

# 一种新的半脆弱彩色图像数字水印算法

王向阳<sup>1,2</sup> 杨红颖<sup>1</sup> 侯丽敏<sup>1</sup>

**摘要** 提出了一种基于内容的半脆弱彩色图像数字水印嵌入算法, 该算法可同时用于彩色图像的版权保护和内容认证. 首先将彩色载体图像从 RGB 空间转换到  $Y C_r C_b$  空间. 然后对亮度 ( $Y$ ) 进行  $L+1$  级小波分解, 并将分解后的小波近似系数用混沌序列进行调制从而生成基于图像内容的数字水印信号. 最后对亮度 ( $Y$ ) 及色差 ( $C_r$  和  $C_b$ ) 进行  $L$  级小波分解, 并结合视觉感知特性及局部系数相关特性, 通过分块量化措施将水印信号嵌入到载体图像 ( $Y$ ,  $C_r$  和  $C_b$ ) 的小波域中. 仿真实验表明, 本文算法不仅具有较好的透明性, 对 JPEG 压缩、叠加噪声、平滑滤波等常规图像处理操作具有较好的鲁棒性, 而且能够对剪切、替换等恶意图像篡改作出报警并确定被篡改位置. 同时常规图像处理下其误检率与漏检率均比较低.

**关键词** 半脆弱水印, 彩色图像, 分块量化, 视觉感知特性, 混沌  
**中图分类号** TP391

## A New Semi-fragile Color Image Watermarking Algorithm

WANG Xiang-Yang<sup>1,2</sup> YANG Hong-Ying<sup>1</sup> HOU Li-Min<sup>1</sup>

**Abstract** A new content-based semi-fragile color image watermarking algorithm is proposed in this paper, which can be used for color image copyright protection and content authentication simultaneously. Firstly, the color image is converted from an RGB color space to a  $Y C_r C_b$  color space. Secondly, the luminance component ( $Y$ ) is decomposed by the  $L+1$  level discrete wavelet decomposition, and the approximate wavelet coefficient matrix of the luminance component ( $Y$ ) and the chaotic sequences are used to generate the content-based and secure watermark. Finally, luminance component ( $Y$ ) and chrominance components ( $C_r$  and  $C_b$ ) are decomposed by the  $L$  level discrete wavelet decomposition, and the watermark is embedded into color components ( $Y$ ,  $C_r$  and  $C_b$ ) by using the technique based on human visual system and block quantization. Experimental results show that our semi-fragile watermarking scheme is invisible and is robust to common image processing (such as JPEG compression, noise adding, filtering). The proposed watermarking algorithm is fragile to content modification (such as cropping), can detect effectively the tampered regions, and has a lower probability of missing or false alarm, compared with other popular semi-fragile watermarking schemes.

**Key words** Semi-fragile watermark, color image, block quantization, human visual system, chaotic

## 1 引言

近年来, 同时用于版权保护与内容认证的半脆弱图像水印技术研究取得了一定进展, 并陆续提出

了诸如基于鲁棒水印原理、与 JPEG 编解码器相结合、基于视觉掩模、基于量化系数等多种半脆弱图像水印算法<sup>[1]</sup>. 例如, Yu 等<sup>[2]</sup> 认为图像小波系数的变化近似服从高斯分布, 提出了基于小波系数加权平均值量化的水印嵌入方法. Fridrich<sup>[3]</sup> 将原始载体划分成等大小的图像子块, 并通过块映射等措施生成水印信号, 进而利用调制技术把水印信息嵌入到 DCT 域内. 孙锐等<sup>[4]</sup> 提出了一种基于分组奇异值分解的半易损水印技术, 该算法是将经过伪随机排序的二值图像通过量化策略嵌入到分组 SVD 分解中最大的奇异值点. Tefas 和 Pitas 等<sup>[5]</sup> 提出了用二维混沌动态系统对二值水印信息进行扩频处理, 再将处理后的水印信息调制到原始图像的空间域或变换域. 董刚等<sup>[6]</sup> 提出了一种基于 JPEG 有损压缩的半脆弱性数字图像水印算法. Queluz<sup>[7]</sup> 以伪随机序列作为数字水印, 提出了基于线性三元组量化的空间域半脆弱图像水印算法等. 理论分析和实验结果表明, 现有半脆弱图像水印算法普遍存在篡改检测较出色、无攻击情形下具有较低误检率等优点 (特别是量化嵌入技术), 但也不同程度存在如下不足<sup>[8]</sup>:

收稿日期 2006-4-10 收修改稿日期 2006-7-26  
Received April 10, 2006; in revised form July 26, 2006  
视觉与听觉信息处理国家重点实验室 (北京大学) 开放基金 (0503), 信息安全国家重点实验室 (中国科学院软件研究所) 开放基金 (03-06), 大连市科技基金 (2006J23JH020), “图像处理与图像通信” 江苏省重点实验室 (南京邮电大学) 开放基金 (ZK205014), 江苏省计算机信息处理技术重点实验室 (苏州大学) 开放课题基金 (KJS0602) 资助  
Supported by Open Foundation of State Key Laboratory of Vision and Auditory Information Processing (Beijing University) (0503), Open Foundation of State Key Laboratory of Information Security of P. R. China (03-06), Natural Science Foundation of Dalian City of P. R. China (2006J23JH020), Open Foundation of Key Laboratory of Image Processing and Image Communication (Nanjing University of Posts and Communications) (ZK205014), Open Foundation of Jiangsu Province Key Laboratory for Computer Information Processing Technology (Soochow University) (KJS0602)  
1. 辽宁师范大学计算机与信息技术学院 大连 116029 2. 北京大学视觉与听觉信息处理国家重点实验室 北京 100871  
1. School of Computer and Information Technique, Liaoning Normal University, Dalian 116029 2. State Key Laboratory of Vision and Auditory Information Processing, Beijing University, Beijing 100871  
DOI: 10.1360/aas-007-0561

1) 所选用的数字水印一般是伪随机序列或具有实际含义的字符串(包括标志图像),安全性较差;2) 嵌入水印信息时,未能充分考虑图像自身的局部相关性及其人眼视觉特性,故数字水印的透明性和鲁棒性有待进一步提高;3) 无攻击情形下误检率较低,但常规图像处理下误检率与漏检率均较高;4) 已有算法基本上是针对灰度图像的,有关彩色图像的半脆弱数字水印方案尚未得到充分研究。

本文提出一种基于内容的半脆弱彩色图像水印嵌入算法,该算法具有以下特点:1) 以混沌理论为基础,选用了基于图像内容的自适应安全数字水印;2) 采纳了基于视觉感知与图像局部相关的自适应分块量化策略;3) 数字水印信息的提取不需要原始载体图像;4) 能够同时进行版权保护与内容认证,并可大致确定篡改发生区域;5) 常规图像处理下具有比较低的误检率与漏检率。

## 2 基于图像内容的数字水印生成

为了提高整个数字水印系统的安全性能,本文结合混沌理论,给出一种全新的数字水印信号选取方法,即从原始载体图像中提取特征信息作为数字水印。

设原始载体为 24 位真彩色图像  $I = \{g(i, j), 1 \leq i \leq M, 1 \leq j \leq N\}$ . 其中,  $g(i, j)$  代表原始载体图像的第  $i$  行、第  $j$  列像素的颜色值. 则基于图像内容的自适应数字水印生成过程如下。

### 2.1 利用混沌序列生成掩蔽矩阵 $M_r$ 和 $M_b$

混沌序列具有许多优良特性<sup>[9]</sup>. 为了满足数字水印的安全性要求,我们将利用混沌序列来生成基于图像内容的自适应数字水印. 为此,需要经过以下步骤来生成实值掩蔽矩阵  $M_r$  和二值混沌矩阵  $M_b$ :

1) 利用 *Logistic* 映射生成实值混沌序列  $x(k)(k = 1, 2, 3, \dots)$ (*Logistic* 迭代函数的初始值为  $K, K$  是密钥)。

2) 从实值混沌序列  $x(k)(k = 1, 2, 3, \dots)$  中选取  $(M/2^{L+1}) * (N/2^{L+1})(L+1$  为小波分解级数) 个元素生成实值掩蔽矩阵  $M_r$ , 并通过实值混沌序列二值化生成二值混沌矩阵  $M_b$ .  $M_b$  由 0 或 1 的元素组成,但其具有实值混沌序列的优点。

3) 将二值混沌矩阵  $M_b$  元素由  $\{0,1\}$  映射为  $\{1,-1\}$ , 即  $0 \rightarrow 1, 1 \rightarrow -1$ .

### 2.2 载体图像的彩色空间变换

为了便于从原始载体图像中提取特征信息作为数字水印,本文选取了  $Y C_r C_b$  彩色空间. 由于人眼对色差 ( $C_r$  和  $C_b$ ) 的分辨能力远比对亮度 ( $Y$ ) 的分辨能力低,说明亮度分量 ( $Y$ ) 中必然包含有原始

彩色图像的更多特征信息,为此本文将从亮度分量 ( $Y$ ) 内提取特征信息作为数字水印。

### 2.3 基于图像内容的数字水印提取

对彩色载体图像的亮度分量 ( $Y$ ) 实施  $L+1$  级小波分解,可得到一系列不同分辨率及不同方向的多种子带,即 1 个第  $L+1$  级的近似小波系数矩阵 ( $S_{L+1}^{LL}$ ) 和  $3L$  个细节(水平、垂直、对角线)小波系数矩阵 ( $S_{L+1}^{HL}, S_{L+1}^{LH}, S_{L+1}^{HH}, \dots, S_1^{HL}, S_1^{LH}, S_1^{HH}$ ). 由小波分析理论知,近似小波系数矩阵  $S_{L+1}^{LL}$  包含了亮度分量 ( $Y$ ) 的大部分能量(特征信息),是其小波变换域中最重要部分. 为此,我们利用其生成基于图像内容的水印矩阵  $W$ :

$$S'_{L+1}^{LL} = S_{L+1}^{LL} * M_r$$

$$w(i, j) = \begin{cases} 1 & s'_{L+1}^{LL}(i, j) \geq T_1 \\ -1 & s'_{L+1}^{LL}(i, j) < T_1 \end{cases}$$

其中,  $w(i, j) \in W, s'_{L+1}^{LL}(i, j) \in S'_{L+1}^{LL}, i = 1, 2, \dots, M/2^{L+1}, j = 1, 2, \dots, N/2^{L+1}, T_1$  为阈值,  $*$  表示点乘。

### 2.4 数字水印的调制

调制上一步所提取出的数字水印矩阵  $W$ , 便可得到基于图像内容的自适应安全水印矩阵  $W_1$ . 对任意  $w_1(i, j)$ :

$$w_1(i, j) = w(i, j) \oplus m_b(i, j)$$

其中,  $w_1(i, j) \in W_1, w(i, j) \in W, m_b(i, j) \in M_b, i = 1, 2, \dots, M/2^{L+1}, j = 1, 2, \dots, N/2^{L+1}, \oplus$  表示异或操作。

## 3 数字水印嵌入

基于内容的半脆弱彩色图像数字水印嵌入方案的主要步骤可描述如下。

### 3.1 载体图像的彩色空间变换

为使数字水印信息能较强地分布于 RGB 三个通道以便抵抗各种对彩色图像进行分色的攻击,本文选取了  $Y C_r C_b$  彩色空间,即首先将彩色载体图像  $I$  从 RGB 空间转换到  $Y C_r C_b$  空间,然后再对  $Y C_r C_b$  空间内图像信息实施水印嵌入。

### 3.2 基于图像内容的数字水印生成

按照第 2 节的操作步骤,提取出基于图像内容的自适应安全水印矩阵  $W_1$ 。

### 3.3 彩色分量的小波变换与子带选取

研究表明:不同攻击对彩色图像的亮度 ( $Y$ ) 和色差 ( $C_r, C_b$ ) 的破坏力是不同的. 其中, JPEG 压

缩、叠加噪声等处理对色差分量 ( $C_r$ 、 $C_b$ ) 的影响较大,对亮度分量 ( $Y$ ) 的破坏相对较小;而锐化等处理则正好相反.为了提高数字水印的隐藏效果,本文算法将分别在彩色载体图像三个彩色分量(即亮度  $Y$ 、色差  $C_r$  和  $C_b$ ) 内嵌入数字水印(共计嵌入 3 次).

对彩色分量实施  $L$  级小波变换,可得到一系列不同分辨率及不同方向的多种子带.为了有效进行版权保护和内容认证,本文选取小波变换域的低频区(即  $LL$  子带)作为数字水印嵌入区.

### 3.4 数字水印的嵌入

本文采用量化调制小波系数方法,将水印信息  $W_1$  嵌入到彩色分量 ( $Y$ 、 $C_r$  和  $C_b$ ) 的小波域(最低频子带  $LL$ ) 内.亮度  $Y$  内嵌入数字水印的关键步骤如下(色差  $C_r$ 、 $C_b$  内嵌入水印方法与之相同).

1) 将小波变换域的最低频子带  $Y_L^{LL}$  划分成大小为  $2 \times 2$  的图像子块(每个图像子块内仅嵌入 1 个比特的水印信息).

2) 计算图像子块所含小波系数绝对值的平均值  $B(i, j)$  ( $i = 1, 2, \dots, M/2^{L+1}, j = 1, 2, \dots, N/2^{L+1}$ ), 然后用量化步长  $\Delta$  对其进行量化,再根据量化结果修改图像子块内元素值,以完成水印信息的嵌入.

令

$$B(i, j) = \frac{1}{4} \sum_{m=1}^2 \sum_{n=1}^2 |Y_L^{LL}(mi, nj)|$$

$$q(i, j) = \left\lfloor \frac{B(i, j)}{\Delta} \right\rfloor$$

则本文所采用的量化嵌入方案为:

将  $\text{mod}(q(i, j), 2)$  之值由  $\{0, 1\}$  映射为  $\{1, -1\}$ , 即  $0 \rightarrow 1, 1 \rightarrow -1$ .

如果  $\text{mod}(q(i, j), 2) \neq w_1(i, j)$ , 则

如果  $w_1(i, j) = 1$ , 则

$$Y_L^{LL}(mi, nj) =$$

$$\begin{cases} q_1 \cdot \Delta - 1, & \text{如果 } Y_L^{LL}(mi, nj) > \Delta \\ q_1 \cdot \Delta + 1, & \text{如果 } Y_L^{LL}(mi, nj) < -\Delta \\ Y_L^{LL}(mi, nj), & \text{如果 } |Y_L^{LL}(mi, nj)| \leq |\Delta| \end{cases}$$

否则

$$Y_L^{LL}(mi, nj) =$$

$$\begin{cases} q_2 \cdot \Delta, & \text{如果 } |Y_L^{LL}(mi, nj)| > |\Delta| \\ Y_L^{LL}(mi, nj), & \text{如果 } |Y_L^{LL}(mi, nj)| \leq |\Delta| \end{cases}$$

如果  $\text{mod}(q(i, j), 2) = w_1(i, j)$ , 则不对  $Y_L^{LL}(mi, nj)$  做任何处理.

其中,  $\Delta$  为量化步长;  $w_1(i, j) \in W_1$ ;  $i = 1, 2, \dots, M/2^{L+1}, j = 1, 2, \dots, N/2^{L+1}; m = 1, 2; n = 1, 2$ . 且

$$q_1 = \left\lfloor \frac{Y_L^{LL}(mi, nj)}{\Delta} \right\rfloor, q_2 = \left\lceil \frac{Y_L^{LL}(mi, nj)}{\Delta} \right\rceil$$

不难看出,与现有图像水印嵌入方法<sup>[1,2,7]</sup>普遍采用单系数量化策略(即  $q(x, y) = \lfloor I(x, y)/\Delta \rfloor$ ,  $I(x, y)$  为单个小波系数)不同,本文算法采用了分块系数量化方案(即  $q(x, y) = \lfloor B(x, y)/\Delta \rfloor$ ,  $B(x, y)$  为图像子块内小波系数绝对值的平均值),其充分利用了相邻系数之间的相关特性,故必然提高对 JPEG 压缩之类常规处理操作的鲁棒性.

另外,对基于量化的图像水印嵌入方法来说,量化步长  $\Delta$  的选取至关重要.为此,我们引入反映人眼视觉系统的感知计算模型,并依据小波域相邻子带相关性,利用相同分解级的两个相邻子带  $Y_L^{LH}$  和  $Y_L^{HL}$  内相同位置的视觉感知特性值  $T_l^\theta(x, y)$  (其中,  $l$  为小波分解层次;  $\theta \in \{LL, LH, HL, HH\}$  表示子带的方向;  $x, y$  表示小波系数位置)来预测小波系数上嵌入的量化步长  $\Delta$  值,即结合载体图像邻域特性确定量化步长  $\Delta$

$$\Delta(i, j) =$$

$$\ln \frac{\sum_{m=1}^2 \sum_{n=1}^2 |T_L^{LH}(mi, nj)| + \sum_{m=1}^2 \sum_{n=1}^2 |T_L^{HL}(mi, nj)|}{8}$$

### 3.5 逆小波变换

用含有数字水印信息的小波系数  $Y_L^{LL}(mi, nj)$  代替  $Y_L^{LL}(mi, nj)$ , 并结合未修改的小波系数进行  $L$  级逆小波变换,便可得到含水印信息的亮度分量  $Y'$ .

### 3.6 彩色分量的彩色空间变换

将含水印信息的彩色分量 ( $Y'$ 、 $C'_r$  和  $C'_b$ ) 从  $Y C_r C_b$  空间转换到 RGB 空间,便可以得到含水印彩色图像  $I'$ .

## 4 数字水印的提取

水印提取是水印嵌入的逆步骤.本文讨论的数字水印检测算法属于目标检测算法,即在检测数字水印时不需要原始的彩色载体图像.设待检测彩色图像为  $I'$ , 则数字水印检测过程如下.

1) 将待检测彩色图像  $I'$  从 RGB 空间转换到  $Y C_r C_b$  空间,并提取出彩色分量 ( $Y'$ 、 $C'_r$  和  $C'_b$ ).

2) 分别从彩色分量  $Y'$ 、 $C'_r$  和  $C'_b$  中提取数字水印信息  $W'_{1,1}$ 、 $W'_{1,2}$  和  $W'_{1,3}$ . 从亮度  $Y'$  中提取水印信息  $W'_{1,1}$  的操作步骤如下 ( $W'_{1,2}$  和  $W'_{1,3}$  提取方法类似).

a) 对待检测亮度  $Y'$  实施  $L$  级小波变换, 并选取最低频子带  $Y'_L{}^{LL}$  用于水印提取.

b) 将所选子带  $Y'_L{}^{LL}$  划分成大小为  $2 \times 2$  的图像子块, 并从图像子块内提取水印信息  $W'_{1,1}$ . 提取方法可以表示为

$$B'(i, j) = \frac{1}{4} \sum_{m=1}^2 \sum_{n=1}^2 |Y'_L{}^{LL}(mi, nj)|, q'(i, j) = \left\lfloor \frac{B'(i, j)}{\Delta} \right\rfloor$$

$$w'_{1,1}(i, j) = \begin{cases} 1 & \text{如果 } \text{mod}(q'(i, j), 2) = 0 \\ -1 & \text{如果 } \text{mod}(q'(i, j), 2) = 1 \end{cases}$$

其中,  $w'_{1,1}(i, j) \in W'_{1,1}$ ,  $i = 1, 2, \dots, M/2^{L+1}$ ,  $j = 1, 2, \dots, N/2^{L+1}$ , 量化步长  $\Delta$  取值为

$$\Delta'(i, j) = \frac{\sum_{m=1}^2 \sum_{n=1}^2 |T'_L{}^{LH}(mi, nj)| + \sum_{m=1}^2 \sum_{n=1}^2 |T'_L{}^{HL}(mi, nj)|}{8}$$

3) 按照“多数原则”计算待检测彩色图像所嵌入的自适应安全水印  $W'_1$ , 其中

$$w'_1(i, j) = \begin{cases} 1 & \text{如果 } w'_{1,r}(i, j) \text{ 中有两个以上为 } 1 \\ -1 & \text{否则} \end{cases}$$

( $r = 1, 2, 3$ )

这里,  $w'_1(i, j) \in W'_1$ ,  $w'_{1,1}(i, j) \in W'_{1,1}$ ,  $w'_{1,2}(i, j) \in W'_{1,2}$ ,  $w'_{1,3}(i, j) \in W'_{1,3}$ .

## 5 版权信息的判断和恶意篡改的认证

设接收到的可能遭受攻击的含水印彩色图像为  $I'$ . 从  $I'$  中提取出的水印信息为  $W'_1$  (参见第 4 节), 而从  $I'$  中重建的基于图像内容的自适应安全水印为  $W_1$  (参见第 2 节), 则版权信息判断与恶意篡改认证的具体工作步骤为:

1) 定义篡改矩阵  $W_1^*$  (篡改矩阵  $W_1^*$  中元素为 1 的区域意味着该区域可能被篡改).

$$W_1^* = W'_1 \oplus W_1 \quad (\oplus \text{为异或运算})$$

2) 对篡改矩阵  $W_1^*$  进行中值滤波 ( $2 \times 2$ ). 实验结果表明, 可以通过篡改矩阵  $W_1^*$  确定篡改发生

位置, 而对含水印图像实施 JPEG 压缩、叠加噪声、平滑滤波等常规处理操作后, 由  $W_1^*$  所确定出的篡改发生区域呈均匀分布或随机分布 (参见图 2(c), Beach 图像, 见下页). 当对篡改矩阵  $W_1^*$  进行中值滤波 ( $2 \times 2$ ) 后, 由常规图像处理操作所引起的篡改区域大部分将被删除.

3) 将篡改矩阵  $W_1^*$  (已经中值滤波) 划分成  $m \times n$  的子块, 并计算每个子块的篡改比率  $F_1^*(u, v)$ .

$$F_1^*(u, v) = \frac{\sum_{i=1}^m \sum_{j=1}^n w_1^*(iu, jv)}{m \times n}$$

其中,  $w_1^*(iu, jv) \in W_1^*$ ,  $u = 1, 2, \dots, M/(2^{L+1} \cdot m)$ ,  $v = 1, 2, \dots, N/(2^{L+1} \cdot n)$ .

4) 计算最大篡改比率  $\tilde{F}_1^*$ .

$$\tilde{F}_1^* = \max_{u,v} (F_1^*(u, v))$$

5) 适当选取检测阈值  $T$ , 进行版权信息判断与恶意篡改认证. 规则如表 1 所示.

表 1 判断认证规则  
Table 1 The authentication rule

| 条件                  | 结果          |
|---------------------|-------------|
| $\tilde{F}_1^* = 0$ | 未遭受任何攻击     |
| $\tilde{F}_1^* < T$ | 已遭受常规图像处理攻击 |
| $\tilde{F}_1^* > T$ | 已遭受恶意篡改攻击   |

另外, 对内容已被恶意篡改的不可靠图像 (即  $\tilde{F}_1^* > T$ ) 来说, 可以通过篡改矩阵  $W_1^*$  确定篡改发生区域 (即  $w_1^*(i, j) = 1$  处图像子块).

## 6 实验结果

为验证本文算法的鲁棒性、脆弱性和高效性, 以下给出了 24 位真彩色图像 (600×400 的 Beach、500×350 的 Greatwall、512×512 的 Lena 等) 的实验结果, 并与 Fridrich 法<sup>[3]</sup>、Queluz 法<sup>[7]</sup>及 Liao 法<sup>[2]</sup> (同样嵌入在  $Y$ 、 $C_r$  和  $C_b$  三个分量内) 进行了对比. 实验中, *Logistic* 迭代的初始值选取为  $K = 0.60772$ , 迭代参数选取为  $\mu = 3.990$ . 小波变换采用了常见的 *Haar* 小波基.  $m \times n$  选取为  $5 \times 5$ . 检测阈值选取为  $T = 0.50$ . 图 1(a) 和 1(c) 为嵌入了水印信息的图像 (Beach 和 Greatwall), 其峰值信噪比分别为 42.7dB 和 42.4dB, 均远大于 Fridrich 法、Queluz 法及 Liao 法建议的 38dB, 而且视觉上与原图像没有区别.

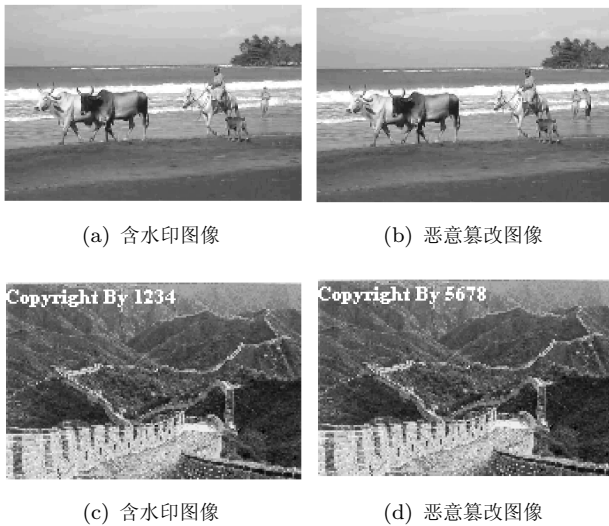


图 1 篡改检测实验结果

Fig. 1 The tamper detection result

### 6.1 对常规图像处理的鲁棒性

为了测试算法的鲁棒性, 我们使用 JPEG 压缩、叠加噪声、平滑滤波等常规信号处理方法对含水印图像进行了处理. 表 2 给出了部分测试结果. 实验数据表明, 本文算法具有较好的鲁棒性, 在含水印图像遭到 JPEG 压缩、叠加噪声、平滑滤波等常规攻击后仍能够检测到图像的版权.

表 2 常规图像处理后的检测结果 (篡改比率  $\tilde{F}_1^*$ )

Table 2 The detection results for common signal processing

| 攻击方式     | 参数                | Beach | Greatwall |
|----------|-------------------|-------|-----------|
| JPEG     | 压缩比为 8            | 0.216 | 0.228     |
|          | 压缩比为 16           | 0.252 | 0.285     |
|          | 压缩比为 32           | 0.317 | 0.309     |
| JPEG2000 | 压缩比为 8            | 0.126 | 0.125     |
|          | 压缩比为 16           | 0.193 | 0.216     |
|          | 压缩比为 32           | 0.281 | 0.287     |
| 叠加噪声     | 椒盐噪声 1%           | 0.121 | 0.128     |
|          | 高斯噪声 30dB         | 0.279 | 0.273     |
| 平滑滤波     | 低通滤波 $3 \times 3$ | 0.148 | 0.158     |
|          | 中值滤波 $2 \times 2$ | 0.233 | 0.133     |
|          | 中值滤波 $3 \times 3$ | 0.190 | 0.204     |
|          | 中值滤波 $4 \times 4$ | 0.262 | 0.272     |

### 6.2 对恶意篡改的脆弱性

为了测定算法的脆弱性, 以及能否在经过一般

处理后找到图像被篡改的区域, 我们首先对测试图像 (含有水印信息的 Beach 图像和 Greatwall 图像) 进行 JPEG 压缩, 然后使用 PhotoShop 改变图像内容. 图 1(b) 和图 1(d) 分别为首先对含水印图像 (图 1(a) 和 1(c)) 进行 50% JPEG 压缩, 然后进一步对其进行恶意篡改的结果.

此时, 对于被恶意篡改的含水印图像 Beach 来说, 篡改比率  $\tilde{F}_1^*=0.61$ , 而篡改矩阵  $W_1^*$  如图 2(a) 所示. 而对于被恶意篡改的含水印图像 Greatwall 来说, 篡改比率  $\tilde{F}_1^*=0.56$ , 而篡改矩阵  $W_1^*$  如图 2(b) 所示.

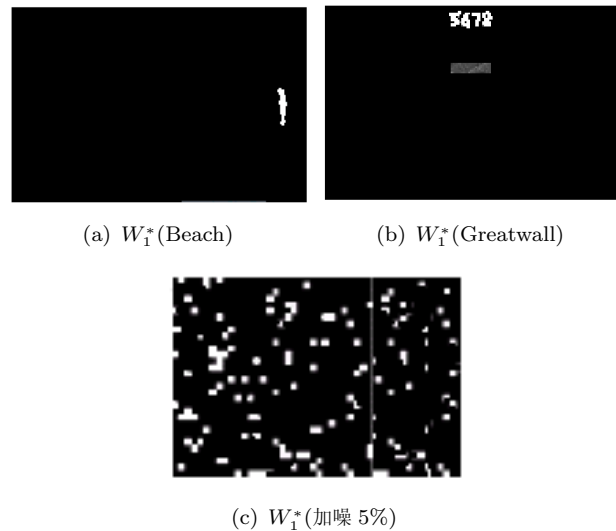


图 2 抽取出的水印及篡改区域检测

Fig. 2 The extracted watermark and tamper detection

实验数据表明, 本文算法不仅对于恶意篡改具有脆弱性, 而且可以通过篡改矩阵  $W_1^*$  大致确定出发生篡改的位置.

### 6.3 误检率与漏检率对比

为了验证算法的高效性, 仿真实验根据误检率与漏检率对本文算法与 Fridrich 法、Queluz 法及 Liao 法的表现进行了比较, 测试结果 (该实验使用了 Beach、Greatwall 及 Lena、Barbara、Peppers 等标准图像共计 10 幅) 如表 3 所示. 考虑到算法比较的客观性与公平性, 仿真实验将四种算法的篡改检测足迹 (footprint) 统一转化为标准的  $8 \times 8$  块. 另外, 对比实验中使用了以下几种容许性常规图像处理操作, 包括: 1) 适度压缩, 以 70% JPEG 为例; 2) 直方图均衡 (均匀分布); 3) 信噪比为 35 dB 的高斯噪声; 4) 1% 的椒盐噪声; 5)  $3 \times 3$  的低通滤波.

表 3 误检率与漏检率的对比  
Table 3 The probabilities of missing and probabilities of false alarm

| 半脆弱水印算法    | 伪造攻击漏检率 | 信号处理攻击误检率 |               |        |             |           |            |
|------------|---------|-----------|---------------|--------|-------------|-----------|------------|
|            |         | 无攻击       | JPEG 压缩 (70%) | 直方图均衡  | 高斯噪声 (35dB) | 椒盐噪声 (1%) | 低通滤波 (3×3) |
| Fridrich 法 | 0.66%   | 1.21%     | 5.01%         | 23.86% | 1.67%       | 18.52%    | 57.14%     |
| Queluz 法   | 1.06%   | 0.01%     | 7.22%         | 87.71% | 32.34%      | 0.78%     | 57.38%     |
| Liao 法     | 16.35%  | 0.24%     | 6.70%         | 59.23% | 1.90%       | 19.47%    | 50.25%     |
| 本文算法       | 0.18%   | 0.01%     | 1.05%         | 18.53% | 1.72%       | 0.78%     | 30.23%     |

## 7 结论

本文提出了一种基于内容的半脆弱彩色图像小波域数字水印嵌入方案. 其主要贡献如下: 1) 以混沌理论为基础, 选用了基于载体图像内容的自适应数字水印, 提高了数字水印系统的安全性; 2) 以视觉掩蔽特性与分块量化为基础, 采纳了新型高效的数字水印嵌入方案, 提高了数字水印系统的透明性和鲁棒性, 并从理论上分析计算了数字水印的误检率和漏检率. 3) 实现了基于内容与视觉掩蔽的半脆弱彩色图像小波域数字水印算法. 实验结果表明, 该算法可同时用于彩色图像的版权保护和内容认证.

## References

- Zhang Jing, Zhang Chun-Tian. Digital watermarking techniques for image authentication. *Journal of Image and Graphics*, 2003, **8**(4): 367~373  
(张静, 张春田. 用于图像认证的数字水印技术. 中国图像图形学报, 2003, **8**(4): 367~373)
- Yu G J, Lu C S, Liao H Y M. Mean quantization-based fragile watermarking for image authentication. *Optical Engineering*, 2001, **40**(7): 1396~1408
- Fridrich J. Security of fragile authentication watermarks with localization. In: *Proceedings of SPIE Security and Watermarking of Multimedia Contents IV*. California, USA, SPIE, 2002. **4675**: 691~700
- Sun Rui, Sun Hong, Yao Tian-Ren. SVD based semi-fragile watermarking method. *Journal of Circuits and Systems*, 2002, **7**(3): 62~65  
(孙锐, 孙洪, 姚天任. 基于奇异值分解的半易损水印算法. 电路与系统学报, 2002, **7**(3): 62~65)
- Tefas A, Pitas I. Image authentication using chaotic mixing system. In: *Proceedings of the IEEE International Symposium on Circuits and System*. Geneva, Switzerland, IEEE, 2000. 216~219
- Dong Gang, Zhang Liang, Zhang Chun-Tian. A semi-fragile digital image watermarking algorithm. *Journal of China Institute of Communications*, 2003, **24**(1): 33~38

(董刚, 张良, 张春田. 一种半脆弱性数字图像水印算法. 通信学报, 2003, **24**(1): 33~38)

- Queluz M P. Spatial watermark for image content authentication. *Journal of Electronic Imaging*, 2002, **11**(2): 275~285
- Ekici O, Sankur B, Akcay M. Comparative assessment of semifragile watermarking methods. *Journal of Electronic Imaging*, 2004, **13**(1): 209~216
- Walton S. Information authentication for a slippery new age. *Dr.Dobb's Journal*, 1995, **20**(4): 18~26



王向阳 辽宁师范大学计算机与信息技术学院教授. 主要研究方向包括网络信息安全技术, 多媒体信息处理技术. 本文通信作者. E-mail: wxy37@126.com  
(WANG Xiang-Yang Professor.

His research interest covers information security and multimedia processing. Corresponding author of this pa-

per.)



杨红颖 辽宁师范大学计算机与信息技术学院副教授. 主要研究方向包括多媒体技术, 计算机辅助教学.

(YANG Hong-Ying Assistant professor. Her research interest covers multimedia technique and CAI.)



侯丽敏 辽宁师范大学计算机与信息技术学院硕士研究生. 主要研究方向包括信息隐藏与数字水印.

(HOU Li-Min Master student at Liaoning Normal University. Her research interest covers information security and digital watermarking.)