

用于 JPEG 图像认证的特征水印算法

王津申 戴跃伟 王执铨

(南京理工大学自动化学院, 南京 210094)

摘要 为了更加快速有效地进行 JPEG 图像认证,提出了一种基于内容的 JPEG 特征编码算法。该算法的基本思想是首先采用 DCT 变换域中不同 8×8 块之间 DCT 能量关系来构造特征码;然后在此基础上给出了 JPEG 图像半脆弱水印方案,即将内容特征码生成方法和水印算法有机地结合在一起。由于特征码具有“半脆弱”特性,即它对于可接受的“内容保持”修改具有鲁棒性,因而对常见的“内容篡改”性修改具有敏感性。另外,由于 DCT 系数块能量的主要部分集中在低频部分,从而使得可以用低频部分来生成特征码,而且可用高频部分来嵌入水印。实验结果表明,该算法计算简单,不仅有很好的抗 JPEG 压缩性能,同时对篡改的定位也很精确。

中图法分类号:TP309 文献标识码:A 文章编号:1006-8961(2008)07-1265-07

JPEG Image Authentication Based on Content Feature Watermarking

WANG Jin-shen, DAI Yue-wei, WANG Zhi-quan

(School of Automation, Nanjing University of Science and Technology, Nanjing, 210094)

Abstract A feature coding scheme based on the content of JPEG image was proposed. The basic logic of the scheme is to use partial energy relation between groups of 8×8 DCT block to produce related feature code. A semi-fragile watermarking scheme combines correctly the content based feature coding with the watermarking scheme. The feature code has the semi-fragile property, meaning that it is robust to the acceptable ‘content preserving’ modifications but sensitive to the ‘content changing’ tampering. The lower DCT region is used to form the feature codes while the higher one is used to embed watermarks. The experimental results demonstrate that the proposed algorithm has the advantages such as simple computation complexity, good robustness to JPEG, and precise location of tampered areas.

Keywords content authentication, feature coding, watermarking, semi-fragile

1 引言

由于数字图像和视频可以方便地编辑、存储、传输和使用,因此越来越广泛地应用于当今社会。但是与此同时,因为其易于修改的特性,即使业余爱好者也能够容易地修改这些数字媒体,并且创作出“完美的”伪造品^[1],使得数字媒体变得不安全,所以数字媒体,包括图像和视频的认证变得日益突出,尤其是在医学、军事和法律的领域。

如今采用数字水印技术对网络传输中的图像进

行认证,已成为当前信息认证领域的研究热点。用于图像认证的数字水印根据对篡改的敏感性不同,可分为脆弱性^[1-5]和半脆弱性^[1,3,6-8]两类,其中脆弱性水印主要用于完全级认证,因此需考虑全部数据,并且不允许任何修改;而半脆弱性水印则主要用于内容级认证。实际应用中,多媒体对象通常具有一些特殊的要求,例如,若多媒体对象是以 JPEG、MPEG 和 H. 26⁺ 等压缩形式提供,则经常会需需要从一种形式转换到另一种形式,或虽是同种形式,但是不同的压缩率,这样就会引起对象的改变。在这些情形中^[1],认证算法要求对“内容保持”的操作是鲁

基金项目:国家自然科学基金项目(60374066)

收稿日期:2006-11-09;改回日期:2007-01-05

第一作者简介:王津申(1978 ~),男,现为南京理工大学自动化学院博士研究生。主要从事信号处理,信息隐藏与数字水印研究。

E-mail:wangjinshe@njust.edu.cn

棒的,而对“恶意的”操作是敏感的。

基于特征的水印是另一种特殊的水印,这种水印不仅可以反映内容的特征,并且这些特征的选择是有针对性的,从而使得它们对“内容保持”的操作不改变,而仅对“恶意”攻击行为敏感。因而,可以认为这些特征应该是某种方式的“半脆弱”特征。通常基于特征的水印是采用鲁棒的方式进行嵌入,以使得该水印本身在保持内容可用的前提下,具有抗攻击性,而特征则对于故意的攻击行为是脆弱的。因此可以通过对提取出的水印内容和计算出的特征进行比较来确定是否有攻击发生以及进行攻击定位。

由于 JPEG 压缩应用的普遍性,抗 JPEG 压缩一直是图像认证水印的重要研究内容及难点。文献[9]根据 JPEG 压缩过程中的不变参量进行水印生成和嵌入调制,并利用小波特性和对图像篡改区域进行定位。文献[10]则根据 JPEG 压缩之后图像的相邻小波高频系数之间的大小关系大多数没有发生变化这一事实,提出了一种半脆弱水印算法。

当图像被转换成 JPEG 格式时,其中的像素值会被先转换为离散余弦变换(DCT)系数,然后再进行量化和变长编码(VLC)。通过尝试性实验发现,经过一定限度内的重复 JPEG 压缩后的两个块(或由若干块构成的组)之间的能量关系能够保持不变,并且 DCT 系数块的能量的主要部分位于低频,这就决定了“内容”的特征。通常可以把 64 个 DCT

系数分为低频和高频两个部分,其中低频部分用来形成特征码,而高频部分则用来嵌入水印。

2 特征编码算法设计

2.1 认证系统对特征码的要求

在描述特征提取算法之前,可首先给出如下一些必要的要求^[1,2]:①灵敏性 认证系统对如剪切、移动、替换等类型的恶意操作是敏感的;②鲁棒性 认证系统对“可接受的”的“内容保持”类操作具有鲁棒性,如 JPEG 压缩、轻微加噪等;③定位能力 认证系统应该能够探测到改动过的位置,并能证实其他区域是完整的。

2.2 特征提取算法

设 JPEG 图像中有 M 个 8×8 数据块,即 $B = \{b_1, b_2, \dots, b_M\}$ 。对于每个 8×8 块, $C_i = \{c_{i,0}, c_{i,1}, \dots, c_{i,63}\}$ 是相应的 DCT 系数。可将 $\{c_{i,j}\}_{j=0, \dots, 63}$ 分割为 $C_i^F = \{c_{i,1}, \dots, c_{i,s}\}$ (上角 F 代表 feature) 及 $C_i^E = \{c_{i,s+1}, \dots, c_{i,63}\}$ (上角 E 代表 embed) 两部分,其中分割索引值 s 可以根据整个图像的平均能量调整。对于特征提取和水印嵌入,一个组内再将一些具有固定排列的 $2n$ 个块分为一个组。这样图像也可以表示为 $G = \{g_1, g_2, \dots, g_L\}$, 且 $M = 2n \times L$ 。

特征提取过程(如图 1 所示)如下:

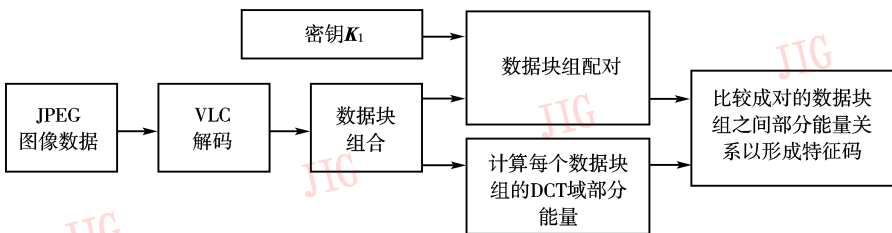


图 1 JPEG 图像内容特征的产生过程

Fig. 1 The generation of content based feature for JPEG image

(1) VLC 解码;

(2) 块组合 即根据预先定义的块的数目 n 将几个相邻的块结合成一个组(例如,取组的大小 $2n=8$),其中块呈矩形排列,而 n 的选择则需要考虑抗 JPEG 压缩的鲁棒性和对篡改的定位精度;

(3) 数据块组配对 组对是特征提取的基本单元,并且一个组可被分为具有相同块数的两部分。为了增强算法的安全性,组的配对要在密钥 K_1 的控制下进行,设 N_1 为组对的总数目,则配对后的组对

重编索引为

$$P = \{p_1, p_2, \dots, p_{N_1}\} \\ = \{(g_1^I, g_1^J), (g_2^I, g_2^J), \dots, (g_{N_1}^I, g_{N_1}^J)\} \quad (1)$$

其中, N_1 是变量。 N_1 的大小也就是特征码的长度;

(4) 部分能量计算 如果先为每个组计算部分能量,然后以图像为单位计算平均部分能量,那么对所有的块 b_i ,它的部分 DCT 能量为

$$E_{i,s} = \sum_{j=0}^s (\theta_{i,j})^2 \quad (2)$$

其中, $1 \leq s \leq 63, i = 1, 2, \dots, N_2, N_2$ 为组的数目, $\theta_{i,j}$ 是 8×8 块中的 DCT 系数, 当 $s = 0$ 时, 则可得到直流成分能量; 当 $s = 63$ 时, 则得到全部频率的能量。这样就可先得到 $64 \times N_2$ 个部分能量值, 然后计算对应于每个索引值 s 的部分能量及其平均值, 即

$$E_s = \sum_{i=1}^{N_2} E_{i,s}, s = 0, 1, 2, \dots, 63 \quad (3)$$

$$\bar{E}_s = \frac{1}{N_2} \sum_{i=1}^{N_2} E_{i,s}, s = 0, 1, 2, \dots, 63 \quad (4)$$

在组的结合和重新索引之后, 每个组对的能量对为 $(E_{k,s}^I, E_{k,s}^J), k = 1, 2, \dots, N_1$;

(5) 分割索引值 s 的选择 可用该索引值将 64 个 DCT 系数分割为两部分, 其中一部分是特征提取区域, 这个区域具有较低频率, 并且占据大部分的能量; 另一部分是水印嵌入区域, 这个区域位于高频, 并且占据较少部分的能量。通常可使用下述迭代过程来搜索分割索引值 s_μ :

FOR $s = 1$ to 63 DO

IF $\frac{\bar{E}_s}{\bar{E}_{63}} \geq \mu\%$ THEN GOTO end

END

这里 μ 是在综合考虑特征提取和水印嵌入两方面要求的基础上确定的合理取值, μ 建议取值为 80 ~ 90;

(6) 部分能量关系的 1 bit 量化 设特征为

$$F = \{f_1, f_2, \dots, f_{N_1}\}, f_i \in (0, 1) \quad (5)$$

$$i = 1, 2, \dots, N_1$$

对每个组对, 特征的计算为

$$f_i = \begin{cases} 0 & \text{如果 } \bar{E}_{i,s}^I - \bar{E}_{i,s}^J \geq 0 \\ 1 & \bar{E}_{i,s}^I - \bar{E}_{i,s}^J < 0 \end{cases} \quad (6)$$

3 水印算法设计

3.1 水印嵌入

水印嵌入步骤如下:

(1) 结合包括特征码 \hat{F} 和版权信息 C 在内的必要信息, 即

$$F = \hat{F} \cup C \quad (7)$$

式中“ \cup ”表示合并操作;

(2) 加密合成信息 F , 以形成水印

$$W = F \oplus K_2 = (w_1, w_2, \dots, w_{N_w}) \quad (8)$$

式中, “ \oplus ”是加密操作(如异或), K_2 是伪随机序列(公钥或对称密钥), N_w 是水印比特数;

(3) 随机置乱 8×8 数据块 为了得到更加均匀的能量分布, 在嵌入水印数据之前, 应先对所有数据块位置进行“随机”置乱, 其过程由密钥 K_3 (伪随机数) 控制;

(4) 块组合 置乱后的数据块用与第 2 节中同样的方法再次组合, 以形成 LC (label-bit-carrying region) 区域, 并且每个 LC 区域包括 A, B 两部分, 每个部分有相同的尺寸 (n 个数据块)。为简单起见, 块组合的控制密钥仍选择 K_1 ;

(5) 使用改进的 DEW (differential energy watermarking) 算法嵌入水印^[11];

(6) 数据块整理, 在密钥 K_3 的控制下, 将所有的块还原到原始的位置(第 3 步的逆过程);

(7) VLC 编码, 并且存储 JPEG 数据。

3.2 水印提取

水印检测过程是盲检测过程, 其可分为水印提取、特征重建、认证 3 个部分。

水印提取过程如下:

(1) JPEG 图像的 VLC 解码;

(2) 在 K_3 控制下进行数据块随机置乱;

(3) 以与第 3.1 节相同的方法组合数据块;

(4) 对所有可能的水印位 $\hat{w}_i \in \hat{W}, 1 \leq i \leq N_w$, 完成下列步骤: 将 LC 区域(具有 $2n$ 个块的组)分割为两个子区域 A, B ; 计算切割索引值 \hat{I}_c , 并选取能量差阈值 \hat{D} (通常 $\hat{D} \leq D$), 则

$$\hat{I}_c = \max \{ c_{\min}, \max \{ j \in (s_\mu, 63) \mid (E^A - E_j^A) > \hat{D} \}, \max \{ k \in (s_\mu, 63) \mid (E^B - E_k^B) > \hat{D} \} \} \quad (9)$$

计算子区域间的能量差

$D_{A,B} = (E^A - E_{\hat{I}_c}^A) - (E^B - E_{\hat{I}_c}^B)$, 如果 $D_{A,B} > 0$ 则 $\hat{w}_i = 0$; 否则 $\hat{w}_i = 1$ 。

(5) 使用密钥 K_2 解密所得到的水印序列 W' , 并从中分离出特征码 $\hat{F}^{(1)}$ 和版权信息 \hat{C} 。

3.3 特征重建和认证

采用与第 2 节相同的方法重新生成特征码 $\hat{F}^{(1)}$ 。设一个组对中两个组的部分能量分别为 \hat{E}_1, \hat{E}_2 , 则重新生成的特征值为

$$\tilde{f} = \begin{cases} 0 & \text{如果 } \hat{E}_1 - \hat{E}_2 \geq \hat{M}_F \\ N & -\hat{M}_F < \hat{E}_1 - \hat{E}_2 < \hat{M}_F \\ 1 & \hat{E}_1 - \hat{E}_2 \leq -\hat{M}_F \end{cases} \quad (10)$$

这里,由于多数重压缩操作有滤波效果,所以本文取 $\hat{M}_F \leq M_F$ (下角 F 代表 feature),另外又由于每一个组对是固定的,并且嵌入的数据需依赖于有关的数据块位置,因此仍然有 $2 \times \hat{M}_F$ 的屏障。

通过对提取出的来自水印的特征码与重新生成的特征码的比较,就可以判断 JPEG 图像是否遭受了恶意篡改。如果发生了篡改,则还可进一步探知被篡改的位置,其有 3 种可能的情形。为了讨论简单,本文假设水印对 JPEG 重压缩足够鲁棒,这意味着提取出的水印与嵌入的水印精确相等 ($\hat{f} = f$)。需要指出的是,这个假设是合理的,因为所提出的这种水印是半脆弱的,第 4 节的实验也证实了本文算法对 JPEG 重压缩具有足够的鲁棒性。

分为以下 3 种情况:

(1) “ $\tilde{f} = 0$ 和 $\hat{f} = 0$ ”及“ $\tilde{f} = 1$ 和 $\hat{f} = 1$ ”:当重新生成的特征码和提取的特征码逐位相等时,则内容就可以被认为是“真实”的。

(2) “ $\tilde{f} = 0$ 和 $\hat{f} = 1$ ”与“ $\tilde{f} = 1$ 和 $\hat{f} = 0$ ”:当出现一个以上不一致时,则可以认为该 JPEG 图

像已经被篡改。由于块组是编号的,从而可以根据组号来确定篡改位置。但是由于一个特征位 (bit) 代表两个组之间的关系,因此怎样确定哪个组遭受攻击?可能的对策是观察与这两个组邻近的那些组。因为数据块组的尺寸一般很小,而通常一种针对内容的篡改会影响不止一个组,所以通过考察相邻组是否有问题即可作出判断。

(3) “ $\hat{f} = 0$ 和 $\tilde{f} = N$ ”与“ $\hat{f} = 1$ 和 $\tilde{f} = N$ ”:当提取的特征码位为“0”或“1”,但是重建的特征码却落入出错区间时,这是一种不确定的情形。特征重建方案中需要恰当地选取特征生成/重新生成、水印嵌入/提取的有关参数,以便使得这个区域尽可能的窄。

4 实验结果和分析

4.1 重复压缩对数据块之间能量关系的影响

为了证实图像经过 JPEG 重压缩后各数据块之间的能量关系,可在图 2 所示的 5 幅 JPEG 图像中随机选取 200 ~ 300 个块对,并用不同的质量因子对这些图像进行重压缩。

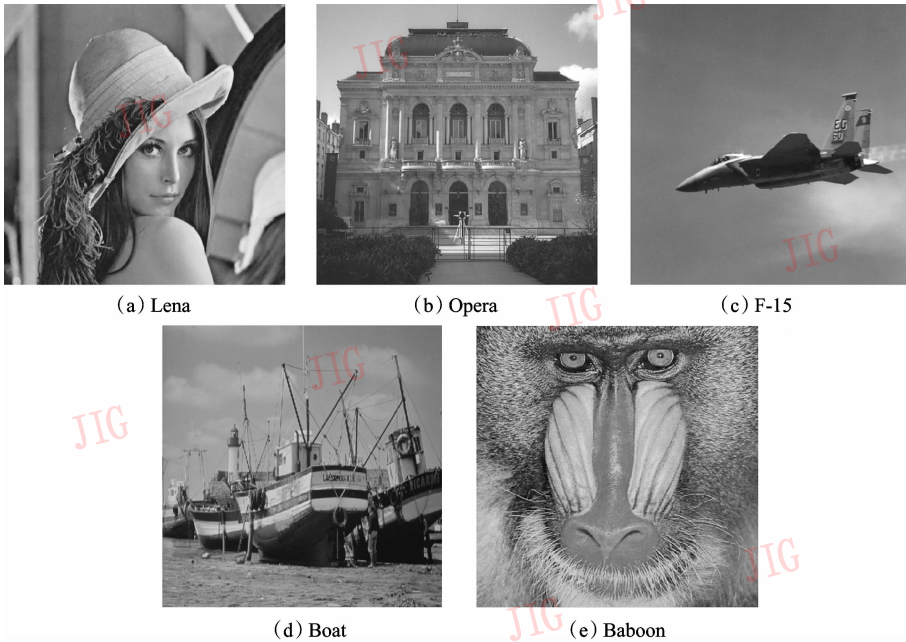


图 2 用于测试的 JPEG 重压缩对数据块之间能量关系的影响

Fig. 2 Images used for testing the energy relationship for block-couples

原始质量因子为 90,重压缩质量因子分别为 80,70,60 和 50。由于可将能量关系简单化为“ \geq ”或“ $<$ ”,所以当能量比在重压缩时,由“ ≥ 1 ”改变为“ < 1 ”或由“ < 1 ”改变为“ ≥ 1 ”,则被认为有能量

“穿越”发生,而发生能量“穿越”的块对数的多少就反映了能量关系的改变情况。表 1 列出了分别在无白噪声和有白噪声影响情况下,进行不同质量因子的重复压缩的实验结果。

表 1 块对之间能量关系实验结果

Tab. 1 Experimental results of the energy relationship for block-couples

	Lena	Opera	F-15	Boat	Baboon
块对总数	264	255	214	195	254
重压缩时发生能量穿越的块对总数	3	16	9	4	5
重压缩时发生能量穿越的块对数目的相对值(%)	1.14	6.27	4.21	2.05	1.97
有白噪声影响情况下重压缩时发生能量穿越的块对总数(白噪声)重压缩时发生能量穿越的块对数目的相对值(%)	5	16	9	4	5
	1.89	6.27	4.21	2.05	1.97

从表 1 中可以看出,如此建立起来的块对能量关系(1 bit 量化后),在遭受不同质量因子压缩前后发生能量“穿越”的数量相对较少,平均相对穿越比例为 3.3%,而且当图像遭受加性白噪声时,不同质量因子重压缩对能量“穿越”数量也没有太大的影响。

4.2 重复压缩对数据块之间部分能量关系的影响

由于实用中需要使用部分 DCT 系数来产生特征码,为此本文选取的分割 DCT 系数索引值为 1,2,3,5,7,10,12,14,并用其来进行重复 JPEG 压缩,质量因子仍取 90,80,70,60 和 50。图 3 为 5 个图像的实验结果。从图中可以看出,当分割索引值大于 10,图像在遭受不同质量因子压缩前后,数据块之间

的部分能量发生“穿越”的数量相对较少。这也为分割索引值的选取提供了依据。

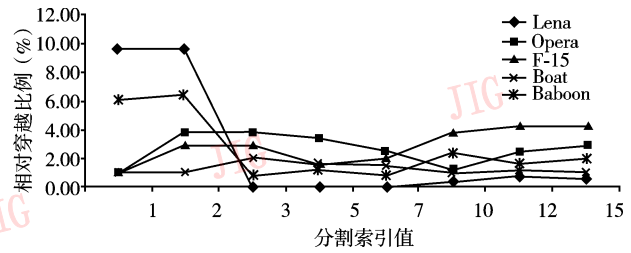


图 3 不同分割索引值下重复压缩对部分能量关系的影响

Fig. 3 Influence to partial energy relationship due to re-compressions

4.3 内容认证实验

为了证明算法的可行性,本文设计了一组实验。实验采用的原始图像如图 4(a)所示,其中的图像原始质量系数是 85,图像大小为 512 × 512 (组的大小 2n = 16)。嵌入水印后的图像如图 4(b)所示。嵌入水印后图像的峰值信噪比(PSNR)如表 2 所示,从表 2 可以发现,嵌入水印后的图像具有很好的视觉质量。

表 2 嵌入水印后的载体图像的 PSNR 值

Tab. 2 PSNR for watermarked images

图像	Lena	Opera	F-15
PSNR 值 (dB)	35.2	35.8	35.5



(a) 原始图像



(b) 嵌入水印后的图像

图 4 原始图像及嵌入水印后的图像

Fig. 4 Original images and watermarked images

为了评测本文提出的图像认证系统的性能,通过设计部分的消失、去除和替换 3 种攻击来进行认证实验。实验以“F-15”图像作为例子,其他两幅图像与其相似,即对每幅图像首先进行修改,然后进行重压缩。图 5、图 6、图 7 分别为实验结果,其中组的大小为 $2n = 16$ 。由实验结果可以得出以下结论:(1)如果参数选择得当,则这种算法能以很高的概率发现恶意篡改行为,且本文算法在某种程度上是半脆弱的,即一方面,算法对“内容篡改”敏感;另一方面,它对于重压缩、添加白噪声等“正常修改”是鲁棒的,可见这种算法是高可信的实用化方法;(2)算法产生的视觉效果影响很小,这主要是由于用块能量的平均效果(多 DCT 系数)取代单个的 DCT 系数所致;(3)遗憾的是,本文算法的虚警概率相对较高,但是漏警概率却很低,这主要可能是由非最优参数组合而引起;(4)对操作定位的能力因组的大小而改变,其中,当组的大小($2n$ 个块)减小时,则定位精度和敏感性增加,但是因为块能量的平均效果变弱,所以对“内容保持”的鲁棒性减少;(5)嵌入容量也因组的大小而改变,即当组的大小增加时,总的嵌入比特减少。

因此有必要在组的大小、能量差和最小分割索引值之间作出一种折衷。从实验中发现,强制能量差越大,水印的鲁棒性越强。但是,因为更多的 DCT 系数不得被丢弃,所以太大的能量差会引起可感知视觉质量的下降。

4.4 与其他算法的比较

为验证本文算法的有效性,将本文算法与文献[10]、[13]算法的图像认证性能进行了比较。比较所用到的载体图像均为 Lena,几种算法的性能比较结果见表 3。

表 3 与其他算法的性能比较

Tab. 3 Performance comparison with other algorithms

算法	载体图像大小	对篡改的定位能力	PSNR 值 (dB)	质量因子
本文方法	512 × 512	相对准确	36.7	70
文献[10]算法	512 × 512	相对准确	43.42	60
文献[13]算法	512 × 512	一般	36.26	75

文献[10]算法与本文的算法相近,但是仍有以下两点主要区别:(1)文献[10]算法根据的是图像相邻小波高频系数之间的大小关系,而本文算法依据的则是 DCT 变换域中不同 8×8 块之间

DCT 能量关系;(2)文献[10]算法中嵌入的水印是与载体图像内容无关的二值图像,而本文中嵌入的水印则是用载体图像在 DCT 变换域中由不同 8×8 块之间的 DCT 能量关系构成的特征码作为水印。在图像认证时,文献[10]算法不仅需要原始水印图像,且要与提取的水印图像进行比较得到的差值图像才能认证;而本文算法中的认证特征码是提取的自载体图像,并且反映的是载体图像的特征。因此本文的算法具有明显的优点,且更具有实用价值。

5 结 论

本文提出一种用于 JPEG 图像内容认证的新颖水印算法。该图像认证方法是基于一种半脆弱特征,由于这种半脆弱特征具有区分“内容保持”和“恶意篡改”的能力,因此本文算法可以用于确定和定位攻击。实验结果表明,该新算法是有效的。此方案今后还可以在下列几方面进一步探讨:(1)对图像对象进行更多实验的性能分析;(2)在不同的应用中寻找决定参数的自适应的方法;(3)对算法的鲁棒性、敏感性、安全性、视觉影响和定位精度进行理论分析;(4)进行参数选取原则和优化组合的研究。

尽管本文仅对 JPEG 图像对象进行实验,但本文的水印算法还可以直接扩展到 MPEG I/II 视频认证。因为当视频信号被转换为 MPEG I/II 格式时,其中的像素值也会被转换为 DCT 系数。考虑到视频对象是由许多图像组所组成,并且每个组的基础是 I 帧,所以可以将这种算法只应用于 I 帧。

参考文献 (References)

- Lin C Y, Chang S F. Semi-Fragile Watermarking for Authenticating JPEG Visual Content [A]. In: Delp E J, Wong P W, eds: Proceedings Electronic Imaging 2000, Security and Watermarking of Multimedia Contents II [C], San Jose, California, USA: SPIE Photonic West, 2000, **3971**:140 ~ 151.
- Fridrich J. Security of Fragile Authentication Watermarks with Localization [A]. In: Delp E J, Wong P W, eds: Proceedings Electronic Imaging 2002, Security and Watermarking of Multimedia Contents IV [C], San Jose, California, USA: SPIE Photonic West, 2002, **4675**:691 ~ 700.
- Lin C Y, Chang S F. Issues and solutions for authenticating MPEG Video [A]. In: Delp E J, Wong P W, eds: Proceedings Electronic Imaging 1999, Security and Watermarking of Multimedia Contents IV

- [C], San Jose, California, USA: SPIE Photonic West, 1999, **3657**:54 ~ 65.
- 4 Dittmann J, Mukherjee A, Steinebach M. Media-independent Watermarking Classification and the need for combining digital video and audio watermarking for media authentication [A]. In: Proceedings of the IEEE Computer Society International Conference on Information Technology: Coding and Computing [C], Las Vegas, Nevada, USA, 2000:62 ~ 67.
 - 5 Wong P W, Memon N. Secret and public key authentication watermarking schemes that resist vector quantization attack [A]. In: Delp E J, Wong P W, eds: Proceedings Electronic Imaging 2000, Security and Watermarking of Multimedia Contents IV [C], San Jose, California, USA: SPIE Photonic West, 2000, **3971**: 417 ~ 427.
 - 6 Celik M U, Sharma G, Tekalp A M, *et al.* Video authentication with self-recovery [A]. In: Delp E J, Wong P W, eds: Proceedings Electronic Imaging 2002, Security and Watermarking of Multimedia Contents IV [C], San Jose, California, USA: SPIE Photonic West, 2002, **4675**:531 ~ 541.
 - 7 Kuato Maeno, Sun Q B, Chang S F, *et al.* New semi-fragile image authentication watermarking techniques using random bias and non-uniform quantization [A]. In: Delp E J, Wong P W, eds: Proceedings Electronic Imaging 2002, Security and Watermarking of Multimedia Contents IV [C], San Jose, California, USA: SPIE Photonic West, 2002, **4675**:659 ~ 670.
 - 8 Mobasseri B G, Evans A T. Content-dependent video authentication by self-watermarking in color space [A]. In: Delp E J, Wong P W, eds: Proceedings Electronic Imaging 2001, Security and Watermarking of Multimedia Contents IV [C], San Jose, California, USA: SPIE Photonic West, 2001, **4314**:35 ~ 44.
 - 9 Zhang Jing, Zhang Chun-tian. Semi-fragile watermarking for JPEG2000 image authentication [J]. Acta Electronica Sinica, 2004, **32**(1):157 ~ 160. [张静, 张春田. 用于 JPEG2000 图像认证的半脆弱性水印算法[J]. 电子学报, 2004, **32**(1):157 ~ 160.]
 - 10 Li Chun, Huang Ji-wu. A semi-fragile image watermarking resisting to JPEG [J]. Journal of Software, 2006, **17**(2):315 ~ 324. [李春, 黄继武. 一种抗 JPEG 压缩的半脆弱图像水印算法[J]. 软件学报, 2006, **17**(2):315 ~ 324.]
 - 11 Setyawan I, Lagendijk R L. Low bit-rate video watermarking using temporally extended differential energy watermarking (DEW) algorithm [A]. In: Delp E J, Wong P W. eds: Proceedings Electronic Imaging 2001, Security and Watermarking of Multimedia Contents IV [C], San Jose, California, USA: SPIE Photonic West, 2001, **4314**:73 ~ 84.
 - 12 Fan Cheng-bo, Zhang Chun-tian. A fragile blind watermark for JPEG image authentication [J]. Signal Processing, 2003, **19**(3): 266 ~ 268. [范成博, 张春田. 适用于 JPEG 图像认证的脆弱性盲水印算法[J]. 信号处理, 2003, **19**(3):266 ~ 268.]