



# 版权保护和内容认证的全盲双功能数字水印算法

薛栋, 周亚训, 金炜

(宁波大学信息科学与工程学院, 浙江 宁波 315211)

**摘要:**针对现有大部分水印算法功能单一且无法实现完全盲检测的局限性,提出一种同时进行版权保护和内容认证的全盲双功能数字水印算法。算法采取子块区域分割的思想,水印产生和嵌入分别利用同一个子块的不同区域。通过判别两个最大奇异值均值的最高位奇偶性产生特征水印,然后自适应地调整相邻区域相同位置的两个离散余弦变换交流系数的大小,实现水印的嵌入。检测端通过产生的特征水印和盲提取的认证水印实现全盲的版权鉴别和内容认证。相比于已报道的一些水印方案,本文提出的水印算法对于常见的攻击具有更好的顽健性,可以实现版权保护功能,同时对于恶意的图像篡改又有较好的敏感性,可以准确定位篡改的区域。

**关键词:** 双功能水印; 特征水印; 全盲检测; 版权保护; 篡改检测

中图分类号: TN911.7

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2017017

## Bifunctional watermarking for copyright protection and content authentication with perfectly blind detection

XUE Dong, ZHOU Yaxun, JIN Wei

College of Information Science and Engineering, Ningbo University, Ningbo 315211, China

**Abstract:** In view of the limitation that most of the watermarking algorithms are single in functions and unable to achieve perfectly blind detection, a bifunctional watermarking algorithm with perfectly blind detection for copyright protection and content authentication was proposed. The algorithm adopted the idea of region segmentation for sub-block, and the generation and embedding of watermark were respectively carried out in the different regions of the same sub-block. A feature watermark was generated by judging the parity of the first digit from the average of maximum singular values, and the watermark was embedded by adjusting two DCT coefficients of adjacent blocks in the same position. Both the image copyright protection and content authentication functions were achieved by comparing the generated feature watermark and blindly extracting authentication watermark in the detection. Compared to some of the reported watermarking schemes, the proposed algorithm not only has better robustness against the common attacks to realize the copyright protection, but also has a good sensitivity to malicious image tampering to accurately locate the tampered area.

**Key words:** dual function watermark, feature watermark, perfectly blind detection, copyright protection, tamper detection

收稿日期: 2016-09-27; 修回日期: 2017-01-05

通信作者: 周亚训, zhouyaxun@nbu.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61271399)

Foundation Item: The National Natural Science Foundation of China (No.61271399)



## 1 引言

数字水印是解决当前数字图像安全问题的一种有效技术方案,其主要实现版权保护和内容认证等功能。实现版权保护的顽健图像水印算法,要求能够很好地抵抗各种攻击;实现内容认证的脆弱图像水印算法,要求对篡改攻击非常敏感。然而,现有的大多数图像水印算法功能比较单一,无法同时实现版权保护和内容认证<sup>[1,2]</sup>。已提出的半脆弱水印算法虽然能够实现版权保护和内容认证功能,但是无法同时具有顽健水印和脆弱水印良好的性能。

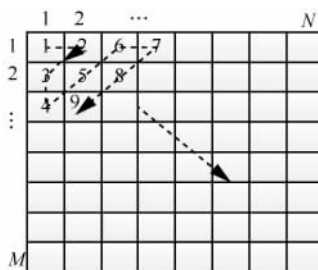
因此,双水印技术应运而生<sup>[3-5]</sup>,即通过向数字图像中同时嵌入顽健和脆弱两种水印以实现双功能的要求。但是,采用双水印技术嵌入的水印信息量自然增大,不可避免地导致图像质量的下降,而且,如果两种数字水印嵌入顺序和强度控制得不好,相互间会产生较大的影响。为了提高多功能水印算法的性能,基于零水印技术的多功能水印算法<sup>[6-8]</sup>被提出。参考文献[6]提出了一种自嵌入双功能图像零水印算法,算法通过提取图像子块奇异值范数的最高位奇偶性作为原始顽健零水印,将其保存在第三方进行版权保护,同时将顽健特征水印嵌入图像各子块每个像素的最低  $m$  位进行内容认证;参考文献[7]提出了一种结合 SUFT 特征的多功能彩色图像零水印算法,算法采用 SUFT 算子提取图像亮度分量的特征点构造出顽健零水印进行版权保护,并将图像子块奇异值范数异或运算产生的脆弱水印嵌入每个子块像素的最低有效位进行内容认证。基于零水印技术的多功能水印算法只嵌入一种水印就实现了两种功能,但是其无法达到全盲检测,仍需要对原始顽健零水印进行存储和传输。

鉴于以上水印算法存在的问题,提出一种能够进行全盲检测的多功能水印算法,算法通过提取与数字图像内容相关的信息产生特征水印并将其嵌入图像中,检测端通过产生的特征水印和盲提取的认证水印进行版权鉴别和内容认证。由于实现了全盲检测,提高了算法的实用性。

## 2 特征水印的产生和嵌入

离散余弦变换(discreet cosine transformation,DCT)是数字图像常用的处理工具,数字图像经过二维 DCT 变换后,进行如图 1 所示的 Zig-Zag 扫描成为一维序列后,第一个系数即 DCT 域的直流(DC)系数,表示图像的平均亮度,其他系数为 DCT 域的交流(AC)系数。AC 系数分布可粗略

地被分为低、中、高 3 个频带,低频系数分布在 Zig-Zag 扫描最前边一部分,是 3 个频带中系数值较大的区域,集中了图像的大部分能量,具有很好的顽健性。中频系数聚集着图像的一小部分能量,高频系数聚集的能量则相对更少,且高频系数很容易受到外在信号处理的影响,例如会被有损的数据压缩所删除<sup>[9-11]</sup>。



一,区域  $FI_k^2$  和  $FI_k^3$  形成组二。当  $k$  为奇数时,选择组一产生特征水印,在组二中嵌入水印;否则,选择组二产生特征水印,在组一中嵌入水印。

(4)对每个子块中选取的2个区域(即组一或组二)分别进行DCT得到同样大小的DCT系数矩阵  $FAC_k^1$  和  $FAC_k^2$ 。

(5)分别对DCT系数矩阵  $FAC_k^1$  和  $FAC_k^2$  前两行两列的元素进行SVD,得到各矩阵最大奇异值  $S_k^1$  和  $S_k^2$ , ( $S_k^1$  是矩阵  $FAC_k^1$  前两行两列的元素进行SVD得到的最大奇异值,  $S_k^2$  是矩阵  $FAC_k^2$  前两行两列的元素进行SVD得到的最大奇异值),求两个最大奇异值的均值  $v_k$ ,即:

$$v_k = \frac{(S_k^1 + S_k^2)}{2} \quad (1)$$

(6)通过判别均值  $v_k$  的最高位数字的奇偶性,产生特征水印  $W_k$ :当  $v_k$  的最高位为奇数时,  $W_k=1$ ;为偶数时,  $W_k=0$ ,即:

$$W_k = \begin{cases} 1, & \text{mod}(hb, 2) = 1 \\ 0, & \text{mod}(hb, 2) = 0 \end{cases} \quad (2)$$

其中,  $hb_k$  是  $v_k$  的最高位数字,  $W_k$  长度为  $(M/8)^2$ , 函数  $\text{mod}(\cdot)$  表示求模运算。

## 2.2 特征水印的嵌入

相邻图像子块的DCT系数之间存在一定的相关性,特别是在相邻图像块的相同位置的系数具有非常高的相似性<sup>[10,11]</sup>。本文水印的嵌入是通过调整相邻子块相同位置DCT系数的大小,使两者之间保持一定差异。具体步骤如下。

(1)为了提高算法的安全性,在特征水印嵌入之前用 Tent 映射<sup>[15]</sup>对其进行加密,其定义为:

$$y_{i+1} = \begin{cases} \mu \times y_i, & 0 \leq y_i \leq 0.5 \\ \mu \times (1 - y_i), & 0.5 < y_i \leq 1 \end{cases} \quad (3)$$

其中,  $y_i \in (0, 1)$ ,  $\mu \in (1, 2)$ , 当  $\mu > 1$  时,系统处于混沌状态,  $i=1, 2, 3, \dots$ 。利用 Tent 混沌序列加密水印的算法过程如下。

**步骤1** 在  $(0, 1)$  之间选择一个任意实数作为  $y_i$  的初始值,同时选择一个实数作为  $\mu$  的值,然后通过式(3)迭代产生一个随机数序列  $y_i, i=1, 2, 3, \dots$ 。从中选取第  $y_{q+1}$  到第  $y_{q+(M/8)^2}$  个随机数构成随机序列  $Y$ , 即  $Y = \{y_{q+1}, y_{q+2}, y_{q+3}, \dots, y_{q+(M/8)^2}\}$ 。将初始值  $y_1$ 、参数  $\mu$  和整数  $q$  作为密钥  $key1$  保存。

**步骤2** 通过式(4)将随机序列  $Y$  二值化为  $\{0, 1\}$  序列  $Z$ , 即:

$$Z_k = \begin{cases} 1, & y_{q+k} \geq T \\ 0, & \text{其他} \end{cases} \quad (4)$$

其中,  $Z_k$  是序列  $Z$  的第  $k$  比特,  $T$  是一个预定义阈值,可作为密钥  $key2$  保存,  $i=1, 2, 3, \dots, (M/8)^2$ 。

**步骤3** 利用得到的二值序列对前面构造得到的特征水印  $W$  进行加密:

$$W'_k = W_k \oplus Z_k \quad (5)$$

其中,  $\oplus$  表示异或运算,  $W'_k$  为加密后特征水印  $W'$  的第  $k$  比特。

(2)将大小为  $M \times M$  的原始图像  $I$  分割成  $8 \text{ dpi} \times 8 \text{ dpi}$  大小的互不重叠子块  $FI_k$ ,  $k$  代表子块的序号,  $k=1, 2, 3, \dots, (M/8)^2$ 。

(3)将子块  $FI_k$  进一步分割成4个大小为  $4 \text{ dpi} \times 4 \text{ dpi}$  的区域  $FI_k^j (j=1, 2, 3, 4)$ , 即  $FI_k = FI_k^1 \parallel FI_k^2 \parallel FI_k^3 \parallel FI_k^4$ 。

(4)将每个子块的4个区域以对角形式分成两组:区域  $FI_k^1$  和  $FI_k^4$  形成组一,区域  $FI_k^2$  和  $FI_k^3$  形成组二。当  $k$  为奇数时,选择组二嵌入水印,否则,选择组一嵌入水印。

(5)对每个子块中选取的2个区域分别进行DCT,得到DCT系数矩阵  $FAC_k^3$  和  $FAC_k^4$ 。

(6)根据式(6),调整每个子块中两个相邻区域的DCT交流系数  $FAC_k^3(2, 2)$  与  $FAC_k^4(2, 2)$  的大小关系,实现加密特征水印的自嵌入:

$$W'_k = 0 \Rightarrow \begin{cases} FAC_k^3(2, 2) \leftrightarrow FAC_k^4(2, 2), FAC_k^3(2, 2) < FAC_k^4(2, 2) \\ FAC_k^q(2, 2) = FAC_k^q(2, 2) (p=3, 4), FAC_k^3(2, 2) \geq FAC_k^4(2, 2) \end{cases}$$

$$W'_k = 1 \Rightarrow \begin{cases} FAC_k^3(2, 2) \leftrightarrow FAC_k^4(2, 2), FAC_k^3(2, 2) > FAC_k^4(2, 2) \\ FAC_k^q(2, 2) = FAC_k^q(2, 2) (p=3, 4), FAC_k^3(2, 2) \leq FAC_k^4(2, 2) \end{cases} \quad (6)$$

其中,符号“ $\leftrightarrow$ ”表示互换其值,  $FAC_k^3(2, 2)$  和  $FAC_k^4(2, 2)$  分别表示DCT系数矩阵  $FAC_k^3$  和  $FAC_k^4$  第二行第二列的一个交流系数。

为了使本文水印算法在保持水印不可见性的同时具有更好的顽健性,对交流系数  $FAC_k^3(2, 2)$  和  $FAC_k^4(2, 2)$  的大小关系作如下进一步修正:

$$W'_k = 0, FAC_k^3(2, 2) - FAC_k^4(2, 2) < \beta \Rightarrow \begin{cases} FAC_k^3(2, 2) = FAC_k^4(2, 2) + \frac{\beta}{2} \\ FAC_k^4(2, 2) = FAC_k^4(2, 2) - \frac{\beta}{2} \end{cases}$$

$$W'_k = 0, FAC_k^4(2, 2) - FAC_k^3(2, 2) < \beta \Rightarrow \begin{cases} FAC_k^4(2, 2) = FAC_k^4(2, 2) + \frac{\beta}{2} \\ FAC_k^3(2, 2) = FAC_k^3(2, 2) - \frac{\beta}{2} \end{cases} \quad (7)$$



其中,参数 $\beta$ 是用来控制水印的嵌入强度,其值由每个图像块的信息权重因子 $PBlock_k$ 自适应选择确定。权重因子 $PBlock_k$ 越大,对应的嵌入强度 $\beta$ 参数值越大:

$$\beta = \begin{cases} \beta_1, & PBlock_k=2 \\ \beta_2, & PBlock_k=1 \\ \beta_3, & PBlock_k=0 \end{cases} \quad (8)$$

其中, $\beta_1 > \beta_2 > \beta_3$ ,而权重因子 $PBlock_k$ 是根据选取2个区域的DCT的直流系数大小确定:

$$PBlock_k = \begin{cases} 2, & FAC_k^3(1,1) > \delta \text{ 和 } FAC_k^4(1,1) > \delta \\ 1, & \text{其他} \\ 0, & FAC_k^3(1,1) \leq \delta \text{ 和 } FAC_k^4(1,1) \leq \delta \end{cases} \quad (9)$$

其中, $FAC_k^3(1,1)$ 和 $FAC_k^4(1,1)$ 分别表示DCT系数矩阵 $FAC_k^3$ 和 $FAC_k^4$ 的直流系数,权重阈值 $\delta$ 是通过将图像4 dpi×4 dpi分块子图进行DCT变换后的直流系数求均值得到。

(7) 将经过调整后的各个DCT系数矩阵 $FAC_k^3$ 与 $FAC_k^4$ 进行逆DCT,再重组后得到嵌入水印后的水印图像。

### 3 水印的提取、版权鉴别和内容认证

检测端通过提取待检测图像的特征水印和认证水印进行图像版权鉴别和内容认证,并对篡改区域进行定位。

#### 3.1 特征水印的提取

从检测端提取特征水印的过程类似于嵌入端特征水印的创建过程。从检测端待检图像 $I'$ 中提取特征水印 $\hat{W}$ 的过程如下。

(1) 将大小为 $M \times M$ 的待检测图像 $I'$ 分割成8 dpi×8 dpi大小的互不重叠子块 $FI'_k$ , $k$ 代表子块的序号, $k=1,2,3,\dots,(M/8)^2$ 。

(2) 将子块 $FI'_k$ 进一步分割成类似于图2顺序排列的4个大小为的区域( $j=1,2,3,4$ ),即 $FI'_k = FI_k^{1'} \parallel FI_k^{2'} \parallel FI_k^{3'} \parallel FI_k^{4'}$ 。

(3) 将每个子块 $FI'_k$ 的4个区域以对角形式分成两组,即区域 $FI_k^{1'}$ 和 $FI_k^{4'}$ 形成组一,区域 $FI_k^{2'}$ 和 $FI_k^{3'}$ 形成组二。当 $k$ 为奇数时,选择组一提取特征水印,否则,选择组二提取特征水印。

(4) 对每个子块中选取的2个区域分别进行DCT得到DCT系数矩阵 $FAC_k^{1'}$ 和 $FAC_k^{2'}$ 。

(6) 分别对DCT系数矩阵 $FAC_k^{1'}$ 和 $FAC_k^{2'}$ 前两行两列的元素进行SVD,得到各矩阵的最大奇异值 $S_k^{1'}$ 和 $S_k^{2'}$ ,求两个最大奇异值的均值 $v_k'$ :

$$v_k' = \frac{(S_k^{1'} + S_k^{2'})}{2} \quad (10)$$

(6) 通过判别均值 $v_k'$ 的最高位数字的奇偶性,提取特征水印 $\hat{W}_k$ ,即:

$$\hat{W}_k = \begin{cases} 1, & \text{mod}(hb_k', 2) = 1 \\ 0, & \text{mod}(hb_k', 2) = 0 \end{cases} \quad (11)$$

其中, $hb_k'$ 是 $v_k'$ 的最高位数字, $\hat{W}_k$ 长度为 $(M/8)^2$ ,函数 $\text{mod}(\cdot)$ 表示求模运算。

#### 3.2 认证水印的盲提取及版权鉴别和内容认证

检测端认证水印的盲提取过程是嵌入端特征水印嵌入过程的逆过程,通过比较待检测含水印图像子块中相邻两个区域的DCT中低频交流系数的大小关系提取出认证水印。具体步骤如下。

(1)、(2) 同特征水印的提取步骤。

(3) 将每个子块的4个区域以对角形式分成两组,区域 $FI_k^{1'}$ 和 $FI_k^{4'}$ 形成组一,区域 $FI_k^{2'}$ 和 $FI_k^{3'}$ 形成组二。当 $k$ 为奇数时,选择组二提取认证水印,否则,选择组一提取认证水印。

(4) 对每个子块的2个区域分别进行DCT得到DCT系数矩阵 $FAC_k^{1'}$ 和 $FAC_k^{4'}$ 。

(5) 通过比较两个相邻区域的DCT交流系数 $FAC_k^{1'}$ (2,2)与 $FAC_k^{4'}$ (2,2)的大小关系,实现认证水印 $\tilde{W}$ 的盲提取:

$$\tilde{W}_k = \begin{cases} 1, & FAC_k^{1'}(2,2) < FAC_k^{4'}(2,2) \\ 0, & FAC_k^{1'}(2,2) \geq FAC_k^{4'}(2,2) \end{cases} \quad (12)$$

(6) 对提取的认证水印 $\tilde{W}$ 进行解密,具体步骤如下。

**步骤1** 利用密钥 $key1$ 通过式(3)迭代产生Tent混沌映射序列 $y_i'$ , $i=1,2,3,\dots$ 。从中选取第 $q+1$ 到第 $q+(M/8)^2$ 个随机数构成随机序列 $Y'$ ,即 $Y' = \{y'_{q+1}, y'_{q+2}, y'_{q+3}, \dots, y'_{q+(M/8)^2}\}$ 。然后,利用密钥 $key2$ 通过式(4)将 $Y'$ 二值化为 $\{0,1\}$ 的序列 $Z'$ 。

**步骤2** 通过式(13)对认证水印 $\tilde{W}$ 进行解密,得到解密后的认证水印:

$$\tilde{W}'_k = \tilde{W}_k \oplus Z'_k \quad (13)$$

其中, $\tilde{W}'_k$ 是解密后的认证水印 $\tilde{W}'$ 的第 $k$ 比特, $Z'_k$ 是序列 $Z'$ 的第 $k$ 比特, $k=1,2,3,\dots,(M/8)^2$ ;

(7) 版权鉴别:计算从待检测含水印图像 $I'$ 中提取的

特征水印 $\hat{W}$ 和解密后的认证水印 $\tilde{W}'$ 之间的归一化相关系数(NC),以此来对图像进行版权鉴别:

$$NC = \frac{\sum_{k=1}^{(M/8)^2} (\hat{W}_k \times \tilde{W}'_k)}{\sqrt{\sum_{k=1}^{(M/8)^2} (\hat{W}_k)^2} \times \sqrt{\sum_{k=1}^{(M/8)^2} (\tilde{W}'_k)^2}} \quad (14)$$

(8)内容认证:通过比较提取的特征水印 $\hat{W}$ 中的第 $k$ 比特 $\hat{W}_k$ 和解密后的认证水印 $\tilde{W}'$ 中的第 $k$ 比特 $\tilde{W}'_k$ 之间是否相同来检测此图像子块(即第 $k$ 子块)是否遭到篡改。即如果 $\hat{W}_k = \tilde{W}'_k$ 成立,则认为此子块没有遭到篡改;反之,则认为此子块遭到篡改,遭篡改的子块用全白像素标识。

为了提高水印算法对篡改定位的准确性,对图3中的3种情形作相应处理:对于情形1,若子块NW和O已检测为篡改子块,则认为子块N和W也是篡改子块;同理,若子块NE和O已检测为篡改子块,则认为子块E和N也是篡改子块;对于情形2和情形3,若子块NE和SE已检测为篡改子块,则认为子块O也是篡改子块。

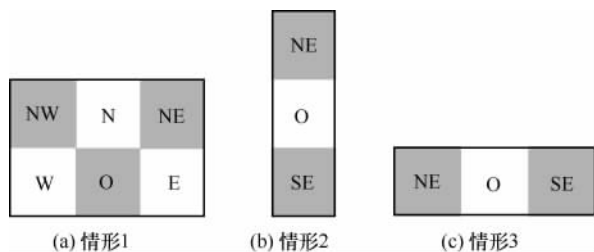


图3 篡改定位的3种情形

可以看到,检测端只需要利用攻击后待检测的含水印图像就可以分别提取特征水印和认证水印,以此可以计算两者之间的归一化相关系数进行版权鉴别,并通过比较两者的水印比特位是否相同进行篡改定位,整个过程不需要借助任何原始图像和原始数字水印的相关信息。因此,水印算法实现了完全盲检测功能。

## 4 实验与结果分析

选择3幅8 bit 512 dpi×512 dpi大小的灰度图像为原始载体图像,验证本文算法的有效性,如图4(a)、图4(b)和图4(c)所示。实验中,Tent映射的初始值选为 $y_1=0.6$ ,参数 $u=1.4$ ,舍弃前400个随机数,阈值 $T=0.55$ ;3幅原始载体图像选择了统一的水印嵌入强度 $\beta_1=33, \beta_2=31, \beta_3=27$ ,

权重阈值 $\delta=465$ 。可以看到,嵌入水印后的图像如图4(d)、图4(e)和图4(f)所示,峰值信噪比分别为36.622 dB、36.686 dB和37.010 dB,视觉上很难感觉到变化,满足了水印不可觉察性要求。这时提取的特征水印和认证水印之间的归一化相关系数为1,说明水印图像在未受任何处理或攻击破坏时,可以完全无损地提取出特征水印和认证水印,因此可用于数字图像的版权保护。作为对比,本文同时设计了算法2,其嵌入的水印是通过Tent映射产生的伪随机序列,即二值序列(其水印信息与原始图像无关),但水印嵌入和提取过程与本文算法完全一致。



图4 原始图像和水印图像

### 4.1 恶意篡改的脆弱性

恶意篡改一般包括剪切、替换、叠加等操作。随着数字图像处理技术的发展,对数字图像的修改更加多样和容易化。现对图4中的3幅水印图像进行恶意篡改检测实验,并以Lena水印图像为主要例子进行详细说明。

#### (1)篡改1

将水印图像中心区域(196:259, 196:259)内的每个像素值分别设置为0和200,得到篡改后的Lena水印图像分别如图5(a)和图6(a)所示。像素值为0显示的黑色与图像背景相差比较大,而像素值为200显示的灰白色与背景很相似。本文算法可以很好地定位出图像的篡改区域,篡改定位检测结果如图5(b)和图6(b)所示;作为对比,图5(c)和图6(c)显示了算法2的篡改定位检测结果,可见其检测定位效果欠佳;图5(d)和图6(d)显示了参考文献[16]算法的篡改定位检测结果,对于篡改实验1和实验2,参考文献[16]算法只能检测出篡改区域的边界部分。



(a) 篡改1-1:篡改图像

(b) 篡改1-1:本文算法检测结果



(c) 篡改1-1:算法2检测结果

(d) 篡改1-1:参考文献[16]算法检测结果

图5 篡改1-1实验结果



(a) 篡改1-2:篡改图像

(b) 篡改1-2:本文算法检测结果



(c) 篡改1-2:算法2检测结果

(d) 篡改1-2:参考文献[16]算法检测结果

图6 篡改1-2实验结果

## (2) 篡改2

对水印图像位于(272: 328, 145: 205)区域内的像素点进行像素值增加操作,例如将该区域内的每个像素值加上30,得到篡改后的Lena水印图像如图7(a)所示。由于水印图像是一个256级的灰度图像,所以对于图像像素值的稍许改变,人眼是很难分辨得出修改区域的。但本文算法能够有效地定位出篡改区域,如图7(b)所示;而算法2没有检测出篡改区域,如图7(c)所示。参考文献[16]算法只能定位出篡改区域的一大部分,如图7(d)所示。



(a) 篡改2:篡改图像

(b) 篡改2:本文算法检测结果



(c) 篡改2:算法2检测结果

(d) 篡改2:参考文献[16]算法检测结果

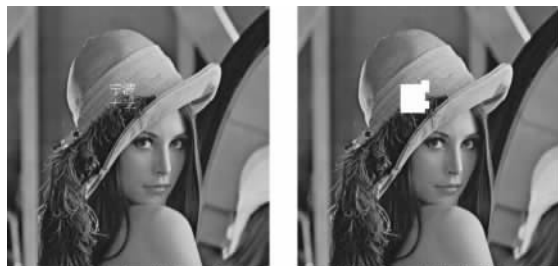
图7 篡改2实验结果

## (3) 篡改3

将图8大小为64 dpi×64 dpi的二值图像的每个像素值乘以80再叠加到水印图像的(146: 209, 196: 259)区域,篡改后的图像如图9(a)所示。本文算法可以很好地检测出篡改区域,如图9(b)所示;而算法2只检测到了篡改区域中很少的一部分,如图9(c)所示,参考文献[16]算法只能定位出篡改区域的一小部分,如图9(d)所示。



图8 宁波大学



(a) 篡改3:篡改图像

(b) 篡改3:本文算法检测结果



(c) 篡改3:算法2检测结果

(d) 篡改3:参考文献[16]算法检测结果

图9 篡改3实验结果

#### (4) 篡改 4

用 Photoshop 对图像进行真实性的篡改:在 Lena 水印图像上插入一个装饰用的蝴蝶如图 10(a)所示。图 10(b)和图 10(c)分别是利用本文算法和算法 2 得到的篡改定位检测结果,参考文献[16]算法得到的篡改定位检测结果如图 10(d)所示;将 Lena 水印图像右下角的白色和灰色波浪形装饰移除如图 11(a)所示。图 11(b)和图 11(c)分别是利用本文算法和算法 2 得到的篡改定位检测结果,参考文献[16]算法得到的篡改定位检测结果如图 11(d)所示;将 Lena 水印图像帽子上一个小花朵进行多次复制如图 12(a)所示。图 12(b)和图 12(c)分别是利用本文算法和算法 2 得到的篡改定位检测结果,图 12(d)显示了参考文献[16]算法得到的篡改定位检测结果。显然,本文算法比算法 2 有更好的定位效果,而且,本文算法篡改定位的准确性优于参考文献[16]算法。



图 10 篡改 4-1 实验结果

显然,由以上剪切、替换、叠加等操作的实验结果来看,本文提出的水印算法能够准确地定位出图像的恶意篡改区域,很好地实现图像内容的完整性认证。本文算法比算法 2 实现更好和更可靠的定位结果,主要原因在于本文算法嵌入了与图像内容相关的特征水印,其对图像内容篡改具有更好的敏感性。同时,由篡改 1 到篡改 4 的实验检测结果可以看出,本文算法比参考文献[16]算法实现了更好和更可靠的篡改定位结果。



图 11 篡改 4-2 实验结果



图 12 篡改 4-3 实验结果

## 4.2 抗攻击的顽健性

为了测试本文算法的抗攻击顽健性,采用一些常见的图像处理操作例如添加噪声、JPEG 压缩、滤波、剪切、重采样和混合攻击等,具体攻击类型见表 1,而对水印图像进行抗攻击检测结果列于表 2 中。由“ $\hat{w}$ 和 $\hat{w}'$ ”栏可以看出,从受攻击后的含水印图像中提取的特征水印和认证水印



表 1 图像攻击类型

| 编号 | 攻击类型                              |
|----|-----------------------------------|
| 1  | 添加高斯噪声(方差为 0.000 1)               |
| 2  | 添加高斯噪声(方差为 0.000 3)               |
| 3  | 添加椒盐噪声(噪声密度为 0.003)               |
| 4  | 添加椒盐噪声(噪声密度为 0.005)               |
| 5  | 3×3 高斯低通滤波( $\sigma=0.5$ )        |
| 6  | 3×3 中值滤波                          |
| 7  | 剪切(左上角 1/16)                      |
| 8  | 剪切(中心 1/16)                       |
| 9  | JPEG 压缩( $Q=60$ )                 |
| 10 | JPEG 压缩( $Q=50$ )                 |
| 11 | JPEG 压缩( $Q=40$ )                 |
| 12 | 重采样(先缩小 0.8 倍再扩大到 1.25 倍)         |
| 13 | 重采样(先缩小到 0.5 倍再扩大到 2 倍)           |
| 14 | JPEG70+中心剪切 1/16                  |
| 15 | JPEG70+3×3 中值滤波                   |
| 16 | JPEG70+3×3 高斯低通滤波( $\sigma=0.5$ ) |

之间的 NC 值都在 0.90(除重采样中的一项)以上,因此,本文算法能够很好地实现数字图像的版权保护。为了进一步显示本文水印算法抗攻击的顽健性,分别与参考文献[11]和参考文献[17]的结果进行了对比。图 13 给出了本文算法与参考文献[11]算法(以 Lena 图像为例)在添加椒盐噪声(噪声密度为 0.01)、添加高斯噪声(方差为 0.001)、中值滤波(窗口大小为 )、对比度增强(50%)以及直方图均衡化的攻击下提取的认证水印与原始水印之间 NC 值的比较,图 14 给出了与参考文献[17]的对比结果。可见,本文算法在抵抗噪声、高斯低通滤波、剪切、重采样和混合攻击等方面具有更好的顽健性。

#### 4.3 实验结果讨论与分析

##### (1)篡改检测的脆弱性

本文嵌入的水印是与图像内容相关的特征信息产生的,其对于恶意图像篡改具有很敏感的脆弱性。当图像遭到恶意篡改时,会对特征水印和认证水印的提取造成一定的

表 2 图像抗攻击的顽健性

| 图像       | 编号                       | 1       | 2       | 3       | 4       | 5       | 6       | 7       | 8       |
|----------|--------------------------|---------|---------|---------|---------|---------|---------|---------|---------|
| Lena     | $\hat{W}$ 和 $\tilde{W}'$ | 0.986 3 | 0.974 6 | 0.974 0 | 0.960 7 | 0.993 5 | 0.942 8 | 0.985 0 | 0.986 0 |
|          | $\hat{W}$ 和 $W$          | 0.986 3 | 0.974 6 | 0.985 7 | 0.979 7 | 0.993 5 | 0.977 8 | 0.997 4 | 0.992 6 |
|          | $\tilde{W}'$ 和 $W$       | 1.000 0 | 1.000 0 | 0.987 3 | 0.980 1 | 1.000 0 | 0.962 1 | 0.987 6 | 0.992 0 |
| Goldhill | $\hat{W}$ 和 $\tilde{W}'$ | 0.987 9 | 0.977 7 | 0.973 3 | 0.957 6 | 0.993 0 | 0.923 1 | 0.985 3 | 0.984 2 |
|          | $\hat{W}$ 和 $W$          | 0.987 9 | 0.977 7 | 0.984 0 | 0.977 9 | 0.993 0 | 0.973 6 | 0.988 8 | 0.996 8 |
|          | $\tilde{W}'$ 和 $W$       | 1.000 0 | 1.000 0 | 0.988 8 | 0.979 7 | 1.000 0 | 0.943 2 | 0.996 5 | 0.992 5 |
| Peppers  | $\hat{W}$ 和 $\tilde{W}'$ | 0.981 6 | 0.967 1 | 0.977 7 | 0.961 1 | 0.986 1 | 0.939 7 | 0.985 6 | 0.984 8 |
|          | $\hat{W}$ 和 $W$          | 0.981 6 | 0.967 1 | 0.988 1 | 0.978 1 | 0.986 1 | 0.972 7 | 0.991 2 | 0.990 9 |
|          | $\tilde{W}'$ 和 $W$       | 1.000 0 | 1.000 0 | 0.989 0 | 0.981 2 | 1.000 0 | 0.962 2 | 0.994 3 | 0.993 4 |
| 图像       | 编号                       | 9       | 10      | 11      | 12      | 13      | 14      | 15      | 16      |
| Lena     | $\hat{W}$ 和 $\tilde{W}'$ | 0.974 7 | 0.970 4 | 0.929 8 | 0.946 2 | 0.893 9 | 0.969 0 | 0.941 4 | 0.981 8 |
|          | $\hat{W}$ 和 $W$          | 0.974 9 | 0.972 3 | 0.968 6 | 0.953 7 | 0.911 8 | 0.975 5 | 0.975 4 | 0.981 8 |
|          | $\tilde{W}'$ 和 $W$       | 0.999 8 | 0.998 1 | 0.961 3 | 0.991 1 | 0.975 9 | 0.991 8 | 0.964 4 | 1.000 0 |
| Goldhill | $\hat{W}$ 和 $\tilde{W}'$ | 0.977 9 | 0.974 7 | 0.951 5 | 0.942 1 | 0.892 7 | 0.967 8 | 0.915 8 | 0.982 6 |
|          | $\hat{W}$ 和 $W$          | 0.977 9 | 0.976 3 | 0.970 5 | 0.949 3 | 0.911 5 | 0.974 4 | 0.967 3 | 0.992 6 |
|          | $\tilde{W}'$ 和 $W$       | 1.000 0 | 0.998 4 | 0.979 4 | 0.990 5 | 0.911 4 | 0.992 5 | 0.943 7 | 1.000 0 |
| Peppers  | $\hat{W}$ 和 $\tilde{W}'$ | 0.970 3 | 0.955 3 | 0.908 9 | 0.943 4 | 0.884 8 | 0.986 1 | 0.937 6 | 0.974 4 |
|          | $\hat{W}$ 和 $W$          | 0.970 5 | 0.959 7 | 0.956 8 | 0.947 9 | 0.894 8 | 0.986 1 | 0.965 4 | 0.974 7 |
|          | $\tilde{W}'$ 和 $W$       | 0.999 3 | 0.994 8 | 0.943 7 | 0.993 6 | 0.981 3 | 1.000 0 | 0.968 4 | 0.999 8 |

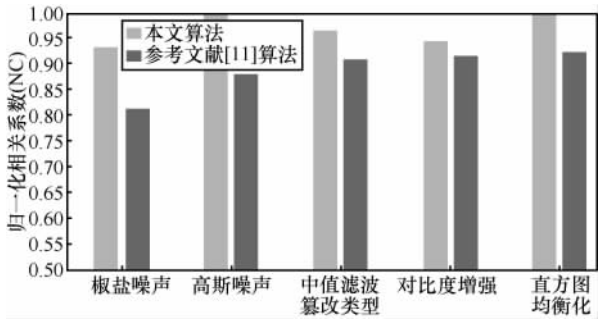


图 13 本文算法与参考文献[11]算法的 NC 值比较

影响,特别是特征水印的提取,大大提高了算法的脆弱性。由第 4.1 节可以看出,在对恶意篡改的脆弱性上,基于图像内容相关的水印算法比基于伪随机序列的水印算法的敏感性要高。所以本文算法具有很敏感的篡改检测

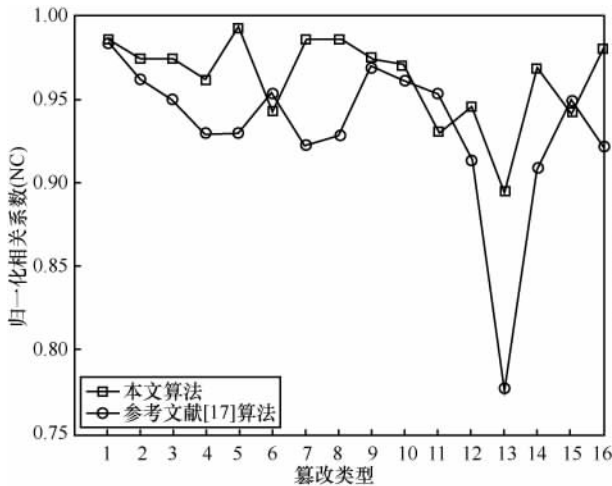
脆弱性。

(2) 抗攻击的顽健性

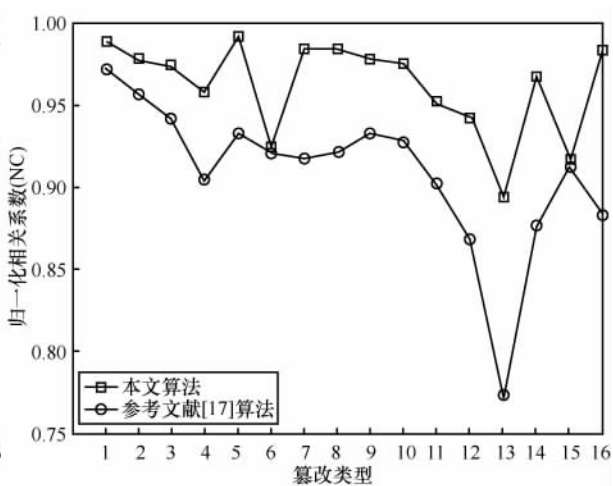
由表 2 的“ $\hat{W}$ 和  $W$ ”栏可知,特征水印产生算法在抗击图像攻击上表现出很好的顽健性,并且由表 2 的“ $\hat{W}'$ 和  $W$ ”栏可知,水印嵌入算法在抗击图像攻击上同样表现出很强的顽健性。特征水印产生算法和水印嵌入算法优异的顽健性,保证了含水印图像在遭受到各种攻击之后仍然能够比较准确提取出特征水印和认证水印,很好地实现图像的版权保护。

(3) 水印嵌入强度选择

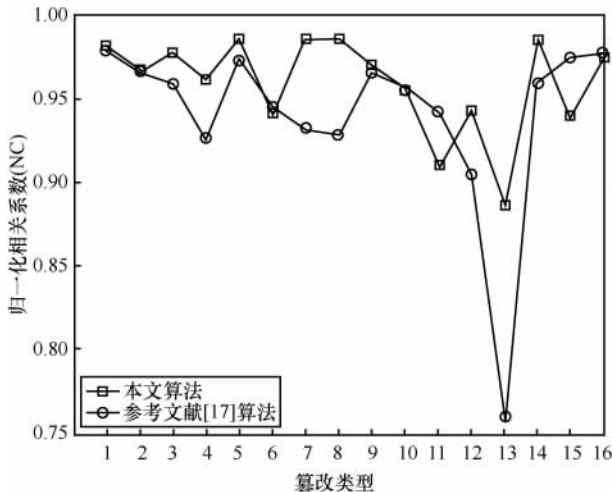
水印嵌入强度  $\beta$  值的大小关系到水印的不可见性和顽健性,水印嵌入强度  $\beta$  值越大,水印顽健性就越好,含水印图像质量就会越差;反之,含水印图像质量越好,但是水



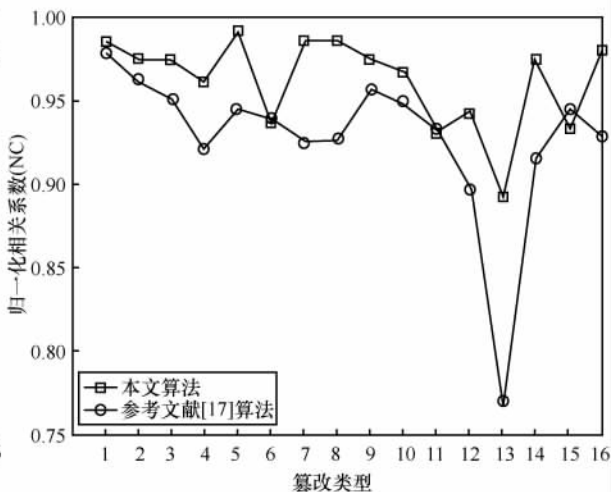
(a) Lena 图像 NC 值比较结果



(b) Goldhill 图像 NC 值比较结果



(c) Peppers 图像 NC 值比较结果



(d) NC 平均值比较结果

图 14 本文算法与参考文献[17]算法的 NC 值比较



印顽健性减弱。因此,  $\beta$  值需在两者之间进行一个折中的选择。每个载体图像的不同区域有比较大的差异, 本文采取了一种自适应水印嵌入强度选择方式, 即根据每个图像块自身信息进行水印嵌入强度的选择, 较好地确保了水印不可觉察性和顽健性之间的平衡。

## 5 结束语

针对现有水印算法功能单一且无法实现完全盲检测的局限性, 提出一种同时进行版权保护和内容认证的全盲双功能数字水印算法。实验结果表明, 相比于已报道的一些水印算法, 本文算法对于常见的图像处理攻击具有更好的顽健性, 能够很好地实现图像的版权保护, 而且能够对图像遭受到恶意篡改区域进行准确的检测和定位, 实现图像的内容认证。本文算法在进行图像版权保护和内容认证的过程中只用到了待检测图像, 实现了全盲检测, 因此具有更大的实用性。

## 参考文献:

- [1] PREDA R O. Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain[J]. Measurement, 2013, 46(1): 367-373.
- [2] 叶天语. 双重功能图像水印算法[J]. 光电子·激光, 2011, 22(4): 612-617.  
YE T Y. An image watermarking algorithm with dual purpose[J]. Journal of Optoelectronics·Laser. 2011, 22(4): 612-617.
- [3] 吕建平, 刘齐. 基于混沌理论和量化方法的双功能水印算法[J]. 西安邮电大学学报, 2014, 19(3): 54-57.  
LV J P, LIU Q. Bifunctional watermarking algorithm based on chaos theory and quantitative methods [J]. Journal of Xi'An University of Posts and Telecommunications, 2014, 19 (3): 54-57.
- [4] 叶天语, 钮心忻, 杨义先. 多功能双水印算法[J]. 电子与信息学报, 2009, 31(3): 546-551.  
YE T Y, NIU X X, YANG Y X. A multi-purpose dual watermark algorithm [J]. Journal of Electronics & Information Technology, 2009, 31(3): 546-551.
- [5] 陈光喜, 尹柳, 易招师. 基于整数提升小波变换的多功能数字水印[J]. 计算机工程与应用, 2010, 46(11): 115-118.  
CHEN G X, YIN L, YI Z S. Multi-purpose digital watermark based on integer lifting wavelet transformation [J]. Computer Engineering and Application, 2010, 46(11): 115-118.
- [6] 叶天语. 自嵌入双功能图像水印算法[J]. 光子学报, 2012, 41(7): 859-867.  
YE T Y. A self-embedding image watermarking scheme with dual purpose[J]. Acta Photonica Sinica, 2012, 41(7): 859-867.
- [7] 朱光, 师文, 朱学芳, 等. 结合 SURF 特征的多功能彩色图像水印算法[J]. 中国图象图形学报, 2013, 18(12): 1694-1702.  
ZHU G, SHI W, ZHU X F, et al. Multi-purpose watermark of color image based on SURF [J]. Journal of Image and Graphics, 2013, 18(12): 1694-1702.
- [8] 赵春晖, 刘巍. 基于压缩感知的交互支持双水印算法 [J]. 电子学报, 2012, 40(4): 681-687.  
ZHAO C H, LIU W. Mutual support dual watermark algorithm based on compressive sensing [J]. Acta Electronica Sinica, 2012, 40(4): 681-687.
- [9] 孟倩, 王希常, 刘江. 基于 DCT 变换的数字水印算法研究[J]. 微型机与应用, 2010, 29(23): 37-40.  
MENG Q, WANG X C, LIU J. Research on the digital watermark based on DCT [J]. Image Processing and Multimedia Technology, 2010, 29(23): 37-40.
- [10] PARAH S A, SHEIKH J A, LOAN N A, et al. Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing[J]. Digital Signal Processing, 2016, 53(C): 11-24.
- [11] DAS C, PANIGRAHI S, SHARMA V K, et al. A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation [J]. AEU-International Journal of Electronics and Communications, 2014, 68(3): 244-253.
- [12] QI X, XIN X. A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization[J]. Journal of Visual Communication & Image Representation, 2015, 30(C): 312-327.
- [13] RANI A, BHULLAR A K, DANGWALD, et al. A zero-watermarking scheme using discrete wavelet transform [J]. Procedia Computer Science, 2015, 70: 603-609.
- [14] 王友卫, 申铨京, 吕颖达, 等. 基于 DCT 和 SVD 变换的盲数字水印算法[J]. 计算机工程与应用, 2011, 47(21): 157-161.  
WANG Y W, SHEN X J, LV Y D, et al. Blind digital watermarking algorithm based on DCT and SVD transform[J]. Computer Engineering and Applications, 2011, 47(21): 157-161.
- [15] 翟依依, 王光义. 基于 Tent 混沌序列的数字图像加密方法[J]. 现代电子技术, 2014, 37(12): 73-77.  
ZHAI Y Y, WANG G Y. Digital image encryption algorithm based on tent chaotic sequence [J]. Modern Electronics Technique, 2014, 37(12): 73-77.
- [16] 叶天语. 基于子块区域分割和自嵌入技术的全盲多功能图像水印算法[J]. 通信学报, 2013, 34(3): 148-156.  
YE T Y. Perfectly blind image watermarking scheme with multi-purpose based on region segment for sub-block and self-embedding technology[J]. Journal on Communications, 2013, 34(3): 148-156.

[17] 叶天语. DWT-SVD 域全盲自嵌入顽健量化水印算法 [J]. 中国图象图形学报, 2012, 17(6): 644-650.

YE T Y. Perfectly blind self-embedding robust quantization-based watermarking scheme in DWT-SVD domain[J]. Journal of Image and Graphics, 2012, 17(6): 644-650.

#### [作者简介]



**薛栋**(1991-),男,宁波大学硕士生,主要研究方向为数字图像处理、数字水印。



**周亚训**(1965-),男,博士,宁波大学教授,主要研究方向为图像信息隐藏和光纤通信。



**金炜**(1969-),男,博士,宁波大学副教授,主要研究方向为遥感图像处理、医学图像处理、压缩感知和光电检测。