基于坐标对准的抗剪裁数字水印盲检测技术

蔡丽敏[1] 冯久超[1,2] 肖永豪[1]

(华南理工大学电子与信息学院 广州 510641)[1] (西南大学电子与信息工程学院 重庆 400715)[2]

摘 要 本文提出了一种基于坐标对准的数字水印方案。它首先对含有版权信息的二值水印序列进行混沌置乱,以提高水印的安全性,然后把置乱的序列嵌入原宿主图像的DCT中频系数中,同时也在宿主图像嵌入了坐标信息,以便接收方对可能受剪裁攻击的图像进行坐标对准,从而在正确的位置提取出水印。仿真结果表明,该水印方案可实现盲水印检测,具有较高的安全性和保真性,不仅能有效抵抗剪裁攻击,而且对JPEG压缩、加噪、均值滤波等也具有很好的鲁棒性。

关键词 数字水印,混沌,DCT中频系数,剪裁,盲检测,坐标对准

A Blind Detection Method of Digital Watermark Based on Coordinates Calibration

CAI Li-Min[1] FENG Jiu-Chao[1,2] XIAO Yong-Hao[1]

(School of Electronic & Information Engineering, South China University of Technology, Guangzhou 510641)[1]

(Faculty of Electronic and Information Engineering, Southwest University, Chongqing 400715)[2]

Abstract A blind detection method of digital watermark based on coordinates calibration is proposed in this paper. The watermark array is first permuted for the sake of security. Then the binary watermark is embedded into the original host image, and the coordinates information are blended in the same image as well. Therefore, the coordinates can be calibrated for restoring watermark from the right place. Simulation results show that the proposed method can realize blind detect for watermark, and is of high security. It is robust to cutting interception, JPEG compression, additional noise, mean filtering, and also cutting in real sense.

Keywords Digital watermark, Chaos, DCT's intermediate frequency coefficient, Cutting, Blind detection, Coordinates calibration

1 引言

传统的信息加密方法可以加密文本信息,保证其传输的安全,但如果要对图像、视频和声音等多媒体信息进行加密,则基于密码学的传统加密方法就比较困难了。随着网络多媒体技术的发展,信息已经不仅仅局限于文本,许多信息是图形图像和视频格式,需要认证和版权保护的声像数据也越来越多。此外,在军事领域可能需要将一幅作战地图隐藏在一幅艺术作品中,等等。由此,数字水印技术应运而生。数字水印技术是将与多媒体内容相关或不相关的一些标示信息直接嵌入多媒体内容当中,但不影响原内容的使用价值,不容易被人的知觉系统觉察或注意到,只有通过专用的检测器或阅读器才能提取。其中的水印信息可以是作者的序列号、公司标志、有特殊意义的文本等,可用来识别文件、图像或音乐制品的来源、版本、原作者、拥有者、发行人、合法使用人对数字产品的拥有权[1]。

嵌入数字多媒体作品中的数字水印须具有以下特性:保真性、鲁棒性和安全性[2,3]。保真性是指不易被察觉,不会引起原来数字作品明显的图像质量下降,即看不到数字水印的存在。鲁棒性即当被保护的信息经过某种改动后,比如在噪声污染、压缩、滤波、图像的几何变换等处理下,数字水印不容易被破坏;而安全性是指加入水印和检测水印的方法对没有授权的第三方是保密的而且不可轻易被破解,即使被黑客检测到了也不能读出。

目前对数字水印的研究主要集中在空间域和变换域,如LSB(Least Significant Bits)、DCT(Discrete Cosine Transform)、DFT(Discrete Fourier Transform)和DWT(Discrete Wavelet Transform)等,它们分别通过改变空间域的某些像素的灰度或变换域的一些系数值来嵌入水印。其中DCT域水印方法,由于其计算量较小,且与国际数据压缩标准(JPEG,MPEG)兼容,至今研究得比较多[4,5]。然而,现有的大多数频率域数字水印算法只具有传统意义上的抗剪切能力,即图像被剪切的位置及大小可以确切得知。但实际应用中,图像在传输过程受到的往往是剪裁攻击,接收方无法知道图像受剪裁的具体情况。

针对上述情况,本文提出了一种基于坐标对准的水印方案能有效抵抗剪裁攻击。该方案采用二值图像作为水印,经过混沌置乱后嵌入到原图像的DCT中频系数中。此外还把坐标信息均匀嵌入在原图像的不同DCT中频系数中,在提取水印信息前对图像进行校准、补全,从而能在正确位置有效提取出水印。

2 水印嵌入算法

文[6]提出一种DCT域的水印算法,其方法是首先对水印信息进行置乱;把原图像分成8×8的不重叠方块,进行方块DCT变换后,即得到由DCT系数组成的频率块;选取每块的中频系数,通过对其作微小变动来表示嵌入的混沌水印信息。在提取水印时,选取相同的DCT系数并根据系数间的关

蔡丽敏 硕士生,主要研究方向:数字水印,混沌与保密通信;**冯久超** 博士,教授,博士生导师,研究领域涉及数字信号处理、数字通信、非线性动力学及混沌理论与应用;**肖永豪** 博士生,讲师,主要研究方向:混沌系统与保密通信、数字图像处理、视频水印与信息安全等。

系抽取比特信息，然后对得出的比特序列进行相应的置乱反变换，则可得到正确的水印信息。

上述方法的不足之处在于，当含有水印的图像受到剪裁攻击时，难以预知受剪裁的具体情况，导致无法确定 8×8 方块的划分位置与嵌入水印时的划分位置是否相符，从而不能正确提取出水印。这也是大多数 DCT 域水印算法存在的不足之处[7~10]。

针对上述情况，本文利用混沌技术的保密性，对水印图像进行混沌置乱，在分块 DCT 算法的基础上增加了坐标的嵌入及校准，为提取水印时对方块的划分提供了可靠的保证。

2.1 水印预处理

把二值水印图像信号转换为一维的二值序列，然后对其置乱以增加安全性。本文用 Logistic 映射[11]对水印序列置乱。Logistic 映射的定义为：

$$x(k+1)=\mu x(k)(1-x(k)) \tag{1}$$

式中，μ 为参数且 $0<\mu\leqslant 4$，$0<x(k)<1$，$k=1,2,\cdots$。该映射具有“似噪声”的统计特性，且对初始条件极端敏感。在不知道密钥 $x(1)$ 和 μ 的情况下，即使获取了图像甚至破解了嵌入算法，也无法正确恢复出水印信息。

置乱的具体算法如下：用 Logistic 算法产生一个与水印序列等长的混沌序列 $X=\{x(i)\mid i=1,2,\cdots,L\}$。对此混沌序列排序，并得到一个新的序列 $X'=\{x(d(i))\mid i=1,2,\cdots,L\}$，根据 X' 对水印序列进行置乱，其置乱规则 f 如下：

$$w'(i)=w(d(i)) \tag{2}$$

其中 $i=1,2,\cdots,L$，w 和 w' 分别为置乱前后的水印信息。

2.2 嵌入水印

把原图像分割成互不重叠的 8×8 个子块，对每一块分别作 DCT 变换，每块取 n 个中频系数，我们选第 k 块的 DCT 系数为：$m_k(1),m_k(2),m_k(3),\cdots,m_k(n)$，接着对 $m_k(n)$ 作如下变换：

$$m_k(n)=\begin{cases}\dfrac{m_k(1)+m_k(2)+\cdots+m_k(n-1)}{n-1}+P, & \text{if } w'(k)=1\\ \dfrac{m_k(1)+m_k(2)+\cdots+m_k(n-1)}{n-1}-P, & \text{if } w'(k)=0\end{cases} \tag{3}$$

其中，P 为水印嵌入强度。P 值越大，则水印鲁棒性越强，但保真性越差。对每个方块作 DCT 反变换，则得到含有水印的图像 W。由此可知，水印信息散布在图像的各处。

2.3 嵌入坐标

由前述可知，若把含有水印的图像 W 剪裁掉部分行(列)，则有可能接收方在进行 8×8 分块时无法和嵌入水印的相应位置对准，导致提取的水印信息无效。此外，若 W 被裁掉部分，则会丢失部分水印信息，改变水印信息长度，在进行水印提取时用混沌反置乱无法恢复出水印。因此，必须首先求出图像受剪裁的具体情况，我们将使用嵌入坐标的方法解决这一问题。

将含有水印的图像 W 分成互不重叠的大小为 8×8 的子块，在行对齐的子块嵌入相同的行号 $r(r=0,1,2,\cdots)$，在列对齐的子块嵌入相同的列号 $c(c=0,1,2,\cdots)$。若在每一个子块上都嵌入行号及列号，则嵌入的信息量相对较大，对原图像的破坏性也较强，因此在同一行(列)方向上，每隔 t(t 为可调，本文取 $t=4$)个子块嵌入相同的行(列)号，并且为了使坐标信息在图像中分布均匀，不易察觉，嵌入行号的子块应与嵌入列号的子块不重复。

嵌入坐标信息的实现方法如下：把每个嵌入的坐标值相同长度的用二进制数表示为：$b_h\cdots b_2b_1$，并保证 $2^0+2^1+\cdots+2^{h-1}$ 大于最大坐标值。对分割后的图像作子块 DCT 变换，取出其中 h 对不同于嵌入水印位置的中频系数 $p(1,i)$ 和 $p(2,i)$($i=1,2,\cdots,h$)，若嵌入值 b_i 为 1，调整数值令 $p(1,i)>p(2,i)$，即：

$$\begin{cases}p(1,i)=p(1,i)+P', & \text{if } p(1,i)>p(2,i)\\ p(1,i)=p(1,i)+P'+T, & \text{if } p(1,i)<p(2,i)\end{cases} \tag{4}$$

若嵌入值 b_i 为 0，调整数值令 $p(1,i)<p(2,i)$，即：

$$\begin{cases}p(2,i)=p(2,i)+P', & \text{if } p(2,i)>p(1,i)\\ p(2,i)=p(2,i)+P'+T, & \text{if } p(2,i)<p(1,i)\end{cases} \tag{5}$$

其中：$T=|p(1,i)-p(2,i)|$，P' 为嵌入强度。对子块进行 DCT 反变换，则得到嵌入坐标后的图像。

3 水印提取算法

3.1 提取坐标序列，确定图像的剪裁情况

1)把待提取的图像 W' 分割成互不重叠的 8×8 子块，选取其中嵌入行号位置的子块，对子块作 DCT 变换，取出 $p(1,i)$ 和 $p(2,i)$。若 $p(1,i)>p(2,i)$，则 $b_i=1$；若 $p(1,i)<p(2,i)$，则 $b_i=0$。把得到的二进制序列 $b_h\cdots b_2b_1$ 转化为十进制数行号值 d，在行对齐的子块提取的 d 中取出现次数最多的那个值作为正确的行号值，再依次得到一行的序列 r'_{11}。

2)考虑到所有可能的被剪裁情况。取 W' 第 1 行、第 2 列的像素点 $A(1,2)$ 作为图像的起始点，重复步骤一，可得行号序列 r'_{12}。依此类推，直到有重复划分的情况出现，我们可以得到行号矩阵：

$$R=\begin{bmatrix}r'_{11} & r'_{12} & \cdots & r'_{1,8t}\\ r'_{21} & r'_{22} & \cdots & r'_{2,8t}\\ \vdots & \vdots & \vdots & \vdots\\ r'_{8t,1} & r'_{8t,2} & \cdots & r'_{8t,8t}\end{bmatrix}$$

3)把 R 中的序列与行序列 r：0,1,2,… 作比较，求出其中最相似的序列 r'_{xy}，由下标 x、y 及其与 r 的对应位置可推出图像被剪裁的行数。

4)用同样方法可求出图像被剪裁的列数。

5)补全图像为 RW，如图 1 所示。

(a)原图像　(b)剪裁后的图像　(c)补全的图像

图 1　图像的剪裁情况

3.2 提取水印

把 RW 分割成互不重叠的 8×8 子块，对每一块分别作 DCT 变换，选取中频系数：$m_k(1), m_k(2), m_k(3), \cdots, m_k(n)$，并按如下规则提取出一组序列 v：

$$v(k)=\begin{cases}1, & \text{if } m_k(n)>\dfrac{m_k(1)+m_k(2)+\cdots+m_k(n-1)}{n-1}\\ 0, & \text{if } m_k(n)<\dfrac{m_k(1)+m_k(2)+\cdots+m_k(n-1)}{n-1}\end{cases} \tag{6}$$

其中 $k=1,2,\cdots,l$，l 为水印序列长度。对 v 作 f 反变换 f'，得水印序列 v'：

$$v'(d(i))=v(i) \tag{7}$$

最后，把 v' 按照原水印规格大小排列，即可得到有效的水印图像。

4 仿真结果

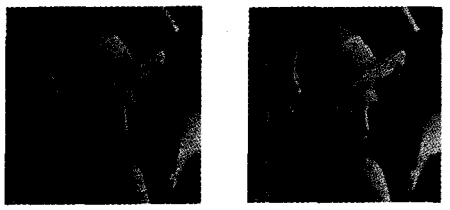
本文采用的原图像为 512×512 的 Lena 图像，水印图像为 64×64 的标有“华南理工”的黑白印章(二值图像)。

4.1 嵌入水印后图像的质量

一般用峰值信噪比(Peak Signal to Noise Ratio, PSNR)衡量图像的失真程度：

$$\mathrm{PSNR(dB)}=10\log_{10}\left\{\frac{255^2}{\frac{1}{N^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}(I(i,j)-I'(i,j))^2}\right\} \tag{8}$$

其中，I 为原图像的像素值，I' 为嵌入水印后图像的像素值，图像的尺寸大小为 $N\times N$。通常，PSNR 值越高，图像失真程度越小。



(a) 原始图像　　(b)嵌入水印及坐标的图像

图 2　原始图像与嵌入信息后的图像对比

采用本算法，我们得到 PSNR=39.09dB。从图 2 可以看出，原图像嵌入水印后基本没有可见失真，具有良好的保真性。

4.2 恢复水印与原水印的相似度

为了验证本文算法的鲁棒性，对嵌入水印的图像分别进行 JPEG 压缩、加噪、均值滤波、剪裁等操作。恢复水印与原水印的相似程度一般用归一化相关系数(Normalized Correlation, NC)表示[6,8]：

$$\mathrm{NC}=\frac{\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}w(i,j)v'(i,j)}{\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}[w(i,j)]^2} \tag{9}$$

其中，w 为原水印，v' 为提取的水印，水印的尺寸大小为 $M\times M$，在仿真中 $M=64$。当 NC>0.7 时，可认为提取出了有效水印。表 1 的实验结果表明：对含有水印的图像进行 JPEG 压缩、加噪、均值滤波、剪裁等多种操作，本文算法都能有效提取出水印。

结论　实验结果表明，本文算法有较好的安全性和保真性，而且对抵抗剪裁攻击是很有效的，甚至在图像被无规律裁减了 40%的面积后仍能有效提取出水印(如图 3 所示)；而对于其他的常规图像攻击，如 JPEG 压缩、加噪、均值滤波等，本水印算法同样具有较强的鲁棒性。

表 1　多种攻击下水印的鲁棒性测试结果

攻击类型		参数及对应条件下所得的 NC			
JPEG 压缩	质量因子	80	75	70	65
	NC	0.9984	0.9192	0.8657	0.7767
高斯噪声	标准差	0.03	0.04	0.05	0.06
	NC	0.9801	0.9397	0.9006	0.8569
椒盐噪声	噪声强度	0.015	0.020	0.025	0.030
	NC	0.8625	0.8292	0.7986	0.7738
均值滤波	NC	0.9136			
剪裁	剪裁面积百分比(%)	10	20	30	40
	NC	0.9426	0.8259	0.7559	0.7093

(a)原水印图像　(b) 0.1 剪裁后提取的水印　(c) 0.2 剪裁后提取的水印　(d) 0.3 剪裁后提取的水印　(e) 0.4 剪裁后提取的水印

图 3　原水印图像与经过多种比例剪裁后提取的水印对比

参 考 文 献

1 Cheng Qiang, Huang T S. Robust optimum detection of transform domain multiplicative watermarks. IEEE Trans. on Signal Proc, 2003, 51(4): 906～924

2 张鸿宾，张帆. 数字水印的应用、性质及性能评测. 计算机科学，2003, 30(8): 59～63

3 Kutter M. Watermarking resisting to translation, rotation, and scaling. In: Proceedings of SPIE International Symposium on Voice, Video, and Data Communications, Boston, U. S. A., 1998

4 易开祥. 数字水印技术研究进展. 中国图像图形学报，2001, 6(2): 111～117

5 Barni M, Podilchuk C I, Bartolini F, Delp E J. Watermark embedding: hiding a signal within a cover image. IEEE Communications Magzine, Aug. 2001. 102～108

6 韩强，马洪. DCT 域上基于 HVS 的盲水印添加方法. 四川大学学报，2005, 42 (3): 444～449

7 Wang Hongxia, He Chen, Ding Ke. Watermark hiding technique based on chaotic map. In: IEEE Int. Conf. Neural Networks & Signal Processing, Nanjing, China, 2003

8 Deng Fengsen, Wang Bingxi. A novel technique for robust image watermarking in the DCT domain. In: IEEE Int. Conf. Neural Networks & Processing. Nanjing, China, 2003

9 Wong P H W, Au O C. A novel blind multiple watermarking technique for images. IEEE Trans. on Circuits and Systems for Video Technology, 2003, 13(8): 813～830

10 Hsu C T, Wu J L. Hidden digital watermarks in images. IEEE Trans. on Image Processing, 1999, 8(1): 58～68

11 Feng Jiu-chao, Xie Shengli. A Noise Reduction Method For Noisy Contaminated Chaotic Signal. In: Proceedings of International Conference on Communications, Circuits and Systems, Chengdu, China, 2005, 2: 1173～1176