一种新的自适应半脆弱水印算法

王向阳 [1,2] 陈利科 [1]

摘 要 提出了一种基于图像内容的自适应半脆弱数字水印算法. 该算法首先结合梯度分割阈值选取策略, 自适应抽取图像内容特征并作为水印信息; 然后利用载体图像邻域特性自适应确定量化步长, 并通过量化调制小波系数嵌入数字水印; 最后通过比对提取出的水印信息与重新抽取出的图像内容特征, 实现对待检测图像的完整性检验和篡改定位. 仿真实验证明, 该自适应半脆弱图像水印算法不仅具有较好的篡改检测与定位能力, 而且具有较强的抗攻击能力.

关键词 半脆弱水印, 图像特征, 梯度, 图像局部特性, 去噪
中图分类号 TP391

A Novel Adaptive Semi-fragile Watermarking Scheme Based on Image Content

WANG Xiang-Yang[1,2] CHEN Li-Ke[1]

Abstract This paper proposes a novel semi-fragile watermarking scheme, which is robust against regular manipulations, for image authentication. The semi-fragile watermarking scheme extracts the content feature (watermark) from the original image by adaptively gradient partitioning, and inserts this content feature back into the image by modulating the wavelet coefficients. To enhance the robustness and invisibility of this scheme, the adaptive quantization step is calculated according to the local image characteristics. The integrity authentication and tamper detection are implemented by comparing the extracted watermark and the extracted content feature. Experimental result shows that if there is no change in the obtained image, the watermark will be correctly extracted, and thus will pass through the authentication system. This scheme is tolerant of regular manipulations (such as JPEG2000 compression), but malicious changes of the image will result in breaches of the watermark detection. In addition, this scheme can detect the exact locations—the illegal modified blocks.

Key words Semi-fragile watermark, image feature, gradient, local image characteristic, denoise

1 引言

近年来, 半脆弱图像水印技术研究取得了一定进展, 陆续提出了诸如基于鲁棒水印原理、与 JPEG 编解码器相结合、基于视觉掩模、基于量化系数等多种半脆弱图像水印算法[1~7]. 其中, 基于内容特征的半脆弱图像水印技术[3,5,6] 已开始引起人们注意, 该类半脆弱水印技术是通过抽取图像特征 (如图像的边缘特征) 生成水印信息并进行嵌入, 认证时根据特征的相似性来判定图像是否被恶意篡改, 同时根据相异特征位置判定篡改发生位置. 基于内容特征的半脆弱图像水印方案不仅可以有效认证恶意篡改, 而且能够容忍一定的常见信号处理操作 (如 JPEG 压缩、叠加噪声等), 同时还具有系统安全等特点. 然而, 理论分析和实验结果表明, 现有基于内容特征的半脆弱图像水印方案不同程度地存在如下不足: 1) 未能真正抽取出反映图像内容特征的信息; 2) 嵌入水印信息时, 未能充分考虑图像自身的局部相关特性及其人眼视觉特性; 3) 篡改检测能力较差; 4) 鲁棒性有待提高等.

本文提出了一种新的自适应半脆弱图像水印算法. 该算法首先结合梯度分割阈值选取策略, 自适应抽取图像内容特征并作为水印信息; 然后利用载体图像邻域特性自适应确定量化步长, 并通过量化调制小波系数嵌入数字水印; 最后通过比对提取出的水印信息与重新抽取出的图像内容特征, 实现对待检测图像的完整性检验和篡改定位.

2 水印信息生成与加密

2.1 水印信息的生成

本文将在小波变换域内, 抽取图像的边缘纹理

收稿日期 2005-11-10 收修改稿日期 2006-2-12
Received November 10, 2005; in revised form February 12, 2006
辽宁省自然科学基金 (20032100)、视觉与听觉信息处理国家重点实验室开放基金 (0503)、大连市科技基金 (2006J23JH020)、"图像处理与图像通信" 江苏省重点实验室开放基金 (ZK205014) 和江苏省计算机信息处理技术重点实验室开放课题基金 (KJS0602) 资助
Supported by the Natural Science Foundation of Liaoning Province of China (20032100), the Open Foundation of State Key Laboratory of Vision and Auditory Information Processing (0503), the Natural Science Foundation of Dalian City of China (2006J23JH020), the Open Foundation of Key Laboratory of Image Processing and Image Communication (Nanjing University of Posts and Communications)(ZK205014), the Open Foundation of Jiangsu Province Key Laboratory for Computer Information Processing Technology (KJS0602)
1. 辽宁师范大学计算机与信息技术学院 大连 116029 2. 北京大学视觉与听觉信息处理国家重点实验室 北京 100871
1. School of Computer and Information Technology, Liaoning Normal University, Dalian 116029 2. National Laboratory on Machine Perception, Peking Universtiy, Beijing 100871
DOI: 10.1360/aas-007-0361

特征作为数字水印信息. 设原始载体图像 (256 级灰度图像) 为 $I=\{g(i,j),1\le i\le M,1\le j\le N\}$. 其中, $g(i,j)$ 表示原始载体图像的第 i 行、第 j 列像素灰度值. 则图像的边缘纹理特征抽取过程如下:

1) 原始图像小波分解. 对原始载体图像 I 实施 L 级小波分解, 可得到 1 个第 L 级的近似子带 (I_L^{LL}) 和 $3L$ 个细节子带 (水平、垂直、对角线)(I_L^{HL}、I_L^{LH}、I_L^{HH}、$\ldots$、I_1^{HL}、I_1^{LH}、I_1^{HH}).

2) 水印信息的生成. 由小波分析理论知: 细节 (水平、垂直、对角线) 子带是原始载体图像中边缘、轮廓、纹理等细节信息的体现, 同时随着频率的增加, 其越容易受到外来噪声干扰, 即稳定性越差. 为了取得数字水印图像视觉质量与抗攻击能力的良好平衡, 本文首先随机选取 2 个第 L 级细节子带 (I_L^{HL}、I_L^{LH} 或 I_L^{HH}) 构造出差值图像 F(以下简称 F 为原始图像的特征矩阵), 即

$$f(i,j)=\mathrm{abs}(I_L^a(i,j)-I_L^b(i,j))$$

其中, $f(i,j)\in F$, $a,b\in\{HL,LH,HH\}$, $i=1,2,\cdots,M/2^L$, $j=1,2,\cdots,N/2^L$, $\mathrm{abs}(\cdot)$ 表示绝对值操作.

然后抽取出图像的边缘纹理特征 W

$$w(i,j)=\begin{cases}1 & f(i,j)\ge T\\ 0 & f(i,j)<T\end{cases}$$

这里, $w(i,j)\in W$, $i=1,2,\cdots,M/2^L$, $j=1,2,\cdots,N/2^L$, T 为分割阈值.

最后再对边缘纹理特征图像进行低通滤波以消除噪声影响, 从而得到待嵌入的数字水印图像信息 W.

不难看出, 如果分割阈值 T 较小, 则会导致图像的边缘纹理特征不明显, 且稳定性也相对较差; 而如果分割阈值 T 较大, 则会造成图像的部分重要内容特征丢失. 另外, 不同的数字图像, 也只有采纳不同的分割阈值 T, 才能各自达到比较好的内容特征抽取效果. 下面将结合梯度分布理论, 给出分割阈值 T 的自适应选取方法.

3) 分割阈值的自适应选取. 大量实验表明, 原始图像的灰度值变化越明显, 其特征矩阵 F 对应位置的系数越大, 也就是说可以将特征矩阵 F 看作是图像灰度变化 (即梯度) 的一个近似, 因此完全可以结合图像梯度自适应确定分割阈值 (即自适应地确定出特征矩阵 F 的分割阈值 T).

而经过对图像梯度分布特点的观察与分析知, 不同图像的梯度直方图有着近似的分布, 如图 1 所示. 其中, A 是梯度均值, $B=A+D$, D 是分布函数的标准差. 另外, 大量梯度图像的分割实验还表明, $g>B$ 的梯度值对应着图像边界的大梯度值; 而 $g<B$ 的梯度值在梯度图像中占有大多数, 它们对应着目标区域和背景区域所产生的大量小梯度值.

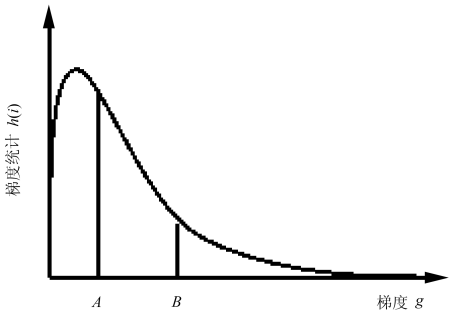


图 1 图像梯度分布曲线

Fig. 1 The image gradient curve

从理论上说, 统计量能够将样本中关于总体分布的信息尽可能地表现出来. 在概率论中, 均值是一个描述主体集中位置的统计特征, 而标准差则是描述主体在均值附近的密集程度的统计特征. 标准差越小, 主体的分布越集中在均值附近, 说明图像中高梯度的位置较少, 梯度分割阈值就应相应降低; 反之, 标准差越大, 主体的分布越分散, 说明图像中高梯度的位置较多, 梯度分割阈值就应相对提高. 由于统计量 B 总是随着不同的图像样本而变化, 因此, B 所体现的信息, 其物理意义就是边界区域梯度值与非边界区域梯度值的分水岭, 即可以利用 B 自适应地分割边界区域梯度值和非边界区域梯度值. 又由于特征矩阵 F 可以看作是梯度图像的一个近似, 故可以将分割阈值 T 定义为如下形式 (即自适应形式)

$$T=E(F)+\sigma(F)$$

$$E(F)=\frac{1}{M/2^L\cdot N/2^L}\sum_{i=1}^{M/2^L}\sum_{j=1}^{N/2^L}f(i,j)$$

$$\sigma(F)=\sqrt{\frac{1}{M/2^L\cdot N/2^L}\sum_{i=1}^{M/2^L}\sum_{j=1}^{N/2^L}[f(i,j)-E(F)]^2}$$

其中, $E(\cdot)$ 和 $\sigma(\cdot)$ 分别表示均值函数和标准差函数.

2.2 数字水印信息的混沌加密

考虑到本文算法所采用的数字水印信息 (即图像的边缘纹理特征) 可以公开提取, 故有必要对其进行加密处理[8]. 本文将采用 Logistic 映射产生混沌密钥, 对数字水印信息进行加密处理, 其工作步骤为:

1) 利用 Logistic 映射产生伪随机序列, 即

$$X_{k+1}=\mu X_k(1-X_k)=f(\mu,X_k)$$

其中, 参数 $1 \le \mu \le 4$. 实验证明, 当 $\mu \in (3.9, 4.0]$ 时, 系统将进入混沌状态, 产生具有 0 均值、互相关性为 0 的混沌序列, 且该序列具有白噪声的统计特性. 显然, 只要使用不同的初值 X_1, 并采用不同的参数 μ, 就可以得到不同的伪随机序列.

2) 将上述伪随机序列二值化并升维成二维掩蔽模板 M

$$M = \left\{ m(i,j) \in \{0,1\},\ i = 1,2,\cdots, M\Big/2^L,\ j = 1,2,\cdots, N\Big/2^L \right\}$$

3) 利用二维掩蔽模板 M 加密数字水印信息 (通过按位异或操作), 即

$$\hat{W} = W \oplus M$$

这里, $\hat{W}$ 表示经过加密处理的数字水印信息.

3　数字水印嵌入

本文将采用量化调制小波系数方法, 将数字水印信息 $\hat{W}$(已经过加密处理) 嵌入到原始载体图像的小波变换域内. 具体步骤如下：

1) 原始载体图像的小波变换. 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个子带. 为了有效进行版权保护和内容认证, 本文选取小波变换域的低频区 (I_L^{LL} 子带) 作为数字水印嵌入区.

2) 量化步长的选取. 对基于量化的图像水印嵌入方法来说, 量化步长 Δ 的选取至关重要. 因为量化步长 Δ 与水印嵌入强度密切相关, Δ 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 Δ 应充分考虑图像自身特点和人眼视觉特性. 本文将以 JPEG2000 图像压缩编码方案为基础, 结合载体图像邻域特性确定量化步长 Δ, 即采用自适应量化策略嵌入水印信息

$$\Delta(i,j) = \ln \frac{\left|I_L^{LH}(i,j)\right| + \left|I_L^{HL}(i,j)\right| + \left|I_L^{HH}(i,j)\right|}{2}$$

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 (I_L^{LH}、I_L^{HL} 和 I_L^{HH}) 内相应位置上的小波系数相对较大, 故应有比较大的量化步长 Δ 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, 会带来更小的失真, 更加符合人眼的视觉特性.

综合考虑 JPEG2000 编码方案与载体图像内容特性, 本文将量化步长 Δ 选取为

$$\Delta(i,j) = \beta \cdot 2^L \cdot \ln \frac{\left|I_L^{LH}(i,j)\right| + \left|I_L^{HL}(i,j)\right| + \left|I_L^{HH}(i,j)\right|}{2}$$

3) 数字水印的嵌入. 用量化步长 Δ 对小波系数进行量化, 并根据量化结果修改近似子带 I_L^{LL} 的小波系数值, 以完成水印信息的嵌入. 本文所采用的量化嵌入方案为

$$I_L^{LL'}(i,j) = Q\left(I_L^{LL}(i,j)\right) + \hat{w}(i,j) \times \Delta(i,j)$$

$$Q\left(I_L^{LL}(i,j)\right) = \mathrm{floor}\left(\mathrm{round}\left(I_L^{LL}(i,j)\Big/\Delta(i,j)\right)/2\right) \times 2\Delta(i,j)$$

其中, $I_L^{LL}(i,j)$ 为原小波系数, $I_L^{LL'}(i,j)$ 为修改后小波系数, round(·) 为舍入取整操作, floor(·) 为截断取整操作.

4) 逆小波变换. 用含有数字水印信息的小波系数 $I_L^{LL'}(i,j)$ 代替 $I_L^{LL}(i,j)$, 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'.

4　数字水印提取与图像内容认证

本文图像内容认证方案所包含的关键步骤如下：

1) 待检测图像的小波变换. 对待检测图像 I^* 实施 L 级小波变换, 以得到一系列不同分辨率及不同方向的多个子带.

2) 抽取待检测图像的内容特征. 首先按照 2.1 节工作步骤, 结合梯度分布理论, 自适应确定分割阈值, 并从第 L 级细节子带中抽取出待检测图像 I^* 的边缘纹理特征 W_1^*; 然后按照 2.2 节工作步骤, 选用同样的初值 X_1 和参数 μ 生成掩蔽模板 M, 对抽取出的边缘纹理特征 W_1^* 进行混沌加密, 以得到 $\hat{W}_1^*$.

3) 提取数字水印信息. 在小波变换域内, 从 I_L^{*LL} 子带中提取水印信息 $\hat{W}_2^*$. 提取方法可以表示为

$$\hat{w}_2^*(i,j) = \mathrm{mod}(\mathrm{round}\left(I_L^{*LL}(i,j)\Big/\Delta(i,j)\right), 2)$$

其中, mod(·, 2) 为模 2 取余操作, $\hat{w}_2^*(i,j) \in \hat{W}_2^*$, $i = 1,2,\cdots, M/2^L$, $j = 1,2,\cdots, N/2^L$, 量化步长 $\Delta(i,j)$ 的计算方法参见第 3 节.

4) 生成篡改矩阵 $\hat{W}^*$(篡改矩阵 $\hat{W}^*$ 中元素为 1 的区域意味着该区域可能被篡改).

$$\hat{W}^* = \hat{W}_1^* \oplus \hat{W}_2^* (\oplus\text{为异或运算})$$

5) 对篡改矩阵 $\hat{W}^*$ 进行去噪处理. 实验结果表明, 可以通过篡改矩阵 $\hat{W}^*$ 确定篡改发生位置, 但对待检测图像实施 JPEG 压缩、叠加噪声、平滑滤波等常规处理操作后, 由 $\hat{W}^*$ 所确定出的篡改发生区域呈均匀分布或随机分布 (即算法会在图像未遭受恶意攻击的情况下产生报警). 为此, 本文将采用篡改矩阵 $\hat{W}^*$ 去除噪声方法, 消除恶意攻击误报 (包括虚警和漏警) 影响.

本文将在 8 连通域内对篡改矩阵 $\hat{W}^*$ 进行去噪处理. 其关键步骤如下:

步骤 1. 去除虚警噪声. 如果某一报警点 $\hat{w}^*(i,j)$ 的 8 连通域内仅有少于 1 个的报警点, 即

$$\sum_{i,j=-1}^{1} \hat{w}^*(i,j) \le 2$$

则判定该位置为虚警, 在篡改矩阵中将其删除 (置 0), 图 2 给出了两个虚警噪声的例子.

(i-1, j-1)	(i-1, j)	(i-1, j+1)
(i, j-1)	(i, j)	(i, j+1)
(i+1, j-1)	(i+1, j)	(i+1, j+1)

(i-1, j-1)	(i-1, j)	(i-1, j+1)
(i, j-1)	(i, j)	(i, j+1)
(i+1, j-1)	(i+1, j)	(i+1, j+1)

图 2 虚警噪声的判定

Fig. 2 False alarm determination

步骤 2. 去除漏警噪声. 如果某一非报警点 $\hat{w}^*(i,j)$ 的 8 连通域内有多于 4 个的报警点, 即

$$\sum_{i,j=-1}^{1} \hat{w}^*(i,j) \ge 4$$

则判定该位置为漏警, 在篡改矩阵中对其进行填补 (置 1), 图 3 给出了两个漏警噪声的例子.

(i-1, j-1)	(i-1, j)	(i-1, j+1)
(i, j-1)	(i, j)	(i, j+1)
(i+1, j-1)	(i+1, j)	(i+1, j+1)

(i-1, j-1)	(i-1, j)	(i-1, j+1)
(i, j-1)	(i, j)	(i, j+1)
(i+1, j-1)	(i+1, j)	(i+1, j+1)

图 3 漏警噪声的判定

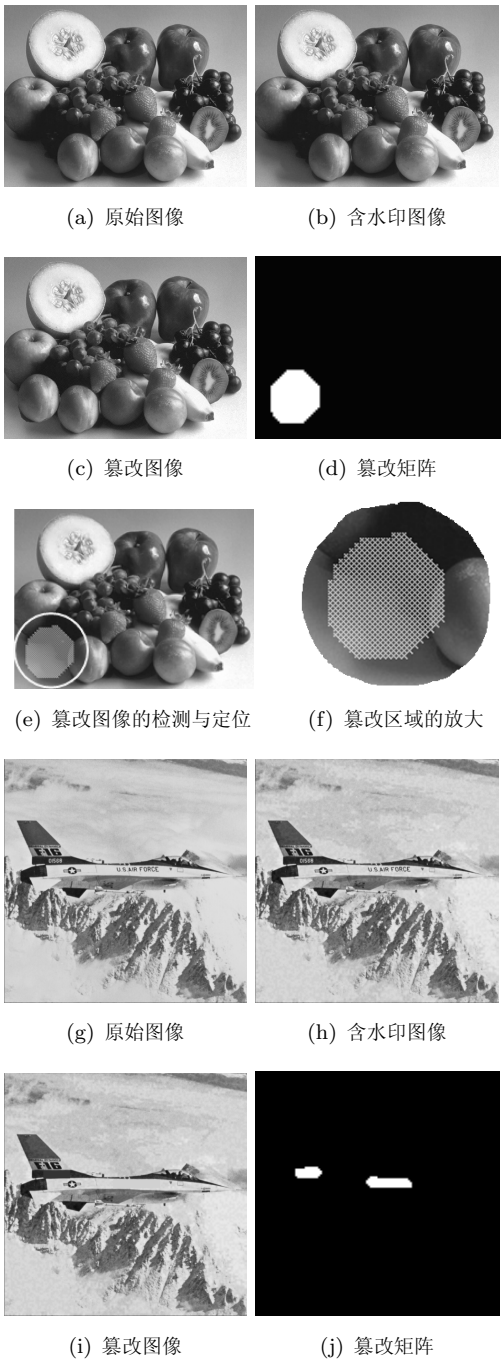
Fig. 3 Miss alarm determination

步骤 3. 重复以上步骤, 以达到满意的结果.

6) 图像块认证. 将待检测图像 I^* 划分成大小为 $2^L \times 2^L$ 的图像子块 $B^*(i,j)(i = 1,2,\cdots,M/2^L, j = 1,2,\cdots,N/2^L)$, 并依据待检测图像 I^* 与篡改矩阵 $\hat{W}^*$(已经过去噪处理) 的对应关系判定图像子块 $B^*(i,j)$ 是否被恶意篡改. 即, 如果 $\hat{w}^*(i,j) = 1$, 则可判定图像子块 $B^*(i,j)$ 被恶意篡改; 否则, 则可判定图像子块 $B^*(i,j)$ 没有被恶意篡改.

5 实验结果与结论

为了验证本文算法的有效性, 以下分别给出了一般性恶意篡改的检测、抗攻击能力的测试、特殊恶意篡改的检测等实验结果, 并与文献 [4] 和 [5] 进行了对比. 实验中, 选用了标准灰度图像 Fruit ($328 \times 440 \times 8$bit, 如图 4(a) 所示) 和 Plane ($512 \times 512 \times 8$bit, 如图 4(g) 所示), 测试环境为 Windows XP、Matlab 6.0. 量化步长的拉伸系数为 $\beta = 2$, 小波变换级数为 $L = 2$, 混沌加密的初值 $X_1 = 0.1$, 参数 $\mu = 4$.



(a) 原始图像 (b) 含水印图像

(c) 篡改图像 (d) 篡改矩阵

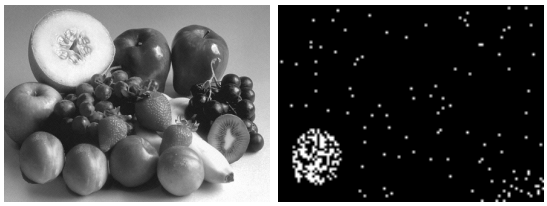
(e) 篡改图像的检测与定位 (f) 篡改区域的放大

(g) 原始图像 (h) 含水印图像

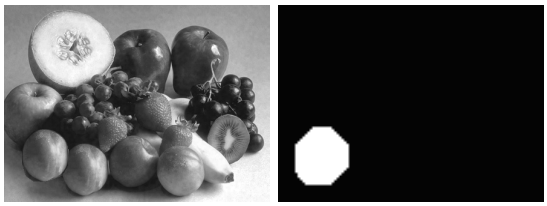
(i) 篡改图像 (j) 篡改矩阵

图 4 恶意篡改的检测与定位

Fig. 4 Authentication and location of tampering

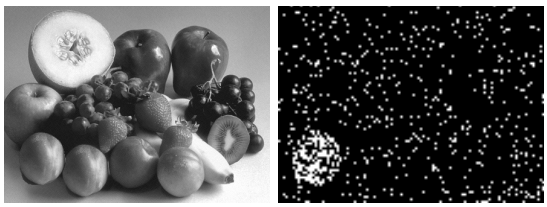


(a) 文献 [4] 篡改图像　(b) 文献 [4] 篡改矩阵

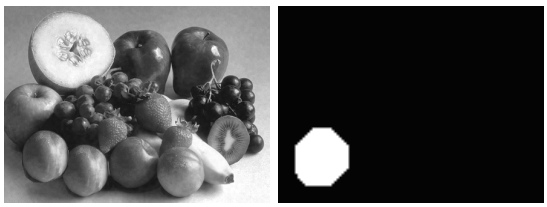


(c) 本文篡改图像　(d) 本文篡改矩阵

(1) 进行 50%的 JPEG2000 压缩

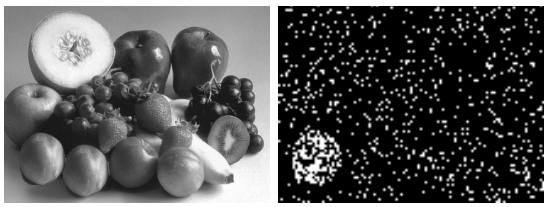


(e) 文献 [4] 篡改图像　(f) 文献 [4] 篡改矩阵

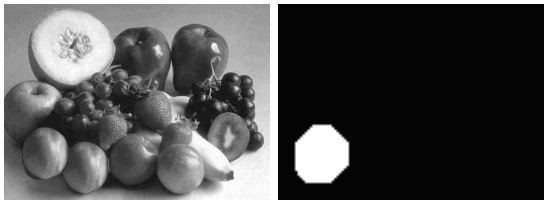


(g) 本文篡改图像　(h) 本文篡改矩阵

(2) 添加 2%的高斯噪声



(i) 文献 [4] 篡改图像　(j) 文献 [4] 篡改矩阵



(k) 本文篡改图像　(l) 本文篡改矩阵

(3) 添加 2%的高斯噪声后再进行 50%的 JPEG2000 压缩

图 5　常规攻击对篡改检测的影响

Fig. 5　Experiment of allied attack

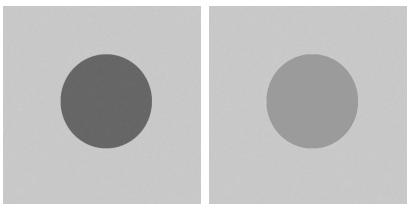
5.1　一般性恶意篡改的检测

图 4(a)~4(j) 分别为原始图像、含水印图像 (利用本文算法)、篡改图像 (一般性恶意篡改)、篡改矩阵、检测与定位结果、篡改区域的放大图.

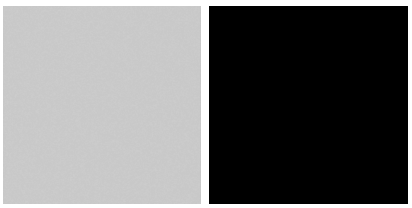
5.2　抗攻击能力的测试

图 5(a)~5(l) 分别给出了本文算法和文献 [4] 算法的抗攻击能力测试结果. 其中, 图 5(a)~5(d) 为进行 50%的 JPEG2000 压缩后的篡改图像和篡改检测结果; 图 5(e)~5(h) 为添加 2%的高斯噪声后的篡改图像和检测结果; 图 5(i)~5(l) 为添加 2%的高斯噪声后再进行 50% 的 JPEG2000 压缩的篡改图像和检测结果. 可见, 本文算法的抗攻击能力在很大程度上优于文献 [4] 中的算法.

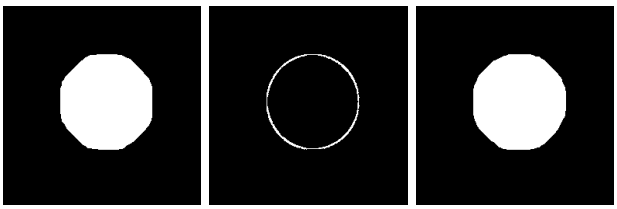
5.3　特殊恶意篡改的检测



(a) 原始图像　(b) 篡改图像 (灰度改变)



(c) 篡改图像 (前景对象删除)　(d) 灰度改变检测结果 (文献 [5])



(e) 灰度改变检测结果 (本文)　(f) 前景对象删除检测结果 (文献 [5])　(g) 前景对象删除检测结果 (本文)

图 6　特殊恶意篡改的检测

Fig. 6　Experiment of special attack

实验结果表明, 现有基于内容特征的半脆弱图像水印方案[3,5,6] 均难以检测诸如灰度改变 (如图 6(b) 所示)、前景对象删除 (如图 6(c) 所示) 之类的特殊恶意篡改形式, 其原因在于抽取图像内容特征时仅考虑了图像的亮度峰值点, 而丢失了图像的平

滑特征. 本文算法并非从低频子带提取特征, 而是结合自适应分割阈值从高频子带提取边缘纹理特征, 并将其加密后嵌入低频子带, 故可以有效检测到平滑区域的篡改. 图 6(d)∼6(g) 分别给出了文献 [5] 和本文算法对于灰度改变、前景对象删除的篡改检测结果. 不难看出, 文献 [5] 算法无法检测到一定程度的灰度改变, 而对于前景对象删除攻击, 也只能在边缘处报警.

本文提出了一种新的自适应半脆弱图像水印算法, 该算法具有以下几个特点: 1) 结合梯度分割阈值选取策略, 自适应抽取图像内容特征 (并作为水印信息), 增强了图像内容特征的稳定性和全面性; 2) 依据图像局部相关特性及人眼视觉特性嵌入水印信息, 提高了数字水印的隐藏效果 (透明性和鲁棒性). 实验结果证明, 该自适应半脆弱图像水印算法不仅具有较好的篡改检测与定位能力, 而且具有较强的抗攻击能力.

References

1 Wu Jin-Hai, Lin Fu-Zong. Image authentication based on digital watermarking. *Chinese Journal of Computers*, 2004, **27**(9): 1153∼1161
(吴金海, 林福宗. 基于数字水印的图像认证技术. 计算机学报, 2004, **27**(9): 1153∼1161)

2 Ekici Ö, Sankur B, Akcay M. Comparative evaluation of semifragile watermarking algorithm. *Journal of Electronic Imaging*, 2004, **13**(1): 209∼216

3 Zhao Y, Campisi P, Kundur D. Dual domain watermarking for authentication and compression of cultural heritage images. *IEEE Transactions on Image Processing*, 2004, **13**(3): 430∼448

4 He Ren-Ya, Chen Qian-Sheng. Digital watermarking embedded in the discrete wavelet domain for authentication. *Journal of Computer Aided-design & Computer Graphics*, 2001, **13**(9): 812∼815
(贺仁亚, 程乾生. 一种用于认证的小波变换域的数字水印技术. 计算机辅助设计与图形学学报, 2001, **13**(9): 812∼815)

5 Xie L H, Arce G R. A class of authentication digital watermarks for secure-multimedia. *IEEE Transactions on Image Processing*, 2001, **10**(11): 1754∼1764

6 Wo Yan, Han Guo-Qiang, Zhang Bo. A new feature-based image content authentication algorithm. *Chinese Journal of Computers*, 2005, **28**(1): 105∼112
(沃炎, 韩国强, 张波. 一种新的基于特征的图像内容认证方法. 计算机学报, 2005, **28**(1): 105∼112)

7 Hu J Q, Huang J W, Huang D R, Shi Y Q. Image fragile watermarking based on fusion of multi-resolution tamper detection. *Electronics Letters*, 2002, **38**(24): 1512∼1513

8 Wang Hong-Xia, He Chen, Ding Ke. Robust public watermarking based on chaotic map. *Journal of Software*, 2004, **15**(8): 1245∼1251
(王宏霞, 何晨, 丁科. 基于混沌映射的鲁棒公开水印. 软件学报, 2004, **15**(8): 1245∼1251)

王向阳 辽宁师范大学计算机与信息技术学院教授, 主要研究领域包括网络信息安全技术、多媒体信息处理技术. 本文通信作者. E-mail: wxy37@263.net
(**WANG Xiang-Yang** Professor. His research interest covers information security and multimedia processing. Corresponding author of this paper.)

陈利科 辽宁师范大学计算机与信息技术学院硕士研究生, 主要研究领域包括信息隐藏与数字水印.
(**CHEN Li-Ke** Master student at Liaoning Normal University. His research interest covers information security and digital watermarking.)