

# 基于视觉掩蔽的半脆弱水印技术研究

王向阳<sup>1),2)</sup> 杨红颖<sup>1)</sup> 陈利科<sup>1)</sup> 赵红<sup>1)</sup>

<sup>1)</sup>(辽宁师范大学计算机与信息技术学院,大连 116029) <sup>2)</sup>(中国科学院软件研究所信息安全国家重点实验室,北京 100039)

**摘要** 以人眼视觉系统的掩蔽特性为基础,提出了一种基于分组量化的自适应半脆弱水印嵌入方案,该方案能够在不参考原始载体的情况下对数字图像同时进行版权保护和内容认证。仿真实验结果表明,所提出的半脆弱水印方案不仅具有较好的透明性,对 JPEG 压缩、叠加噪声、平滑滤波等常规图像处理操作具有较好的鲁棒性,而且能够对剪切、替换等恶意图像篡改做出报警并确定被篡改位置。同时常规图像处理下其误检率与漏检率均比较低。

**关键词** 半脆弱水印 视觉掩蔽特性 分组量化

中图分类号: P391 文献标识码: A 文章编号: 1006-8961(2005)12-1548-06

## A New Semi-fragile Image Watermarking Based on Visual Masking

WANG Xiang-yang<sup>1),2)</sup>, YANG Hong-ying<sup>1)</sup>, CHEN Li-ke<sup>1)</sup>, ZHAO Hong<sup>1)</sup>

<sup>1)</sup>(School of Computer and Information Technique, Liaoning Normal University, Dalian 116029)

<sup>2)</sup>(State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100039)

**Abstract** A new semi-fragile image watermarking algorithm based on visual masking is proposed in this paper. On the basis of the visual masking of human visual system, the watermark can be adaptively embedded into host image in the wavelet domain by using group quantization in our algorithm. The proposed semi-fragile watermarking is effective for copyright protection and content authentication simultaneously without resorting to the original host image. Experimental results show that our semi-fragile watermarking scheme is invisible and is robust to common image processing (such as JPEG compression, noise adding, filtering). The proposed watermarking algorithm is fragile to content modification (such as cropping), can detect effectively the tampered regions, and has a lower probability of missing and lower probabilities of a false alarm compared with other popular semi-fragile watermarking schemes.

**Keywords** semi-fragile watermarking, visual masking, group quantization

## 1 引言

作为数字媒体作品知识产权保护的一种有效手段,数字水印(digital watermarking)技术得到了广泛关注,并已成为国际学术界的一个研究热点<sup>[1]</sup>。依据应用范围,通常可以把数字水印技术划分为图像水印技术、视频水印技术和音频水印技术。而根据含水印信号的抗攻击能力,又可将数字水印划分为鲁棒水印、脆弱水印和半脆弱水印。其中,鲁棒水印对常见的信号处理方法都具有鲁棒性;脆弱水印对

任何信号处理都非常敏感;半脆弱水印对特定的信号处理方法有鲁棒性而对其他的信号处理方法无鲁棒性。考虑到实际应用中,数字图像一般数据量较大,需要以压缩方式存储及传输,且最终用户所需通常是原始图像经压缩或其他保持图像内容的操作处理后的图像,因此,半脆弱图像水印技术更为实用,其在网络时代具有更重要的应用价值。

近年来,图像数字水印技术的研究取得了很大进展,陆续提出了诸如空域、变换域、压缩域、基于统计学、基于生理模型等多种图像水印算法<sup>[2]</sup>。然而,现有图像水印算法绝大多数是鲁棒型和脆弱型

基金项目:辽宁省自然科学基金项目(20032100);信息安全国家重点实验室开放基金项目(03-02)

收稿日期:2004-06-16;改回日期:2005-03-21

第一作者简介:王向阳(1965~),男,教授,硕士。主要研究领域为网络信息安全技术、多媒体信息处理技术。E-mail:wxy37@263.net

的,半脆弱型图像水印算法研究显得相对滞后,已有的半脆弱型水印算法普遍存在透明性较差、对某些常规信号处理不够鲁棒、常规图像处理下误检率与漏检率较高等不足<sup>[3-8]</sup>。

以人眼视觉掩蔽特性为基础,提出了一种基于分组量化的自适应半脆弱水印嵌入方案,该方案能够在不参考原始载体的情况下对数字图像同时进行版权保护和内容认证。实验结果表明,所提出的半脆弱水印方案不仅具有较好的透明性,对 JPEG 压缩、叠加噪声、平滑滤波等常规图像处理操作具有较好的鲁棒性,而且能够对剪切、替换等恶意图像篡改做出报警并确定被篡改位置。同时常规图像处理下其误检率与漏检率均比较低。

## 2 基于掩蔽特性的半脆弱水印技术

### 2.1 视觉掩蔽特性值的计算

对于图像来说,人眼视觉系统(HVS)的掩蔽特性主要表现在 3 个方面,即亮度特性、频域特性和图像类型特性<sup>[9]</sup>。其中,亮度特性是最基本的一种,主要关于人眼对亮度变化的敏感性。一般说来,人眼对高亮度区域所附加噪声的敏感性较小,这意味着,如果图像的背景亮度越高,那么它所能嵌入的附加信息就越多。对于频域特性来说,如果将图像从空域变换到频域,则频率越高,人眼的分辨能力就越

低;而频率越低,人眼的分辨能力就越高。人眼视觉系统的频域特性告诉我们,人眼对高频内容的敏感性较低。从图像类型特性来说,图像可分为平滑区域和纹理区域。人眼的视觉系统对于平滑区域的敏感性要远高于纹理密集区域,也就是说,图像中的纹理越密集,其所能够嵌入的信息就越多。

为了很好地刻画人眼的视觉掩蔽特性,以下结合文献[9]所建立的视觉掩蔽模型,给出小波域的视觉掩蔽特性值计算方法。假设

(1)原始图像为  $I_{M \times N}$ ,  $M$  和  $N$  分别表示原始图像的高度和宽度;

(2)已对原始图像  $I_{M \times N}$  进行  $l$  级小波分解,并得到  $3 \times l + 1$  个不同小波子带的小波矩阵。

则小波域的视觉掩蔽特性值为

$$T_l^\theta(x, y) = \lambda(l, \theta) \Lambda(l, x, y) \Xi(l, x, y) \quad (1)$$

其中,  $l$  表示小波分解层次,  $\theta \in \{LL, LH, HL, HH\}$  表示子带的方向;  $x, y$  表示小波系数位置。具体请参见文献[9]。

### 2.2 半脆弱水印嵌入算法

设原始载体为 256 级灰度图像  $I = \{g(i, j), 1 \leq i \leq M, 1 \leq j \leq N\}$ , 数字水印为二值图像  $W = \{w(i, j), 1 \leq i \leq P, 1 \leq j \leq Q\}$ 。其中,  $g(i, j)$  和  $w(i, j)$  分别代表原始载体图像和二值水印图像的第  $i$  行、第  $j$  列像素灰度值。则半脆弱图像水印嵌入过程(关键步骤)如图 1 所示。

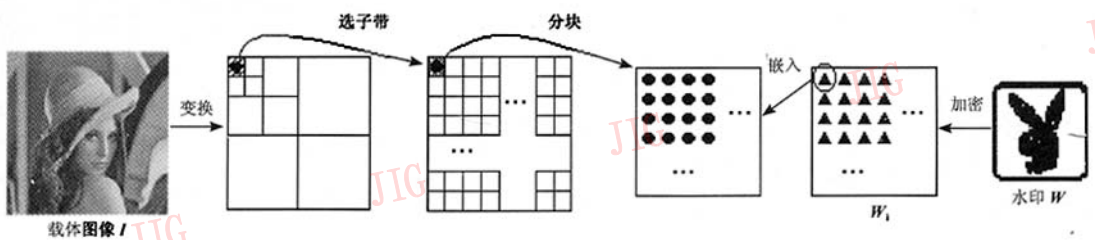


图 1 数字水印嵌入的基本步骤

Fig. 1 The watermark embedding

#### 2.2.1 水印图像的置乱加密

为了消除二值水印图像的像素空间相关性,满足数字水印的安全性要求,以确保图像某一部分受到破坏后仍能全部或部分地恢复水印,应首先对二值水印图像进行置乱加密。这里采用文献[10]的 Arnold 变换对二值水印图像进行置乱加密。设

$$W_1 = \{w_1(i, j) \in \{0, 1\}, 1 \leq i \leq P, 1 \leq j \leq Q\}$$

为已置乱二值水印矩阵。

#### 2.2.2 原始载体图像的小波变换与子带选取

对原始载体图像  $I$  实施  $L$  级小波变换,可得到一系列不同分辨率及不同方向的多种子带。为了有效进行版权保护和内容认证,选取小波变换域的低频区( $T_L^L$  子带)作为数字水印嵌入区,这是因为:

(1)水印编码可看作是在强背景(原始图像)下叠加

一个弱信号(水印)。只要叠加的信号低于对比度门限,视觉系统就无法感觉到信号的存在。而根据 Weber 定律,对比度门限和背景信号的幅值成正比例。由于低频系数的幅值一般远大于高频系数,故低频系数具有比较大的感觉容量。也就是说,在低频系数内嵌入水印信息不会引起原始图像视觉质量的明显改变。(2)根据信号处理理论,嵌入水印的图像最有可能遭遇到的常规信号处理过程,如 JPEG 压缩、叠加噪声、平滑滤波等,对低频系数的保护比高频系数好。

同时,为了更好地发挥小波变换作用,应依据载体图像大小确定小波变换级数  $L$ 。一般说来,载体图像尺寸(长和宽)较大,对其进行小波变换的级数也应该比较大;反之,若载体图像尺寸(长和宽)较小,对其进行小波变换的级数也应该比较小。结合实验给出了小波变换级数  $L$  的自适应确定方法,即

$$L = \log_2 \left( \frac{\min(M, N)}{2^7} \right)$$

### 2.2.3 所选子带的分块与数字水印的嵌入

采用自适应量化调制小波系数方法,将已置乱二值水印矩阵  $W_1$  嵌入到小波变换域的低频子带  $I_L^{LL}$  内。具体步骤为

(1)将小波变换域的低频子带  $I_L^{LL}$  划分成大小为  $\frac{M}{P2^L} \times \frac{N}{Q2^L}$  的图像子块(每个图像子块内仅嵌入 1 个比特的水印信息)。

(2)计算图像子块所含元素(系数)的绝对值和  $S(i, j)$  ( $i = 1, 2, \dots, P; j = 1, 2, \dots, Q$ ),然后用  $\Delta$  对其进行量化,再根据量化结果修改图像子块内元素值,以完成水印信息的嵌入。数字水印的嵌入规则为

如果  $\text{mod}(q(i, j), 2) \neq w_1(i, j)$ , 则

$$I_L^{LL}(m_i, n_j) = \begin{cases} I_L^{LL}(m_i, n_j) - \text{sign}(I_L^{LL}(m_i, n_j)) \times \\ \Delta/2 + \text{rem}(I_L^{LL}(m_i, n_j), \Delta) & I_L^{LL}(m_i, n_j) \geq 0 \\ I_L^{LL}(m_i, n_j) + \text{sign}(I_L^{LL}(m_i, n_j)) \times \\ \Delta/2 - \text{rem}(I_L^{LL}(m_i, n_j), \Delta) & I_L^{LL}(m_i, n_j) < 0 \end{cases}$$

如果  $\text{mod}(q(i, j), 2) = w_1(i, j)$ , 则

$$I_L^{LL}(m_i, n_j) = \begin{cases} I_L^{LL}(m_i, n_j) + \text{sign}(I_L^{LL}(m_i, n_j)) \times \\ \Delta/2 - \text{rem}(I_L^{LL}(m_i, n_j), \Delta) & I_L^{LL}(m_i, n_j) \geq 0 \\ I_L^{LL}(m_i, n_j) - \text{sign}(I_L^{LL}(m_i, n_j)) \times \\ \Delta/2 + \text{rem}(I_L^{LL}(m_i, n_j), \Delta) & I_L^{LL}(m_i, n_j) < 0 \end{cases}$$

其中,  $\Delta$  为量化步长,  $i = 1, 2, \dots, P, j = 1, 2, \dots, Q, m = 1, 2, \dots, M/(P2^L), n = 1, 2, \dots, N/(Q2^L)$ , 且

$$S(i, j) = \sum_{m=1}^{M/(P2^L)} \sum_{n=1}^{N/(Q2^L)} |I_L^{LL}(m_i, n_j)|$$

$$q(i, j) = \left\lfloor \frac{S(i, j)}{\Delta} \right\rfloor$$

$$\text{sign}(x) = \begin{cases} 1 & x \geq 0 \\ -1 & x < 0 \end{cases}$$

$$\text{rem}(x, y) = x - \text{fix}\left(\frac{x}{y}\right) \cdot y$$

$\text{fix}\left(\frac{x}{y}\right)$  是返回  $\frac{x}{y}$  的整数部分。

不难看出,与现有图像水印嵌入方法<sup>[3,7,8]</sup>普遍采纳单系数量化策略(即  $q(x, y) = \left\lfloor \frac{I(x, y)}{\Delta} \right\rfloor, I(x, y)$  为单个小波系数)不同,本文算法采用了分块系数量化方案(即  $q(x, y) = \left\lfloor \frac{S(x, y)}{\Delta} \right\rfloor, S(x, y)$  为图像子块内小波系数绝对值和),其充分利用了相邻系数之间的相关特性,故必然提高对 JPEG 压缩之类常规处理操作的鲁棒性。

另外,对基于量化的图像水印嵌入方法来说,量化步长  $\Delta$  的选取至关重要。因为量化步长  $\Delta$  与水印嵌入强度密切相关,  $\Delta$  取值越大,数字水印鲁棒性能越好(但同时也更容易给图像引入失真)。选取确定量化步长  $\Delta$  应充分考虑图像自身特点和人眼视觉特性。然而,现有图像水印嵌入方案<sup>[3,7,8]</sup>普遍采用了均匀量化策略,即对整幅图像采用一个相同的量化步长  $\Delta$ 。这样,如果取值  $\Delta$  较小,则会影响水印的抗攻击性;而如果  $\Delta$  取值较大,则会给图像质量带来较大影响。另外,不同的载体图像,只有采纳不同的量化步长  $\Delta$  值才能各自达到比较好的隐藏效果。

为此,引入了反映人眼视觉感知特性的视觉掩蔽特性值计算模型,并依据小波域相邻子带相关性,利用相同分解级的两个相邻子带  $I_L^{LH}$  和  $I_L^{HL}$  内相同位置的视觉掩蔽特性值  $T_i^q(x, y)$  来预测小波系数上嵌入的量化步长  $\Delta$  值,即结合载体图像邻域特性自适应确定量化步长

$$\Delta(i, j) = \ln \left\{ \left[ \sum_{m=1}^{M/(P2^L)} \sum_{n=1}^{N/(Q2^L)} |T_L^{LH}(m_i, n_j)| + \sum_{m=1}^{M/(P2^L)} \sum_{n=1}^{N/(Q2^L)} |T_L^{HL}(m_i, n_j)| \right] / 2 \right\}$$

显然,对原始载体图像的纹理复杂区域而言,

与待量化小波系数处于同一分解级相邻子带(LH子带和HL子带)内相应位置的视觉掩蔽特性值 $T_i^0(x,y)$ 相对较大,故有比较大的量化步长 $\Delta$ 值,于是实现了嵌入强度与区域特性的自适应。同时,对数运算可将小波系数的指数增长转为线性增长方式,会带来更小的失真,更加符合人眼的视觉特性。

2.2.4 逆小波变换

用含有数字水印信息的小波系数 $I'_L{}^{LL}(m_i, n_j)$ 代替 $I_L{}^{LL}(m_i, n_j)$ 并结合未修改的小波系数进行 $L$ 级逆小波变换,便可得到含水印信息的灰度图像 $I'$ 。

2.3 半脆弱水印提取算法

水印提取是水印嵌入的逆步骤。在数字水印提取过程中,含水印图像首先进行小波变换,然后在已知所选择子带上通过图像子块划分、自适应反量化等措施来提取数字水印信息,整个水印提取过程不需要原始载体图像。数字水印的提取步骤如下(设含水印图像为 $I'$ ):

(1)对含水印图像 $I'$ 实施 $L$ 级小波变换,并选取低频子带 $I'_L{}^{LL}$ 用于水印提取。

(2)将所选子带 $I'_L{}^{LL}$ 划分成大小为 $\frac{M}{P2^L} \times \frac{N}{Q2^L}$ 的图像子块,并从图像子块内提取水印信息 $W'_1$ 。提取方法可以表示为

$$S'(i,j) = \sum_{m=1}^{M/(P2^L)} \sum_{n=1}^{N/(Q2^L)} |I'_L{}^{LL}(m_i, n_j)|$$

$$q'(i,j) = \left\lfloor \frac{S'(i,j)}{\Delta} \right\rfloor$$

$$w'_1(i,j) = \begin{cases} 0 & \text{mod}(q'(i,j), 2) = 0 \\ 1 & \text{mod}(q'(i,j), 2) = 1 \end{cases}$$

其中, $w'_1(i,j) \in W'_1, i=1, 2, \dots, P, j=1, 2, \dots, Q$ ,量化步长 $\Delta$ 取值为

$$\Delta'(i,j) = \ln \left\{ \left[ \sum_{m=1}^{M/(P2^L)} \sum_{n=1}^{N/(Q2^L)} |T_L{}^{LH}(m_i, n_j)| + \sum_{m=1}^{M/(P2^L)} \sum_{n=1}^{N/(Q2^L)} |T_L{}^{HL}(m_i, n_j)| \right] / 2 \right\}$$

3 版权的判断和恶意篡改的认证

设 $W_1$ 是置乱原始水印图像 $W$ 而得到的二值水印矩阵, $W'_1$ 为从接收到含水印图像 $I'$ 中所提取出的二值水印矩阵,则版权信息判断与恶意篡改认证的具体步骤为

(1)定义篡改矩阵 $\tilde{W}_1$ (篡改矩阵 $\tilde{W}_1$ 中元素为1的区域意味着该区域可能被篡改)

$$\tilde{W}_1 = W'_1 \oplus W_1 (\oplus \text{为异或运算})$$

(2)对篡改矩阵 $\tilde{W}_1$ 进行中值滤波( $2 \times 2$ )。实验结果表明,可以通过篡改矩阵 $\tilde{W}_1$ 确定篡改发生位置,而对含水印图像实施JPEG压缩、叠加噪声、平滑滤波等常规处理操作后,由 $\tilde{W}_1$ 所确定出的篡改发生区域呈均匀分布或随机分布。当对篡改矩阵 $\tilde{W}_1$ 进行中值滤波( $2 \times 2$ )以后,由常规图像处理操作所引起的篡改区域大部分将被删除。

(3)定义篡改比率

$$\tilde{F}_1 = \frac{\sum_{i=1}^P \sum_{j=1}^Q \tilde{w}_1(i,j)}{P \times Q}$$

其中, $\tilde{w}_1(i,j) \in \tilde{W}_1$ ( $\tilde{W}_1$ 已经过中值滤波)。

(4)适当选取阈值 $T$ ,进行版权信息判断与恶意篡改认证。规则如表1所示。

表 1 判断认证规则

Tab.1 The rule for identification

条件	结果
$\tilde{F}_1 = 0$	未遭受任何攻击
$\tilde{F}_1 < T$	已遭受常规图像处理攻击
$\tilde{F}_1 > T$	已遭受恶意篡改攻击

另外,对内容已被恶意篡改的不可靠图像来说(即 $\tilde{F}_1 > T$ ),可以通过篡改矩阵 $\tilde{W}_1$ 确定篡改发生区域(即 $\tilde{w}_1(i,j) = 1$ 处图像子块)。

4 实验结果

为验证本文算法的鲁棒性、脆弱性和高效性,给出了 $512 \times 512 \times 8\text{bit}$ 标准灰度图像(Lena和Barbara)的实验结果,并与Fridrich法<sup>[5]</sup>、Queluz法<sup>[6]</sup>及Liao法<sup>[7]</sup>进行了对比。实验中,数字水印选用了 $32 \times 32$ 的二值图案“Rabbit”,小波变换采用了常见的Haar小波基。检测阈值选取为 $T = 0.35$ 。图2(a)、(c)为嵌入了水印信息的标准图像(Lena和Barbara),其峰值信噪比分别为41.6dB和41.2dB,均远大于Fridrich法<sup>[5]</sup>、Queluz法<sup>[6]</sup>及Liao法<sup>[7]</sup>建议的38dB,而且视觉上与原图像没有区别。

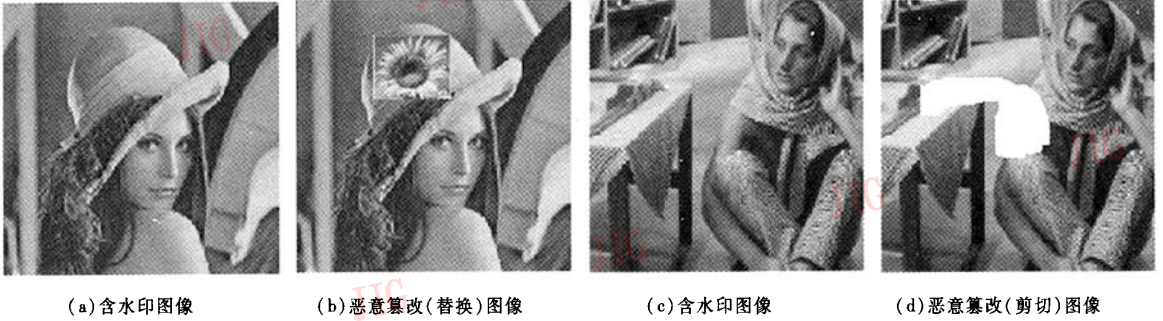


图 2 篡改检测实验结果

Fig.2 The tampered region detection

4.1 对常规图像处理的鲁棒性

为了测试算法的鲁棒性,使用 JPEG 压缩、叠加噪声、平滑滤波等常规信号处理方法对含水印图像进行了处理。表 2 给出了部分测试结果。图 3 给出了从受攻击的含水印图像 Barbara 中抽取出的水印图像。其中,图 3(a)为原始水印图像,图 3(b)为直接从含水印图像 Barbara 中提取出的二值水印图像,未受到任何攻击(归一化相关系数  $NC = 0.993$ )。图 3(c)是进行 JPEG 压缩(压缩比为 32)后提取的水印( $NC = 0.783$ );图 3(d)是进行 JPEG2000 压缩(压缩比为 32)后提取的水印( $NC = 0.851$ );图 3(e)是添加高斯噪声(30dB)后提取的水印( $NC = 0.950$ );图 3(f)是中值滤波( $3 \times 3$ )后提取的水印( $NC = 0.923$ )。

表 2 常规图像处理后的检测结果(篡改比率  $\tilde{F}_1$ )

Tab.2 The watermark detection results for various attacks

攻击方式	参数	Lena	Barbara
JPEG	压缩比为 8	0.217	0.134
	压缩比为 16	0.271	0.178
	压缩比为 32	0.314	0.312
JPEG2000	压缩比为 8	0.122	0.115
	压缩比为 16	0.193	0.203
	压缩比为 32	0.286	0.291
叠加噪声	椒盐噪声 1%	0.124	0.123
	高斯噪声 30dB	0.273	0.272
	低通滤波 $3 \times 3$	0.146	0.153
平滑滤波	中值滤波 $2 \times 2$	0.134	0.132
	中值滤波 $3 \times 3$	0.186	0.185
	中值滤波 $4 \times 4$	0.255	0.268

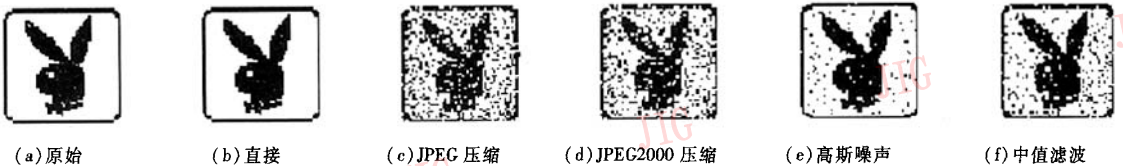


图 3 原始水印和抽取出的水印

Fig.3 The origin watermark and the extracted watermark

实验数据表明,本文算法具有较好的鲁棒性,在含水印图像遭到 JPEG 压缩、叠加噪声、平滑滤波等常规攻击后仍能够检测到图像的版权。

4.2 对恶意篡改的脆弱性

为了测定算法的脆弱性,以及能否在经过一般处理后找到图像被篡改的区域,首先对测试图像(含有水印信息的 Lena 图像和 Barbara 图像)进行 JPEG 压缩,然后使用 PhotoShop 改变图像内容。图 2(b)为首先对含水印图像图 2(a)进行 50% JPEG 压缩,然后在其中添加物体(Flower)的结果。

图 2(d)为首先对含水印图像图 2(c)进行 50% JPEG 压缩,然后进一步对其进行剪切的结果。

图 4(a)是从图 2(b)(被恶意篡改的含水印图像 Lena)中提取的水印( $NC = 0.577$ ),此时,篡改比率  $\tilde{F}_1 = 0.44$ ,而篡改矩阵  $\tilde{W}_1$  如图 4(c)所示。图 4(b)是从图 2(d)(被恶意篡改的含水印图像 Barbara)中提取的水印( $NC = 0.534$ ),此时,篡改比率  $\tilde{F}_1 = 0.52$ ,而篡改矩阵  $\tilde{W}_1$  如图 4(d)所示。

实验数据表明,本文算法不仅对于恶意篡改具有脆弱性,而且可以通过篡改矩阵  $\tilde{W}_1$  大致确定出

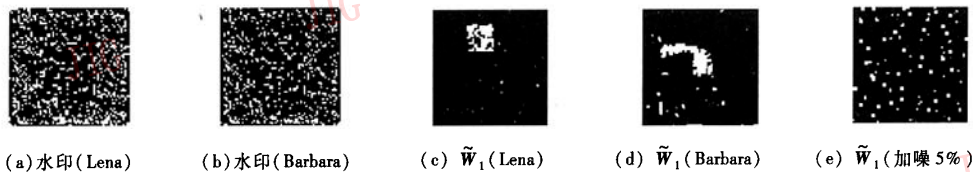


图 4 抽取出的水印及篡改区域检测

Fig.4 The extracted watermark and the tampered region detection

发生篡改的位置。

4.3 误检率与漏检率对比

为了验证算法的高效性,仿真实验根据误检率与漏检率对本文算法与 Fridrich 法、Queluz 法及 Liao 法的表现进行了比较,测试结果如表 3 所示。考虑到算法比较的客观性与公平性,仿真实验将 4 种算法的篡

改检测足迹 (footprint) 统一转化为标准的  $8 \times 8$  块。另外,对比实验中使用了儿种容许性常规图像处理操作,包括:(1)适度压缩,以 70% JPEG 为例;(2)直方图均衡 (均匀分布);(3)信噪比为 35dB 的高斯噪声;(4)1% 的椒盐噪声;(5)  $3 \times 3$  的低通滤波。

表 3 误检率与漏检率的对比

Tab.3 The false detection and missed detection probability

半脆弱 水印算法	伪造攻击 漏检率 (%)	信号处理攻击虚检率 (%)					
		无攻击	JPEG 压缩 (70%)	直方图均衡	高斯噪声 (35dB)	椒盐噪声 (1%)	低通滤波 ( $3 \times 3$ )
Fridrich 法	0.65	1.15	5.02	23.11	1.72	18.40	58.01
Queluz 法	1.03	0.01	7.28	87.67	32.43	0.79	58.23
Liao 法	16.12	0.21	6.73	59.42	1.93	19.51	53.08
本文算法	0.28	0.01	0.98	18.76	1.90	0.78	30.91

5 结 论

本文以人眼视觉系统掩蔽特性为基础,提出了一种基于分组量化的自适应半脆弱水印嵌入方案。该半脆弱水印方案具有以下特点:(1)采纳了基于人眼视觉特性的自适应分组量化策略;(2)数字水印信息的提取不需要原始载体图像;(3)能够同时进行版权保护与内容认证,并可大致确定篡改发生区域;(4)具有较低的误检率与漏检率。此外,该数字水印嵌入方案还具有计算简单、容易实现等优点,这大大扩展了其应用范围。

参考文献 (References)

1 Lu C S, Liao H Y M. Multipurpose watermarking for image authentication and protection [J]. IEEE Transactions on Image Processing, 2001, 10(10): 1579 ~ 1592.  
 2 Cox I J, Miller M I. The first 50 years of electronic watermarking [J]. Journal of Applied Signal Processing, 2002, 56 (2): 126 ~ 132.  
 3 Zhang Jing, Zhang Chunt-ian. Digital watermarking techniques for

image authentication [J]. Journal of Image and Graphics, 2003, 8(4): 367 ~ 373. [张静, 张春田. 用于图像认证的数字水印技术[J]. 中国图象图形学报, 2003, 8(4): 367 ~ 373.]  
 4 Lu Z M, Liu C H. Semi-fragile image watermarking method based on index constrained vector quantisation [J]. IEE Electronics Letters, 2003, 39(1): 35 ~ 36.  
 5 Fridrich J. Security of fragile authentication watermarks with localization [A]. In: Proceedings of SPIE Photonic West, Electronic Imaging 2002, Security and Watermarking of Multimedia Contents [C], San Jose, California, 2002, 4675: 691 ~ 700.  
 6 Queluz M P. Spatial watermark for image content authentication [J]. Journal of Electronic Imaging, 2002, 11(2): 275 ~ 285.  
 7 Gwo-Jong Y, Lu C-S, Liao H-Y M. Mean quantization-based fragile watermarking for image authentication [J]. Optical Engineering, 2001, 40(7): 1396 ~ 1408.  
 8 Ekici Ö, Sankur B, Akçay M. Comparative assessment of semifragile watermarking methods [J]. Journal of Electronic Imaging, 2004, 13(1): 209 ~ 216.  
 9 Lewis A S, Knowles G. Image compression using the 2-D wavelet transformation [J]. IEEE Transactions on Image Processing, 1992, 1(4): 244 ~ 250.  
 10 Qi Dong-xu. Fractal and computer application [M]. Beijing: Science Press, 1994. [齐东旭. 分形及其计算机生成 [M]. 北京: 科学出版社, 1994.]