抗 JPEG 压缩和图像合并的水印算法

伍宏涛 胡 云 钮心忻 杨义先
(北京邮电大学信息安全中心 北京 100876)

摘 要：该文首次阐述水印在图像合并操作下的应用，综合考虑 JPEG 有损压缩的影响，提出了通用的解决方案，并作了相应的安全性分析。在该方案的指导下，提出了一种抗 JPEG 压缩和图像合并的水印算法，通过试验，证明该算法具有很强的抗压缩性和抗合并性。

关键词：图像合并，数字水印，JPEG 压缩
中图分类号：TP391 **文献标识码**：A **文章编号**：1009-5896(2005)06-0914-05

Watermarking Algorithm with Resistance to JPEG Lossy Compressing and Images Uniting

Wu Hong-tao Hu Yun Niu Xin-xin Yang Yi-xian
(*Information Security Center, BUPT, Beijing* 100876, *China*)

Abstract It is the first time to expound the watermark application under images uniting in this paper. With the affecting of JPEG lossy compressing, the universal solving scheme is proposed, and the corresponding security analysis is made. In the direction of this scheme, a watermark algorithm is proposed which can resist the JPEG lossy compressing and images uniting question. The test results prove its both characters.

Key words Images uniting, Digital watermark, JPEG compressing

1 引言

数字水印是信息隐藏[1,2]技术研究领域的重要分支。最新的研究强调水印嵌入的方法与压缩算法的紧密结合。文献[3]描述了基于不同压缩算法得到水印方案的方法，这种方法生成的水印方案对于有损压缩和滤波、剪切、旋转等具有鲁棒性；文献[4]针对 JPEG 图像的版权保护提出了修正的 DCT 变换，可以抵抗压缩、加噪、滤波和几何变换等攻击；文献[5]结合 JPEG2000 压缩标准提出了在小波系数的比特平面编码中嵌入水印的方法，同时考虑了视觉补偿。水印嵌入的载体在不断的扩展；文献[6, 7]对矢量图像和二维矢量地图的水印嵌入进行了讨论，提出了有效的解决算法。在水印嵌入的实际方法中，变换域系数的量化调制是逐步兴起的重要方法，因此，文献[8]对量化水印的失真进行了最优补偿研究；文献[9]则分析了小波域下的量化水印，得到了一般情况下的简洁的失真的表达式。从发表的文献内容分析，目前数字水印技术的研究已经从简单载体扩展到其他的数字产品上，更加强调水印的强鲁棒性，安全性和容量成为第二重要的因素，水印采用的方法趋向于变换系数的量化调制。

本文将水印的应用扩展到这样的情况：嵌入水印的图像由于应用的原因合并成一幅图像，版权所有者希望在合并的图像中也能检测出版权信息；同时图像中嵌入的水印具有很强的鲁棒性，可以抵抗 JPEG 压缩和其他攻击，例如几何剪切等。这样的应用是很多的，如建筑 CAD 的分幅图纸、大型照片的小块分幅照片，这些分幅图像遵循内在的空间关系，可以任意裁剪和合并。我们解决的问题是：将相同的水印分别嵌入分块图像中，分块图像可以提取出水印，在任意分块图像合并后的图像中也可以提取出嵌入的水印，同时，该水印算法可以抵抗 JPEG 压缩和几何剪切。

我们提出的抵抗图像合并操作的水印方案已经在工程实践中得到了应用，并且具有很好的效果。该方案将水印嵌入的实际修改载体抽象成数据的集合，该数据集合按照一定规则分成 M 个分类，每个分类具有各自的统计值，通过修改分类的统计值实现水印的嵌入。不同的分块图像嵌入相同的水印，即分块图像的各个分类的统计值是一致的，我们在图像合并之后，水印提取算法没有变化，而水印的鲁棒性得到了加强，同时，水印方案能够抵抗 JPEG 压缩，即使在质量因子为 10%的情况下，也能够可靠的提取出嵌入比特。

2004-01-12 收到，2004-09-17 改回
国家重点基础研究发展规划项目(1999035804)、国家自然科学基金(60073049)和国家重点实验室基金(51436060101DZ0801)资助课题

本文的安排如下：第 2 节提出通用的水印解决方案，第 3 节进行方案的安全性分析，第 4 节详细描述水印算法的流程，第 5 节分析试验结果，最后是总结。

2　水印方案

2.1 嵌入部分

为了适应 JPEG 压缩，我们选择在图像的 DCT 系数上进行微小修改。我们将图像所有的 DCT 系数看成数据集合，在这个集合中，元素没有顺序和结构的特征。

我们将 DCT 系数集合分成 M 类，每类 N 个元素。在每一类中嵌入 1 个比特，我们将嵌入 M 比特。记每类的正数个数为 $Z(i)$，负数个数为 $F(i)$，i 表示类别，如果二值水印 $wm(i)$=1(或者＝0)，则判断 $Z(i)$是否大于(或者小于)$F(i)$，若是，则不修改；否则，调整 $Z(i)$和 $F(i)$中绝对值小于 δ 的值到 0。这样，就完成了水印的嵌入。

2.2 提取部分

图像 DCT 系数集合的分类必须依靠密钥，如果没有密钥，很难找到相同的分类，这说明单纯就分类而言，攻击将是指数增长的计算量问题。这大大增强了水印系统的安全性。

水印的提取将很简单，在 DCT 系数的分类中，判断各分类中正数与负数的关系，即可提取水印：

如果 $Z(i)>F(i)$，则 $wm(i)$=1；

如果 $Z(i)<F(i)$，则 $wm(i)$=0。

2.3 方案分析

每多合并一个分块图像之后，其 DCT 系数的集合元素就会增多。但是我们分类的数目没有变化，每个分类的元素都有增加，增加部分是由分块图像的对应的分类的元素组成，由于分块图像嵌入了相同的水印，因此每类元素的正数和负数的关系没有变化。对整个分类而言，其统计关系得到了加强，更有利于水印提取。具体方案流程如图 1 所示。

水印方案中分类算法是重要的组成部分，它提供了系统的部分安全性。在上述水印算法中，我们确定图像的分块 DCT 系数为水印嵌入的载体，对载体数据的分类算法需要满足两个基本条件：其一是分类算法必须确保每个类别包含足够的数据，即不存在空类，同时各类包含的数据要大于一定的数目，这样的类别中我们才可以统计承载水印的特征，才能确定在水印嵌入过程中要修改的数据和修改的强度；其二是分类算法对于不同的载体数据是固定的，这里的固定的涵义是指分块图像的载体数据的相同分类，在图像合并之后，合并的载体数据的分类应该等于分块时载体数据分类的直接叠加，即相同分类在合并操作之后合并到了同一个分类之中。

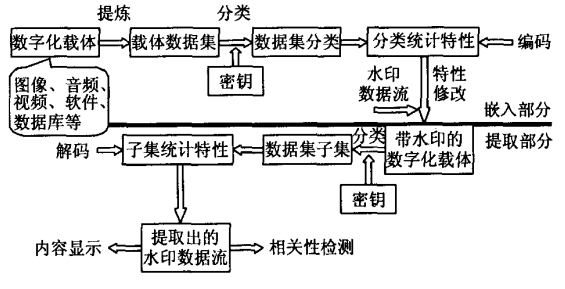


图 1　抗图像合并的水印方案流程图

我们在此提出分类算法的一个简单实例来说明如何设计分类算法。为简单起见，我们以载体数据的坐标数据作为分类的依据，并且使每个分类都有相同数目的数据。假设要嵌入 32bit 数据，我们的分块图像为 128×128 像素，对该分块图像作 8×8 分块 DCT 变换，将分块 DCT 系数做 Zigzag 扫描，得到 256×64 个系数，这里共有 256 个分块，每块 64 个系数，记为 $A(i,j)$，$i=1,\cdots,256$，$j=1,\cdots,64$。我们设 $\mathrm{FL}(j)=\{A(i,j+s)\,|\,i=1,\cdots,256\}$，$j=1,\cdots,32$（$s$ 固定，例如 s=5)。这样我们就简单的将部分 DC 系数作了 32 个分类。

这个分类算法与上述算法设计的基本条件比较，首先是不存在空类，每类都具有相同数目的数据，其次是图像合并时，来自不同分块图像的相同分类合并为同一个分类。这样的算法是有效的。

如果载体数据集合数目很小时，该系统是不安全的。因为系统安全性完全基于算法的保密，如果算法公开，载体数据集合分类可以被猜测；如果统计特性编码比较简单，统计特性在攻击之后难以保持，将导致安全性丧失。

3　安全性分析

上节提到的分类算法，仅仅考虑了 $A=\{A(i,j)\}_{j=6,\cdots,33}^{i=1,\cdots,256}\in A$ 中的 AC 系数，这样 32 个分类都有 256 个数据。假设我们确定实际的载体就是这 $N=|A|$ 个系数，如果要嵌入 Mbit，并且每类数目相等，则每类数目 $L=N/M$，我们取集合 A 的一个排列 $P=\Pi(A)$，Π 为排列算子，依次按照顺序从 P 中每取出 L 个数据即组成一个分类，记 $\mathrm{FL}(i)=\Pi_i(A)$，$i=1,\cdots,M$。这里的分类算子 Π_i 就是分类密钥，而且这排列算子必须满足下述基本条件：

$$\Pi_i(A)+\Pi_i(A)=\Pi_i(A+B),\quad \forall A,B\in A$$

这里的“+”表示集合元素的相加。满足这个条件的分类算子就可以适用于我们提出的水印方案。

水印算法中的分类算法提供了基于算法的安全性，如果不知道水印嵌入的实际载体，不知道载体的分类算法，可能使攻击者无从下手。载体数据集合按照密钥分类，为系统提供了强大的保护，可以证明，在适当的假设条件下，系统的安全性与载体数据集合大小成指数增长关系。假设载体数据集合 X 的大小为$|X|$，它所有分类的可能为 $|X|^{|X|}$ 的数量级，

因此猜测分类是非常困难的。

载体集合分类的统计特性的编码增强了系统的安全性，当分类的统计特性自由度多时，这种安全性得到加强。上节提出判断分类中正数与负数的个数的比较，作为水印信息的编码特性，仅仅是利用了载体数据的符号特性，我们还可以针对载体数据的奇偶性、模数的同余性等来设计承载水印信息的编码方案，具体的设计方案需要实际的系统需求来综合考虑。

4 水印算法

根据上述方案，我们提出一个基于 DCT 变换的实际算法。该算法既可以实现图像合并之后水印依然可以提取，还可以抵抗图像的 JPEG 压缩。

我们假设水印长度为 Mbit，因此我们将 DCT 系数集合分成 M 类，记为 $\mathrm{FL}(i)$，$i=1,\cdots,M$，分类方法由密钥 $K=\{\Pi_i\}_{i=1,\cdots,M}$ 决定。

4.1 嵌入算法

(1) 对图像作 8×8 分块 DCT 变换，由密钥 K 计算 DCT 系数的分类 $\mathrm{FL}(i)$，$i=1,\cdots,M$；

(2) 对 $\mathrm{FL}(i)$ 量化后取整为 $\lfloor\lambda(\mathrm{FL}(i))\rfloor$，尾数记为 $\mathrm{WFL}(i)=\lambda(\mathrm{FL}(i))-\lfloor\lambda(\mathrm{FL}(i))\rfloor$，量化函数 $\lambda(\cdot)$ 中的量化步长取自 JPEG 压缩标准量化矩阵；

(3) 计算 $\lfloor\lambda(\mathrm{FL}(i))\rfloor$ 的取正数的数目 $Z(i)$，取负数的数目 $F(i)$；

(4) 计算满足 $0<\lfloor\lambda(\mathrm{FL}(i))\rfloor<\delta$，及 $-\delta<\lfloor\lambda(\mathrm{FL}(i))\rfloor<0$ (这里 $\delta>0$ 称为水印的**嵌入修改强度**)区间中 i 的集合 index_+ 和 index_-，记 $|\mathrm{index}_-|$ 和 $|\mathrm{index}_+|$ 分别表示这两个集合的势；

(5) 根据要嵌入的比特值判断：

嵌入 1 如果 $Z(i)>F(i)+q$ (这里 q 称为水印的**鲁棒性强度**)则不需要处理；

否则，如果 $|\mathrm{index}_-|\geq q-(Z(i)-F(i))+1$，则随机选择 index_- 集合中的 $q-(Z(i)-F(i))+1$ 项，将其数值更改为 0；如果 $0.5\times(q-(Z(i)-F(i))+1)\leq|\mathrm{index}_-|<q-(Z(i)-F(i))+1$，则随机选择 index_- 集合中的 $0.5\times(q-(Z(i)-F(i))+1)$ 项，将其数值更改为相反数；其它，调整 δ 的值，回到第 4 步。

嵌入 0 如果 $F(i)>Z(i)+q$，则不需要处理；

否则，如果 $|\mathrm{index}_+|\geq q-(F(i)-Z(i))+1$，则随机选择 index_+ 集合中的 $q-(F(i)-Z(i))+1$ 项，将其数值更改为 0；如果 $0.5\times(q-(F(i)-Z(i))+1)\leq|\mathrm{index}_+|<q-(F(i)-Z(i))+1$，则随机选择 index_+ 集合中的 $0.5\times(q-(F(i)-Z(i))+1)$ 项，将其数值更改为相反数；其它，调整 δ 的值，回到第四步。

这里 $q>0$ 是水印的鲁棒性强度，$\delta>0$ 是水印的嵌入修改强度。我们希望 q 足够大，而 δ 足够小。

(6) 将嵌入水印的 $\lfloor\lambda(\mathrm{FL}(i))\rfloor$ 系数加上尾数 $\mathrm{WFL}(i)=\lambda(\mathrm{FL}(i))-\lfloor\lambda(\mathrm{FL}(i))\rfloor$，然后乘上对应的量化步长，代入载体数据集，通过逆 DCT 变换，恢复成嵌入水印的图像。

4.2 提取算法

(1) 将图像 8×8 分块进行 DCT 变换，得到 DCT 系数集合；

(2) 按照密钥提取分类，提取 $\mathrm{FL}(1)$ 到 $\mathrm{FL}(M)$；

(3) 计算 $\mathrm{FL}(i)$ 的取正数的数目 $Z(i)$，取负数的数目 $F(i)$；

(4) 判断：如果 $Z(i)>F(i)$，则水印比特 $w(i)=1$；否则 $w(i)=0$。

(5) 显示水印比特或者进行相关性检测，判断水印存在与否。

5 试验结果分析

我们试验采用 256×256 的 256 灰度 Lena 图像，嵌入水印分别为随机生成的 8bit、16bit、32bit，嵌入水印前后的 Lena 图像在视觉上是不可区分。嵌入水印前后图像的比较如图 2 所示。试验中我们取水印鲁棒性强度 q=5，水印嵌入的修改强度 δ<2。

(a) Lena 原图　(b) 嵌入 8bit 水印的 Lena 图像

(c) 嵌入 16bit 水印的质量因子为 10% 的 LenaJPEG 图像　(d) 嵌入 32bit 水印的质量因子为 10% 的 LenaJPEG 图像

图 2 嵌入水印前后及压缩后的 Lena 图像比较

根据 $SNR = 20\lg\sqrt{\sum_i\sum_j a_{ij}^2}\Big/\sqrt{\sum_i\sum_j (a_{ij}-b_{ij})^2}$，$PSNR = 20\lg\dfrac{b_m}{\sqrt{\dfrac{1}{M\times N}\sum_i\sum_j (a_{ij}-b_{ij})^2}}$，得到嵌入水印的信噪比和峰值信噪比分别为

$SNR_8 = 25.5409\text{dB}$，$PSNR_8 = 32.4701\text{dB}$

$SNR_{16} = 25.5278\text{dB}$，$PSNR_{16} = 32.4569\text{dB}$

$SNR_{32} = 25.3479\text{dB}$，$PSNR_{32} = 32.2770\text{dB}$

这里 a_{ij}、b_{ij} 表示嵌入水印前后的图像像素值，b_m 表示图像像素的最大值。

我们将嵌入水印的 Lena 图像进行 JPEG 压缩，压缩方法采用 Fldsee5.0 自带的存储功能，我们将 bmp 图像存储为质量因子为 90、80、70、60、50、30、20、10 的 JPEG 图像，然后分别进行水印提取，提取出来的效果非常好，即使在质量因子为 10%的 JPEG 压缩图像里，我们提取的水印比特正确率为 100%。如表 1 所示。

表 1 水印提取正确率与图像质量因子的关系

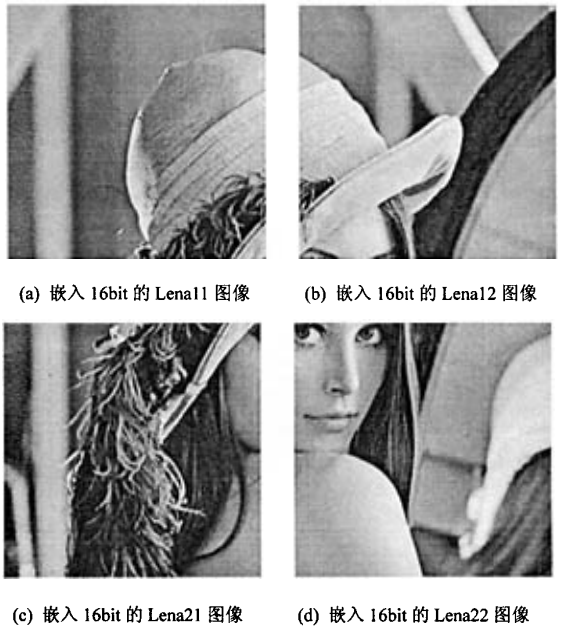
图像格式	图像大小 (Byte)	质量因子	压缩比(%)	水印提取正确率(%)
bmp	66,614	100	100	100
jpg	12,036	90	18.07	100
jpg	10,115	80	15.18	100
jpg	9,104	70	13.67	100
jpg	8,726	60	13.10	100
jpg	8,237	50	12.37	100
jpg	7,856	40	11.79	100
jpg	7,683	30	11.53	100
jpg	7,503	20	11.26	100
jpg	7,417	10	11.13	100

显然，这种方法对 JPEG 压缩是具有完全的鲁棒性。

我们将 521×512 的 Lena256 原始灰度图像分成 4 等份，每份 256×256 像素，分别嵌入相同的水印比特，如图 3 所示。我们将嵌入水印的 4 幅图像合并起来，重新构成 512×512 的 Lena 图像，然后从中提取水印，试验发现，水印强度得到加强，效果非常理想，水印能够完美的提取出来。实际上，我们只要分块图像的大小是由整数个 8×8 块组成，每块嵌入相同的水印，不管多少分块图像合并在一起，我们都可以在合并后的整体图像中提取出水印。

由统计思想设计的水印方案最大的缺陷是隐藏容量不大，隐藏容量与安全性存在一定的矛盾，但隐藏容量越小水印的鲁棒性越强，因此可以根据实际的需求，安排容量、安全性、鲁棒性三者之间的关系。

系统隐藏容量首先与分块图像的最小尺寸相关，因为不同分块图像嵌入相同的水印，最小的分块图像包含了所有水印信息；其次分类中数据的只嵌入 1bit 水印制约了水印的容量。增加水印的容量，可以从分类方法的改进着手，在保证每个分类有一定数目的数据的同时，将载体数据分成更多的分类；再次水印的嵌入算法，利用同一分类中数据的不同统计特性，将多比特嵌入在同一个分类中，如除了符号特性外，可以考虑数据的某一位的奇偶特性或者模数的同余性等，这些特性能否应用，将是下一步的研究工作。



(a) 嵌入 16bit 的 Lena11 图像　(b) 嵌入 16bit 的 Lena12 图像

(c) 嵌入 16bit 的 Lena21 图像　(d) 嵌入 16bit 的 Lena22 图像

图 3　分块图像分别嵌入相同的水印

6　结束语

数字水印系统的发展促使版权保护的应用不断出现新的需求，基于图像的合并是数字水印应用中出现的新问题，嵌入水印的图像在合并后是否还具有鲁棒性，以前的文献很少考虑。本文从工程实际出发，研究这一类满足需求的水印系统方案，设计了一种抗图像合并和抗 JPEG 压缩的图像水印算法，试验结果显示，该算法具有很强的鲁棒性和抗合并性。目前，在图像数据库和建筑 CAD 设计图纸的版权保护中，该算法得到了工程上的实际应用，取得了很好的效果。

参 考 文 献

[1]　吴秋新，钮心忻，杨义先，等. 信息隐藏技术－隐写术与数字水印. 北京：人民邮电出版社，2001.

[2] Cox I J, Miller M L. A review of watermarking and the importance of perceptual modeling. in Proc. SPIE Conf. Human Vision and Electronic Imaging II, 1997, Vol. 3016: 92 – 99.

[3] Herrera-Joancomartí J, Minguillón J, Megías D. A family of image watermarking schemes based on lossy compression. ITCC 2003, Proceedings. International Conference on Information Technology: Coding and Computing [computers and Communications], Las Vegas, Nevada USA, April 28 – 30, 2003: 559 – 563.

[4] Noore A. An improved digital watermarking technique for protecting JPEG images. ICCE 2003. IEEE International Conference on Consumer Electronics, Los Angeles, California USA, June 17 – 19, 2003: 222 – 223.

[5] Li Kan, Zhang Xiao-Ping. An image watermarking method integrating with JPEG-2000 still image compression standard. CCECE 2003, IEEE Canadian Conference on Electrical and Computer Engineering, Montreal, Canada, May 4 – 7, 2003. Vol.3: 2051 – 2054.

[6] Li Yuanyuan, Xu Luping. A blind watermarking of vector graphics images. ICCIMA 2003. Fifth International Conference on Computational Intelligence and Multimedia Applications, Xi'an, P.R.China, Sept 27 – 30, 2003: 424 – 429.

[7] Ohbuchi R, Ueda H, Endoh S. Watermarking 2D vector maps in the mesh-spectral domain. SMI 2003. International Conference on Shape Modeling and Applications, Seoul, Korea, May 12 – 15, 2003: 216 – 225.

[8] Staring M, Oostveen J, Kalker T. Optimal distortion compensation for quantization watermarking. ICIP 2003. IEEE International Conference on Image Processing, Barcelona Spain, Sept. 14 – 17, 2003, Vol. 2: 727 – 730.

[9] Ashourian M, Ho Yo-Sung. Analysis of quantization watermarking in the wavelet transform domain. ISSPA 2003. Seventh International Symposium on Signal Processing and Its Applications, Paris, France, July 1 – 4, 2003, Vol. 2: 375 – 378.

伍宏涛： 男，1973年生，工程师，博士生，研究方向为信息隐藏、数字水印、保密通信等.

胡 云： 男，1974年生，助理研究员，博士生，研究方向为信息隐藏、数字水印、现代密码等.

钮心忻： 女，1963年生，博士，副教授，主要研究方向包括：软件无线电、伪装式信息安全、信息隐藏、数字水印、数字信号处理.

杨义先： 男，1961年生，博士，教授，博士生导师，主要研究方向为编码密码学、信息与网络安全、信号与信息处理等.