基于等级结构的二值文本图像认证水印算法

李赵红 [1] 侯建军 [1] 宋 伟 [1]

摘 要 针对二值文本图像的结构特点, 定义了度量图像中像素点 "可翻转性" 的像素扩展差, 在此基础上, 提出了一种基于等级结构的用于图像完整性和所有者认证的脆弱水印算法. 根据等级结构, 将原始图像划分为多等级子块, 然后对各等级子块进行独立的水印生成和嵌入. 根据像素扩展差的大小, 将图像块内的像素点划分为 "可翻转" 和 "不可翻转" 像素点. 将混沌调制后的 "不可翻转" 像素点的值映射为混沌系统的初值, 经过混沌迭代生成水印信号, 然后将水印信号替代 "可翻转" 的像素点, 完成水印的嵌入. 另外, 在图像的最高级子块中嵌入所有者信息, 实现对所有者的认证. 实验结果表明, 该算法具有良好的视觉透明性, 可对二值图像的均匀区域进行有效保护, 并对图像的内容篡改进行多级检测与定位.

关键词 图像认证, 所有者认证, 脆弱水印, 二值图像, 混沌
中图分类号 TP309.2

Binary Document Image Authentication Watermarking Technique Based on Hierarchical Structure

LI Zhao-Hong[1] HOU Jian-Jun[1] SONG Wei[1]

Abstract A concept of pixel spread deviation (PSD) is defined to measure the "flippability" of the pixels in binary document images, and a corresponding fragile watermarking technique for image authentication and ownership verification is proposed. According to the hierarchical structure, we divide the image into blocks in a multi-level hierarchy, then calculate and embed the block watermarks in each hierarchy level, respectively. The pixels in the image are divided into two groups determined by PSD: one is "the pixels that can be flipped" and the other is "the pixels that cannot be flipped". The values of the pixels that cannot be flipped are mapped into the initial value of the chaotic system, and then the watermark can be obtained by iterating the chaotic system from the initial value. The pixels that can be flipped are substituted by the watermark to obtain the watermarked image. Experimental results show the imperceptibility of the watermarking process, the effective protection of the uniform regions in the binary image, and successful detection and localization of content modifications with multi-level authentication.

Key words Image authentication, ownership verification, fragile watermarking, binary images, chaos

近年来, 随着计算机网络通信和多媒体技术的发展, 数字产品的版权保护以及内容认证越来越受到重视. 数字水印作为保护数字图像版权和完整性的有效手段, 已成为信息安全领域的研究热点. 数字水印按其功能可分为鲁棒型水印和脆弱型水印两种, 其中脆弱型水印[1−15] 特别适用于数字产品的认证, 内容篡改的证明和完整性证明. 现有的大多数脆弱数字水印算法主要是针对灰度或彩色图像的, 而对二值图像的研究相对较少. 然而在实际应用中有许多的文本图像 (如图片、文档、签字、支票、合同、证明和印章等) 是需要保护其合法权利不被侵犯的.

随着二值图像的广泛应用, 二值图像水印技术也越来越受到国内外学者的重视. 近年来许多学者进行了大量探索, 设计出了一些可行的数字水印算法[1−3, 5−6]. 为了能够在保证嵌入足够信息量的前提下, 仅造成较小的视觉差异, 一种典型的算法就是通过在空间域翻转图像中的个别像素来嵌入水印. 在这类算法中主要有三个问题需要考虑: 1) 如何选择翻转的像素点, 尽量使得图像的更改不可见; 2) 如何构造翻转像素与嵌入水印信息的关系, 使得这种关系有利于盲检, 有更好的安全性; 3) 如何保护二值图像的均匀区域 (即全黑、全白区域), 并使算法具有篡改定位能力, 特别是对均匀区域的添加 (在空白背景上添加内容) 和删除 (删除局部区域上的内容, 使之变为空白区域) 攻击.

针对第一个问题, Wu 等[1] 提出了一种很有效的衡量像素点可翻转性的方法 (简称 Wu 评分准则). 该方法首先建立以像素点为中心的 3×3 图像块, 通过考察翻转这一像素所引起的图像块连通性与平滑性的变化, 对这个像素的可翻转性进行评分, 建立了图像块中像素点可翻转性的查找表 (Look-up table, LUT). 朱从旭等[2] 定义了区域的最不重要像素块 (Least significant pixel block, LSPB), 用于评

收稿日期 2007-06-06 收修改稿日期 2008-01-21
Received June 6, 2007; in revised form January 21, 2008
北京交通大学科技基金 (2006XM002) 资助
Supported by Science and Technology Foundation of Beijing Jiaotong University (2006XM002)
1. 北京交通大学电子信息工程学院 北京 100044
1. School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044
DOI: 10.3724/SP.J.1004.2008.00841

价像素点的可翻转性 (简称 LSPB 评分准则). 在实际应用中, 为了更准确地对像素点的可翻转性进行评价, 应考虑更多的与像素点相邻的像素和细节, 因此需要考察以像素点为中心的更大的图像块[1], 比如 5×5, 7×7 等. 此时上述两种方法都有一定的局限性: Wu 评分准则不易扩展、计算量大, 且需要额外的空间来储存更大的 LUT; 而 LSPB 评分准则只定义了针对 3×3 图像块的 LSPB.

在算法的安全性和篡改定位两方面, Wu 算法[1] 易受到 Hae[3] 提出的 "校验攻击", 且不具有篡改定位能力. LSPB 算法[2] 则易受到 Holliman 和 Menon[4] 提出的 "矢量量化攻击", 虽然具有篡改定位能力, 但是没有对图像的均匀区域进行保护. 如果删除的图像内容块大于定位图像块, 将无法检测与定位篡改的区域. 为了保护图像的均匀区域, 张小华[5] 对图像的均匀区域和非均匀区域用标记符号进行区分, 将生成的水印图像和标记符号一并传送给接收者. 这种方法可以定位对图像均匀区域的篡改, 不足之处是需要传送和管理额外的附加信息, 且附加信息较大. Yang 等[6] 则利用了基于块相关的认证方法, 由于图像块水印的生成不仅与自身有关, 且与领域内的图像块有关, 因此这种方法可以有效地保护均匀区域, 但是图像块的改变将导致领域内图像块的虚警, 很大程度上降低了定位精度.

综上所述, 已有的二值图像的认证水印算法在像素的可翻转性、水印的安全性和篡改的定位精度三方面仍存在一些不足. 针对这些问题, 本文首先提出了一种计算简单、易于扩展的衡量像素点可翻转性的方法, 以保证水印嵌入的不可见性. 再将等级结构[7] 应用到二值图像的认证水印算法中, 即将图像划分成等级子块, 低等级子块用于保证良好的篡改定位精度, 高等级子块用于保证较高的水印安全性, 以此实现对均匀区域的保护和篡改定位. 但是与灰度图像不同, 在二值图像中, 不同的最低级子块包含的可嵌入水印容量不同, 所以引入一个可变参数用于分配水印容量. 另外, 目前仅有少量的文献能够在不需要附加信息的情况下同时实现图像的完整性认证和所有者认证, 且都是针对灰度图像的[8−10]. 而本文通过在图像的最高级子块中嵌入所有者信息的方法, 可以在不需要任何附加信息的情况下同时实现对二值图像的完整性认证和所有者的认证.

1 等级结构和混沌映射

1.1 等级结构

基于数字水印的图像认证技术的一个很重要的优势在于它具有篡改定位能力. Wong 等[8] 在 1998 年提出了基于块独立的认证水印算法, 实现了对篡改区域的精确定位. 但是很快这种基于块独立的认证算法就被著名的 "矢量量化攻击" 攻破. 为了抵抗 "矢量量化攻击", 人们提出了很多改进的或新的认证水印算法, 例如基于块编号和图像编号的水印算法[10]. 但这些方法都是在水印的安全性和定位精度之间折中, 不能兼顾水印的高安全性和高定位精度. 为了解决水印安全性和定位精度之间的矛盾, Celik 等[7] 针对灰度图像提出了一种基于等级结构的水印算法, 其主要内容如下:

给定一个 $M\times N$ 的灰度图像 X, 将其划分为 H 级, 第 h 级子块记为 X_{ij}^h, $h=1,2,\cdots,H$, $i=0,1,\cdots,(2^{h-1}-1)$, $j=0,1,\cdots,(2^{h-1}-1)$, 其中 i 和 j 分别表示该子块在空间域的横坐标和纵坐标位置. 相邻两级子块之间满足关系

$$X_{ij}^h=\begin{pmatrix} X_{2i,2j}^{h+1} & \| & X_{2i,2j+1}^{h+1} \\ X_{2i+1,2j}^{h+1} & \| & X_{2i+1,2j+1}^{h+1} \end{pmatrix} \tag{1}$$

其中, 最高级子块 X_{00}^1 为原始图像, 即 $X_{00}^1=X$. $H=3$ 时的等级划分如图 1 所示.

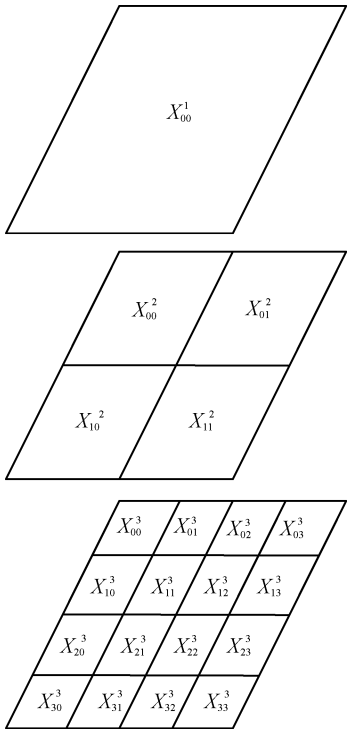


图 1 三级等级划分

Fig. 1 Hierarchical structure with three levels

每一级图像块的水印信号均为 Hash 函数产生的 128 比特, 再将生成的水印信号嵌入到最低级子块 X_{ij}^H 的最低有效位中. 采用等级结构的水印生成和嵌入方式, 最低级的子块最小, 定位精度最高, 而越高级的子块越大, 认证定位精度越低, 但抵抗 "矢量量化攻击" 的能力越强, 最高级子块的认证即整

个图像的认证则可以完全抵抗 “矢量量化攻击”, 以此有效地解决了水印安全性和定位精度之间的矛盾.

但是, 在二值图像中, 如果对图像进行相同的等级划分, 将导致不同的最低级子块能够嵌入的水印信息量不同. 例如在均匀区域, 由于嵌入水印信号将导致极大的视觉差异, 可嵌入的水印量为零. 针对二值图像的特殊情况, 引入一个可变参数对最低级子块的水印容量进行分配, 以保证低等级子块的良好定位精度和高等级子块的较高安全性. 各等级子块的水印信号生成和嵌入独立完成, 其中水印信号由混沌映射生成.

1.2　混沌映射

相对于 Hash 函数, 混沌映射计算简单, 生成序列速度快, 序列长度可以灵活变动, 更适合于本文算法. 混沌水印信号具有以下三方面的优点: 1) 易于产生, 仅需采用一维混沌映射方程, 水印信号生成速度快; 2) 数量众多, 混沌系统模型、参数和初值的不同选择即可得到互不相关的两个序列; 3) 保密性好, 在不知道混沌模型及相关参数的前提下, 几乎不可能破译. 因此混沌映射可以有效地解决实际应用中大量数字水印产生的问题及数字水印标准化问题, 有利于数字水印技术走向实际应用.

Logistic 映射是一类非常简单并被广泛研究的混沌动力系统, 可用非线性差分方程来描述

$$x_{n+1}=\lambda x_n(1-x_n),\quad \lambda\in[0,4],\ x_n\in(0,1) \tag{2}$$

当 $\lambda=4$ 时, 序列的均值为 0.5, 所以可以通过门限函数 $n_0(x)$ 把实值混沌序列转化为二进制混沌序列.

$$n_0(x)=\begin{cases}1, & x\geq 0.5\\ 0, & x<0.5\end{cases} \tag{3}$$

2　基于等级结构的二值图像认证算法

2.1　像素的可翻转性与像素扩展差

二值图像的像素非 0 即 1, 不像灰度图像那样具有丰富的灰度级, 从而可以孤立地考虑每一个像素. 由于一黑一白视觉反差极大, 因此每一个像素都是具有特定含义的信息载体, 在修改一个像素嵌入信息时, 必须要考虑该像素的各个邻域像素的情况. 否则对其作任何不当的改动, 即使很细小都会引起明显的修改痕迹, 甚至破坏图像所要表达信息的正确性. 为了度量像素点 d 的 “可翻转性”, 首先考察一个以 d 为中心, 大小为 $w\times w$ 的图像块 B, 其中 $w=3,5,7,9,\cdots$, 图像块 B 中所有像素点的值记为 $B(m,n)$, (m,n) 为像素点的坐标, $m=n=1,2,\cdots,w$. 那么点 d 的坐标为 (m_c,n_c), $m_c=n_c=(w+1)/2$. 假设图像块 B 的均值为 μ, 那么像素点 $B(m,n)$ 的偏差为 $\delta(m,n)=|B(m,n)-\mu|$. 根据 Cheng 等[12] 的描述, 为了更准确地衡量像素点的 “可翻转性”, 需要考虑图像块内各个像素点的方向, 因此, 我们引入了一个和图像块 B 大小一样的权重矩阵 W, 定义如下

$$W(m,n)=\begin{cases}1, & m=m_c,n=n_c\\ \dfrac{1}{\sqrt{(m-m_c)^2+(n-n_c)^2}}, & \text{其他}\end{cases} \tag{4}$$

定义 1. 图像块 B 的像素扩展 (Pixel spread, PS) 为

$$PS=\sum_{m=1}^{w}\sum_{n=1}^{w}\delta(m,n)\cdot W(m,n) \tag{5}$$

定义 2. 假设图像块 B 的中心点 d 翻转前的像素扩展为 PS, 翻转后的像素扩展为 PS', 那么点 d 的 “可翻转性” 由其翻转前后图像块的像素扩展差 (Pixel spread deviation, PSD) 来衡量, 表示如下

$$PSD=|PS-PS'| \tag{6}$$

利用式 (6), 计算出每个像素点的 PSD 值. 设定阈值 τ, 将 $PSD\leq\tau$ 的像素点定为 “可翻转”, 将 $PSD>\tau$ 的像素点定为 “不可翻转”.

2.2　水印的嵌入方法

利用 Logistic 映射生成水印信号, 水印生成和嵌入算法的具体步骤如下:

1) 将原始图像 X 划分成不重叠的 $w\times w$ 的块, 其中 w 为计算像素点 PSD 值时用到的图像块大小. 利用式 (6), 计算出每个 $w\times w$ 块的中心点的 PSD 值, 并根据设定的阈值 τ, 将 $PSD\leq\tau$ 的中心点定为 “可翻转” 像素点, 其他的像素点定为 “不可翻转” 像素点.

2) 将 X 按等级结构划分为 H 级, 记为 X_{ij}^h, $h=1,2,\cdots,H$. X_{ij}^h 包含了 $P=4^{H-h}$ 个最低级子块, 每个最低级子块中包含的 “可翻转” 像素点记为 $\boldsymbol{f}_p$, $\boldsymbol{f}_p$ 的长度 (即 “可翻转” 像素点个数) 记为 l_p, $p=1,2,\cdots,P$. 首先引入参数 η 对 $\boldsymbol{f}_p$ 进行分配, 如图 2 (见下页) 所示, $\boldsymbol{f}_p=\boldsymbol{f}_p^H\|\boldsymbol{f}_p^{H-1}\|\cdots\|\boldsymbol{f}_p^1$, 其中 $\boldsymbol{f}_p^h$ 表示第 p 个最低级子块中第 h 级的可翻转像素点, “$\|$” 表示并运算, l_p^h 表示 $\boldsymbol{f}_p^h$ 的长度

$$\eta=\left(\sum_{h=1}^{H}\frac{1}{h}\right)^{-1} \tag{7}$$

$$l_p^h=\left\lfloor\frac{\eta\cdot l_p}{H-h+1}\right\rfloor,\quad h=2,3,\cdots,H \tag{8}$$

$$l_p^1 = l_p - \sum_{h=2}^{H} l_p^h \tag{9}$$

其中, $\lfloor\cdot\rfloor$ 表示向下取整. 那么分配给 X_{ij}^h 的可翻转像素点为 $\boldsymbol{r}_{ij}^h$, $\boldsymbol{r}_{ij}^h$ 的长度 L_{ij}^h 为

$$\boldsymbol{r}_{ij}^h = \boldsymbol{f}_1^h \| \boldsymbol{f}_2^h \| \cdots \| \boldsymbol{f}_P^h, \quad L_{ij}^h = \sum_{p=1}^{P} l_p^h \tag{10}$$

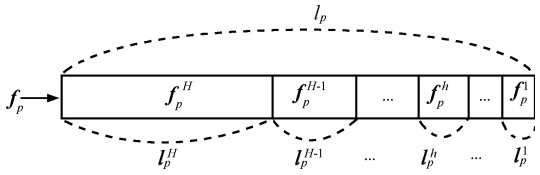


图 2 水印容量的分配

Fig. 2 Assignment of the watermark capacity

3) 对各级子块 X_{ij}^h 进行独立的水印生成和嵌入, 如图 3 所示. 将 X_{ij}^h 中所有的 "可翻转" 像素点置零, 得到 $\tilde{X}_{ij}^h$. $\tilde{X}_{ij}^h$ 中像素点的值记为 $\boldsymbol{v}_m$, $m = 1, 2, \cdots, M$, M 为像素点的个数. 设定 k 为整个水印系统的密钥, $k \in (0, 1)$. 将 k 作为初值代入混沌迭代式 (2), 产生长度为 M 的实值混沌序列 $\boldsymbol{c}_m$, 再将 $\boldsymbol{c}_m$ 代入式 (3) 得到二值混沌序列 $\boldsymbol{b}_m$. 对 $\tilde{X}_{ij}^h$ 进行混沌调制

$$\boldsymbol{u}_m = \boldsymbol{b}_m \oplus \boldsymbol{v}_m \tag{11}$$

其中, $\oplus$ 表示异或. 则图像块 X_{ij}^h 的混沌初值 x_{ij}^h 为

$$x_{ij}^h = \frac{1}{2}\left(k + \frac{1}{M}\sum_{m=1}^{M} \boldsymbol{u}_m\right) \tag{12}$$

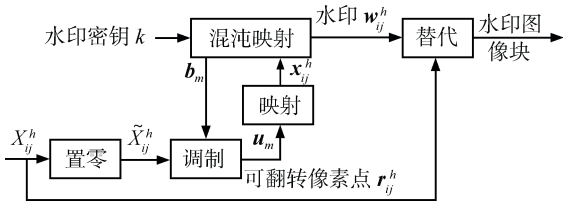


图 3 水印嵌入算法框图

Fig. 3 Watermark embedding

4) 将初值 x_{ij}^h 代入混沌迭代式 (2), 生成长度为 L_{ij}^h 的实值混沌序列. 再将实值混沌序列通过式 (3) 生成二进制序列, 也就是水印信号 $\boldsymbol{w}_{ij}^h$.

5) 将生成的水印信号 $\boldsymbol{w}_{ij}^h$ 替代可翻转像素点 $\boldsymbol{r}_{ij}^h$, 完成水印的嵌入.

6) 对第 2 级至第 H 级子块 X_{ij}^h 进行步骤 3) ∼ 5) 的操作.

7) 为了实现图像所有者的认证, 需要在最高级子块中嵌入所有者信息 $\boldsymbol{s}$. 首先将 $\boldsymbol{s}$ 扩展成最高级子块水印信号 $\boldsymbol{w}_{ij}^1$ 的长度, 记为 $\boldsymbol{s}'$, 再将 $\tilde{\boldsymbol{s}} = \boldsymbol{s}' \oplus \boldsymbol{w}_{ij}^1$ 替代 $\boldsymbol{r}_{ij}^1$, 得到水印图像 X_w.

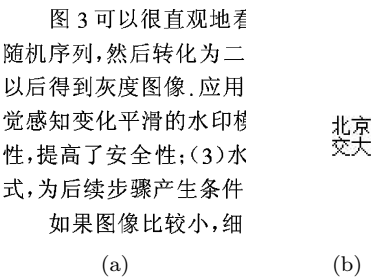
2.3 水印的提取与图像认证

水印的提取和水印的生成方法一致. 水印图像 X_w 经过同样的等级划分, 得到等级子块 $\dot{X}_{ij}^h$, 利用相同的参数 η 对最低级子块的 "可翻转" 像素点进行分配. 对各等级子块 $\dot{X}_{ij}^h$ 经过水印的产生步骤 3) 和 4), 利用正确的密钥 k, 可得到各等级子块的水印信号 $\dot{\boldsymbol{w}}_{ij}^h$.

脆弱水印有一个很大的特性, 就是能够定位出恶意篡改的区域. 由于采用了等级结构, 使得算法可以对图像进行多级检测与定位. 如果对图像进行第 h 级的认证, 首先取出第 h 级的水印信号 $\dot{\boldsymbol{w}}_{ij}^h$, 提取出 $\dot{X}_{ij}^h$ 所包含的最低级子块中第 h 级的 "可翻转" 像素点 $\dot{\boldsymbol{r}}_{ij}^h$. 如果 $\dot{\boldsymbol{w}}_{ij}^h = \dot{\boldsymbol{r}}_{ij}^h$, 则判定图像块 $\dot{X}_{ij}^h$ 未被篡改; 如果 $\dot{\boldsymbol{w}}_{ij}^h \neq \dot{\boldsymbol{r}}_{ij}^h$, 则判定图像块 $\dot{X}_{ij}^h$ 被篡改. 另外, 提取出最高级子块的 $\dot{\boldsymbol{w}}_{ij}^1$ 和 $\dot{\boldsymbol{r}}_{ij}^1$, 可以得到扩展后的所有者信息 $\dot{\boldsymbol{s}} = \dot{\boldsymbol{w}}_{ij}^1 \oplus \dot{\boldsymbol{r}}_{ij}^1$, 再将 $\dot{\boldsymbol{s}}$ 缩减为原始所有者信息的长度, 得到 $\bar{\boldsymbol{s}}$. 当且仅当图像块 $\dot{X}_{ij}^1$ 未被篡改, 所有者信息才能被正确地提取, 即 $\bar{\boldsymbol{s}} = \boldsymbol{s}$, 否则 $\bar{\boldsymbol{s}}$ 将类似噪声. 也即如果 $\bar{\boldsymbol{s}}$ 类似噪声, 判定图像块 $\dot{X}_{ij}^1$ 被篡改; 如果 $\bar{\boldsymbol{s}}$ 显示了所有者信息, 那么判定图像块 $\dot{X}_{ij}^1$ 未被篡改.

3 实验结果

为了说明本文算法的有效性, 下面给出了几个仿真结果. 大小为 384×384 的二值中文图像和大小为 25×27 的所有者图像如图 4 所示. 取 $k = 0.3$, $\lambda = 4$, $w = 3$ 和 $H = 5$.



(a) (b)

图 4 原始图像 ((a) 二值中文图像; (b) 所有者图像)

Fig. 4 Original images

((a) Binary Chinese image; (b) Owner image)

3.1 水印的不可见性

脆弱水印的一个重要特性是不可见性. 为了说明 PSD 的有效性, 利用结构相似性 (Structural similarity, SSIM)[13] 衡量准则来考察水印图像和原始图像之间的视觉相似性. SSIM 从图像亮度、对比度和结构三个方面来考察两个不同图像的相似性,

经理论和实验验证符合人类视觉系统, 且适用于任意两个相同长度的信号, 其定义如下

$$SSIM = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (13)$$

其中, μ_x 和 μ_y 分别是信号 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的均值, σ_x 和 σ_y 分别是信号 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的标准差, C_1 和 C_2 为远小于 1 的常数, σ_{xy} 是信号 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的估计相关系数, 在离散区域中可表示为

$$\sigma_{xy} = \frac{1}{N-1}\sum_{i=1}^{N}(\boldsymbol{x}_i - \mu_x)(\boldsymbol{y}_i - \mu_y) \quad (14)$$

其中, N 为信号 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的长度.

由于 Wu 评分准则同时考虑了图像的连通性与平滑性, 符合人类视觉系统, 且已取得了普遍认可, 具有代表性, 因此分别利用 Wu 评分准则和本文方法对原始图像的像素点 “可翻转性” 进行评分. Wu 评分准则将像素点 “可翻转性” 分为 6 个等级, 而本文方法将像素点 “可翻转性” 分为 13 个等级. 分别将 Wu 评分准则前 5 个等级的像素点设为 “可翻转” 像素点, 再将 “可翻转” 的像素点随机嵌入 0 或 1, 得到 5 个具有不同水印容量 (“可翻转” 像素点的个数) 的水印图像. 而分别将本文方法前 12 个等级的像素点设为 “可翻转” 像素点, 同样可以得到 12 个具有不同水印容量的水印图像. 具有不同水印容量的水印图像和原始图像之间的 $SSIM$ 值如图 5 所示. 根据文献 [13] 中的理论, $SSIM$ 值越接近于 1, 两个图像在视觉上越相似. 由图 5 可知: 1) 两种方法对 $SSIM$ 值、水印容量的测定结果一致性非常好, 即如果嵌入的水印容量相同, 水印图像的 $SSIM$ 值将非常接近; 2) 两种方法都可以使得水印图像同时满足良好的视觉透明性和较大的水印容量; 3) 相对于 Wu 评分准则, 本文方法对像素点的 “可翻转性” 划分了更多的等级, 水印容量和 $SSIM$ 值具有更多的选择, 更适合于实际应用要求的多样性. 另外, 本文方法考察以像素点为中心的更大图像块时易于扩展, 只需调整 ω 的值, 不需要额外的存储空间. 由此可知, 本文定义的 PSD 可以很好地控制水印的容量和不可见性, 可以根据实际的应用要求选择合适的阈值, 以保证水印图像具有良好的不可见性, 同时具有较大的嵌入容量.

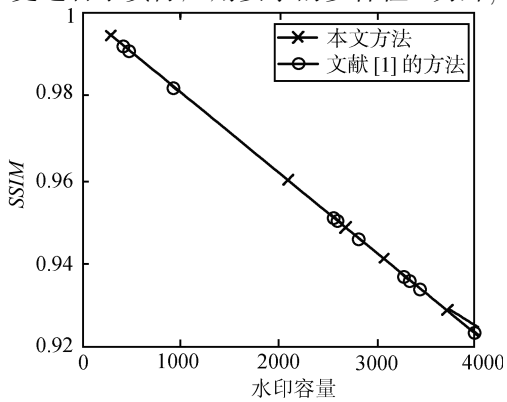


图 5　$SSIM$ 和水印容量

Fig. 5　$SSIM$ and watermarking capacity

3.2　篡改的检测与定位

为了测试本文算法对恶意篡改的定位能力, 特别是对均匀区域的添加和删除攻击, 对图 6 (a) 所示的水印图像 ($\tau = 0.8$, 水印容量为 2 795, $SSIM = 0.946\,1$) 进行了不同的篡改攻击: 1) 在第 1 行开始处添加了 “如”; 2) 将第 5 行的 “提高” 篡改为 “降低”; 3) 将第 5 行的 “3” 删除. 篡改后的图像如图 6 (b) 所示. 第 5 级至第 2 级的认证定位结果如图 6 (c) ∼ 6 (f) 所示, 用黑色小块指示被篡改的图像块.

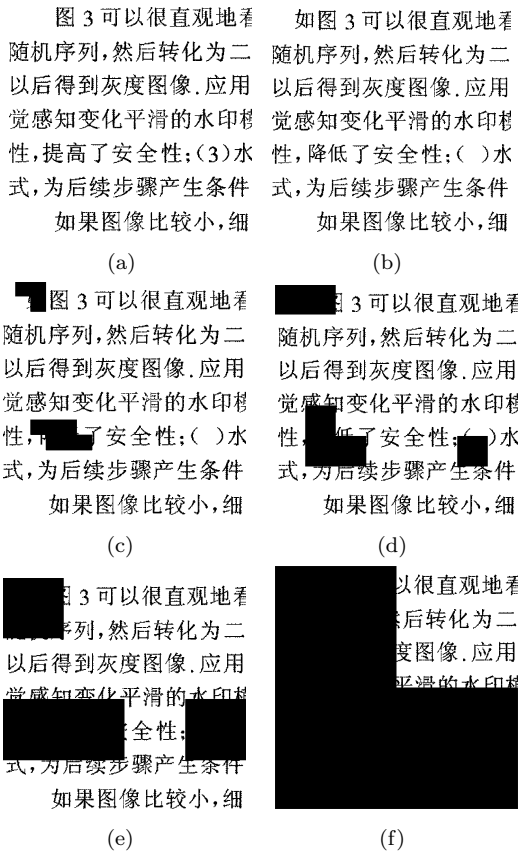


图 6　水印图像的篡改与定位 ((a) 水印图像; (b) 篡改图像; (c) 第 5 级定位图像; (d) 第 4 级定位图像; (e) 第 3 级定位图像; (f) 第 2 级定位图像)

Fig. 6　Modifications and localizations on the watermarked image ((a) Watermarked image; (b) Altered image; (c) Localized image with the fifth level; (d) Localized image with the forth level; (e) Localized image with the third level; (f) Localized image with the second level)

由图 6 可知, 各等级认证对图像内容的篡改均具有良好的检测与定位能力. 其中第 5 级认证结果的定位精度最高, 提供的图像原始信息最多. 但是在第 5 级认证中, 没有检测到删除 “3” 的攻击, 这是因为删除的图像块大于第 5 级子块的大小, 使其变为空白区域, 不再有 “可翻转” 的像素点, 导致无法检测. 但是, 第 4 级至第 2 级的认证中对图像的上述篡改均能检测及定位. 另外, 图像的第 1 级认证结果如图 7 所示, 图 7 (a) 为利用正确密钥对未被篡改的水印图像的认证结果, 正确地显示了所有者信息, 实现了所有者认证. 图 7 (b) 为利用正确密钥对篡改图像的认证结果, 显示图像类似噪声, 没有显示任何的所有者图像特征, 从而也认证了整个图像被篡改.

(a) (b) (c)

图 7 第 1 级图像和所有者认证 ((a) 正确密钥水印图像; (b) 正确密钥篡改图像; (c) 错误密钥水印图像)

Fig. 7 Ownership verification with the first level authentication ((a) Watermarked image with the right key; (b) Altered image with the right key; (c) Watermarked image with the wrong key)

对图像均匀区域的添加或删除攻击中, 如果篡改的区域大于该等级子块, 那么在这个等级的认证中将无法检测到篡改, 但是, 篡改的区域一定小于更高或最高等级子块, 那么更高或最高等级的认证一定能检测到篡改, 实现对图像均匀区域的保护. 也就是说, 低等级认证的定位精度高, 漏检率也高, 而高等级认证的漏检率低, 但是定位精度也低, 即各等级的定位精度与漏检率之间存在矛盾. 因此, 在图像划分时形成等级结构, 可得到不同定位精度和漏检率的定位结果. 我们可以根据实际应用对定位精度和漏检率的不同要求选择不同等级的定位结果, 或通过比较所有等级的认证结果推测篡改的区域及受到的攻击类型. 例如通过比较图 6 (c) ∼ 6 (f) 及图 7 (b) 的认证结果可以推测图像受到三处篡改, 且 “( )” 处被删除.

为了进一步研究各等级认证的漏检率, 对图像进行了 48 处各种类型的篡改, 包括添加、删除、复制等. 从理论上分析, 第 h 级认证的平均漏检率 $\overline{P}_{md}^{h}$ 为

$$\overline{P}_{md}^{h}=2^{-\overline{L}_{ij}^{h}},\quad \overline{L}_{ij}^{h}=4^{1-h}\cdot\sum_{i=0}^{2^{h-1}-1}\sum_{j=0}^{2^{h-1}-1}L_{ij}^{h}\quad(15)$$

漏检率的理论值 $\overline{P}_{md}^{h}$ 和实验值 $P_{md}^{h}=N_{md}^{h}/N_t$ 如图 8 所示, N_{md}^{h} 为第 h 级检测到的篡改图像块个数, N_t 为实际的被篡改图像块个数. 由图 8 可知, 实际测试结果和理论分析结果基本一致, h 越大, 漏检率越大. 第 5 级和第 4 级的漏检率较大, 第 3 级至第 1 级的漏检率为零. 但即使是第 5 级认证, 漏检率也只有 0.0833. 导致低等级认证的漏检率相对较高的主要原因是删除或添加的图像块大于低等级子块, 而小于高等级子块. 另外, 由于第 3 级子块的大小为 96×96, 如果第 3 级认证无法检测到某个删除攻击, 说明删除的图像块应该大于 96×96, 这时即使不用第 2 级或第 1 级认证, 通过人眼也能明显地识别出该篡改.

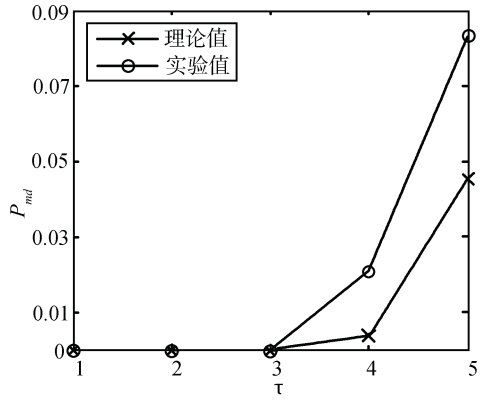


图 8 各等级漏检率的理论值与实验值

Fig. 8 Experimental and theoretical miss detection ratio of different hierarchies

3.3 水印的安全性

首先利用混沌映射生成了与图像内容相关的水印信息, 且对图像内容进行了预先的混沌调制, 使得不同的图像隐藏的水印信号不同, 既可以增强系统抵御统计攻击的能力, 又避免了在检测端额外提供原始水印信息. 同时, 利用了等级结构, 越高级图像块的认证对 “矢量量化攻击” 的抵抗能力越强, 其中, 最高级图像块的认证可以完全避免 “矢量量化攻击”. 另外, 通过改变单个像素点的值而不是整个图像块来嵌入水印, 即将图像块分为两部分, 一部分用于水印的生成, 另一部分用于水印的嵌入, 与 Hae[3] 描述的可完全抵抗 “校验攻击” 的方法一致, 所以本文提出的水印嵌入方法可以完全避免 “校验攻击”. 最后, 提供了一个水印密钥 k, k 为混沌映射的初值, 用于控制水印的生成. 由于混沌映射对初值的极端敏感性, 在检测端, 稍有差异的错误密钥将导致与原始水印截然不同的水印信号. 图 7 (c) 所示为利用极小差异的密钥 ($k=0.30001$) 对未篡改的水印图像的最高级认证结果, 类似噪声没有显示任何的所有者信息, 所以只有拥有正确的水印密钥 k, 才能正确

地提取出水印信息和所有者信息, 这也极大地增强了系统的安全性.

3.4　与现有算法的性能比较

表 1 从认证水印的重要特性, 即不可见性、篡改定位、安全性和鲁棒性方面比较了现有算法[1−2, 5−6]的优缺点以及与本文算法的性能差异.

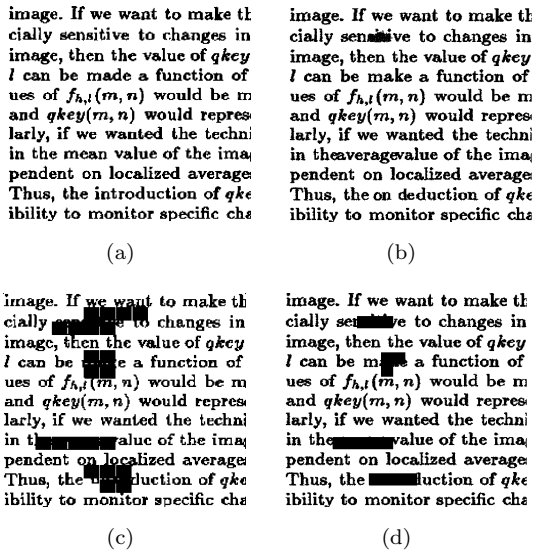
在水印的不可见性方面, 本文提出的像素点可翻转性的评分准则 (像素扩展差) 与具有代表性的 Wu 评分准则具有一致性, 且相对于 Wu 评分准则, 本文的评分准则具有多等级、易于扩展、不需要存储空间的优点.

在水印的篡改定位方面, 本文算法对图像的内容篡改具有多重定位能力, 特别是能对图像的均匀区域进行保护, 且不需要任何的附加信息, 优于现有的算法[1−2, 5−6]. 而文献 [1] 的算法不具有篡改定位能力, 文献 [2] 的算法不能对图像的均匀区域进行保护, 文献 [5] 的算法需要较大的附加信息, 文献 [6] 的算法中图像块的改变将导致领域内图像块的虚警, 降低了定位精度, 本文算法的篡改定位精度高于文献 [6] 的算法, 如图 9 所示.

在水印的安全性方面, 本文算法可以完全抵抗矢量量化攻击和校验攻击, 优于文献 [1−2] 中的算法, 文献 [1] 的算法不能抵抗校验攻击, 文献 [2] 的算法不能抵抗矢量量化攻击.

在水印的鲁棒性方面, 本文算法没有考虑水印的鲁棒性, 与文献 [2, 5−6] 中的算法一样属于完全脆弱水印算法. 文献 [1] 的算法在水印的鲁棒性方面优于本文算法, 水印信息可经受高质量的打印、扫描处理.

另外, 本文实现了所有者认证, 与文献 [1] 的算法具有相同的优缺点. 优点在于在图像未被篡改时, 接收者可以提取图像的所有者信息, 对于接收者可以确定发送者的身份, 对于发送者具有不可否认性, 优于其他算法[2, 5−6]. 缺点在于图像一经篡改, 提取的所有者信息将无法辨认类似噪声, 不能同时实现对二值图像的版权保护.



(a) (b) (c) (d)

图 9　篡改定位精度的比较 ((a) 水印图像; (b) 篡改图像; (c) 采用文献 [6] 算法的定位图像; (d) 本文算法的第 5 级定位图像)

Fig. 9　Comparison of the localization accuracy ((a) Watermarked image; (b) Altered image; (c) Localized image with the algorithm in [6]; (d) Localized image with the fifth level)

4　结束语

本文提出了等级结构应用在二值图像认证水印技术中的一个新的方法, 将图像的 “不可翻转” 像素点和密钥结合起来映射为 Logistic 映射的初值生成水印信息, 并通过改变 “可翻转” 像素点的值, 设计了水印嵌入算法. 该算法具有以下几个优点: 1) 具有

表 1　与现有算法的性能比较

Table 1　Performance comparison with existing algorithms

算法	不可见性	篡改定位	安全性	鲁棒性
文献 [1]	提出了评分准则, 但不易扩展和计算	无	可以完全抵抗矢量量化攻击, 但易受校验攻击	可经受高质量的打印、扫描处理
文献 [2]	提出了评分准则, 但不能扩展	有, 但不能保护均匀区域	属于块独立算法, 易受矢量量化攻击	无
文献 [5]	提出了评分准则, 但没有考虑连续性	有, 能保护均匀区域, 但需要较大的附加信息	可抵抗矢量量化攻击, 但需要存储水印集合	无
文献 [6]	利用已有的评分准则	有, 能保护均匀区域, 但定位精度不高	属于块相关算法, 可抵抗矢量量化攻击	无
本文	提出了评分准则, 易于扩展	有, 能保护均匀区域, 定位精度较高	可以完全抵抗矢量量化攻击和校验攻击	无

良好的视觉透明性, 根据像素扩展差, 将水印嵌入到"可翻转" 的像素点中, 保证了水印图像的良好视觉品质; 2) 能够对均匀区域进行有效保护, 对恶意攻击具有很强的敏感性, 利用了等级结构的多级定位思想, 使算法具有良好的篡改定位能力; 3) 具有很强的安全性, 最高级子块的认证可以完全抵抗 "矢量量化攻击", 并提供了水印密钥, 可以有效地防止攻击者对水印信息的提取和篡改; 4) 通过在最高级子块中嵌入所有者信息, 实现了所有者的认证, 如果图像未被篡改, 则能正确地提取所有者信息. 图像的完整性和所有者认证均不需要任何的附加信息, 从而实现了水印的盲检测.

如何设计水印的鲁棒性, 同时实现二值图像的完整性认证和版权保护是我们下一步的研究重点.

References

1 Wu M, Liu B D. Data hiding in binary image for authentication and annotation. *IEEE Transactions on Multimedia*, 2004, **6**(4): 528−538

2 Zhu Cong-Xu, Chen Zhi-Gang. Sensitive chaotic fragile watermarking technique for binary images verification. *Mini-Micro Systems*, 2006, **27**(1): 151−154
(朱从旭, 陈志刚. 一种灵敏的文本图像认证混沌脆弱水印技术. 小型微型计算机系统, 2006, **27**(1): 151−154)

3 Hae Y K. A new public-key authentication watermarking for binary document images resistant to parity attacks. In: Proceedings of IEEE International Conference on Image Processing. Washington D. C., USA: IEEE, 2005. 1074−1077

4 Holliman M, Menon N. Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes. *IEEE Transactions on Image Processing*, 2000, **9**(3): 432−441

5 Zhang Xiao-Hua. Image Authentication Technique Based on Digital Watermarking [Ph. D. dissertation], Xidian University, 2004
(张小华. 基于数字水印的图像认证技术研究 [博士学位论文], 西安电子科技大学, 2004)

6 Yang H J, Alex C K. Binary image authentication with tampering localization by embedding cryptographic signature and block Identifier. *IEEE Signal Processing Letters*, 2006, **13**(12): 741−744

7 Celik U M, Sharma G, Saber E, Murat T A. Hierarchical watermarking for secure image authentication with localization. *IEEE Transactions on Image Processing*, 2002, **11**(6): 585−595

8 Wong P W. A public key watermark for image verification and authentication. In: Proceedings of IEEE International Conference on Image Processing. Chicago, USA: IEEE, 1998. 455−459

9 Patra J C, Ang K K, Ang E L. Hierarchical multiple image watermarking for image authentication and ownership verification. In: Proceedings of IEEE International Conference on Image Processing. Washington D. C., USA: IEEE, 2004. 2661−2664

10 Wong P W, Memon N. Secret and public key image watermarking schemes for image authentication and ownership verification. *IEEE Transactions on Image Processing*, 2001, **10**(10): 1593−1601

11 Yuan H, Zhang X P. Multiscale fragile watermarking based on the Gaussian mixture model. *IEEE Transactions on Image Processing*, 2006, **15**(10): 3189−3200

12 Cheng J, Kot A C. Objective distortion measure for binary images. In: Proceedings of IEEE Region 10 Conference on TENCON 2004: Analog and Digital Techniques in Electrical Engineering. Piscataway, USA: IEEE, 2004. 355−358

13 Wang Z, Bovik A C, Sheikh H R, Simoncelli E P. Image quality assessment: from error visibility to structural similarity. *IEEE Transactions on Image Processing*, 2004, **13**(4): 600−612

14 Li C H, Ling H F, Lu Z D. Semi-fragile watermarking based on SVM for image authentication. In: Proceedings of IEEE International Conference on Multimedia and Expo. Washington D. C., USA: IEEE, 2007. 1255−1258

15 Zhang X P, Wang S Z. Statistical fragile watermarking capable of locating individual tampered pixels. *IEEE Signal Processing Letters*, 2007, **14**(10): 727−730

李赵红 北京交通大学电子信息工程学院博士研究生. 主要研究方向为数字水印技术. 本文通信作者.
E-mail: zhaohong.li@126.com
(**LI Zhao-Hong** Ph. D. candidate at the School of Electronics and Information Engineering, Beijing Jiaotong University. Her main research interest is digital watermarking. Corresponding author of this paper.)

侯建军 北京交通大学电子信息工程学院教授. 主要研究方向为非线性电路系统, 数字图像处理.
E-mail: houjj@bjtu.edu.cn
(**HOU Jian-Jun** Professor at the School of Electronics and Information Engineering, Beijing Jiaotong University. His research interest covers nonlinear circuit system and digital image processing.)

宋 伟 北京交通大学电子信息工程学院博士研究生. 主要研究方向为数字水印技术. E-mail: 06111031@bjtu.edu.cn
(**SONG Wei** Ph. D. candidate at the School of Electronics and Information Engineering, Beijing Jiaotong University. His main research interest is digital watermarking.)