

# 基于块特征和混沌序列的图像篡改检测与恢复

张君捧<sup>1,2</sup>, 张庆范<sup>1</sup>, 杨红娟<sup>2</sup>

(1. 山东大学控制科学与工程学院, 山东 济南 250100;

2. 山东建筑大学信息与电气工程学院, 山东 济南 250101)

**摘要:** 为提高图像篡改检测与恢复性能, 提出一种基于块特征与混沌序列的图像认证水印方案。对  $2 \times 2$  分块离散余弦变换系数编码产生块特征, 嵌入到其他图像块像素的低两位, 块嵌入的映射关系通过混沌序列产生; 结合奇偶检测法对常规的认证方式进行改进, 并通过提取有效块的特征信息实现被篡改区域的自恢复。试验表明, 该方案嵌入水印信息量少, 安全性高, 对常规篡改可进行精确定位, 并能较好的实现自恢复, 还可以有效地检测出仅图像内容的攻击。

**关键词:** 图像认证; 数字水印; 篡改检测; 自恢复; 混沌

**中图分类号:** TP391 **文献标志码:** A

## Images tamper detection and recovery based on block features and chaotic sequence

ZHANG Junpeng<sup>1,2</sup>, ZHANG Qingfan<sup>1</sup>, YANG Hongjuan<sup>2</sup>

(1. School of Control Science and Engineering, Shandong University, Jinan 250100, Shandong, China;

2. School of Information & Electrical Engineering, Shandong Jianzhu University, Jinan 250101, Shandong, China)

**Abstract:** To improve the performance of images tamper detection and recovery, an authentication watermarking scheme based on block features and chaotic sequence was presented. For each block of size  $2 \times 2$  pixels, discrete cosine transform (DCT) coefficients were used to generate watermarking and embedded into the two least significant bits of its mapping block which was determined by chaotic sequence. The conventional authentication methods were improved by combining parity detection and the tampered region could be self-recovered by extracting characteristic information of the valid block. Experimental results demonstrated that the proposed method not only improved the quality and security of watermarked images, but also could detect tampered regions accurately and reconstruct images while keeping the recognition quality. Additionally, the scheme was not vulnerable to the content-only attack.

**Key words:** image authentication; digital watermarking; tamper detection; self-recovery; chaos

## 0 引言

随着网络技术与多媒体技术的发展, 人们已经越来越关注于多媒体内容的完整性认证, 尤其是图像的完整性验证<sup>[1-2]</sup>。其解决方案主要采用数字签

名和数字水印技术。数字签名方案虽然能够达到内容认证的目的, 但是图像信息发生细微变化, 签名都会发生变化而不能通过认证, 此外, 签名无法实现篡改区域的定位, 当图像受到恶意篡改时, 被破坏的重要数据不能得到恢复<sup>[3-4]</sup>。为了解决这一问题, 学者们开始提出基于数字水印的图像认证方案。数字

收稿日期: 2014-04-04 网络出版时间: 2014-06-30 15:58

网络出版地址: <http://www.cnki.net/kcms/doi/106040/j.issn.1672-3961.0.2014.098.html>

基金项目: 国家自然科学基金资助项目(61303087)

作者简介: 张君捧(1978-), 女, 河北保定人, 博士研究生, 主要研究方向为图像处理与信息安全. E-mail: zjpeng1234@sdu.edu.cn

水印技术通常分3种:鲁棒水印、半脆弱水印和脆弱水印。鲁棒水印能够经受各种恶意攻击,主要用于多媒体版权保护方面。半脆弱水印和脆弱水印主要用于图像认证方面,半脆弱水印能够检测出恶意篡改,但允许非恶意操作通过。脆弱水印技术是一种比较敏感的水印,不允许图像信息有任何的改动。在实际应用中,被篡改的图像信息不仅需要精确地定位出来,对于有价值的部分还需要能够被恢复出来。因此,越来越多的研究学者们提出了各种各样的篡改定位与恢复算法<sup>[5-13]</sup>。

Zhenxing Qian 等人提出一种基于  $8 \times 8$  分块 DCT 的自嵌入脆弱水印算法,根据分块的平滑与粗糙程度对 DCT 系数进行不同长度的编码来产生水印,并嵌入到图像块的低3位上<sup>[7]</sup>。该方案修改每个像素值的低3位,对图像的影响较大,同时,篡改定位的块效应较明显,因为若图像块中仅有一位像素被篡改,定位的结果却是把  $8 \times 8$  块都判定为篡改,因此降低了定位精度。金喜子等提出一种针对 JPEG 的篡改检测方案,但仅在篡改区域小于1%时可准确找到所有篡改小块,同时,因为采用  $8 \times 8$  分块,定位精度也不是很高<sup>[8]</sup>。文献[10]提出一种无错恢复能力的脆弱水印方案,但是,该方案也仅是在图像篡改比例小于3.2%时才可以实现无错恢复。Lee 等人提出一种图像篡改与检测的双水印方案,在这种方案中,分别在载体图像的上半部分和下半部分嵌入同一水印,一旦其中一个水印被破坏时还可以提供二次恢复的机会。该双水印方案定位精度高,可以提高恢复图像的质量<sup>[11]</sup>。但是该方案也有3个主要的缺点:第一,水印嵌入负载增加;第二,不能检测仅图像内容篡改的攻击;第三,通过线性关系获得水印块与嵌入块之间的映射关系,安全性不高。

在综合研究上述文献的基础上,本研究提出一种有效的图像篡改检测与恢复水印方案,该方案利用  $2 \times 2$  分块 DCT 系数编码作为块特征,嵌入到由混沌序列产生的映射块中,对文献[11]中的篡改检测方法进行了改进。相比于其他文献,该方案有如下优点:(1)块特征作为水印增加方案的可恢复性;(2)降低像素错误的敏感性与篡改检测的块效应;(3)非线性混沌序列的应用增加算法的安全性;(4)对于仅图像内容篡改的攻击具有较好的定位性能。

## 1 水印算法描述

假设原始图像大小为  $m \times n$ ,  $m$  和  $n$  均是2的整数倍。

### 1.1 水印的产生

采取自嵌入水印的方案,一方面可以不需要其他的水印参照信息,避免固定标识的水印为攻击者提供分析和破译的信息,另一方面可以方便的对篡改进行盲检测并能提高检测率。考虑到需要对篡改区域进行恢复,则所嵌入的水印需要包含原始图像的某特征信息。图像经过离散余弦变换(discrete cosine transform, DCT),其主要能量集中在 DCT 直流分量和低频系数上。此外,对每个  $2 \times 2$  子块来说,其直流系数要远大于其他系数,所以可以用其直流分量来产生水印。

(1) 把原始图像  $X$  分解为  $N$  个不重叠的  $2 \times 2$  子块并把像素低两位置零处理,  $X_i$  表示第  $i$  个块。

(2) 对每个  $2 \times 2$  子块进行 DCT 变换,  $D_i$  表示块  $X_i$  的 DCT 变换系数。

$$D_i = \text{DCT}(X_i) = \begin{bmatrix} D_{i1} & D_{i2} \\ D_{i3} & D_{i4} \end{bmatrix}, i = 1, 2, \dots, N. \quad (1)$$

(3) 每个子块  $X_i$  产生8位的特征信息  $F_i = \{f_{i1}, f_{i2}, f_{i3}, f_{i4}, f_{i5}, f_{i6}, f_{i7}, f_{i8}\}$ , 其中  $f_{i1} \sim f_{i6}$  为恢复数据,定义为  $f_{ij} = \lfloor \sqrt{D_{i1}}/2^{6-j} \rfloor \bmod 2$ ,  $f_{i7} \sim f_{i8}$  为认证数据,  $f_{i7}$  取  $f_{i1} \sim f_{i6}$  的异或操作,当  $f_{i7} = 0$  时,  $f_{i8} = 1$ , 否则,  $f_{i8} = 0$ 。

(4) 每个块的特征信息  $F_i$  可作为水印  $W_i$  嵌入到其他子块中。

### 1.2 块映射关系

为了尽可能地避免水印嵌入对图像特征信息的影响,从块  $X_i$  中提取的块特征并不是直接嵌入到自身块中,而是按照一定的块映射关系嵌入到其他块  $X_{i'} (i' = 1, 2, \dots, N, i' \neq i)$  中。通常,块  $X_i$  与  $X_{i'}$  之间的映射关系  $(i \rightarrow i')$  应该具有高度的随机性,否则,从多个含水印的图像可以完全确定其中的映射关系,其安全程度不高。何<sup>[5]</sup>提出一种伪随机序列的非线性方式取得了较好的效果。基于混沌序列对初始值和小扰动的敏感性,采用 Logistic 混沌序列的非线性方式来产生块映射关系,Logistic 序列的表达式为

$$s_{n+1} = \mu s_n (1 - s_n), s_n \in (0, 1), 0 \leq r \leq 4. \quad (2)$$

当满足  $r > 3.57$  时,序列  $\{s_n | n = 1, 2, \dots\}$  具有典型的混沌随机特征。对于每个图像块  $X_i$ ,通过以下步骤产生与其对应的图像块  $X_{i'}$ :

(1) 以初始密钥  $s_0, \mu$  和  $k_1$  产生 Logistic 混沌序列  $S = \{s_i | i = 1, 2, \dots, N + k_1\}$  和  $S' = \{s'_j | s'_j = s_{j+k_1}, j = 1, 2, \dots, N\}$ ;

(2) 对  $S'$  序列排序, 使其满足  $s'_{t_1} \leq s'_{t_2} \leq \dots \leq s'_{t_N}$ , 得到索引序列  $(t_1, t_2, \dots, t_N)$ ;

(3) 令  $i' = t_i$ , 得到图像块  $X_i$  与  $X_{i'}$  之间的嵌入映射关系, 即  $i' = t_i, X_{i'} = X_i$ 。

### 1.3 水印嵌入与提取

以图像块  $X_i$  产生的水印信息  $W_i$  修改块  $X_i$  像素的低两位, 修改方法为

$$x_{ij} = \lfloor x_{ij}/4 \rfloor + 2w_{ij} + w_{i(j+4)}, j=1, 2, 3, 4. \quad (3)$$

水印提取的过程为水印嵌入的逆过程。假设  $Y^*$  为待检测的含水印图像, 把检测图像  $Y^*$  分解为  $N$  个不重叠的  $2 \times 2$  子块并把像素低两位位置零处理, 得到图像块  $Y_i^* \{i \in [1, N]\}$ , 从图像块  $Y_i^*$  像素的低两位提取水印  $w_i^* = \{w_{ij}^* | j=1, 2, \dots, 8\}$ , 其中  $w_{ij}^*$  满足

$$w_{ij}^* = \begin{cases} \text{mod}(y_{ij}^*, 4), & j=1, 2, 3, 4; \\ \text{mod}(y_{i(j-4)}^*, 2), & j=5, 6, 7, 8. \end{cases} \quad (4)$$

## 2 篡改检测与恢复

### 2.1 篡改检测

自嵌入水印的认证方法, 通常是对提取的水印信息与重新获得的图像特征进行比较, 如不相符, 则确定为篡改, 具体算法描述如下:

对待检测图像的每个图像块  $Y_i^*$ , 重新计算特征信息  $F_i^*$ , 同时, 以相同的初始密钥  $s_0, \mu$  和  $k_1$  产生 Logistic 混沌序列及  $(Y_i^*, X_{i'})$  块嵌入映射关系, 并提取块  $Y_{i'}^*$  的水印  $W_{i'}^* = \{w_{ij}^* | j=1, 2, \dots, 8\}$ 。比较  $F_i^*$  和  $W_{i'}^*$ , 并定义检测标记  $P = \{p_i | i=1, 2, \dots, N\}$  为

$$p_i = \begin{cases} 0, & (f_{ij}^* = w_{ij}^*), j=1, 2, \dots, 8; \\ 1, & \text{其他}. \end{cases} \quad (5)$$

其中  $p_i = 1$  表示图像块  $Y_i^*$  被篡改;  $p_i = 0$  表示该块未遭到篡改, 为有效块。该算法可以检测篡改位置, 但理论分析表明, 其误检测率比较高。因为, 假设  $X_i$  的特征嵌入到块  $X_j$ ,  $X_j$  的特征嵌入到  $X_k$ , 若块  $X_j$  受到篡改, 则  $F_i^* \neq W_j^*$  和  $F_j^* \neq W_k^*$  可能会同时成立, 从而这 3 个块均会判为篡改。鉴于水印生成中的奇偶认证位, 可采用奇偶校验的方法进行篡改定位。

由图像块  $Y_i^*$  提取水印  $W_i^* = \{w_{ij}^* | j=1, 2, \dots, 8\}$ , 对高 6 位进行异或运算, 结果记为  $w_{i7}^{**}$ 。定义检测标记  $Q = \{q_i | i=1, 2, \dots, N\}$ ,  $q_i = 1$  表示图像块  $Y_i^*$  被篡改, 反之表示有效块。

$$q_i = \begin{cases} 0, & w_{i7}^* = w_{i7}^{**}, w_{i7}^* \neq w_{i8}^*; \\ 1, & \text{其他}. \end{cases} \quad (6)$$

该奇偶校验检测篡改方法类似于文献 [11] 中

的方法, 但文献 [11] 中的水印采取灰度值的均值生成并嵌入到像素的低 3 位, 虽能够获得较好的检测和恢复性能, 但却是以增大嵌入容量为代价, 同时, 对于仅图像内容变化而保持奇偶关系不变的篡改, 方法 [11] 会检测失败, 导致漏检率极高。为此, 定义了另一种篡改检测标志  $T = \{t_i | i=1, 2, \dots, N\}$  为

$$T = \begin{cases} Q, & r \leq \delta; \\ P, & r > \delta. \end{cases} \quad (7)$$

其中,  $r = \frac{\sum_i p_i}{\sum_i q_i}$ ,  $\delta$  为阈值。对于常规篡改有  $r < 1$ , 而对于仅图像内容的改变  $r \gg 1$ , 可通过合理设置阈值  $\delta$  来提高检测率。

为了提高篡改区域定位的精度, 采取了  $3 \times 3$  邻域法对篡改区域进行优化。对于每一个被标记为有效的图像块  $Y_i^*$ , 以  $Y_i^*$  为中心的  $3 \times 3$  邻域块, 若其  $3 \times 3$  邻域中被篡改的块数目大于 4, 则该块被标记为篡改, 否则视为有效。

### 2.2 篡改恢复

经过篡改区域的定位与优化, 图像块都已被标记, 对于被标记为篡改的图像块, 需要进行恢复。假设被标记为篡改的图像块为  $Y_i^*$ , 则根据映射矩阵生成方法, 采取相同的密钥  $s_0, \mu$  和  $k_1$ , 找到对应的嵌入块  $Y_{i'}^*$ 。

(1) 若图像  $Y_{i'}^*$  为有效块, 则提取图像块  $Y_{i'}^*$  中的水印  $W_{i'}^* = \{w_{ij}^* | i'=1, \dots, N, j=1, 2, \dots, 8\}$ , 计算直流系数  $d_{i1}^* = [\sum_{j=1}^6 W_{ij}^* \times 2^{6-j}]^2$ , 然后进行离散余弦逆变换  $D_{i1}^* = \text{IDCT} \begin{bmatrix} d_{i1}^* & 0 \\ 0 & 0 \end{bmatrix}$ , 以  $D_{i1}^*$  代替图像块  $Y_i^*$  的各像素值即可恢复被篡改的部分。

(2) 若图像块  $Y_{i'}^*$  已被标记为篡改, 则以图像块  $Y_i^*$  的  $3 \times 3$  邻域内其他块像素的均值来恢复被篡改的图像块。

(3) 对篡改区域, 用模板为  $3 \times 3$  的中值滤波方法, 去掉恢复区域中的一些离散点。

## 3 试验结果及分析

### 3.1 水印不可见性分析

试验中选取了多种不同类型的图像作为测试对象, 限于篇幅, 仅列出了标准图像 Lena 作为载体的实验结果。图 1 为载体图像及嵌入水印后的图像, 图 1(a) 为载体图像, 大小为  $512 \text{ bits} \times 512 \text{ bits} \times 8 \text{ bits}$ , 嵌入水印之后的图像如图 1(b) 所示。含水印图像的质量使用峰值信噪比 (peak signal to noise

ratio , PSNR) 度量 , 表 1 为含水印图像的 PSNR 值 , 分别列出了不同载体图像使用本文算法和文献 [11] 算法的对比结果。可见 , 该方案的 PSNR 平均可达到 44.2 dB , 高于文献 [11] , 具有较好的视觉质量。

根据相似度定义  $NC = \frac{\sum_{i,j} w^*(i,j) f^*(i,j)}{\sum_{i,j} w^{*2}(i,j)}$  , 计算

从图 1( b) 中提取的水印  $W^*$  和重新生成的特征  $F^*$  之间的相似度为 1 , 表明两者完全一致。



图 1 载体图像及含水印图像  
Fig.1 Cover image and watermarked image

3.2 算法安全性分析

本算法是一种自嵌入水印算法 , 产生的特征水

印和原始图像之间具有很强的相关性 , 在水印嵌入位置选择上 , 通过 Logistic 混沌映射确定生成水印块与嵌入水印块之间的映射关系 , 该非线性映射关系具有很强的随机性 , 并且对初值敏感 , 不知道初始密钥  $s_0$ 、 $\mu$  和  $k_1$  的非法者是无法确定水印嵌入块位置的 , 也就无法正确的提取水印 , 从而不能通过认证。

表 1 含水印图像的 PSNR  
Table 1 PSNR of watermarked images

载体图像	Lena	Sailboat	Cameraman	Pepper	Baboon	Girl
文献 [11]	40.66	40.69	40.70	40.72	40.73	40.72
本算法	44.14	44.16	44.26	44.28	44.31	44.06

3.3 篡改检测及恢复性能

(1) 常规篡改检测

当含水印图像遭受到不同程度的常规裁剪时 , 得到的定位效果如图 2 所示。图 2( a) ~ ( d) 为被篡改的图像 , 篡改比例分别为 3.56%、16.21%、38.32%、71.23% , 图 2( a<sub>1</sub>) ~ ( d<sub>1</sub>) 分别为对应的篡改定位结果 , 黑色区域表示图像没有受到篡改 , 而发生篡改的区域被标识为白色。图 2( a<sub>2</sub>) ~ ( d<sub>2</sub>) 为相应的恢复结果 , 恢复图像的 PSNR 分别为 38.42 , 33.13 , 23.41 , 9.54 dB。

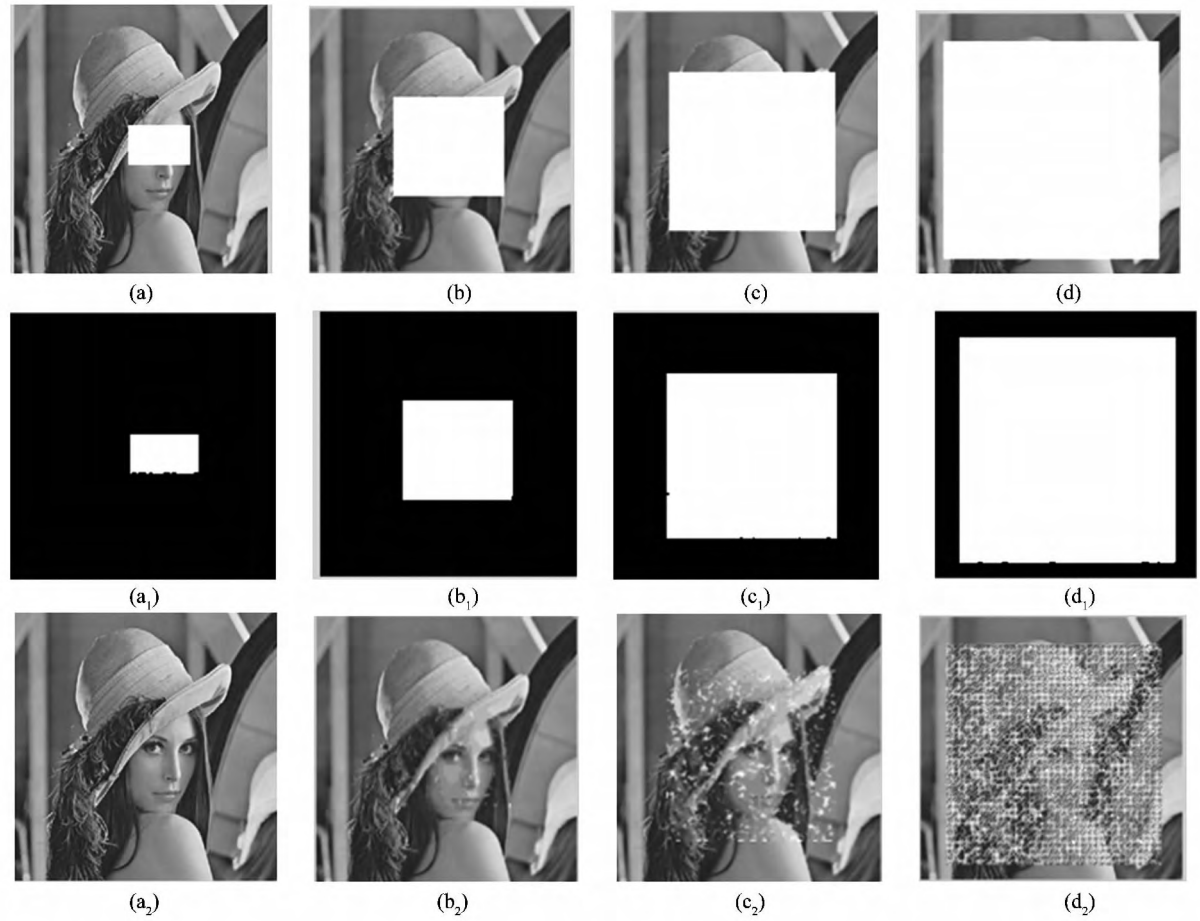


图 2 剪切篡改检测与恢复  
Fig.2 Tamper detection and recovery by cropping tamper

图3为拼贴篡改检测与恢复结果,其中(a)~(d)分别为受到不同程度拼贴篡改的图像,其篡改比例分别为6.96%、15.63%、25.78%和66.87%。相应的篡改定位结果如图3(a<sub>1</sub>)~(d<sub>1</sub>)

所示。可见,对于常规剪切和拼贴篡改,算法能够精确地定位出被篡改的区域。图3(a<sub>2</sub>)~(d<sub>2</sub>)为相应的恢复结果,恢复图像的PSNR分别为37.05, 33.34, 31.37, 14.14 dB。

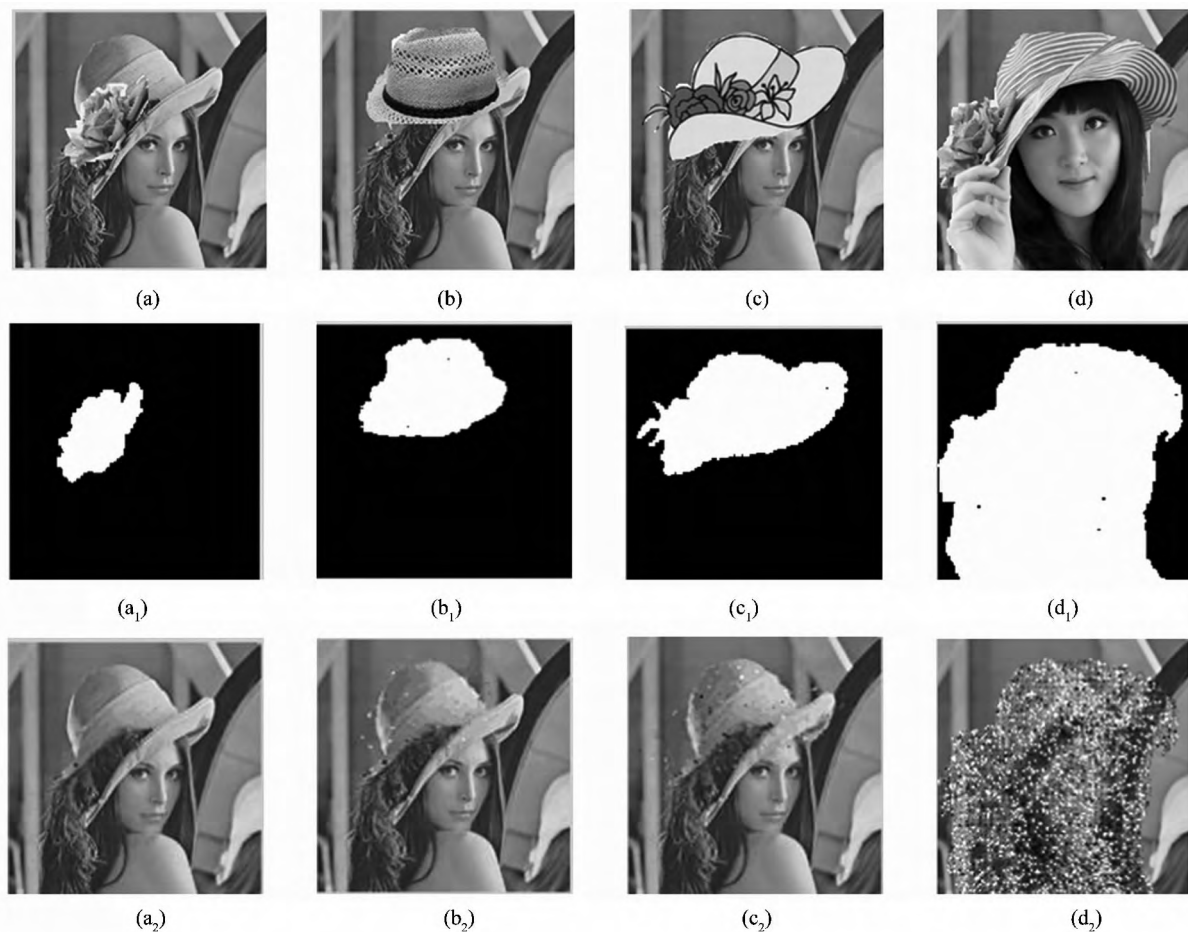


图3 拼贴篡改检测与恢复

Fig. 3 Tamper detection and recovery by collage attack

为了更好地描述算法针对篡改的检测能力,定义2个度量指标:漏警率(miss alarm probability, MAP)和虚警率(false alarm probability, FAP)。

$$\text{MAP: } p_{ma} = (1 - N_{td}/N_t) \times 100\% \quad (8)$$

$$\text{FAP: } p_{fa} = N_{fd}/(m \times n - N_t) \times 100\% \quad (9)$$

式中,  $N_t$  表示被篡改区域的像素总数,  $N_{td}$  表示篡改区域中能被算法正确定位的像素数,  $N_{fd}$  为未发生篡改而被算法标记为篡改的像素数。

图4给出了多幅图像在不同篡改比例下的平均漏警率和虚警率曲线,可见该检测方法的漏警率基本接近于0,而虚警率随着篡改范围的加大而增加,但即使篡改区域达到整幅图像的80%时,虚警率仍低于1%,可见,该算法的检测精度较高,可以较准确的定位被篡改的区域。图5为在不同篡改比例下恢复图像的峰值信噪比PSNR,通常只要PSNR > 30 dB,人的视觉就很难感到图像质量的变化。由图5

可知,在常规篡改下,当篡改比例低于30%时,恢复图像均能满足人眼视觉要求。

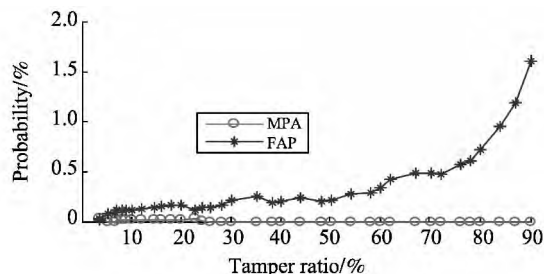


图4 漏警率和虚警率

Fig. 4 Values of MAP and FAP

## (2) 仅图像内容的攻击

仅图像内容的攻击由Chang等提出<sup>[12]</sup>。对图像的篡改可能是图像内容(高6位)的改变,也可能是低两位水印被篡改,或者是两者同时被篡改。其中对图像内容的篡改会破坏原始图像的使用价值,因此检测算法必须能检测出该类攻击并能定位篡改。

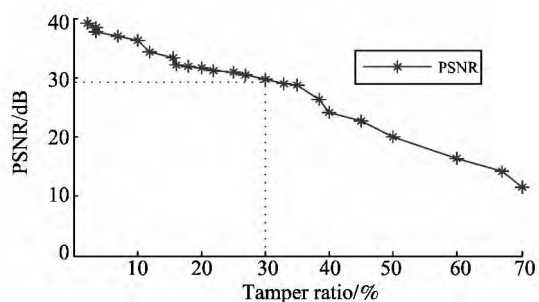


图5 恢复图像的 PSNR

Fig. 5 PSNR of restored images

图6给出了仅图像攻击篡改时的检测与恢复情况。图6(a)是把脸部区域像素增加80以提亮肤色,

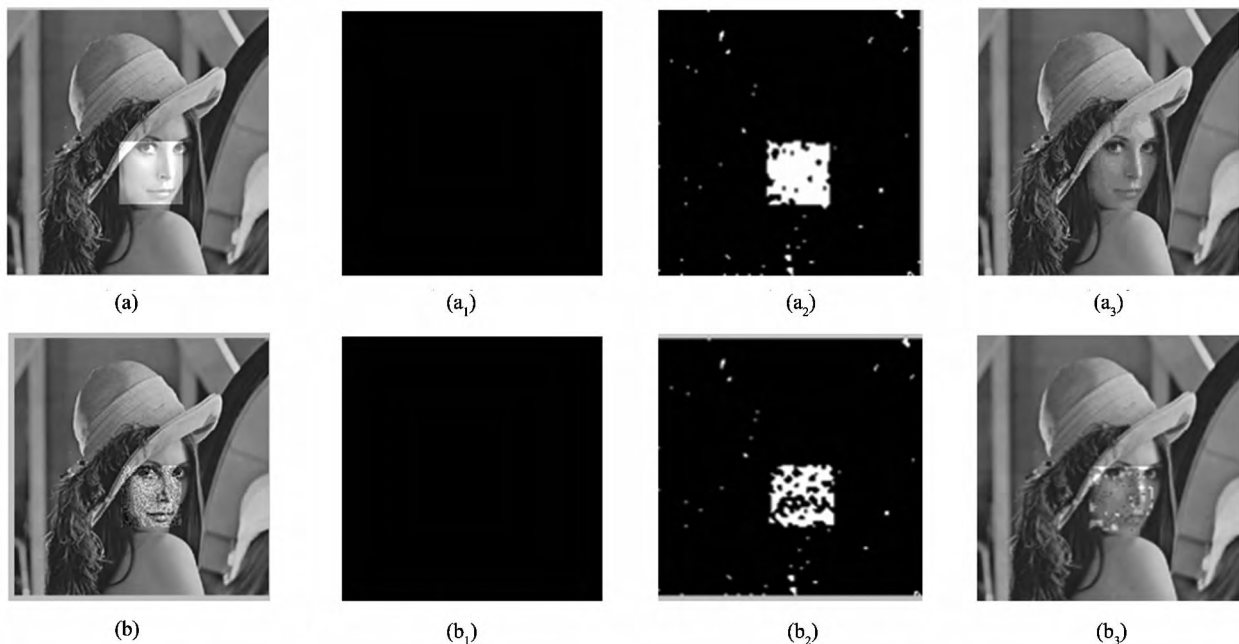


图6 仅内容篡改的检测与恢复

Fig. 6 Tamper detection and recovery by content-only attack

## 4 结论

设计并实现了一种新的脆弱水印算法。该算法通过分块的DCT直流系数来产生图像块特征作为水印,嵌入到其他图像块像素的低两位,嵌入水印信息量少,很好的保证了不可见性。并通过Logistic混沌序列来产生块嵌入的映射关系,既保证了安全性又提高了检测性能。在篡改定位部分,采取了奇偶检测和常规认证方式结合的方法。试验结果表明,在图像常规篡改达到80%时都能够实现较精确地定位,同时还能检测出仅图像内容的篡改;当常规篡改区域小于30%时,能够对篡改部分实现较精确地恢复。但是对于较大范围的仅图像内容篡改攻击,其篡改恢复还有待于进一步提高,将是下一步研究的方向。

图(b)是把脸部区域像素的二进制码的高7位和低3位交换,从视觉上两者都可以明显看出篡改,但都能够满足保持高6位的奇偶性不变。图6(a<sub>1</sub>)、(b<sub>1</sub>)分别为文献[11]的检测结果,可见Lee的方法对这种仅图像内容的篡改检测无效,图6(a<sub>2</sub>)、(b<sub>2</sub>)分别为本文算法检测结果,白色区域表示被篡改。图6(a<sub>3</sub>)和(b<sub>3</sub>)分别为恢复结果,虽存在一些错误检测块,但相对来说篡改的定位结果比较满意。大部分篡改区域都能够恢复出来。而文献[11]算法对于该类型的篡改不能够检测成功,也就无法实现篡改恢复。

## 参考文献:

- [1] Wong P W, Memon N. Secret and public key image watermarking schemes for image authentication and ownership verification [J]. IEEE Transactions on Image Processing, 2001, 10(10): 1593-1601.
- [2] Ghoshal Nabin, Mandal Jyotsna Kumar. A novel technique for image authentication in frequency domain using discrete Fourier transformation technique [J]. Malaysian Journal of Computer Science, 2008, 21(1): 24-32.
- [3] Chun-Shien Lu, Hong-yuan Mark Liao. Structural digital signature for image authentication: an incidental distortion resistant scheme [J]. Multimedia Security Workshop 8th ACM International Conference on Multimedia, 2003, 5(2): 161-173.
- [4] Sun Q, Shih-Fu Chang. A secure and robust digital signature scheme for JPEG 2000 image authentication [J]. IEEE Transactions on Multimedia, 2005, 7(3): 480-494.

- [5] He Hong-jie, Zhang Jiashu, Chen Fan. Adjacent-block based statistical detection method for self-embedding watermarking techniques [J]. Signal Processing, 2009, 89(8): 1557-1566.
- [6] Radharani S, Valarmathi M L. A study on watermarking schemes for image authentication [J]. International Journal of Computer Applications, 2010, 2(4): 24-30.
- [7] Qian Zhenxing, Feng Guorui, Zhang Xinping, et al. Image self-embedding with high-quality restoration capability [J]. Digital Signal Processing, 2011, 21(2): 278-286.
- [8] 金喜子, 姜文哲. 块级篡改定位的 JPEG 图像脆弱水印 [J]. 电子学报, 2010, 38(2): 1585-1589.  
JIN Xizi, JIANG Wenzhe. Fragile watermarking capable of locating tampered blocks in JPEG Images [J]. Acta Electronica Sinica, 2010, 38(2): 1585-1589.
- [9] 叶天语. 自嵌入完全盲检测顽健数字水印算法 [J]. 通信学报, 2012, 33(10): 8-15.  
YE Tianyu. Self-embedding robust digital watermarking algorithm with perfectly blind detection [J]. Journal on Communications, 2012, 33(10): 8-15.
- [10] Zhang Xinpeng, Wang Shuozhong. Fragile watermarking with error-free restoration capability [J]. IEEE Trans Multimedia, 2008, 10(8): 1490-1499.
- [11] Tien-You Lee, Shinfeng D Lin. Dual watermark for image tamper detection and recovery [J]. Pattern Recognition, 2008, 41(11): 3497-3506.
- [12] Chang Chin-chen, Fan Yi-hsuan, Tai Wer-liang. Four-scanning attack on hierarchical digital watermarking method for image tamper detection and recovery [J]. Pattern Recognition, 2008, 41(2): 654-661.
- [13] Luo Hao, Yu Fa-Xin. Blind image watermarking based on discrete fractional random transform and subsampling [J]. International Journal for Light and Electron Optics, 2011, 122(4): 311-316.

(编辑: 陈斌)

(上接第18页)

- [10] TAKAMURA Hiroya, INUI Takashi, OKUMURA Manabu. Extracting semantic orientation of words using spin model [C]//Proceedings of the Association for Computational Linguistics. Morristown: ACL Press, 2005: 133-140.
- [11] LIU Qun, LI Sujian. Word similarity computing based on howNet [C]//Proceedings of the 3th Chinese Lexical Semantic Workshop. Taipei: CLSW Press, 2002: 45-56.
- [12] 江敏, 肖诗斌, 王弘蔚, 等. 一种改进的基于《知网》的词语语义相似度计算 [J]. 中文信息学报, 2008, 22(5): 84-89.  
JIANG Min, XIAO Shibin, WANG Hongwei, et al. An improved word similarity computing method based on hownet [J]. Journal of Chinese Information Processing, 2008, 22(5): 84-89.
- [13] 朱嫣岚, 闵锦, 周雅倩, 等. 基于 HowNet 的词汇语义倾向计算 [J]. 中文信息学报, 2006, 20(1): 14-20.  
ZHU Yanlan, MIN Jin, ZHOU Yaqian, et al. Semantic orientation computing based on howNet [J]. Journal of Chinese Information Processing, 2006, 20(1): 14-20.
- [14] TURNEY Peter. Semantic orientation applied to unsupervised classification of reviews [C]//Proceedings of ACL. Morristown: ACL Press, 2002: 417-424.
- [15] 杨超, 冯时, 王大玲, 等. 基于情感扩展技术的网络舆情倾向性分析 [J]. 小型微型计算机系统, 2010, 04: 691-695.  
YANG Chao, FENG Shi, WANG Daling, et al. Analysis on Web public opinion orientation on extending sentiment lexicon [J]. Journal of Chinese Computer System, 2010, 04: 691-695.
- [16] KU Lunwei, LO Yongsheng, CHEN Hsinhsi. Using opinion scores of words for sentence-level opinion extraction [C]//Proceedings of the 6th NACSIS Test Collections for IR Workshop Meeting on Evaluation of Information Access Technologies. Tokyo: NTCIR Press, 2007: 316-322.
- [17] YANG Yiming, PEDERSEN Jan. A comparative study on feature selection in text categorization [C]//Proceeding of the 14th International Conference on Machine Learning. San Francisco: Morgan Kaufmann Press, 1997: 412-420.

(编辑: 陈燕)