一种基于 HVS 的图像易碎水印

胡军全,黄继武,黄达人
(中山大学信息科学与技术学院,广东广州 510275)

摘 要: 作为多媒体认证和篡改检测的一种新技术,易碎水印正得到越来越多的关注. 基于小波变换,结合量化调制过程,本文提出了一个易碎水印算法. 该算法具有以下特点:(1)构造水印金字塔,便于实现水印的多分辨率检测;(2)结合视觉特性量化调制,尽可能减小视觉失真;(3)结合图像融合技术的多分辨率检测,使检测结果更准确;(4)抵抗一定程度的 JPEG 有损压缩. 为了实现篡改的检测,本文给出了一个攻击判别方案,以区分恶意攻击和偶然攻击. 实验表明,嵌入的水印在脆弱性和鲁棒性上达到了较好的统一,能够抵抗一定程度的压缩而不影响篡改检测的精确性.

关键词: 易碎水印; 信息隐藏; 水印金字塔; 图像融合; 篡改检测
中图分类号: TP391 **文献标识码**: A **文章编号**: 0372-2112 (2003) 07-1057-05

An Algorithm for Fragile Watermarking Based on HVS

HU Jun-quan, HUANG Ji-wu, HUANG Da-ren
(School of Information Science and Technology, Zhongshan University, Guangzhou, Guangdong 510275, China)

Abstract: As an effective method for multimedia authentication and tamper detection, fragile watermarking is drawing extensive attention recently. In this paper, we propose a novel fragile watermarking scheme based on HVS in DWT domain. By use of a specifical modulation, we embed the mark into the DWT coefficients of the original image. The features of proposed algorithm are as follows: i) The algorithm constructs a pyramid structure of the watermark for multi-resolution tamper detection; ii) According to the visual model, the algorithm modifies the coefficients to reduce the perceptible distortion; iii) The algorithm presents a new scheme for tamper detection by using image fusion. We propose several rules to distinguish the type of tamper between mild distortion and severe distortion. The experimental results demonstrate that the watermarks generated with the proposed algorithm can give the precise result of tamper detection when the image has been suffered from malicious tamper while tolerating JPEG lossy compression to a certain extent.

Key words: fragile watermarking; information hiding; watermark pyramid; image fusion; tamper detection

1 引言

信息隐藏,古已有之. 近年来,迎合信息安全技术的新要求,数字水印逐渐成为研究热点. 按照应用目的,水印可分为稳健水印和易碎水印[1~5]. 稳健水印是指经受攻击后依然可以提取出来的水印,当然,其稳健度有赖于算法[6,7]. 易碎水印则对任何加诸于图象的变化敏感,通过检测嵌入水印的存在与否、真实与否以及完整与否,确保原始图像的可信度. 与传统的数字签名(Digital Signature)技术不同,易碎水印并不在文件尺寸上作变化,而是直接在图像中嵌入有意义水印或认证符号;另一方面,数字签名的认证信息与原信息密切相关,原信息的任何改动会导致签名的改变,而易碎水印则可以承受一定的非篡改性的修改. 此外,水印系统可以依据嵌入的信息对原图像被篡改部分进行修复,而这是数字签名技术所无法达到的. 因此,易碎水印作为数字签名的有效补充手段,在数据完整性证明、多媒体数据认证方面具有广阔的应用前景. 表面上看,越敏感的方案越好. 但是从实际应用来看却并非如此,能够承受一些常见图像处理手段(如 JPEG 有损压缩)而不影响篡改探测结果的易碎水印方案可能有更广泛的应用.

易碎水印已成为数字水印研究中的一个重要方面. S Walton[8]通过校验和(check-sum)思想实现了易碎水印的图像真伪鉴定. Yeung[9]提出了一种全新的空间域算法,通过一个值域为{0,1}的二进制映射函数和一个扰动过程,完成水印的嵌入过程,任何灰度级的变化都将反应在提取水印上. 但是 Yeung 的易碎水印对“拼图”攻击非常脆弱,后继者通过研究其缺点,提出了改进算法[10~12]. 但都不能从根本上解决问题,只是或多或少的增加了攻击的难度. 在 DCT 变换域,Wu[13]通过一个查找表实现了图像易碎水印;Wong[14]通过公有密钥方案同样实现了水印的易碎. 而 Marvel[15]则把原始信息的 hash 作为嵌入信息,实现了图象的真伪认证. 他们在继承了 DCT

收稿日期:2001-12-28;修回日期:2002-06-15
基金项目:国家自然科学基金重点项目(No. 60133020);国家自然科学基金(No. 60172067,69975011);国家“863”计划(2002AA144060);教育部博士点基金(No. 2002558038);广东省自然科学基金重点项目(No. 013164)

变换优良性质的同时也具有很大的安全隐患. Lin[16]实现了水印的半易碎,量化过程中通过特殊的调制操作,水印可以承受JPEG有损压缩,但承受能力却受算法限制. Kundur[17]尝试在小波域中加入水印,水印信号以基于量化的方法嵌入到小波系数中. 由于小波变换特有的多分辨率特性,使得 Kundur 的方案可以检测到不同分辨率下的水印篡改图,从而使得篡改的检测更加精确. 但其用以完成调制的量化阈值是从高分辨率到低分辨率单调递增的,这有违人类视觉系统,容易导致水印图在视觉上失真.

本文通过对现有易碎水印算法的研究和易碎水印应用前景的分析,希望所实现的易碎水印系统达到如下三个目标: (1)结合 HVS(Human Visual System),降低水印图像的失真; (2)基于小波变换,使得水印具有多分辨率检测的能力; (3)结合量化调制,使得水印可以抵抗诸如JPEG压缩等一些非恶意攻击. 为此,本文试图借鉴图像压缩领域的量化思想,探索在小波域中进行基于 HVS 的调制量化来进行水印嵌入的可行性.

2 HVS 系统和所提出的易碎水印系统

图像的最终接收者为人. 因此,充分研究 HVS 系统,对于图像信息的处理有非常重要的意义. 研究发现,人眼具有下述视觉特性[21]: (1)对亮度响应的非线性特征. 在平均亮度大的区域,人眼对灰度误差不敏感. 著名的韦伯定律就是这一特性的描述; (2)人眼对于不同频率的信号有不同的灵敏度,对高频分量不敏感; (3)人眼易感觉到边缘位置的变化,而对于边缘区域象素的灰度误差,人眼并不敏感.

HVS 的上述特性说明,对于可接受范围之内的象素值变动,人眼会认为没有改变. 而数字水印则刚好作为一种微弱的变化引入图像,其内在要求之一就是不可见. 这一问题解决得好与否,直接影响到水印方案质量的好与坏. 另一方面,在图像压缩领域,类似问题同样困扰着研究者,早先所采用的均匀量化方案,会带来均匀量化噪声,从而导致图像有人为修改的痕迹. 通过研究,Watson[18]认为可以把这种量化噪声限制在人眼可接受的范围,也就是说视觉上不可见. 为此,针对 9-7 双正交小波滤波器,Watson 提出了一个特殊的量化矩阵. 通过该矩阵,解压缩图像在视觉上与原图一致. 由于本文的方案是通过量化调制来实现水印嵌入的,因此,为了满足水印图像的不可见性,我们借鉴了 Watson 量化矩阵.

本文算法的基本思想是通过对原图小波变换系数的不大于相应量化步长的调制来嵌入水印. 首先,为了方便在小波分解后的多分辨率分层结构中嵌入水印信息,需要构造一个相应的水印金字塔. 其次,依据一定的准则,按照分辨率从高到低进行的顺序,以水印金字塔的相应层数据作为嵌入内容,将对应分辨率的高频带系数进行特定的量化调制. 最后做小波逆变换得到水印图像. 本文采用 9-7 双正交小波滤波器.

3 金字塔结构的二值水印

在本文的工作中,水印是一个二值图像,而水印的嵌入则是在小波域中完成的. 因此,相应的也要构造一个分层的水印结构,使每一层分别包含水印信息的不同分辨率成分,然后在原图的每个分辨率子带都嵌入相应水印信息,达到多分辨率检测的目的. 而且水印分层结构跟原始图像小波分解后的各子带相对应,可以大大方便水印信息的嵌入. 由此,我们尝试构造一个分辨率逐渐递减的水印金字塔. 一般来讲,在行和列方向都作隔行采样是最直接的分辨率递减方法,但在很多情况下,这样做会丢失图像的很多细节. JBIG 标准提供了一种分辨率递减的方法[19],在保持图像细节方面具有良好效果. 低分辨率层由上一层相关象素点和本层相关象素点计算得来. 计算图示如图 1.

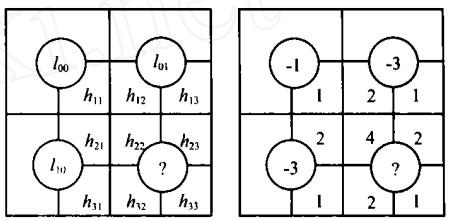

图 1 分辨率递减时,相关像素位置图及其相应像素权重图. (方块代表上一级较高分辨率,圆圈代表当前较低分辨率,问号处为当前待求像素值)

根据图 1,计算

$$l = 4h_{22} + 2(h_{12} + h_{21} + h_{23} + h_{32}) + (h_{11} + h_{13} + h_{31} + h_{33}) - 3(l_{01} + l_{10}) - l_{00}$$

若 $l > 4.5$,则当前像素值取为 1,反之为 0. 计算顺序按照从上到下,从左到右的次序进行. 计算完毕后,用上一层图像减去当前低分辨率图像即得差分层. 上述过程将进行三次,得到两个差分层和一个低分辨率层,如下图 2 所示.

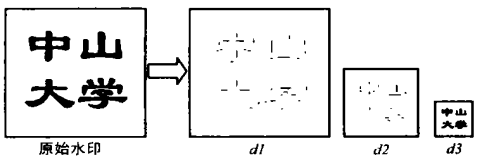

图 2 原始水印经过分辨率递减后分解为 $d1$、$d2$ 两个差层和最低分辨率层 $d3$

4 水印嵌入方案

对原图进行小波分解,记 $f_{k,l}$为分解后第 l 级第 k 方向上的小波系数. 其中 $k = h$(水平)、v(垂直)、d(对角); $l = 1, \cdots, L$. 为了在第 l 级某特殊方向上的子带中嵌入水印,需要计算

$$Q_{i,j} = \begin{cases} 0 & \lfloor f(i,j)/JND(i,j) \rfloor \text{ 为偶数} \\ 1 & \lfloor f(i,j)/JND(i,j) \rfloor \text{ 为奇数} \end{cases}$$

其中 $JND(\cdot,\cdot)$为 Watson 量化矩阵, $\lfloor\cdot\rfloor$为地板函数, $f(i,j)$为该子带内 (i,j) 处的小波系数. 令 $s = \lfloor f(i,j)/JND(i,j) \rfloor$,对于预先选定的常数 m,把区间 $[sJND(i,j), (s+1)JND(i,j)]$ 等分为 2^{m-1}个小区间. 根据当前系数所在的区间序号,我们相应修改系数即可完成嵌入,记该区间序号为 $t \in [1, 2^{m-1}]$,区间长为 $length$. 水印每次嵌入 m 位,取当前 m 位水印的第一位为 $w(i,j)$. 余下 $m-1$ 位取其十进制整数值并记为 r,范围为 $[0, 2^{m-1})$. 则修改后的系数为:

$$\tilde{f}(i,j) = \begin{cases} f_1 & \text{if } Q_{i,j} = w(i,j) \\ f_2 & \text{if } Q_{i,j} \neq w(i,j) \end{cases}$$

其中 $f_1 = \begin{cases} f(i,j) & \text{if } t = r+1 \\ JND(i,j)\cdot s + (r+0.5)\cdot length & \text{if } t \neq r+1 \end{cases}$

$f_2 =$

$$\begin{cases} JND(i,j)\ (s+1) + (r+0.5)\ length \\ \quad \text{if } t = r+1 \text{ and } \dfrac{length}{2} < f(i,j) - JND(i,j)\cdot s - r\cdot length \\ JND(i,j)\ (s-1) + (r+0.5)\ length \\ \quad \text{if } t = r+1 \text{ and } \dfrac{length}{2} > f(i,j) - JND(i,j)\cdot s - r\cdot length \\ JND(i,j)\ (s+1) + (r+0.5)\ length \quad \text{if } t > (r+1) \\ JND(i,j)\ (s-1) + (r+0.5)\ length \quad \text{if } t < (r+1) \end{cases}$$

为了增强水印的安全性,可以对水印数据和嵌入位置进行置乱,并用密钥控制. 这样,攻击者很难在没有先验知识的情况下恢复水印.

5　水印提取算法

与水印嵌入一样,首先对待测图像进行小波分解,记分解后的系数为 f',同样,对于嵌入水印子带,计算

$$Q'_{i,j} = \begin{cases} 0 & \llcorner f'(i,j)/JND(i,j) \lrcorner \text{ 为偶数} \\ 1 & \llcorner f'(i,j)/JND(i,j) \lrcorner \text{ 为奇数} \end{cases}$$

令　　$s' = \llcorner f'(i,j)/JND(i,j) \lrcorner$

则有　　$t' = \llcorner (f'(i,j) - s'\cdot JND(i,j))/length \lrcorner$

那么,提取的水印为:

$$w = Q'_{i,j}\cdot 2^{m-1} + t'$$

则只需求 w 的二进制值就可得到 m 位提取水印.

6　水印脆弱性分析

理论上,当 m 增大时,可嵌入的水印的数据量也增大,但这是以水印的脆弱性增强为前提的. 由于实际当中往往并不是要求水印对任何操作作出攻击的判断. 也就是说,水印的脆弱性可以忍受某些特定攻击(JPEG压缩、轻度滤波等)而不给出错误的报告,但是对于既定攻击,水印的正确判断应该不受到影响. 按照 Kundur 的理论[17],攻击可分为两类:一类是偶然的,比如轻度滤波以及JPEG压缩等;而另外一类是恶意的,比如严重的线性或非线性滤波,随机位错误、图像内容替换等等. 它们反映在小波系数上的变化可以认为服从高斯分布,唯一的区别是恶意攻击的方差大于偶然攻击. 且它们存在关系:$\sigma_m = c\cdot\sigma_l$. 本文的目的是设计算法对偶然攻击给出正确的检测. 即要检测到水印无变化. 令一个攻击分布为 $N(0,\sigma_v^2)$. 水印正确检测概率函数为:

$$p = \frac{2^m}{jnd}\int_0^{jnd}\left[\ erf\left(\frac{\zeta}{2\sigma_v}\right)\right]^{m-1} d\zeta$$

那么水印的误检率为 $p_e = 1 - p$. 如图 3(a) 所示.

由图中看到,m 越大,水印的误检率越高,也就是说水印越来越脆弱,这在一定程度上反映了水印脆弱性的变化,也同理论上的分析是一致的. 此外,水印的嵌入区域也会影响水印的脆弱性. 通过实验发现:嵌入低频区域要比嵌入高频区域脆弱,而嵌入低分辨率区域要比嵌入高分辨率区域脆弱. 这是因为量化矩阵中低频区的量化值要小于高频区的量化值,所以允许的修改量比较小,从而水印就表现得更加脆弱. 另外一方面,由于JPEG压缩会滤去部分高频信息. 因此,只把水印加在高频区会导致水印对JPEG压缩敏感. 鉴于以上考虑,算法中把水印加在 LL_3、HH_2 以及 HH_1.

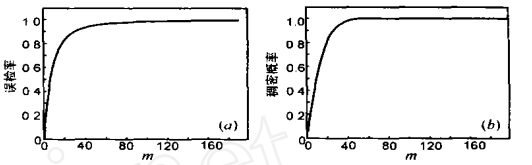

图 3　(a) 误检率随 m 变化图;
(b) 水印差图像素点稠密概率随 m 变化图

7　篡改攻击的判别

令 $W'(i,j)$ 为提取出来的水印. 计算差图

$$D(i,j) = |W(i,j) - W'(i,j)|$$

由于偶然攻击对小波系数的影响近似服从高斯分布,且其方差较小. 因此,在差图上的表现就是大部分都是孤立点,即聚集在一块的概率较小. 另外,假设当前像素点为 $x(i,j)$. 记其水印误检率为 $p(x)$,则在差图上该点不孤立的概率 p_d 为 $1 - (1 - p(x))^8$(见图 3(b)). 由图中可知,m 越大,稠密的概率越大,而且当 m 相当大时,稠密概率近乎 1,在这种情况下,轻微的攻击都会对图像造成极大的影响. 这种现象的产生是因为算法对修改的敏感度增加,所允许的修改量自然变小. 一般从应用的角度,水印算法应该达到如下预期目的:(1) 给出攻击类别的判断;(2) 对于偶然攻击,要求水印的检测准确无误. 而由上述分析,偶然攻击会令大部分检测错误点孤立,为了达到这种效果,必须选择较小的 m. 另外一方面,m 的大小会直接影响到嵌入水印的容量,进而影响到检测的精确度. 而一般来讲,当稠密概率小到 10 %以下时,大部分检测错误点已经呈现孤立状态. 因此,实验中取 $m = 4$($p_d = 0.09$),这既满足了大部分检测错误点都孤立的要求,又可以保证嵌入水印在容量上不致太小;(3) 对于恶意攻击,能够定位篡改区域. 为了给出一个量化的评判标准,需要对每个水印嵌入的频率区域做如下定义:

稠密点　当前水印检测错误点 $x(i,j)$ 是稠密的是指它的八个临近像素点至少有一个是检测错误点.

稀疏点　当前水印检测错误点 $x(i,j)$ 是稀疏的是指八个临近像素点没有一个是检测错误点.

$area_{l,dense} = \{$稠密区面积$\} = \{$稠密点个数$\}$;

$area_{l,sparse} = \{$稀疏区面积$\} = \{$稀疏点个数$\}$;

$area_{l,total} = area_{l,dense} + area_{l,sparse}$;

$area_l = \{$第 l 个分块面积$\} = \{$第 l 个分块像素点总数$\}$;

$$\lambda_l = \frac{area_{l,total}}{area_l},\quad \delta_l = \frac{area_{l,dense}}{area_{l,total}};$$

λ 和 δ 在一定程度上反映了篡改的程度和强度,因此,可以作为攻击类别判断的依据. 为此,定义如下判断准则:

(1) 对于任意 l,$\lambda_l = 0$,那么无修改;

(2) 若存在 l,使得 $\lambda_l > 0$ 且,$\delta_l < \alpha$,那么认为是偶然修改. α 是预先取定的 0.5 到 1 之间的一个实数;

(3) 对于任意 l,$area_{l,dense} = area_{l,total}$,认为是恶意攻击.

阈值 α 的选取依据的是最小均方误差准则,使得提取水印达到视觉可以接受的程度. 通过对具有不同纹理图像的实验,阈值确定为 0.55 时效果比较理想. 为了使经受 JPEG 压缩后提取出来的水印依然可以辨认,还必须把那些由于压缩而带来的偶然的系数值改变,从而使得水印检测错误的像素点去除. 而由上述分析,这些点稠密的概率非常小,换句话说就是这些点往往呈现孤立的状态. 为了去掉这些孤立点,增强提取水印的效果,可以先对各子频带水印提取图先进行滤波,然后再组合成一幅提取水印图. 对于区域篡改,算法要求定位篡改区域,这也可以从金字塔型的差图中得到. 依据图像融合技术[20],本文的算法达到了较好的篡改区域定位能力. 图 4 给出了 $L=3$ 时水印嵌入以及篡改检测过程的具体图示.

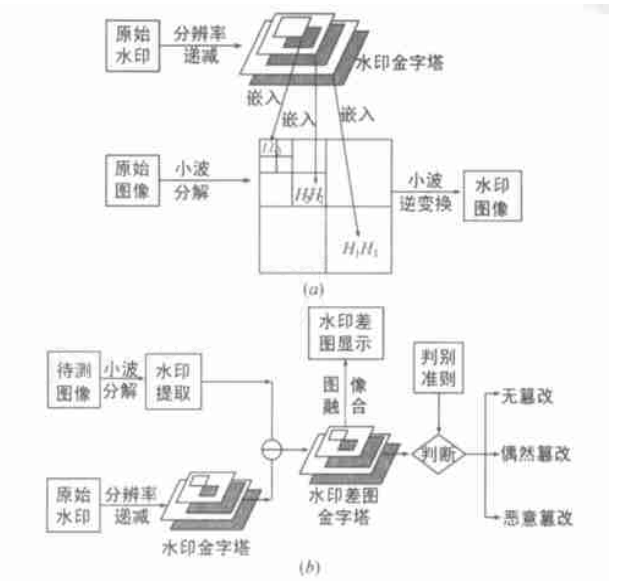

图 4 算法流程图.
(a) 嵌入流程; (b) 水印提取和篡改判断流程图

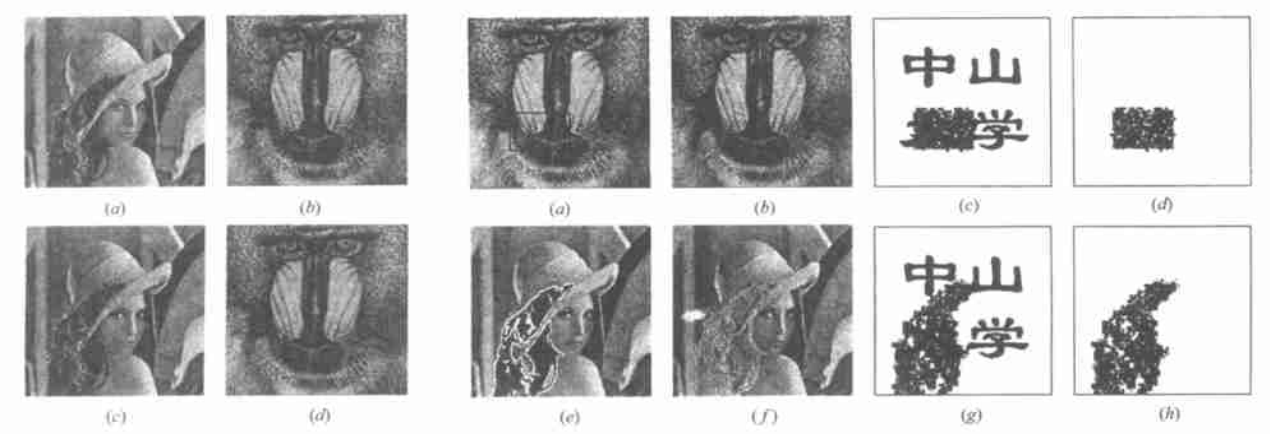

图 5 (a)、(b) 为原始图像;
(c) 水印图像(PSNR = 38.43dB);
(d) 水印图像(PSNR = 31.86dB);

图 6 篡改探测图. (a) 水印图像,黑框内内容将被篡改,以原始图像内容替换; (b) 篡改后图像; (c)、(d) 分别为相应水印提取图和差图; (e) 水印图像,白线区域内头发将被篡改,亮度加大; (f) 篡改结果图; (g)、(h) 分别为相应水印提取图和差图

8 实验结果

我们的实验对象是具有不同纹理特征的 lena 和 baboon 图像(图 5(a),(b),均 256 ×256 ×8bits). 由于选取 $m=4$,因此水印与原始图像具有相同尺寸. 图 5(c),(d) 表示嵌入水印后的图像. 图 7 和表 1 分别给出了在 JPEG 压缩质量因子为 90 %,80 %,70 %,60 %,50 % 时的水印提取图和判定攻击类别. 从图中看到质量因子为 50 %、60 % 的时候,已经很难看出水印的原来面目,我们也根据判断准则给出了恶意攻击的判断. 当质量因子为 90 %,80 %,70 % 时,水印图中的"中山大学"四个字还可以辨认出来,攻击判断为偶然攻击. 对于恶意篡改,比如部分替换、修改等,也给出了判断结果. 从表中可知,通过所提出的判断方案,区域修改被认为是恶意攻击. 图 6 显示出了篡改区域,从图中可知,本文的方案对于恶意篡改的检测非常

表 1 对上述攻击的攻击类别判断表

攻 击	JPEG 压 缩					区 域 修 改	
	90 %	80 %	70 %	60 %	50 %	替 换	增 亮
λ_1	0.02	0.12	0.30	0.40	0.44	/	/
λ_2	0.32	0.44	0.46	0.49	0.49	/	/
λ_3	0.23	0.48	0.49	0.50	0.50	/	/
δ_1	0.10	0.25	0.42	0.92	0.93	1	1
δ_2	0.87	0.93	0.95	0.96	0.96	1	1
δ_3	0.80	0.98	0.99	0.99	0.99	1	1
攻击判断	偶然攻击	偶然攻击	偶然攻击	恶意攻击	恶意攻击	恶意攻击	恶意攻击

敏感,对于篡改区域的定位较为准确.

图 7　JPEG 压缩后水印提取图,从左到右分别对应压缩因子 90 %,80 %,70 %,60 %,50 %

9　结论

本文根据视觉特点,结合量化过程完成水印嵌入.所提出的易碎水印系统具有以下特点:

(1)创建水印金字塔,便于嵌入以及多分辨率检测;

(2)结合视觉特性量化调制,引入图像压缩领域的 Watson 量化矩阵,消除了由于水印嵌入而导致的视觉失真;

(3)结合图像融合技术的多分辨率检测,不同分辨率下的检测结果合成为一副细节更丰富的检测结果图,使得检测精度大大增加;

(4)能够抵抗一定程度的 JPEG 有损压缩,使本系统成为一个半易碎水印系统,更加迎合了实际的需要;

(5)给出一个攻击判别方案,区分恶意攻击和偶然攻击,使得水印对于偶然攻击鲁棒,而对于恶意攻击,篡改探测结果依然精确,从而把 JPEG 压缩与恶意篡改有效的区分开来.

从实验结果可以看到,本文的方案是有效的.进一步的改善主要在于提高抗偶然攻击的能力.

参考文献:

[1] 黄继武,谭铁牛. 图像隐形水印[J]. 自动化学报,2000,26(5):645 - 655.

[2] 孙圣和,陆哲明. 数字水印处理技术[J],电子学报,2000,28(9):85 - 90.

[3] J Fridrich. Methods for tamper detection in digital images[A]. Proc. ACM Workshop on Multimedia and Security[C]. Orlando:ACM,1999. 19 - 23.

[4] E T Lin,E J Delp. A review of fragile image watermarks[A]. Proc. of the Multimedia and Security Workshop (ACM Multimedia '99)[C]. Orlando:ACM,1999. 25 - 29.

[5] 张春田,苏育挺,管晓康. 多媒体数字水印技术[J]. 通信学报,2000,21(9):46 - 52.

[6] 黄继武, Yun Q Shi, Yi Shi. Embedding image watermarks in DC components[J]. IEEE Trans. on Circuits and Systems for Video Technology,2000,10(6):974 - 979.

[7] 黄继武, Yun Q Shi. An adaptive image watermarking scheme based on visual masking[J]. IEE Electronics Letters,1998,34(8):748 - 750.

[8] S Walton. Information authentication for a slippery new age[J]. Dr. Dobbs Journal,1995,20(4):18 - 26.

[9] M Yeung, F Mintzer. An invisible watermarking technique for image verification[A]. Proc. of the IEEE Int. Conf. on Image Processing[C], Santa Barbaa, California: IEEE,1997.

[10] N memon, S Shende, et al. On the security of the yeung-mintzer authentication watermark[A]. Proc. of the IS&T PICS Symposium[C]. Savannah, Georgia: PICS,1999.

[11] J Fridrich, N Memon, et al. Further attacks on yeung-mintzer fragile watermarking scheme[A]. Proc. of the SPIE Electronic Imaging 2000 [C]. San Jose: SPIE,2000.

[12] J Fridrich, M Goljan, et al. New fragile authentication watermark for images[A]. Proc. of the IEEE Int. Conf. on Image Processing[C]. Vancouver, Canada: IEEE,2000.

[13] M Wu, B Liu. Watermarking for image authentication[A]. Proc. of the IEEE Int. Conf. on Image processing[C]. Chicago, Illinois: IEEE, 1998.

[14] P W Wong. A public key watermark for image verification and authentication[A]. Proc. of the IEEE Int. Conf. on Image Processing[C]. Chicago, USA: IEEE,1998.

[15] L M Marvel, W Hartwig, et al. Compression-compatible fragile and semi-fragile tamper detection[A]. SPIE International Conf. On Security and Watermarking of Multimedia Contents Ⅱ[C]. San Jose, USA: IEEE,2000.

[16] Lin Ching-yung, Chang Shih-Fu. Semi-Fragile watermarking for authentication jpeg visual content [A]. SPIE Security and Watermarking of Multimedia Content Ⅱ[C]. San Jose: IEEE,2000.

[17] D Kundur, D Hatzinakos. Towards a telltale watermark techniques for tamper-proofing[A]. Proc. of the IEEE Int. Conf. on Image Processing [C]. Chicago, Illinois: IEEE,1998.

[18] B Watson, G Y Yang, et al. Visibility of wavelet quantization noise[J]. IEEE Trans. On Image Processing,1997,6:1164 - 1175.

[19] ITU-T T. 82. Information technology-Coded representation of pictures and audio information-Progressive bi - level image compression[S].

[20] M Costantini, A Farina. The fusion of different resolution SAR images [J]. Proceedings of The IEEE,1997,85:139 - 146.

[21] 姚庆栋,毕厚杰,王兆华,徐孟侠. 图像编码基础[M]. 浙江:浙江大学出版社,1993. 37 - 68.

作者简介:

胡军全　男,1977 年 3 月生于浙江,中山大学计算机软件与理论专业博士研究生,研究兴趣包括信息安全和多媒体信息处理技术,目前主要从事数字水印技术、多媒体信息认证技术以及小波理论的研究与应用.