印图像

以下各图分别是文中改进算法中含水印的载体图像经过不同的 JPEG 压缩、滤波、裁剪、高斯噪声、缩放等攻击后的含水印的载体图像和从中提取出的水印图像，实验结果如图 2 ~ 图 6 所示.

从实验结果图中可以看出文中的算法在经过各种攻击后，水印图像依然能很清晰的被提取出来，尤其是 JPEG 压缩，在压缩比为 10,50,90 的情况下，提取出的 NC 值都为 1，而在其他的攻击下，水印的 NC 值也很高，表 1 的对比也可以得知与文献[10] 相比，本文算法的水印不可见性更好.

(a)压缩10 (b)提取的水印(NC=1) (c)压缩50 (d)提取的水印(NC=1)

图2 JPEG 压缩攻击实验结果

(a)中值滤波 (b)提取的水印(NC=0.993 2) (c)均值滤波 (d)提取的水印(NC=0.996 6)

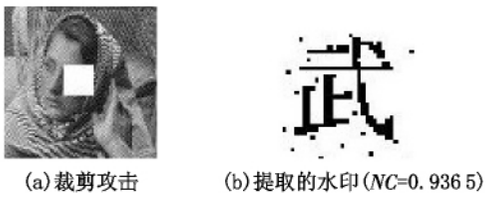
图3 滤波攻击实验结果

(a)高斯噪声(0.002) (b)提取的水印(NC=1) (c)椒盐噪声(0.01) (d)提取的水印(NC=0.993 3)

图4 噪声攻击实验结果

(a)缩小1/4 (b)提取的水印(NC=1) (c)放大2倍 (d)提取的水印(NC=1)

图5 缩放攻击实验结果



(a)裁剪攻击 (b)提取的水印(NC=0.936 5)

图6 裁剪攻击实验结果

表1 与文献[6]中算法(NC)的对比

攻击操作	JPEG(70)	JPEG(50)	椒盐噪声(0.01)	高斯噪声(0.002)	中值滤波
本文算法	1	1	0.993 3	1	0.993 2
文献[6]算法	1	0.999 2	0.957 6	0.986 6	0.979 6

4 结论

文中提出了一种基于 DCT 域的水印嵌入算法，其中结合了水印图像的 Arnold 置乱，边缘检测，载体图像低频系数的正负量化，有效地提高了水印的鲁棒性，并且实现了盲提取. 实验结果表明文中的算法对噪声、裁剪、滤波、JPEG 压缩等攻击都具有良好

的鲁棒性.

5　参考文献

[1] 孙圣和,陆哲明,牛夏牧. 数字水印技术及应用 [M]. 北京: 北京科学出版社,2004: 456-461.

[2] Cox I J,Kilian J,Leighton T,et al. Secure Spread Spectrum Watermarking for Multimedia [J]. IEEE Trans on Image Processing,1997,6(12): 1673-1687.

[3] 郑融,金聪,魏文芬,等. 一种基于混沌加密的 DCT 域数字图像水印算法 [J]. 计算机应用,2005,25(10): 2365-2373.

[4] 张志明,王磊. 基于混沌加密的 DCT 域图像水印算法 [J]. 计算机工程,2003,37(17): 102-104.

[5] 王洪秀,王冰. 基于图像纹理复杂度的数字水印算法 [J]. 计算机工程,2011,37(17): 102-104.

[6] 姚磊,王冰. 一种基于 DCT 中频的数字水印算法 [J]. 计算机技术与发展,2008,181(1): 192-195.

[7] 粟伟峰,杨小帆,柏森,等. 基于离散余弦变换和边缘检测的图像水印技术 [J]. 重庆大学学报: 自然科学版,2004,27(12): 78-81.

[8] 贾伟,张佑生,周庆松,等. 基于边缘检测的块分类水印算法 [J]. 合肥工业大学学报: 自然科学版,2004,27(2): 168-171.

[9] 陈涛,吴敏,张彪. 奇偶量化 DCT 系数实现文本信息隐藏 [J]. 计算机工程与应用,2011,47(9): 127-133.

[10] 李昊,吕建平,杨芳芳. 基于正负量化的 DCT 域数字图像盲水印算法研究 [J]. 计算机工程与应用,2011,47(5): 186-245.

[11] 李军,向长城. 基于混沌置乱的土家织锦图像数字水印算法 [J]. 江西师范大学学报: 自然科学版,2010,2010,34(2): 143-146.

The Blind Watermarking Algorithms Based on Edge Detection and Quantify the Positive and Negative

ZHAO Xiao-hua,ZHANG Gui-cang*

(College of Computer Science and Engineering,Northwest Normal University,Lanzhou Gansu 730070,China)

Abstract: A blind watermarking algorithm based on DCT domain edge detection and positive and negative quantitative is proposed. First the algorithm used Arnold scrambling method to encrypt watermark image,and carried on the positive and negative transformation,then used edge detection operator to carrier image edge extraction. Select different quantization value in accordance with the setting of the threshold value to embed watermark. Extract the watermark does not require the participation of the original image,realizing blind extraction. The experiments show that the algorithm has good robustness and invisibility to attacks such as cutting,compression,noise, filtering,scaling.

Key words: watermark; discrete cosine transform(DCT); quantization of plus or minus; robustness

(责任编辑: 冉小晓)