

文章编号:1000-582X(2009)08-0882-05

一种统计特性的数字水印算法

廖晓峰, 金渊智, 张艳珂, 周 庆

(重庆大学 信息安全与计算机智能研究所, 重庆 400030)

摘要:提出一种鲁棒的 DCT 域盲水印算法, 将 DCT 系数进行特殊的自定义排列分组, 并根据奇偶差实现水印的最优化嵌入。该算法突破了传统的分块、寻找合适中频系数模式, 解决了合适中频系数难找且嵌入容量小的问题。实验表明该算法计算简单, 且具有良好的不可见性, 并且在抵抗噪声和 JPEG 压缩攻击方面具有较强的鲁棒性。

关键词:数字水印; 离散余弦变换; 奇偶差

中图分类号: TP309.7

文献标志码: A

Watermarking algorithm based on statistical property

LIAO Xiao-feng, JIN Yuan-zhi, ZHANG Yan-ke, ZHOU Qing

(Institute of Computational Intelligence and Information Security, Chongqing 40030, P. R. China)

Abstract: A novel robust blind watermarking algorithm in DCT domain was proposed. The DCT coefficients are arranged in a specific way, and then the watermark is embedded based on odd-even difference for optimal embedding. This algorithm works in a new pattern other than block-division and search of the DCT coefficients in the middle frequencies in the traditional pattern, which can overcome the problem in searching suitable coefficients in the middle frequencies for watermark embedding and the small embedding capacity. Experimental results show that the algorithm is simple and good at perceptual transparency as well as robustness against noise and JPEG compression.

Key words: digital watermarking; discrete cosine transform (DCT); odd-even difference

按照嵌入方法可以将水印分为两类: 空间域水印和变换域水印。空域水印直接修改图像的像素, 特点是算法简单、计算复杂度低, 但鲁棒性差, 典型的算法有: 最低有效位法 (LSB)^[1-2] 算法, patchwork 算法^[3] 等; 变换域方法通过改变数据变换域中的一些系数来隐藏水印^[4-7], 典型的算法有: 离散余弦变换 (DCT)、离散傅立叶变换 (DFT) 和离散小波变换 (DWT) 等^[8-14], 其中 Cox 等提出的“扩展频谱”算法, 将水印信息嵌入在图像的 DCT 变换域中, 满足了水印的不可感知性和鲁棒性要求^[3]。Barni 在中提出将水印嵌入在 DCT 域固定的中频段^[15], 以便

在没有原始图像时仍能确定水印的嵌入位置, 从而将 Cox 的算法发展成盲水印算法。由于 DCT 域水印方案, 本身计算量较小, 且与国际数据压缩标准 (JPEG, MPEG) 兼容, 有利于水印算法的标准化, 故目前研究的比较多。为了平衡水印的不可见性和鲁棒性, 传统算法将水印嵌入到 DCT 域的中频系数上, 但这样使得满足条件的中频系数难找且嵌入容量受到很大限制^[16]。提出了一种空域水印嵌入算法, 即用二值图像奇偶块来嵌入水印信息, 这种算法虽然提供了很大的信息嵌入容量, 但其稳健性和不可见性较弱, 且主要适用于电子文档传输, 在传输图

收稿日期: 2009-03-15

基金项目: 国家自然科学基金重点资助项目 (60573047); 国家博士后科学基金资助项目 (20060400714)

作者简介: 廖晓峰 (1964-), 男, 重庆大学教授、博士生导师, 主要研究方向为信息安全与计算智能神经网络等,

(E-mail) xfliao@cqu.edu.cn.

欢迎访问重庆大学期刊社 <http://qks.cqu.edu.cn>

像时,会引起像素值的改变从而导致无法准确恢复出原始水印信息。笔者提出的基于 HVS 和统计特性的 DCT 域盲水印算法,突破了传统的分块、寻找合适的中频系数模式,它充分考虑了人眼视觉空间频率的敏感性,将变换后的 DCT 系数按照作者提出的“类对角线”方式排列成新矩阵,这样使得图像的高、低频分量集中在矩阵的 4 个角上,从而在中间部分选取可用集合(即嵌入位置)和嵌入强度,然后通过统计可用集合中 DCT 系数值的奇偶差来嵌入水印信息,这样使得嵌入信息量大且鲁棒性强。该算

法在水印检测时不需要某些假设或处理,同时通过对水印信息进行置乱加密及随机产生嵌入位置来保证水印的安全性,使嵌入的水印从根本上不可逆。

1 关于矩阵变换的定义及分析

对 $n \times n \times 8$ 的灰度图像进行 DCT 变换,对变换后的系数矩阵 $A[n, n]$,按照下图“类对角线”方式,从左上角到右下角的次序依次进行重新排列,得到新的系数矩阵 B ,具体排列方法如下图 1 所示:

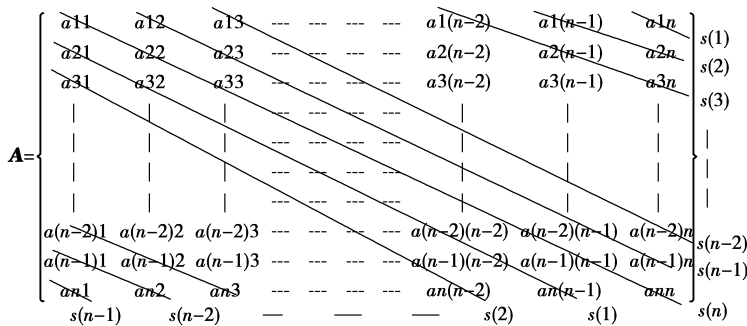


图 1 “类对角线”方式排列方法

$$\begin{aligned}
 S(1) &= \{a_{1n}, a_{21}, a_{32}, \dots, a_{(n-1)(n-2)}, a_{n(n-1)}\}; \\
 S(2) &= \{a_{1(n-1)}, a_{2n}, a_{31}, \dots, a_{(n-1)(n-3)}, a_{n(n-2)}\}; \\
 &\dots; \\
 S(n) &= \{a_{11}, a_{22}, a_{33}, \dots, a_{(n-1)(n-1)}, a_{nn}\}; \\
 B^T &= \{S(1), S(2), S(3), \dots, S(n)\}.
 \end{aligned}$$

定义 1 将上述矩阵 A 到矩阵 B 的变换记为: $A \Rightarrow B$, 并将其逆变换记为: $B \Rightarrow A$ 。

定义 2 $S(i)$ 中奇数的个数与偶数的个数差的绝对值叫奇偶差, $i=1, 2, \dots, n$ 。

由于 DCT 后人眼敏感部分,即低频主要集中在矩阵左上角,高频主要分布在矩阵的右下角,而将 DCT 系数按照上述“类对角线”方式排列后,所得矩阵的高低频分布示意图如图 2 所示:

的前 s 行 $S(1), S(2), \dots, S(s)$ 和后 s 行 $S(n-s), S(n-s+1), \dots, S(n)$ 都包含有高、低频分量,从而在中间行 $S(s+1), S(s+2), \dots, S(n-s-1)$ 选取可用集合(即嵌入位置)和嵌入强度,这样通过控制 s 的取值来确保水印的不可见性;此外通过对水印信息进行信号的“放大”,即用每行的 n 个系数来表达一位水印信息,来保证水印的鲁棒性。

2 信息的嵌入与提取

2.1 水印预处理

水印图像置乱是一种常见的水印加密方法,它使得合法使用者可以自由控制算法的选择、参数的选择以及使用随机数技术,这就加大了攻击者非法破译的难度^[18]。由于 Arnold 算法易于实现,其置乱次数可以为隐藏系统提供密钥(Key),从而增强了系统的安全性和保密性,同时该算法实现的置乱克服了随机置乱的不可恢复性。故本文采用 Arnold 变换对水印信息进行置乱。

对 $M \times M$ 的水印图像按照式(1)进行 Arnold 变换,

$$\begin{bmatrix} x' \\ y' \end{bmatrix} =$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod M, (x, y) \in \{0, 1, \dots, M-1\}.$$

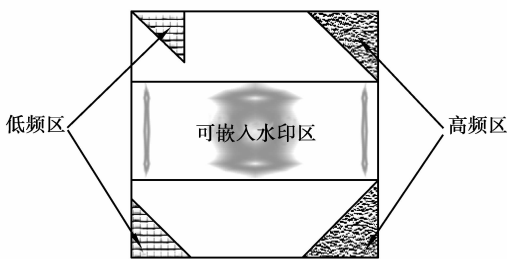


图 2 高低频分布示意图

显然,图像的高、低频分量被分散地转移到矩阵的 4 个角上,从而增大了水印的可嵌区域。因矩阵

再将得到的矩阵按行优先转换为一维二进制序列 m , 即下面要嵌入的信息序列 m 。

2.2 信息的嵌入

1) 设嵌入的信息序列为 k 位二进制序列 m :

$$\{m \mid m = m_1, m_2, \dots, m_k, m_i \in \{0, 1\}, k \leq n - 2s\}$$

现将 k 位信息按照私密密钥散列到向量组 $S(s+1) \dots S(n-s-1)$ 中, 设 Su 为选中的向量组, 则 $Su(r) \subseteq S(i)$, 其中 $r=1, 2, \dots, k, i=s+1, s+2, \dots, n-s$ 。

2) 统计向量 $Su(r)$ 中的奇偶差, 并对放入数组 $D(r)$ 中。

3) 如果 $m_i=1$, 即在 $Su(r)$ 中嵌入的信息是 '1', 定义不等式:

$$D(r) > d. \quad (2)$$

其中 d 是水印嵌入强度, 要想正确提取出原始信息, d 的取值应该大于载体图像的最大奇偶差 $D(\max)$ (其值取决于图像自身)。那么在此直接修改 $Su(r)$ 中的一部分数据, 使奇偶差人为的扩大到满足不等式(2)。为了提高算法的效率和拥有较好的不可见性, 在嵌入信息前先统计要嵌入信息中 '0' 和 '1' 个数的多少, 用人为扩大的奇偶差来表示个数少的 (此处假定 '1' 的个数较少), 以减少对 DCT 系数值的修改。具体方法如下:

① $Su(r)$ 中奇数个数大于偶数个数, 将一定量的偶数加上一个奇数 j 或者减一个奇数 j 变成奇数。

② $Su(r)$ 中偶数个数大于奇数个数, 将一定量的奇数加上一个奇数 j 或者减一个奇数 j 变成偶数。

这里的奇数 j 不能设置过大, 否则对图像的视觉效果影响很大。究竟每次要改变多少个奇数为偶数或者改变多少个偶数为奇数呢? 可以根据下面方程求出:

方程变量的说明:

a : 表示向量 $Su(r)$ 中理想的奇数个数

a' : 表示向量 $Su(r)$ 中实际的奇数个数

b : 表示向量 $Su(r)$ 中理想的偶数个数

b' : 表示向量 $Su(r)$ 中实际的偶数个数

则 a, b 满足如下方程:

$$\begin{cases} a+b=n \\ a-b=d \end{cases} \quad (\text{奇大于偶}) \quad \begin{cases} a+b=n \\ b-a=d \end{cases} \quad (\text{偶大于奇})$$

$$\Downarrow \quad \Downarrow$$

$$\begin{cases} a=\frac{n+d}{2} \\ b=\frac{n-d}{2} \end{cases} \quad \begin{cases} a=\frac{n-d}{2} \\ b=\frac{n+d}{2} \end{cases}$$

故偶数变奇数的最小改变量为: $b'-b=b'-\frac{n-d}{2}$;

奇数变偶数的最小改变量为: $a'-a=a'-\frac{n-d}{2}$ 。

此处的改变量与水印算法的鲁棒性有很大关系, 最小改变量由水印嵌入强度 d 决定。为了提高水印的鲁棒性, 实际的改变量 Q 应满足:

$$Q = b' - b + \Delta t \quad \text{或者} \quad Q = a' - a + \Delta t$$

其中 Δt 是最小改变量在理论值的基础上对水印嵌入强度的修正值。

4) 如果 $m_i=0$, 即要在 $Su(r)$ 中嵌入的信息是 '0', 根据 d 的选取原则, 不等式(2)一定不成立, 则不必修改 $Su(r)$ 中奇、偶数的个数。

5) 水印序列 m 嵌入完毕后, 将所得矩阵按照定义 1 中的逆变换转化为矩阵 U , 再对矩阵 U 进行逆 DCT 变换得到含有水印信息的图像。

2.3 水印信息的提取

水印的提取过程是嵌入的逆过程, 即对含有水印的图像进行 DCT 变换, 再根据 $A \Rightarrow B$ 将系数矩阵变型, 根据密钥选出水印嵌入位置 $Su(r), r=1, 2, 3, \dots, k$, 再统计 $Su(r)$ 中奇偶差的绝对值, 并放入 $D(r)$ 中, $r=1, 2, 3, \dots, k$

$$\text{if } D(r) > d \Rightarrow m_i = 1$$

$$\text{else } m_i = 0$$

恢复出序列 m 并重构二值图像, 最后用 Arnold 置乱算法对其进行恢复, 得到水印图像。

3 试验结果及分析

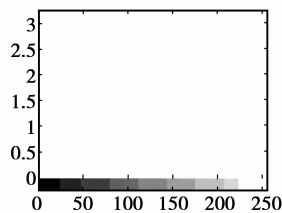
本文算法全部在 MATLAB 7.0.1 平台上得以实现, 并对多幅不同的图像进行了实验, 限于篇幅, 仅以 Lena $512 \times 512 \times 8$ 的灰度图像作为例子, 同时为了直观的显示水印的提取结果, 以下实验嵌入的信息来自于了一幅为 "金" 字的 10×10 的二值图像。

3.1 不可见性测试

水印的不可见性即在对原始载体图像嵌入水印信息后, 通过对比原始载体图像与含有水印的图像, 人眼不能分辨出明显的差别。现将 256 bit, 512 bit 的水印信息嵌入 Lena 图像中, 得到含有水印的图像如下图 3, 图 4 所示:



(a) 嵌入256bit后的图像



(b) 与原始Lena图像的像素值差的直方图

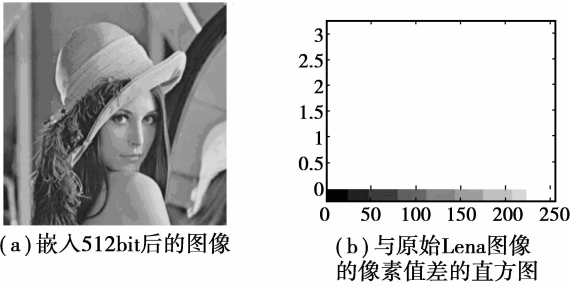


图 4 含有水印的图像($s=0, d=200$)

通过以上对比,可以看到水印的隐蔽性较好,在达到最大水印嵌入量时(嵌入 512 bit),外观几乎与 Lena 原图没有差别。但是通过与原始图像做差的直方图可以看出,在像素值上还是有所差别的,但差值绝大多数集中在 0 附近,这说明该算法具有良好的不可见性。

3.2 JPEG 压缩测试

将嵌入 256 bit 后的 Lena 图像进行 JPEG 压缩,压缩比为 6 : 1,提取出的水印图像如图 5 所示:

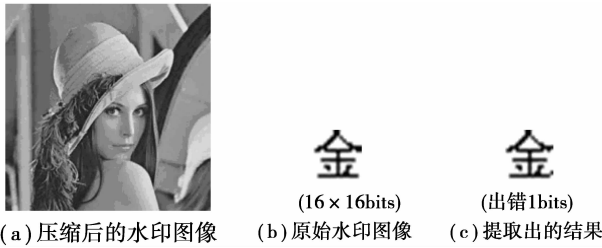


图 5 含有水印的图像($s=50, d=280$)

从实验结果可以看出,提取出的水印仅有一比特的误差,如果压缩比设置高的话,提取的正确率有所降低,但只要压缩过的水印图像与原始图像相比不存在较大的视觉失真,都能有效的提取水印信息。

3.3 噪声攻击测试

将嵌入 256 bit 后的 Lena 图像加入强度为 0.02 的椒盐噪声,提取出的水印图像如图 6 所示:

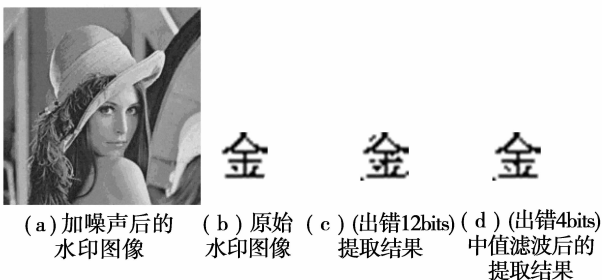


图 6 含有水印的图像($s=50, d=300, \Delta t=30$)

从图中可以看出,直接从加噪声的图像中提取水印信息具有较大的误差,即便是在嵌入强度 $d=300$,同时修正值 $\Delta t=30$ 在条件下。在经过对加噪声的图像进行中值滤波后,提取率大大提高。

4 结 论

文章提出的 DCT 域盲水印算法,根据人眼视觉的敏感性,通过将 DCT 系数进行特殊的排列分组,来确定嵌入位置,这就避开了传统的寻找合适的中频系数,且提高了水印的嵌入容量,再通过对水印信息进行信号“放大”,同时通过控制水印嵌入强度及其修正值来嵌入水印信息,这就提高了水印的鲁棒性。此水印方案有 3 个优点:一为盲水印,提取水印时不需要原始图像;二是在 DCT 域嵌入水印,适应 JPEG 压缩标准;三是利用了人眼视觉敏感特性,具有较好的视觉透明性。这给数字图像的版权认证提供便利,因此具有一定的实际应用价值。

参考文献:

[1] VAN SCHYNDEL R G, TRIKEL A Z, OSBORNE C F. A Digital Watermark [C]// Proceedings 1994 International Conference on Image Processing, Nov 13-16, 1994. Austin, Texas, USA. [s.l.]: IEEE, 1994: 86-90.

[2] WOLFGANG R B, DELP E J. A watermark for digital image [C]// Proceedings of 3rd IEEE International Conference on Image Processing, Sep 16-19, 1996, Lausanne, Switzerland. [s.l.]: IEEE, 1996: 219-222.

[3] BENDER W, GRUHL D, MORIMOTO N, et al. Techniques for data hiding [J]. IBM System Journal, 1996, 35(3/4): 313-316.

[4] LEE C H, LEE Y K. An adaptive digital image watermarking technique for copyright protection [J]. IEEE Transactions on Consumer Electronics, 1999, 45(4): 1005-1015.

[5] PODILCHUK C I, ZENG W J. Image-adaptive watermarking using visual models [J]. IEEE Journal on Selected Areas in Communications, 1998, 16(4): 525-539.

[6] HERNANDEZ J R, AMADO M, PEREZGONZALEZ F. DCT-domain watermarking techniques for still images. Detector performance analysis and a new structure [J]. IEEE Transactions on Image Processing, 2000, 9(1): 55-68.

- [7] TAO B, DICKINSON B. Adaptive watermarking in the DCT domain [C]//1997 IEEE International Conference on Acoustics, Speech and Signal Proceedings, Apr 21-24, 1997, Lausanne, Switzerland. [s. l.]: IEEE, 1997: 2985-2988.
- [8] COX I J. Secure spread spectrum watermarking for multimedia [J]. IEEE Trans on Image Processing, 1997, 6(12):1673-1687.
- [9] COX I J, LINNARTZ J P M G. Some general methods for tampering with watermarks [J]. IEEE Journal on Selected Areas in communications, 1998, 16(4): 587-593.
- [10] 宋玉杰,刘瑞祯,谭铁牛等. 数字水印技术在印刷品防伪中的应用[J]. 中国图像图形学报, 2001, 6(5): 450-454.
SONG YU-JIE, LIU RUI-ZHEN, TAN TIE-NIU, et al. Digital watermarking for forgery detection in printed materials[J]. Journal of Image and Graphics, 2001, 6(5):450-454.
- [11] TADASHI M, KINEO M. Robustness investigation of DCT Digital watermark for printing and scanning [J]. Electronics and Communications in Japan Part III: Fundament-all Electronic Science, 2003,86(4):11-19.
- [12] LIN C Y, CHANG S F. Distortion modeling and invariant extraction for digital image print-and-scan process [C/OL]//International Symposium on Multimedia Information Processing (ISMIP 99), Dec. 11-13, 1999, Taipei, Taiwan. [2009-03-01]. <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.40.2569>.
- [13] LIN C Y. Public watermarking surviving general scaling and cropping: An application for print-and-scan process[C/OL]// Multimedia and Security Workshop at ACM Multimedia 99, Oct. 1999, Orlando, FL, USA. [2009-03-01]. <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.46.1006>.
- [14] 钮心忻,杨义先. 基于小波变换的数字水印隐藏与检测算法[J]. 计算机学报, 2000, 23(1): 21-27.
NIU XIN-XIN, YANG YI-XIAN. A new algorithm for digital watermarking based on the wavelet transform. [J]. Chinese Journal of Computers, 2000, 23(1): 21-27.
- [15] BARNI M, BARTOLINI F, CAPPELLINI V. A DCT-domain system for robust image watermarking [J]. Signal Processing 1998, 66(3): 357-372.
- [16] 刘春庆,戴跃伟,王执铨. 一种新的二值图像信息隐藏方法[J]. 东南大学学报, 2000, 33(增刊): 98-101.
LIU CHUN-QING, DAI YUE-WEI, WANG ZHI-QUAN. A novel information hiding method in binary images [J]. Journal of Southeast University, 2000, 33(suppl): 98-101.
- [17] PODOCJIK C, ZENG W. Perceptual watermarking of still images[C]// IEEE First Workshop on Multimedia Signal Processing, Jun 23-25, 1997, Princeton, NJ, USA. [s. l.]: IEEE, 1997: 363-368.
- [18] 程兴国,刘传清. 一种有效的基于 DCT 域的数字水印算法[J]. 微计算机信息, 2007, 7(3): 313-314.
CHENG XIN-GUO, LIU CHUAN-QING. An effective digital watermarking algorithm in DCT domain [J]. Microcomputer Information, 2007, 7(3): 313-314.

(编辑 张小强)