能区分图像或水印篡改的脆弱水印方案

和红杰, 张家树, 田 蕾
(西南交通大学信号与信息处理四川省重点实验室, 四川成都 610031)

摘 要: 针对现有脆弱型水印方案不能区分是图像内容还是水印被篡改的问题, 提出一种能区分图像或水印篡改的脆弱水印方案. 该方案用原始图像高 7 位的小波低频系数非均匀量化后生成的低频压缩图像作为水印, 并用混沌系统对水印进行置乱加密, 将安全性得到增强的水印直接嵌入到图像的 LSB 位; 认证时通过差值图像定位图像内容被篡改的位置并指出图像中的水印是否被篡改. 理论分析和仿真实验表明: 该算法不但能精确定位图像内容被篡改的位置, 而且能区分是图像内容被篡改、水印被篡改还是两者同时被篡改.

关键词: 脆弱水印; 混沌; 标量量化; 置乱
中图分类号: TP391 文献标识码: A 文章编号: 0372-2112 (2005) 09-1557-05

A Fragile Watermarking Scheme with Discrimination of Tampers on Image or Watermark

HE Hong-jie, ZHANG Jia-shu, TIAN Lei
(*Sichuan Key Lab of Signal and Information Processing, Southwest Jiaotong University, Chengdu, Sichuan 610031, China*)

Abstract: The existing fragile watermarking algorithms can't recognize whether the modification made to the watermarked image is on the image contents or the embedded watermark or both tampered by attackers. In this paper a fragile watermarking scheme with discrimination of tampers on image or watermark is proposed. The low-frequency compressed image, whose low-frequency wavelet coefficients of 7 Most Significant Bits (MSBs) of original image are nonuniform scalar quantization, is converted into a binary sequence as the watermark is to be embedded. The improved security watermark scrambled by chaotic systems is embedded into the LSB of the image data. During image authentication, the proposed method is able to detect the tampered location and discriminate tampers on Image or watermark from the difference image between the low-frequency compressed image and reconstructed image by watermark. Theoretic analysis and simulation results show that the proposed algorithm may not only provide excellent results of detecting the tampered location, but also indicate whether the modification made to the watermarked image is on the image contents or the embedded watermark or both.

Key words: fragile watermark; chaos; scalar quantization; scrambling

1 引言

采用数字水印技术进行网络传输中的图像认证已成为当前国内外图像信息认证领域的研究热点. 在一些应用中, 例如法律证据图像、新闻图像、医疗图像等, 对图像的一点修改就会使人对图像的真实性产生怀疑, 脆弱水印正是针对这一类应用而设计的. 脆弱水印通常应该满足下特点: 不可见性、对加入水印图像篡改的敏感性、篡改定位能力、提取水印不需要原始图像等.

文献[1]、[2]在文献[3]的基础上, 分别通过添加参数和分层来克服文献[4]提出的矢量攻击(VQ attack); 文献[5]基于混沌对初值的极端敏感性, 将原始图像最低位置零后的像素灰度值经若干次混沌迭代生成水印, 然后将生成的水印嵌入图像的 LSB. 这些水印算法的共同特点是: 根据图像块(或单个像素)的高七位采用特定的算法生成水印, 将生成的水印嵌入到该图像块的 LSB 位; 认证时通过比较被测图像块高七位计算得到水印与存放在该图像块最低位(LSB)的水印是否相同, 判定该图像块是否被篡改. 不足之处在于: 它们仅能指出对图像的篡改位置, 而不能区分是高七位(7 MSBs)图像内容被篡改、是 LSB 位的水印被篡改, 或是两者同时被篡改. 由于对图像内容的篡改会破坏原始图像的使用价值, 脆弱水印算法对此类篡改必须能检测出并精确定位, 以保证认证的可靠与有效; 而对水印的篡改不影响图像的使用价值, 这种仅水印被篡改的图像应当通过认证, 否则不加区分地一律不通过认证, 致使本来可以直接使用的图像必须重新传输, 从而降低数字图像的交换效率, 造成真实的图像不能得到有效的利用,

收稿日期: 2004-09-06; 修回日期: 2005-05-28
基金项目: 四川省杰出青年带头人培养基金(No. 03ZQ026-033); 国家部级基金项目(No. 51430801040T2201); 专利(申请号: 200410040433.6).

妨碍数字图像认证技术的推广与应用. 例如: 作为诉讼证据使用的数字图像, 若采用上述方法进行认证与鉴别, 可能会出现这样的情况: 使本来可以作为证据使用的真实图像受到怀疑而无法作为有效的证据; 新闻图像若采用此种方法进行认证与鉴别, 使本来能反映事实真相的新闻信息也将受到怀疑, 无法满足新闻传播及时性的要求. 另一方面也给攻击者以有机可乘, 攻击者可以通过篡改水印来伪造对图像内容的篡改, 使本来真实的图像不能通过认证, 从而达到他们的某种目的. 因此, 能区分是图像内容还是水印被篡改的脆弱水印技术就成为数字图像认证技术推广与应用必须解决的问题.

针对现有脆弱型水印方案不能区分是图像内容还是水印被篡改的问题, 本文从水印选取和认证两个方面进行改进, 提出了一种能区分图像与水印篡改的脆弱水印方案. 该方案用原始图像高 7 位小波低频系数标量量化生成的低频压缩图像作为水印, 通过混沌置乱加密, 将安全性得到增强的水印直接嵌入到原始图像的LSB 平面; 认证时通过从水印中恢复的低频压缩图像, 可以看出原始图像的"概貌"; 通过差值图像可以定位图像内容被篡改的位置, 并能指明图像被篡改的方式: 图像内容被篡改、水印被篡改还是两者均被篡改; 二者结合可以直观地看出攻击者对图像作了怎样的篡改. 该算法性能稳定、原理清晰、容易实现且认证结果直观, 仿真结果也证实了该算法的有效性.

2 水印的生成

小波分析(Wavelet Analysis) 是公认的最新时-频分析工具, 图像经小波分解后在低频系数中保存了图像的大量信息, 在兼顾篡改定位、视觉特性和水印容量的基础上, 本文选取二维一级小波分解的低频系数, 对其作 4 比特非均匀标量量化(Scalar Quantization) 生成低频压缩图像, 其对应的二进制作为水印.

基于混沌映射数量众多, 以及混沌系统对初值的极端敏感性、良好的随机性和容易再生等特点, 本文利用混沌序列对水印置乱加密来增强水印的安全性. 置乱加密后的水印既保存原始图像的大量信息又具有随机分布的优点, 并且认证时可以区分对图像内容和水印的篡改. 水印生成算法框图如图 1 所示.

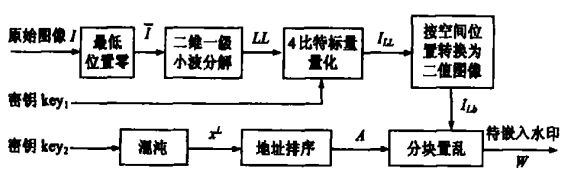


图 1 水印生成算法框图

水印生成步骤:

Step1: 将原始图像 I(大小为 $m*n$) 的最低位置零生成 $\bar{I}$, 对 $\bar{I}$ 作二维一级小波分解(本文用 DB1 小波基), 其低频系数记为 LL;

Step2: 对低频系数 LL 作基于密钥 key1 的 4 比特非均匀标量量化, 生成低频压缩图像 I_{LL};

量化过程用公式描述为:

$$I_{LL} = Q(LL, \text{key}_1) \tag{1}$$

对应规则 Q 为:

$$I_{LL_{ij}} = \begin{cases} k, & ll_{ij} \in [\min + kq + \delta_k, \min + (k+1)q + \delta_{k+1}) \\ 15, & ll_{ij} = \max \end{cases} \tag{2}$$

其中, $i = 1, 2, \cdots, m/2, j = 1, 2, \cdots, n/2$, $q = \lceil \frac{\max - \min}{32} \rceil$ 称为均匀量化步长, max 和 min 分别为 LL 中元素的最大值和最小值, $\lceil\ \rceil$ 表示上取整. $\{\delta_k, k = 0, 1, \cdots 15\}$ 为基于密钥 key1 产生的取值不超过 $(-q/4, q/4)$ 的随机序列, 图 2 为非均匀量化图示.

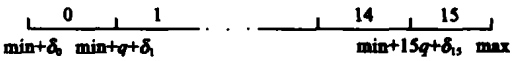


图 2 基于密钥 key1 的非均匀标量量化

Step3: 把低频压缩图像 I_{LL} 的每个元素转换为 4 位二进制, 按空间顺序排列为二值矩阵 I_{Lb}.

$$(I_{LL})_{(m/2)*(n/2)} \rightarrow (I_{Lb})_{(m/2)*(n/2)} \tag{3}$$

其中, $(I_{LL_{ij}})_{10} = (b_3 b_2 b_1 b_0)_2$, $I_{Lb_{ij}} = \begin{bmatrix} b_3 & b_2 \\ b_1 & b_0 \end{bmatrix}$, $i = 1, 2, \cdots, m/2, j = 1, 2, \cdots, n/2$;

Step4: 利用混沌系统生成长度为 L 的混沌序列 x^L, 采用稳定的排序法生成地址有序序列 A.

本文采用文献[6, 7]Hènon 混沌映射系统:

$$x_{n+1} = (1 + 0.3(x_{n-1} - 1.08) + 379x_n^2 + 1001 * y_n^2) \bmod 3 \tag{4}$$

其中, y_n 可以是任意的混沌序列(本文取 logistic 离散混沌映射), 初值在 ± 1.5 之间时系统具有混沌吸引子. 由于 y_n 的加入, 使得混沌序列的周期加大, 从而混沌系统对初值的敏感性会更高并且能够克服有限字长的影响[6, 7].

地址有序序列 A 的生成: 设混沌序列 $x^L = \{x_1, x_2, \cdots, x_i, \cdots, x_L\}$, 确定 $1, 2, \cdots, L$ 的一种排列 $p_1, p_2, \cdots, p_L$, 使其相应的混沌序列 $\{x_{p_1}, x_{p_2}, \cdots, x_{p_L}\}$ 满足非递减(或非递增) 关系.

令: $A(i) = p_i, \quad i = 1, 2, 3, \cdots, L$ (5)

称 A 为混沌序列 $x^L = \{x_1, x_2, \cdots, x_i, \cdots, x_L\}$ 的地址有序序列.

Step5: 利用上步的地址序列 A 对 I_{Lb} 分块置乱生成待嵌入的水印 W.

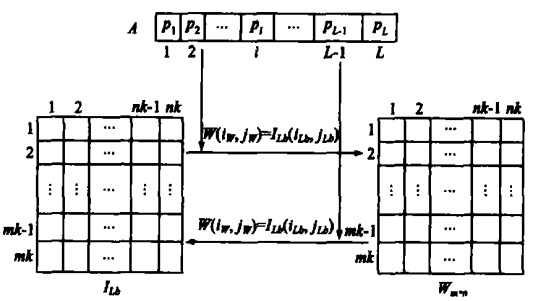


图 3 水印分块置乱与恢复框图

将二值矩阵 I_{Lb} 分为大小相同的块, 设用 nk、mk 分别表示每行、列的块数, 则 $L = mk * nk$. 根据上步生成的地址有序序列 A 重排 I_{Lb} 中每一块的位置, 得到置乱后的二值矩阵 W. 图 3 示出置乱恢复框图, 相应的公式描述如下:

$$W(i_w, j_w) \underset{\text{置乱}}{\overset{\text{恢复}}{\rightleftharpoons}} W_{Lb}(i_{Lb}, j_{Lb}) \tag{6}$$

其中,
$$i_w = \lfloor (A(\text{temp}_{ij}) - 1)/nk \rfloor + 1$$
$$j_w = A(\text{temp}_{ij}) - (i_w - 1) * nk$$
$$\text{temp}_{ij} = (i_{Lb} - 1) * nk + j_{Lb}$$

上述算法产生的水印序列具有以下特点: ①由水印图像和密钥很容易得到唯一的水印序列, 且对图像的变化敏感; ②没有密钥 key1 很难伪造水印序列; ③不同图像的水印序列互不相同; ④水印类似随机分布、水印中保存了原始图像的大量信息并且可以恢复出来; ⑤利用混沌置乱可以使局部像素点的有关信息在水印中均匀(随机)分布.

3　水印算法

3.1　水印嵌入

为了在保证不可见的前提下尽可能多的嵌入水印, 本文直接将水印嵌入图像的 LSB 位. 用公式描述为:

$$\overline{I} = \lfloor I/2 \rfloor * 2, \qquad I^w = \overline{I} + W \tag{7}$$

其中, I 为原始图像, I^w 为水印图像.

3.2　水印提取与认证

根据上述嵌入算法可知, 由于最低位平面就是相应的水印, 因此, 提取水印不需要原始图像, 即

$$W^* = \text{mod}(I^*, 2) \tag{8}$$

这里, I^* 表示被测图像. W^* 是从被测图像中提取的水印.

图像认证时, 通过从水印中恢复的低频压缩图像, 可以看出原始图像的"概貌"; 通过比较原始图像与被测图像的低频压缩图像是否相同判定对图像的篡改方式. 认证框图如图 4 所示, 具体步骤如下:

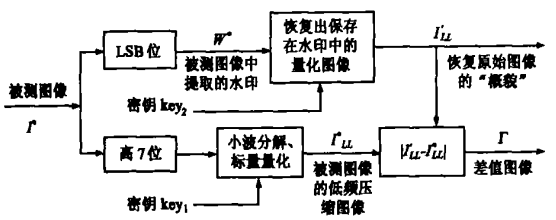


图 4　水印的提取与认证算法框图

Step1: 根据混沌密钥 key$_2$ 和被测图像提取的水印 W^* 恢复原始图像的低频压缩图像 I'_{LL}, 根据 I'_{LL} 可以看原始图像的"概貌".

Step2: 由密钥 key$_1$, 采用水印生成步骤中的 step1 和 step2, 计算被测图像 I^* 的低频压缩图像 I^*_{LL};

Step3: 定义差值图像 $\Gamma = |I'_{LL} - I^*_{LL}|$, 通过差值图像上非零点的分布判定图像是否被篡改及被篡改的方式.

若水印没有被篡改, 由 step1 步恢复的 I'_{LL} 等于原始图像的低频压缩图像 I_{LL}; 若水印被篡改, 对局部水印的篡改经置乱恢复后, 被篡改的水印信息在整个水印中呈随机分布, 由 step1 步恢复的 I'_{LL} 上会出现随机分布的噪声点(与 I_{LL} 不相等的点), 但 I'_{LL} 仍然可以近似反映水印图像的基本内容; I^*_{LL} 是被测图像 I^* 的低频压缩图像, 当被测图像未被篡改时, I^*_{LL} 和 I_{LL} 相等; 当图像内容被篡改时, 对应篡改区域 I^*_{LL} 和 I_{LL} 的值不相等. 因此, 当水印被篡改时, 差值图像 Γ 出现类似随机分布的小块不为零的噪声点; 当图像内容被篡改时, 差值图像 Γ 中的非零点集中于图像被篡改的区域.

采用本文方法定位图像内容被篡改的位置并判别不同篡改方式的方法可描述为:

若差值图像中存在若干呈随机分布且无集中分布的非零点, 认定水印被篡改; 若差值图像中有若干非零点集中于某区域且无随机分布的非零点, 说明该区域的图像内容被篡改; 若差值图像中同时存在随机分布的非零点和若干非零点集中于某区域的情况, 表明该图像内容和水印被同时被篡改. 此时, 根据非零点集中区域面积 ΔS 大小可以定位图像内容被篡改的位置, 即当 $\Delta S \geqslant T$ (T 为阈值模板)时, 认定对应区域的图像内容被篡改.

本文选取置乱块的大小为 2* 2, 阈值模板 T 为 3* 3. 下面分析选取阈值模板 T 为 3* 3 的依据: 设水印的篡改量为 Δw, 则由于水印改变而造成差值图像 Γ 中某点不为零的概率 $p_1 = \Delta w/(m * n)$, 根据概率论可知, 由于水印改变造成 3* 3 区域中所有点均为 1 的概率为 $p_{3*3} = (p_1)^9$. 在认证水印算法中, 攻击者的目的不是破坏水印, 对水印的篡改量不会太大, 因此由于水印改变而造成 Γ 中 3* 3 区域全为 1 的概率 p_{3*3} 很小; 若对图像信息的篡改块大于 6* 6, 有后面的篡改定位能力分析可知, 对图像信息的篡改超过一定范围就一定会造成对应的位置点非零, 因此对大于 6* 6 的图像信息篡改造成 Γ 中 3* 3 非零点的概率较大. 因此, 当 Γ 中非零点的面积 $\Delta S \geqslant 3 * 3$ 时, 判定该位置的图像内容被篡改.

由上述分析可见, 当图像和水印同时被篡改时, 虽然本文算法存在不能区分小块图像内容(小于 6* 6)与水印篡改的缺陷, 但考虑到攻击者对图像有意义的篡改区域往往比较大, 因此这个缺陷在实际应用中是可以接受的.

4　性能分析

4.1　不可见性分析

为了衡量水印图像与原始图像之间的差别, 定义峰值信噪比 PSNR (Peak Signal-to-Noise Ratio)为:

$$\text{PSNR} = 10\log_{10}\left[\frac{255 * 255}{\frac{1}{m * n}\sum_{i=1}^{m}\sum_{j=1}^{n}[I(i,j) - I^w(i,j)]^2}\right] \tag{9}$$

把水印信息嵌入到图像的 LSB 位, 最差的情况是原始图像与水印图像的最低位都不相同, 即 $\sum_{i=1}^{m}\sum_{j=1}^{n}[I(i,j) - I^w(i,j)]^2$ 为 $m * n$, 此时计算 PSNR = 48.1308, 也就是说在 LSB 位嵌入水印的水印图像与原始图像的 PSNR 一定大于 48.1308. 从概率论的角度, 因为 LSB 平面的每个比特是独立的, 即 $P_0 = P_1 = 0.5$ (P_0、P_1 表示 $I(i,j) - I^w(i,j))^2$ 为 0、1 时的概率), 由此可得 $E([I(i,j) - I^w(i,j)]^2) = 0.5$, 则对应的 PSNR 数学期望为 E(PSNR) = 51.1411. 可见, 本算法能得到很高的峰值信噪比, 可满足脆弱水印不可见性的要求.

4.2　篡改定位能力分析

算法通过差值图像 $\Gamma = |I^{w'}_{LL} - I^*_{LL}|$ 定位图像被篡改的位

置. 下面以 DB1 小波基为例来说明算法的篡改定位能力.

DB1 小波基的二维小波变换从数学角度可以近似用下述公式描述:

$$I_{IL}(i,j)=\mathrm{sum}(I(2*i-1{:}2*i,2*j-1{:}2*j))/2 \quad (10)$$

其中, $i=1,2,\cdots,m/2, j=1,2,\cdots,n/2$.

8 位灰度图像每一个像素的取值范围为$[0,255]$, 因此 I_{LL} 的取值范围为$[0,510]$, 做 4 比特均值标量量化时的量化步长为 $q<(510/16)=32$. 对一个像素值或一块 2* 2 像素值的和改变超过 64, 使其量化值不相等, 从而可以定位出图像内容被篡改的位置.

4.3 区分篡改分析

该算法通过从水印中恢复的低频压缩图像和差值图像 Γ 定位图像内容被篡改的位置, 并指出是图像内容被篡改、水印被篡改或是两者同时被篡改.

若水印没有被篡改, 则从水印中恢复的低频压缩图像 I'_{LL} 等于原始图像高 7 位的低频压缩图像 I_{LL}; 当水印被篡改, 对局部水印的篡改经置乱恢复后, 被篡改的水印信息在整个水印中呈随机分布, I'_{IL} 上就会出现随机分布的噪声点, 但 I'_{IL} 仍然可以近似反映原始图像的基本内容. I^*_{IL} 是被测图像高 7 位的低频压缩图像, 有公式 $\Gamma=|I'_{IL}-I^*_{LL}|$ 计算差值图像. 当图像内容被篡改时, 差值图像 Γ 中对应图像内容被篡改的位置不为零, 不为零的区域与篡改的区域的形状相似; 当水印被篡改时, 中出现类似随机分布的小块不为零的篡改点.

4.4 时间复杂度分析

该算法中的水印嵌入和提取是两个对称的过程, 时间复杂度是同一个数量级的.

设图像的大小为 $m*n$, 算法的规模用 N 表示, 即 $N=m*n$, 算法的主要操作是小波分解、低频系数的 4 比特量化和二值图像置乱. 一级小波分解的时间复杂度为 $O(N)$; 设用 t 表示将一个实数量化为 4 比特数所需要的时间, 则对低频系数的量化时间复杂度为 $O(t*(N/4))$; 二值图像置乱的主要的操作: 混沌序列的产生、排序及置乱, 设置乱块的大小为 N_k(置乱块中的元素个数), 则对图像置乱的时间复杂度为 $O((N/N_k)2)$, 所以该算法的时间复杂度为:

$$f(N)=O\left(N+t*\frac{N}{4}+\left(\frac{N}{N_k}\right)^2\right) \quad (11)$$

可以看出, $f(N)\propto 1/N_k$, N_k 越大, 时间复杂度越小, 阈值 T 的选取越大, 对图像的小块篡改与水印的篡改不易区分, 所以必须在计算复杂度和区分不同篡改之间做折衷考虑.

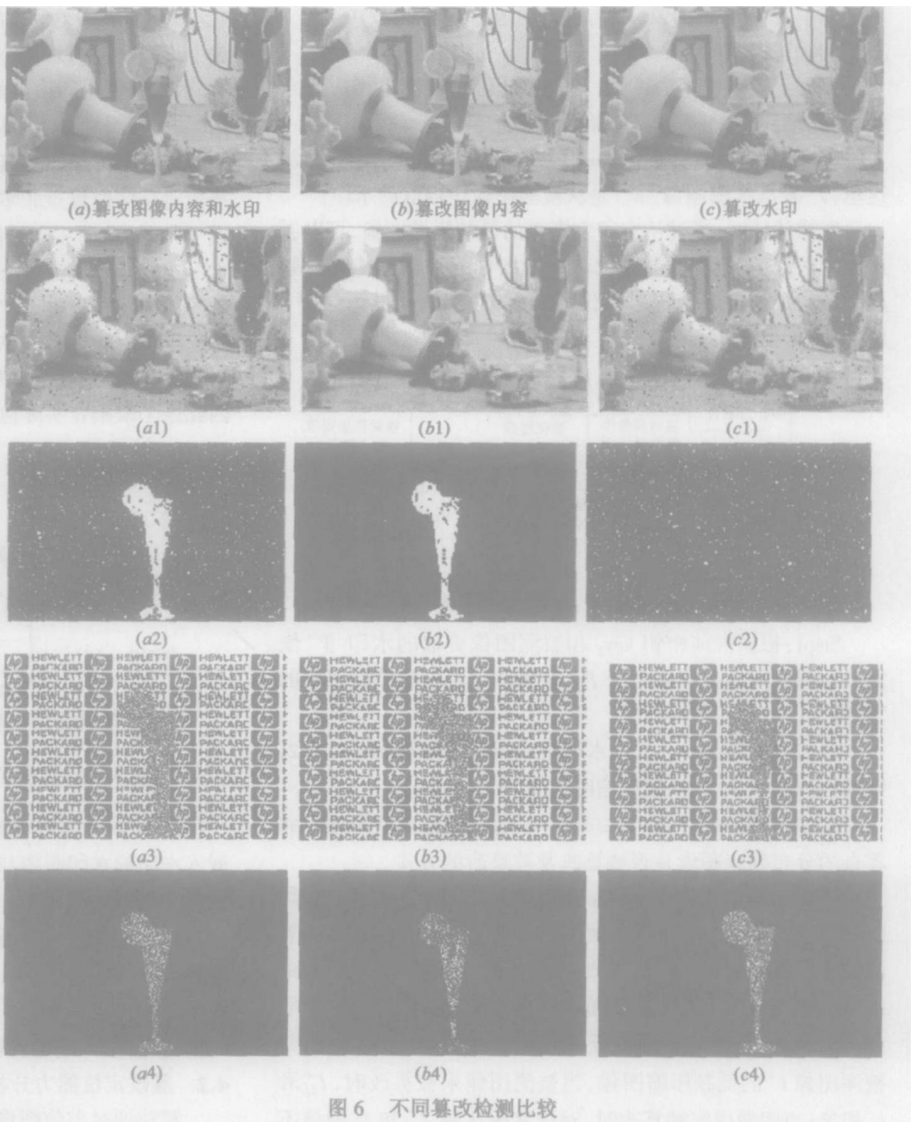
4.5 仿真结果

被测图像为 208* 328* 8 的"vase"灰度图像, 有 256 个灰度级, 像素值介于[0, 255]之间. 以下结果由 MATLAB 仿真所得.

(a)原始图像 (b)水印图像

图 5 原始图像和添加水印后图像

4.5.1 不可见性 图 5 示出原始图像和水印图像, 按公式(8)计算的水印图像与原始图像的PSNR 为 51.2108dB, 与理论



(a)篡改图像内容和水印 (b)篡改图像内容 (c)篡改水印

(a1) (b1) (c1)

(a2) (b2) (c2)

(a3) (b3) (c3)

(a4) (b4) (c4)

图 6 不同篡改检测比较

分析结果E(PSNR) = 51.1411基本一致. 无论是从图5(b)还是数值仿真结果都验证了本文算法能满足脆弱水印不可见性的要求.

4.5.2 不同篡改检测　图6示出对三种不同篡改的检测结果. 使用photoshop编辑软件在水印图像上添加一个酒杯, 该图像称为直接篡改图像如(*a*)所示; (*b*)为直接篡改图像的高7位+水印图像的LSB; (*c*)为水印图像的高7位+直接篡改图像的LSB;

(*a*1), (*b*1), (*c*1)分别是从相应不同篡改图像提取的水印中恢复出来的低频压缩图像, (*a*1)和(*c*1)中有类似随机分布的"噪声", 说明相应图像的水印被篡改; (*b*1)中没有类似随机分布的"噪声", 说明相应图像中的水印没有篡改; (*a*1)和(*b*1)中没有"酒杯", 而被测图像中有酒杯, 可以直观判断被篡改的图像是在图像中加了一个"酒杯". (*c*1)与被测图像相比看不出有明显的变化, 可以初步判定该被测图像仅是水印部分被修改, 不影响图像的使用价值;

(*a*2)、(*b*2)和(*c*2)是相应被测图像的差值图像, (*a*2)中既存在非零点集中区域, 又存在类似随机分布的"噪声", 判定被测图像中的图像内容和水印同时被篡改, 其中非零点集中区域为图像内容被篡改的位置; (*b*2)中仅存在非零点集中区域, 判定被测图像中非零点集中区域的图像内容被篡改; (*c*2)中仅有"噪声", 而无非零点集中的区域, 判定该被测图像仅有水印被篡改. 从图6(*a*1)、(*b*1)、(*c*1)和(*a*2)、(*b*2)、(*c*2)仿真结果可以看出与理论分析相一致.

文献[2]中, 使用有意义的二值图像作为水印, 对这三种不同篡改的检测结果如图6(*a*3), (*b*3), (*c*3)所示; 文献[5]中, 使用篡改定位矩阵来检测图像的篡改, 对这三种不同篡改的检测结果如图6(*a*4), (*b*4), (*c*4)所示; 从图中可以看出, 这两种算法对这三种不同篡改检测的结果相同, 均是给出了图像被篡改的位置, 而不能区分这三种不同篡改.

5 结论

针对现有定位型脆弱水印算法不能区分是图像内容还是水印被篡改的问题, 本文提出了一种能区分图像或水印篡改的定位型脆弱水印算法, 该算法通过对图像内容(低频压缩图像)的比较来检测图像是否被篡改、定位篡改的位置, 并能区分是图像内容被篡改、水印被篡改还是两者均被篡改. 同时, 在生成水印时, 使用基于密钥的非均匀标量量化, 进一步扩大密钥空间, 使水印算法更安全. 理论分析与实验仿真结果表明: 该算法在保留现有定位型脆弱水印算法具有的篡改定位、不可见性和提取不需要原始图像等优点的同时, 还可以明确判断是图像内容被篡改、水印被篡改还是两者同时被篡改, 其认证结果直观, 视觉效果好, 为定位型脆弱水印开辟了一条新的路径, 有一定的实用价值.

参考文献:

[1] P W Wong, et al. Secret and public key image watermarking schemes for image authentication and ownership verification[J]. IEEE Trans on Image Processing, 2001, 10(10): 1593-1601

[2] M U Celik, et al. Hierarchical watermarking for secure image authentication with localization[J]. IEEE Trans on Image Processing. 2002, 11(6): 585-595.

[3] P W Wong, et al. Public key watermark for image verification and authentication[A]. Proc of 1998 IEEE Int Con on Image Processing[C]. Chicago, IL, USA: IEEE, 1998, 1: 455-459.

[4] M Holliman, et al. Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes[J]. IEEE Trans on Image Processing, 2000, 3(9): 432-441.

[5] 丁科, 何晨, 王宏霞. 一种定位精确的混沌脆弱数字水印技术[J]. 电子学报, 2004, (6): 1009-1012
DING Ke, HE Chen, WANG Hong-xia. A Chaotic Fragile Watermarking Technique with Precise Localization[J]. Chinese Journal of Electronics, 2004, (6): 1009-1012. (Chinese Source)

[6] 张家树, 田蕾. 基于密钥的混沌数字水印方法[J], 通信学报 2004, 25(8): 126-131.
ZHANG Jia-shu, TIAN Lei. A new chaotic digital watermarking method based on private key[J]. Journal of China Institute of communications, 2004, 25(8): 126-131. (Chinese Source)

[7] J S Zhang, et al. A new watermarking method based on chaotic map [A]. IEEE International Conference on Multimedian an Expo[C]. Taiwan: IEEE, 2004.

作者简介:

和红杰　女, 1971年生于河南省平顶山市, 西南交通大学博士研究生, 主要研究方向为图像处理、信息隐藏技术等. E-mail: hehojie@sohu.com.

张家树　男, 1965年生于四川省西充市, 四川省学术与技术带头人, 西南交通大学教授、博士生导师, 中国电子学会高级会员, 主要研究方向为混沌信息工程学、现代信号与智能信息处理、通信理论与电子对抗技术等.

田　蕾　女, 1979年生于陕西定边, 硕士, 主要研究方向为数字水印技术.