一种能区分水印或内容篡改的脆弱水印算法

王国栋[1],刘粉林[1],刘 媛[2],姚 刚[2]
(1. 解放军信息工程大学信息工程学院,河南郑州 450002; 2. 解放军信息工程大学理学院,河南郑州 450002)

摘 要: 针对目前脆弱水印算法大多无法区分水印被篡改还是内容被篡改的问题,本文基于多重水印技术提出了一种能区分水印或内容篡改的脆弱水印算法. 该算法由子块的主要 DCT 系数生成恢复水印,将其嵌入到偏移子块的次低位;待恢复水印嵌入后,将恢复水印作为子块内容的一部分生成认证水印,将其嵌入到子块的最低位. 理论分析和实验结果表明:本文算法在抵抗量化攻击的同时,不仅能准确定位图像内容被篡改的位置,而且能区分是水印被篡改还是图像内容被篡改,并且在一定条件下可以对内容被篡改的区域进行恢复.

关键词: 脆弱水印; 混沌; 篡改定位; 恢复
中图分类号: TP391 **文献标识码**: A **文章编号**: 0372-2112 (2008) 07-1349-06

An Image Authentication Scheme with Discrimination of Tampers on Watermark or Image

WANG Guo-dong[1], LIU Fen-lin[1], LIU Yuan[2], YAO Gang[2]
(1. *Information Engineering Institute, the PLA Information Engineering University, Zhengzhou, Henan* 450002, *China*;
2. *College of Science, the PLA Information Engineering University, Zhengzhou, Henan* 450002, *China*)

Abstract: The existing fragile watermarking algorithms almost can't recognize the modification made to the watermarked image is on the image content or on the embedded watermark. In this paper, a novel fragile watermarking scheme is proposed. The recovery watermark of each block is embedded into the Hypo-LSB of the corresponding excursion block selected by a key, and the authentication watermark of each block is embedded into its LSB. Theoretical analysis and simulation results show that the proposed algorithm can not only thwart the VQ attack and locate tampered blocks accurately, but also discriminating tampering watermark from that of content. And in some case, it can restore the tampered region effectively.

Key words: fragile watermarking; chaos; tamper location; recovery

1 引言

伴随着计算机网络及通信技术的飞速发展,数字媒体的应用取得了惊人的进展,它以其独特的优点给人们的生活带来了极大的便利. 然而,利用网络的开放性和计算机强大的处理能力所进行的一些恶意行为,如信息篡改等,不仅使使用者难以判断数字载体的真伪,甚至会造成严重的后果. 以数字图像为例,医学数据库中的原始照片经过不经意的压缩或修改可能会造成误诊,作为法庭证据的照片如果被恶意篡改后就可能扭曲事实真相,等等. 在这些场合下,需要对数字图像的完整性和真实性进行认证,基于数字水印的认证技术是解决上述问题的有效方法之一[1].

基于数字水印的图像认证技术可分为精确认证和模糊认证两类,前者要求水印算法能够检测出任何改变图像像素值或破坏图像完整性的操作,可以准确定位图像被篡改的区域,甚至可以对篡改区域进行恢复,后者则允许在保证图像内容真实的条件下,可以对图像进行一般的处理操作(如压缩及格式转换等). 精确认证和模糊认证有着不同的应用场合,本文关注的是图像的精确认证问题.

基于分块的精确认证算法是一种常见的认证技术. 1998 年,Wong[2]提出了一种基于独立分块的图像认证算法,将图像分割为不重叠的小块,在各个小块上嵌入由各自内容生成的水印,该算法可将篡改定位到独立子块,但文献[3]指出该算法由于分块的独立性,极易受到量化攻击(VQ 攻击);文献[4~6]在文献[2]的基础上,分别通过添加参数、分层及滑动窗口技术以克服量化攻

收稿日期:2007-07-02;修回日期:2007-10-22
基金项目:国家 863 高技术研究发展计划(No. 2006AA01Z409);河南省科技攻关(No. 0623021500);河南省基础与前沿技术研究计划(No. 082300410150)

击,但是降低了文献[2]算法的篡改定位精度;文献[7]结合滑动窗口和层次结构以嵌入水印,通过层次认证可将篡改定位到大小为 2 ×2 的子块,但是 2 ×2 子块的漏检概率高达 1/2,且存在 4 ×4 及 2 ×2 子块的量化攻击问题.这类水印算法的共同特点是:根据图像块的高位内容采用特定算法生成水印,并将水印嵌入到图像的低位,它们在一定程度上可以对图像的篡改区域进行定位,但是无法区分水印被篡改、图像内容被篡改或是两者都被篡改.由于水印被篡改并不影响图像的使用价值,若认证算法能对被篡改加以区分,这将会提高图像的利用效率,在某些场合具有广泛的应用前景.因此,能区分篡改的脆弱水印技术逐渐成为图像认证领域研究的热点之一.

文献[9]提出了一种能区分水印或内容篡改的脆弱水印方案,利用原始图像高七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,利用混沌系统对水印进行置乱加密后嵌入图像的LSB 位,认证时通过差值图像中篡改点的分布特点以区分水印被篡改或内容被篡改,并设定阈值以定位图像内容被篡改的区域.文献[10]提出了一种基于混沌置乱的分块自嵌入水印算法,将由图像块生成的水印按空间位置生成二值水印图像,利用混沌序列加密后嵌入到图像的最低位,认证时将计算所得水印和提取的水印相减生成差值图像,通过比较差值图像块中非零点的个数与设定阈值的关系以区分水印被篡改或内容被篡改.通过分析发现,文献[9]与文献[10]算法在水印篡改较小或内容篡改量较大时,能以较高的概率区分水印或图像内容被篡改,但是当内容篡改量较小或水印篡改量较大时,其认证算法将难以对篡改进行区分.实际中,攻击者对含水印图像的篡改往往是无法预测的且阈值的选取比较困难,这将可能会导致文献[9]及文献[10]由假设篡改量而获得的阈值不再合适,进而增加了其认证算法在区分水印或内容篡改时的误判概率.

针对上述问题,本文结合分块算法和自嵌入[9]水印算法,提出了一种能区分水印或内容篡改的图像认证方案.该方案由图像块高位的主要 DCT 系数生成恢复水印,将其嵌入到偏移子块的次低位;待恢复水印嵌入后,将其作为子块内容的一部分生成认证水印,并将认证水印嵌入到子块的最低位.双重水印的嵌入使得本文算法不仅能准确定位图像内容被篡改的位置,而且能区分水印被篡改还是内容被篡改,并且在一定条件下可以对被篡改的区域进行恢复.

2 偏移子块的选取

设一个映射函数 T, $T(b_i)$ 表示子块 b_i 的偏移子块,由映射函数 T 选取偏移子块时应满足以下要求:

(1) 映射 T 应为一一对应.

(2) 图像块 b_i 与其偏移子块 $T(b_i)$ 在图像上要相距较远,从而使得两块同时被修改的概率尽可能小.

(3) 控制映射函数的用户密钥应有较大的密钥空间以保证其安全性.

本文使用对初值具有极端敏感性的混沌系统来选取子块的偏移子块,具体描述如下:

大小为 $M \times N$(M 和 N 若不是 8 的整数倍则补足)图像 X 分割为 8 ×8 的子块 $b_1, b_2, \cdots b_i, \cdots b_r$($r$ 为图像总块数).考虑如下一个具有 $[0, a), [a, b), [b, 1-a), [1-a, 1]$ 四个子区间的一维分段线性混沌映射:

$$g(x) = \begin{cases} 4x, & 0 \le x < a \\ 2 - 4x, & a \le x < b \\ g(1-x), & b \le x \le 1 \end{cases} \quad (1)$$

选择对 $g(x)$ 定义区间的第 3 子区间 $c_3 = [b, 1-a)$ 进行扩散,将片断 c_3 按照 $e:1-e$ 的比例分成两段 $c_{31} = [b, b + e/r_0)$, $c_{32} = [b + e/r_0, 1-a)$, e 为扩散系数,且 $e \in (0,1)$, r_0 为常量.取 $a = 4$, $b = 0.5$, $r_0 = 4$,按照选择性扩散的扰动算法形成新的分段线性混沌映射:

$$f(x) = \begin{cases} g(x), & x \notin c_3 \\ g\left(\dfrac{4}{2e}(x - 0.5)\right), & x \in c_{31} \\ g\left(\dfrac{x - \left(0.5 + \frac{e}{4}\right)}{1-e} + 1 - 0.25\right), & x \in c_{32} \end{cases} \quad (2)$$

为简单起见,本文中取扩展系数 $e = 0.001$.设 x_0 为混沌系统的初值.在构造混沌序列时只需要给定初值 x_0 即可.关于该混沌系统的更多性质请参阅文献[13].

给定混沌初值 x_0 及四个距离 d_0, d_1, d_2, d_3.首先使用 x_0 产生四值(0,1,2,3)混沌阵列,然后用距离 d_i(i = 0,1,2,3)在混沌阵列中寻找各个子块的偏移子块.具体步骤如下:

Step 1:设定迭代次数为 r 次.

Step 2:用式(2)进行 r 次迭代,得到混沌轨迹.给混沌轨迹设置阈值 $T_1 = 0.25$, $T_2 = 0.5$, $T_3 = 0.75$,将得到的轨迹四值化,得到长为 r 的 0、1、2、3 混沌序列.即如果 $0 \le f(x) \le T_1$,置为 0;如果 $T_1 < f(x) \le T_2$,置为 1;如果 $T_2 < f(x) \le T_3$,置为 2;如果 $T_3 < f(x) \le 1$,置为 3,四值化为 0、1、2、3 序列.

Step 3:将上一步得到的序列按顺序排列成和图像块数大小相同的混沌阵列.

Step 4:记录混沌阵列中 0,1,2,3 的个数,设序列中 i(i = 0,1,2,3)的个数为 n_i,构造四个一维数组,$a_0[n_0], a_1[n_1], a_2[n_2], a_3[n_3], a_i[n_i]$ 中记录混沌阵列中每 i 个在阵列中的位置.例如 $a_0[100] = 199$ 表示序

列中第 100 个 0 是混沌阵列中第 199 个数(按照从上到下,从左到右的顺序).

Step 5:对于混沌阵列中每个 $i(i=0,1,2,3)$ 的位置记为 (x_i, y_i),其对应的图像块为 $b_{(x_i,y_i)}$,然后在混沌阵列中寻找与 (x_i, y_i) 相距 d_i 个 i 的位置 (x_i', y_i'),其对应图像块为 $b_{(x_i',y_i')}$,那么 $b_{(x_i',y_i')}$ 将作为图像块为 $b_{(x_i,y_i)}$ 的偏移子块.

混沌阵列中的所有元素被分为了 $i(i=0,1,2,3)$ 组,每一组由距离值 d_i 来控制其各个元素的偏移位置. 这相当于将图像 X 的所有子块分为 i 组,每一组都由 d_i 作为偏移值来选择偏移子块,这样子块与其偏移子块将形成一一对应关系. 同时,通过调整适当的距离值可以保证子块与其偏移子块在图像上相距较远. 混沌系统及距离值的引入增大了密钥空间,因而增强了算法的安全性.

当然,也可以采用其它算法来选取偏移子块,如固定偏移值、小 m 序列等,只是我们在实验中发现由该混沌系统结合距离值选取偏移子块的效果较好,能满足偏移子块的要求,故采用该混沌系统.

3　方法原理

3.1　水印生成与嵌入

设原始图像 X 的大小为 $M \times N$,将其分割为 8 ×8 的图像块 $b_1, b_2, \cdots, b_i, \cdots, b_r$. 图像块 b_i 的偏移子块可记为 $b_j = T(b_i)$,则 b_i 的恢复水印 $W_{i\text{-}R}$ 将嵌入到 $T(b_i)$ 的次低位;b_i 的认证水印 $W_{i\text{-}R}$ 则嵌入到自身的最低位. 水印生成和嵌入的流程如图 1 所示.

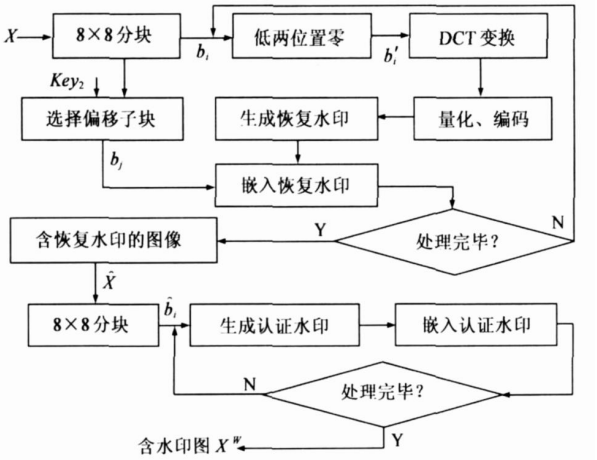


图 1　水印生成和嵌入流程图

水印生成与嵌入具体步骤如下:

(a) 恢复水印的生成与嵌入

(1) 将 b_i 的低两位置零得到 b_i';

(2) 生成 b_i 得恢复水印 $W_{i\text{-}R}$;

Step 1:对 b_i 做 DCT 变换,得到 DCT 系数矩阵 F_i;

Step 2:以质量因子为 0.5 的 JPEG 量化表对 F_i 量化,量化后的 DCT 系数矩阵记为 F_i';

Step 3:用适当的码长分配表对 F_i 进行二值编码,调整码流的长度为 64 比特,记为 $\overline{W}_{i\text{-}R}$,以 Key_1 为密钥加密后作为块 b_i 的恢复水印 $W_{i\text{-}R}$.

(4) 由密钥 Key_2 控制混沌系统(2)以选取 b_i 的偏移子块 $T(b_i)$;

(5) 将 $W_{i\text{-}R}$ 嵌入到 b_i 的偏移子块 $T(b_i)$ 的次低位.

X 中各个图像块的恢复水印均嵌入到其偏移子块后,可将 X 记为 $\hat{X}$.

(b) 认证水印的生成与嵌入

(1) 生成图像块 b_i 的认证水印 $W_{i\text{-}A}$;

记 $\hat{b}_i = (\hat{p}_i^1, \hat{p}_i^2, \cdots, \hat{p}_i^{64})^{\mathrm{T}}$($\hat{p}_i$ 为像素值),选择单向哈希函数对 $\hat{b}_i$ 做哈希运算,得到固定长度比特的信息摘要 $\hat{M}_i$

$$\hat{M}_i = Hash(\hat{b}_i, x, y) = (\hat{M}_i^1, \hat{M}_i^2, \cdots, \hat{M}_i^m \cdots), \hat{M}_i^m \in \{0,1\} \tag{4}$$

上式中 x, y 表示图像块 $\hat{b}_i$ 在图像 $\hat{X}$ 中的位置信息. 由密钥 Key_3 选取 $\hat{M}_i$ 中某些位置上的 64 比特,作为图像块 b_i 的认证水印 $W_{i\text{-}A}$.

(2) 将认证水印 $W_{i\text{-}A}$ 嵌入到图像块 b_i 的最低位.

待所有子块的认证水印均嵌入后,便得到含水印图像 X^W.

3.2　篡改检测与恢复

设 $\tilde{X}$ 为待检测图像,篡改检测过程如图 2 所示. 图像 $\tilde{X}$ 分割为大小为 8 ×8 的图像块 $\tilde{b}_1, \tilde{b}_2, \cdots, \tilde{b}_i, \cdots, \tilde{b}_r$ (r 为图像总块数),图像块 $\tilde{b}_i$ 认证的具体步骤如下:

(1) 由 $\tilde{b}_i$ 的偏移子块 $T(\tilde{b}_i)$ 的次低位提取 $\tilde{b}_i$ 的恢复水印 $W_{i\text{-}R}'$;同时,由图像块 $\tilde{b}_i$ 的最低位提取其认证水印 $W_{i\text{-}A}'$;

(2) 按照水印生成算法生成 $\tilde{b}_i$ 的恢复水印 $W_{i\text{-}R}''$ 和认证水印 $W_{i\text{-}A}''$.

图像的认证流程如图 2 所示:

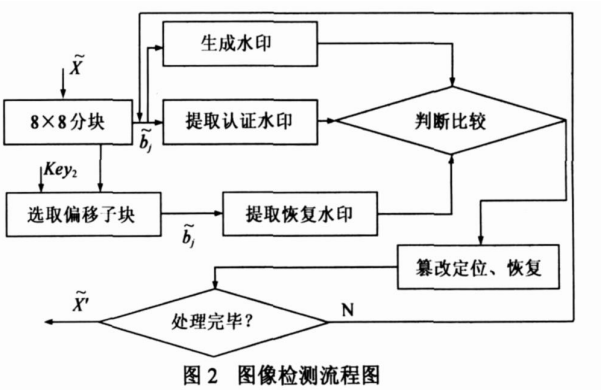


图 2　图像检测流程图

对任意图像块 $\tilde{b}_i$:

(1) 若 $W_{i\text{-}A}' = W_{i\text{-}A}''$, $W_{i\text{-}R}' = W_{i\text{-}R}''$,则判定图像块 $\tilde{b}_i$ 没有被篡改,通过认证;

(2) 若 $W_{i\text{-}A}' \neq W_{i\text{-}A}''$, $W_{i\text{-}R}' = W_{i\text{-}R}''$,则判定图像

块 $\tilde{b}_i$ 中有水印被篡改,块 $\tilde{b}_i$ 通过认证;

(3) 若 $W_{i-A}' = W_{i-A}''$, $W_{i-R}' \neq W_{i-R}''$,则判定图像块 $\tilde{b}_i$ 的偏移子块 $\tilde{b}_j$ 中恢复水印被篡改,此时,块 $\tilde{b}_i$ 通过认证;

(4) 若 $W_{i-A}' \neq W_{i-A}''$, $W_{i-R}' \neq W_{i-R}''$,则判定图像块 $\tilde{b}_i$ 中内容被篡改或内容和水印均被篡改. 此时,判定其偏移子块 $\tilde{b}_j$ 中水印是否被篡改,若 $\tilde{b}_j$ 中水印未被篡改,则 W_{i-R}' 可用来对图像块 $\tilde{b}_i$ 进行恢复;否则,则无法恢复出图像块 $\tilde{b}_i$.

依次处理各个子块,直到所有子块处理完毕便可得到篡改定位结果及恢复后的图像 $\tilde{X}$!

4 算法分析和实验仿真

4.1 算法分析

(1) 图像质量分析

嵌入水印后图像的质量可用峰值信噪比来(*PSNR*)衡量,设原始图像为 X,含水印图像为 X',图像的大小为 $M \times N$,则 *MSE* 和 *PSNR* 分别定义如下:

$$MSE = \frac{\sum_{i}^{M}\sum_{j}^{N}\left(X_{(i,j)} - X_{(i,j)}'\right)^2}{M \times N} \tag{5}$$

$$PSNR = 10 \times \log_{10}\frac{255^2}{MSE} \tag{6}$$

本文把水印信息嵌入到图像的低两位,设 P_{e-k} 为像素值改变 $k(k=0,1,2,3)$ 的概率,则含水印图像和原始图像单个点像素值差值平方的数学期望:

$$E\left((X_{(i,j)} - X_{(i,j)}')^2\right) = \sum_{k=0}^{3} k^2 \times P_{e-k} = \frac{7}{2} \tag{12}$$

由此得到 *MSE* 和 *PSNR* 的数学期望分别为:

$$E(MSE) = \frac{7}{2} \tag{13}$$

$$E(PSNR) = 42.69\text{dB} \tag{14}$$

即使在所有像素点的像素值的低两位都改变,即每个像素点的像素值都改变 3 的最坏情况下,嵌入水印图像的峰值信噪比也能达到 38.59dB,完全符合文献[13]提出的含水印图像的峰值信噪比高 35dB 的要求.

可见,本文算法能得到较高的峰值信噪比,完全符合图像质量的要求.

(2) 篡改检测分析

篡改检测包括虚警概率、漏警概率及篡改定位精度. 虚警概率是指在非篡改区域上检测到篡改的概率. 根据本文算法,当图像没有被篡改时,由其内容计算所得水印和提取的水印将会完全相同,不可能存在误判. 因此,本算法的虚警概率 $P_{FA} = 0$.

漏警概率是指图像被恶意篡改,检测器并未检测到. 本算法中,单独 8×8 的块漏检的概率为 $1/2^{64}$,能以 $1 - 1/2^{64} \approx 1$ 的概率将篡改定位到 8×8 的像素块. 由于在生成子块的认证水印时,使用块的位置信息消除了分块的独立性,因此本算法可抵抗量化攻击.

(3) 区分篡改的分析

攻击者对一副图像的篡改包括篡改水印,篡改内容及篡改水印和内容. 在这三种篡改中篡改水印不会影响图像的使用价值,因此,水印算法若能对水印被篡改加以区分,而对另外两种篡改可准确定位,这无疑将会提高篡改图像的利用效率.

本文算法由图像块的高位内容生成恢复水印,将恢复水印嵌入偏移子块的次低位;同时,恢复水印嵌入后,将其作为图像内容的一部分生成图像块的认证水印,并嵌入自身的最低位. 在认证过程中,分为两级认证以达到区分水印或内容被篡改:

①比较计算所得的认证水印和提取所得的认证水印. 若两者相等,则该子块可通过一级认证;否则,该子块无法通过一级认证,进行二级认证.

②比较计算所得的恢复水印和提取所得的恢复水印. 若两者相等,则说明该图像块无法通过一级认证的原因是由于图像块的水印被篡改,此时并不影响图像块的使用价值,该块可通过二级认证;否则,说明图像块内容被篡改或内容和水印均被篡改.

4.2 实验仿真

(1) 密钥的选取

Step 1:以 $Key_1 = 0.55$ 为混沌系统(9)的初值生成长为 64 的混沌序列 $S_{64} = (s_1, s_2, \cdots, s_{64})$:

$$s_{i+1} = \mu s_i(1 - s_i),\ \mu \in [1,4]\ \ i = 0,1,2,\cdots \tag{9}$$

将 S_{64} 转化为二值序列 Z_{64}:以 0.5 为阈值,当 $s_i \geq 0.5$ 时对应的 $z_i = 1$;否则 $z_i = 0$. 则将 $\overline{W}_{i-R}$ 与 Z_{64} 按位异或,可得 b_i 的恢复水印 W_{i-R}.

Step 2:以 $Key_2 = 0.555$ 为混沌系统(2)的初值,$d_0 = 100$, $d_1 = 1000$, $d_2 = 10000$, $d_3 = 100000$ 为距离值,生成混沌阵列,以选取各子块的偏移子块.

Step 3:生成块 b_i 的认证水印时选取 MD5 消息摘要算法,得到 128 位的消息摘要,定义 Key_3 为选取前 64bit,可得 b_i 的认证水印 W_{i-A}.

(2) 实验结果

在 C ++ Builder6.0 平台下仿真了本实验,所用的码长分配表如图 3 所示:

$$\begin{bmatrix} 7 & 7 & 6 & 4 & 3 & 0 & 0 & 0 \\ 6 & 6 & 3 & 3 & 0 & 0 & 0 & 0 \\ 5 & 3 & 3 & 0 & 0 & 0 & 0 & 0 \\ 3 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

图 3 系数的码长分配表

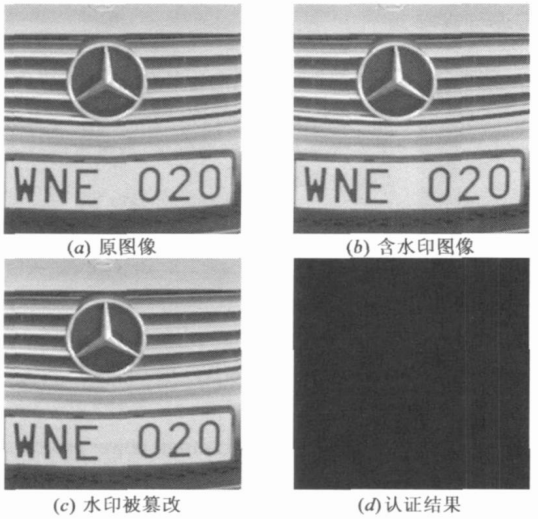
对多幅标准图像进行测试.认证图像中黑色表示认证通过,白色表示认证失败,下面是部分实验结果:

表 1 给出了一组不同图像用本文方法嵌入水印后图像的 *PSNR*,从表中可以看出所有图像的峰值信噪比都达到了 35dB 以上,和理论分析完全一致,满足了脆弱水印算法对不可见性的要求.

表 1　图像嵌入水印后的 PSNR

Image	Lena	Bamboo	Bird	Boat	Car
PSNR	44.15	44.12	44.08	44.13	44.12

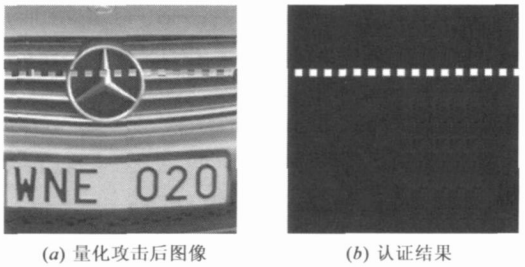
图 4(*a*)是原始 256 ×256car.bmp 灰度图;图 4(*b*)是用本文算法嵌入水印后图像;图 4(*c*)是图 4(*b*)中水印被篡改(各像素的最低位置反)后的图像,图 4(*d*)是其认证结果.由于水印被篡改,并不影响图像的使用价值,此时图 4(*c*)仍可通过二级认证,与一般的无法区分篡改的认证算法相比较,本文算法提高了图像的利用率.



(*a*) 原图像　(*b*) 含水印图像　(*c*) 水印被篡改　(*d*) 认证结果

图 4　水印被篡改及其认证结果

图 5 是量化攻击及其认证结果.其中,图 5(*a*)是图 4(*b*)中第 9 行偶数列 8 ×8 子块被第 19 行偶数列 8 ×8 子块替换所得;图 5(*b*)是对篡改图像块的定位结果.

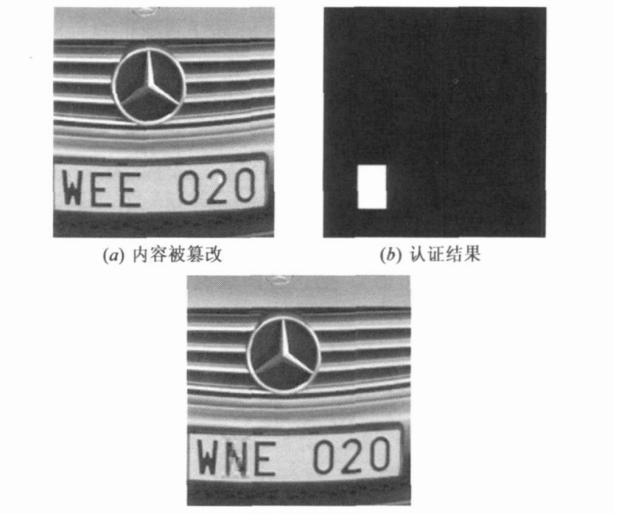


(*a*) 量化攻击后图像　(*b*) 认证结果

图 5　量化攻击及其认证结果

图 6(*a*)是图 4(*b*)中内容被篡改的认证及其恢复结果.其中,图 6(*a*)内容被篡改的含水印图像;图 6(*b*)认证结果;图 6(*c*)恢复结果.

由上面的实验结果可看出,本文算法在生成认证水印时使用位置信息,因而可以抵抗量化攻击;使用双重水印技术,即使在水印篡改量较大或内容篡改量较小的情况下也能准确对篡改加以区分,并对内容被的区域进行准确定位;同时,在一定条件下可对内容被篡改的区域进行恢复.与通过篡改点的分布特点及选取阈值对篡改进行区分的认证算法相比较,本文算法不受篡改量大小的限制.



(*a*) 内容被篡改　(*b*) 认证结果　(*c*) 恢复结果

图 6　内容被篡改的认证及其恢复

5　结束语

针对目前大多脆弱水印算法无法区分水印被篡改或内容被篡改的问题,本文基于双重水印技术提出了一种能区分水印或内容被篡改的图像认证方案,理论分析和实验结果表明:本方案能够有效定位图像内容被篡改的区域;能抵抗量化攻击;双重认证使得本文算法可以区分是水印被篡改或内容被篡改,并可对图像内容被篡改的区域进行恢复.同时,结合混沌系统选取偏移子块及加密水印使得本算法具有较高的安全性.

参考文献:

[1] B B Zhu, M D Swanson, A H Tewfik. When seeing isn't believing[J]. IEEE Signal Processing Magazine, 2004, 21(2): 40 - 49.

[2] P W Wong. A public key watermark for image verification and authentication[A]. Proceedings of the IEEE International Conference on Image Processing[C]. Chicago, USA, 1998, 455 - 459.

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

[4] P W Wong, N Memon. Secret and public key image waterm-

arking schemes for image authentication and ownership verification[J]. IEEE Transactions on Image Processing, 2001, 10 (10): 1593 - 1601.

[5] M U Celik, G Sharma, E Saber, et al. Hierarchical watermarking for secure image authentication with localization[J]. IEEE Transactions on Image Processing, 2002, 11(6): 585 - 595.

[6] A H Ouda, M R El-sakka. Localization and security enhancement of block-based image authentication[A]. Proceedings of IEEE International Conference on Image Processing[C]. vol. 1, 2005, 673 - 676.

[7] 张宪海, 杨永田. 基于脆弱水印的图像认证算法研究[J]. 电子学报, 2007, 35(1): 34 - 39.
Zhang Xian-hai, Yang Yong-tian. Image authentication scheme research based on fragile watermarking[J]. Acta Electronica Sinica, 2007, 35(1): 34 - 39. (in Chinese)

[8] 和红杰, 张家树, 田蕾. 能区分图像或水印篡改的脆弱水印方案[J]. 电子学报, 2005. 33(9): 1557 - 1561.
He Hong-jie, Zhang Jia-shu, Tian Lei. A fragile watermarki-ng scheme with discrimination of tampers on image or watermark [J]. Acta Electronica Sinica, 2005, 33(9): 1557 - 1561. (in Chinese)

[9] 和红杰, 张家树. 基于混沌置乱的分块自嵌入水印算法. 通信学报, 2006, 27(7): 80 - 85.
He Hong-jie, Zhang Jia-shu. Chaos-based scramble self-embedding watermarking algorithm[J]. Journal of China Institute of Communications, 2006, 27(7): 80 - 85. (in Chinese)

[10] J Fridrich, M Goljan. Images with self-correcting capa-bilities [A]. Proceedings of International Conference on Image Processing[C]. IEEE Press, Kobe, Japan, 1999. 25 - 28.

[11] 刘镔, 张永强, 刘粉林. 一种新的数字化混沌扰动方案, 计算机科学[J], 2005, 32(4): 71 - 74.
Liu Bin, Zhang Yong-qiang, Liu Fen-lin. A new scheme on perturbing digital chaotic systems[J]. Chinese journal of computer science, 2005, 32(4): 71 - 74. (in Chinese)

[12] S Samuel, W T Penzhorn. Digital watermarking for copyright protection[A]. IEEE 7th AFRICON Conference in Africa [C]. Gaborone, Botswana, 2004, 2: 953 - 957.

作者简介:

王国栋 男, 1982 年生于河南三门峡. 解放军信息工程大学信息工程学院网络工程系硕士研究生, 主要研究方向为数字水印技术、信息隐藏技术等.
E-mail: wgdguodong2006@163.com

刘粉林 男, 解放军信息工程大学信息工程学院教授、博士生导师. 1964 年出生于江苏溧阳. 主要研究方向为网络安全、数字水印技术、信息隐藏技术等.

(上接第 1318 页)

space-time block coding with a variable transmit diversity gain in OFDM systems[J]. IEEE Transactions on Consumer Electronics, 2004, 50(2): 478 - 483.

[10] Y Hashimoto, S Sampei, N Morinaga. Channel monitor-based unequal error protection with dynamic OFDM subcarrier assignment for video transmission[A]. IEEE Vehicular Technology Conference 2002[C]. Vancouver, BC, Canada, 2002. 913 - 917.

[11] S T Chung, A J Goldsmith. Degree of freedom in adaptive modulation: a unified view[J]. IEEE Trans Commun, 2001, 49 (9): 1561 - 1571.

[12] J Campello. Optimal discrete bit loading for multicarrier modulation systems[A]. IEEE International Symposium on Information Theory[C]. Cambridge, MA, USA, MA, 1998. 193.

[13] J Jiho, B L Kwang, H L Yong. Transmit power and bit allcoations for OFDM systems in a fading channel[A]. Proc IEEE Globecom[C]. San Francisco, CA, USA 2003. 858 - 862.

[14] A Fasano. On the optimal discrete bit loading for multicarrier systems with constraints[A]. Proc IEEE VTC[C]. Jeju, South Korea, 2003. 915 - 919.

[15] Y W Cheong, R S Cheng, et al. Multiuser OFDM with adaptive subcarrier, bit, and power allocation[J]. IEEE Journal on selected areas in communications, 1999, 17(10): 1747 - 1758.

[16] Channel models for fixed wireless applications, IEEE 802.16 Broadband Wireless Access Working Group [OL]. http://ieee802.org/16/tg3/contrib/802163c-01_29r2.pdf, July, 2001.