元胞自动机变换可恢复图像认证算法

金 军[1]，舒红平[2]

(1. 四川大学计算机学院 成都 610065; 2. 成都信息工程学院计算机系 成都 610041)

【摘要】提出一种基于元胞自动机变换的可恢复图像认证算法，将图像分割成不重叠子块，对每个子块进行两层二维元胞自动机变换CAT，从第二层低频系数生成子块认证水印和恢复水印，分别嵌入当前子块和对应子块的第一层低频系数，形成含水印图像；用认证水印进行图像认证；用恢复水印恢复被篡改图像子块。实验表明，该算法安全性高，且具有很强的抗VQ攻击能力。

关 键 词 元胞自动机变换; 图像认证; 图像恢复; 安全; 篡改定位

中图分类号 TP309 **文献标识码** A doi:10.3969/j.issn.1001-0548.2009.06.028

Restorable Image Authentication with Cellular Automata Transform

JIN Jun[1] and SHU Hong-ping[2]

(1. College of Computer Science, Sichuan University Chengdu 610065;

2. Department of Computers, Chengdu University of Information Technology Chengdu 610041)

Abstract A restorable image authentication with cellular automata transform is proposed. The original image is splited into non-overlppin blocks and two layer cellular automata transform (CAT) is performed on each block. Authentication watermark and restoration watermark are produced from the second-layer low frequency coefficients and embedded into the first-layer low frequency coefficients of the current block and the corresponding block separately. Image authentication is played with the authentication watermark, and the tampered blocks can be restored with restoration watermark. Experiment results show that the scheme's security is strong and can resist vector quantization attack effectively.

Key words cellular automata transform; image authentication; image restoration; security; tamper location

基于脆弱性水印的图像认证技术已成为研究热点。目前已经有很多图像认证算法[1-3]，它们的共同特点是具有良好的篡改定位能力，并能容忍一些正常的图像处理操作，但这些算法的缺点是不能对篡改图像进行有效恢复。在一些实际应用场合，对于被篡改的图像内容仅仅进行检测和定位还不能满足要求，人们更希望能够近似恢复被篡改的内容，得到原来真实的信息。文献[4]提出了一种图像保护的自嵌入方法，将一幅图像的重要内容作为水印嵌入其自身之中，能够在检测篡改的同时近似地恢复被篡改的内容，但该算法为可逆算法，抵抗伪造攻击的能力不强。文献[5]提出将由图像块高 7 位的系数生成的水印嵌入到偏移子块的最低位，该算法在一定条件下可近似恢复原始图像，但恢复图像的质量和算法的安全性均不高。文献[6]通过分析系数的特性，重新进行码长分配来产生水印，使得篡改恢复的质量进一步提高，但该算法对篡改图像块的定位存在不确定性。文献[7]通过将子块的压缩编码与偏移子块的认证信息加密后作为水印嵌入到偏移子块的最低位以解决文献[6]的定位不确定性，但是图像块漏检的概率较高，且存在恢复可信性的问题。

本文借鉴空域的 LSB(least significant bit)算法，提出一种基于元胞自动机变换的可恢复图像认证算法，能检测并精确定位篡改位置，在发生篡改的情况下还能尽可能地恢复图像，并能抵抗针对子块内容认证的矢量量化(vector quantization，VQ)攻击[8]。因为利用了元胞自动机变换丰富复杂的性质，算法的安全性较高。

1 元胞自动机变换

元胞自动机(cellular automata，CA)[9]是一种时间、空间、状态均离散的动力学系统。元胞自动机变换(cellular automata transform，CAT)[10]能将已知的现象和元胞自动机演化联系起来。图像的二维

收稿日期：2008 – 06 – 17；修回日期：2009 – 01 – 23

基金项目：四川省青年科技基金(06ZQ026-054)

作者简介：金 军(1970 –)，女，博士生，主要从事数字图像处理和智能计算等方面的研究.

CAT变换表示如下：

$$c_{kl}=\frac{\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}f_{ij}A_{ijkl}}{N}\qquad i,j,k,l=0,1,\cdots,N-1\qquad(1)$$

式中　f_{ij}表示数字图像；A_{ijkl}表示二维基函数；c_{kl}表示变换系数；N表示元胞空间大小。

2　基函数

基函数的数量巨大，性质各异，CAT的目的就是根据问题需要，从中找到具有所期望性质的基函数并得到CAT变换系数。基函数是从CA的演化域产生的，所以要先建立CA模型，CA建模是根据其数学和动力学模型，通过一系列参数设置实现的，CA的典型建模参数如表1所示。

表1　CA建模参数

序　号	建模参数
1	局部规则
2	元胞状态集合
3	邻居元胞个数
4	元胞总数
5	初始构型
6	边界条件
7	元胞空间的形状
8	元胞空间的维度
9	变换类型
10	基函数类型

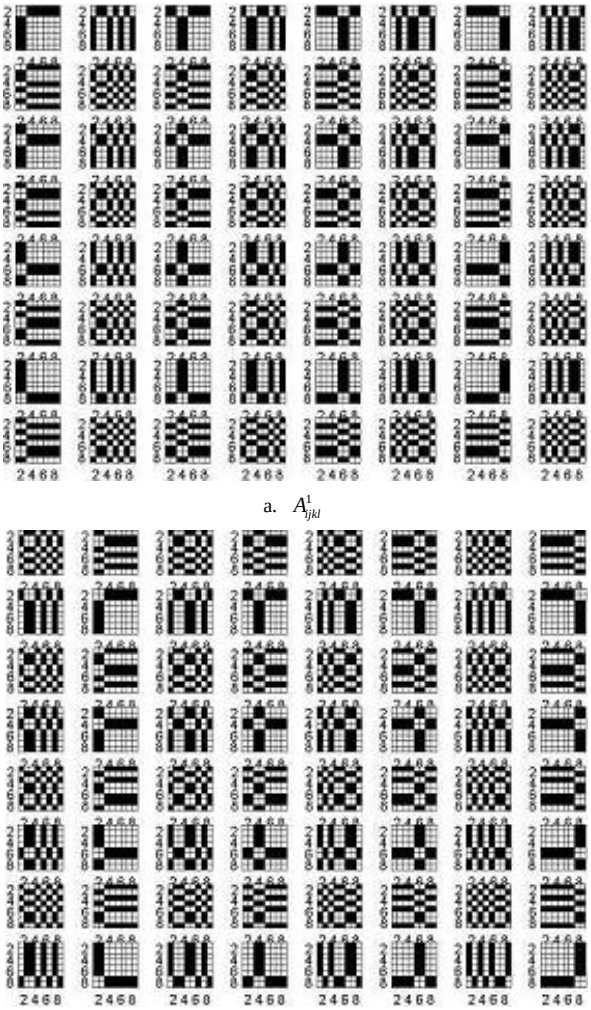
如果由二维CA演化产生二维基必须构造复杂的二维CA并进行复杂的运算。文献[10]提出了另一种比较简单的方法：先由结构简单的一维CA演化产生一维基，再由一维基的规范产品(canonical product)产生二维基，将所产生的二维基称为Type$_8$二维基：

$$A_{ijkl}=L_w\{(a_{ik}a_{ki}+a_{jl}a_{lj})\bmod L_w\}-(L_w-1)\qquad(2)$$

式中　a_{ik}是一维CA第i个元胞k时刻的状态；L_w是状态数。

目前，对CAT的讨论还处于初始阶段，相关的文献并不多，许多研究工作仍是尝试性的。通过对CA建模参数进行分析和简化，并结合Type$_8$二维基的生成方式，本文提出一个基密钥base_key=(一维基类型、局部规则、初始构型、边界条件)，输入基密钥后可以直接产生一个Type$_8$二维基。因为要对图像作二维正交CAT变换，需要一个二维正交基，所以选择Type$_2$一维正交基[10]，由其产生的Type$_8$二维基就是一个二维正交基。对基密钥进行不同设置可以产生不同性质的基函数，用其对图像进行CAT变换后，相同坐标位置的变换系数表示的图像特征或信息可能不同，这正反映了CAT丰富复杂的变换性质。

两个基密钥base_key$_1$=(Type$_2$,14,D4,cycle)和base_key$_2$=(Type$_2$,43,7E,cycle)分别产生的两个二维基A^1_{ijkl}和A^2_{ijkl}，如图1所示。



a.　A^1_{ijkl}

b.　A^2_{ijkl}

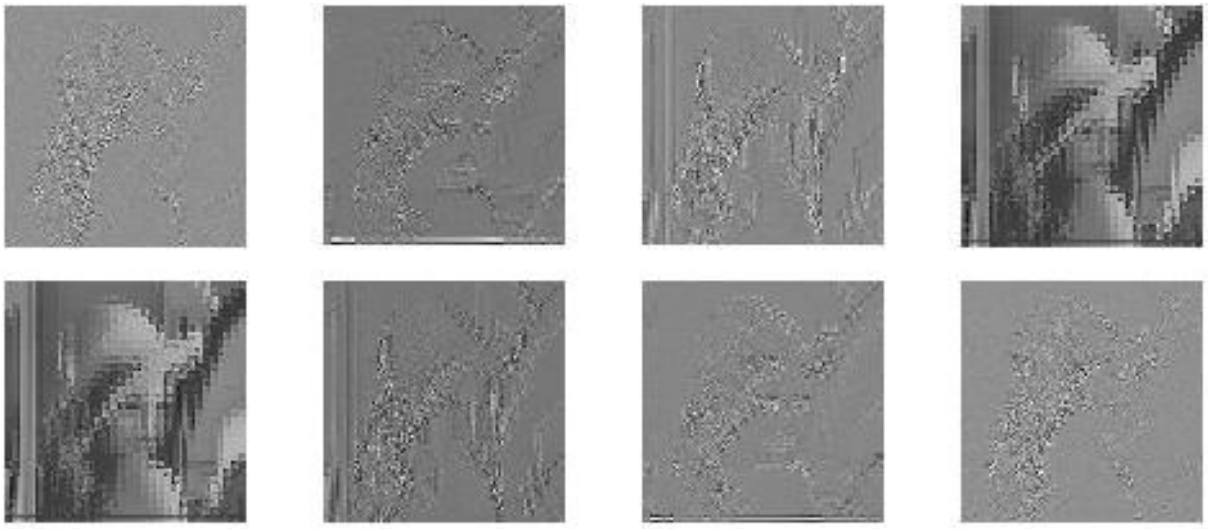
图1　不同基密钥产生的二维基函数

用A^1_{ijkl}和A^2_{ijkl}分别对一幅灰度图像进行二维CAT得到的各对应位置的变换系数c_{kl}如图2所示。

可以看出：(1) 使用A^1_{ijkl}得到的k和l都是奇数位置的c_{kl}，是图像的低频系数，其余位置的c_{kl}是图像高频系数。(2) 使用A^2_{ijkl}得到的k和l都是偶数位置的c_{kl}，是图像的低频系数，其余位置的c_{kl}是图像高频系数。可见，不同的基密钥可以产生不同性质的基函数，从而可能导致图像CAT变换系数的性质不确定。这种变换系数性质对基密钥的敏感性以及变换基的丰富多样性可以用来隐藏水印信息。对应的图像CAT及ICAT分别为：

$$c_{kl}=\left(\sum_{i=0}^{7}\sum_{j=0}^{7}f_{ij}A_{ijkl}\right)/8 \tag{3}$$

$$f_{ij}=\left(\sum_{k=0}^{7}\sum_{l=0}^{7}c_{kl}A_{ijkl}\right)/8 \tag{4}$$



a. k 和 l 都是偶数位置的 c_{kl} b. k 是偶数、l 是奇数位置的 c_{kl} c. k 是奇数、l 是偶数位置的 c_{kl} d. k 和 l 都奇是数位置的 c_{kl}

图 2 使用 A^1_{ijkl} 和 A^2_{ijkl} 进行 CAT 得到的 c_{kl}

3 多层CAT变换

图像CAT变换的低频系数构成的子图可以继续进行CAT变换，这就是图像的多层CAT分解。多层分解可持续到低频子图只含16个系数为止。对图像二维CAT变换系数进行分析，将灰度图像lena进行3层二维CAT分解后，将c_{kl}分别组成不同的系数子图，对各层c_{kl}按子图进行统计分析与能量分布分析。经过大量图像CAT实验发现：图像经多层CAT分解后，最高层低频系数集中了图像的大部分能量，反映了图像中最重要的内容特征。在水印算法中可以用数量较少但很重要的低频系数作为图像的恢复信息。图像二维CAT变换系数统计分析如表表2所示，其中c_{fij}表示各分解系数子图编号。

表2 图像二维CAT变换系数统计分析表

图号	最大值	最小值	均 值	方 差	能量比/(%)	层能量合计/(%)
c_{f34}	2 074.200 000 0	−180.970 000 0	782.178 800 0	370.660 000 0	96.830 000 0	
c_{f33}	532.720 000 0	−583.840 000 0	−2.953 700 0	113.690 000 0	1.670 000 0	99.550 000 0
c_{f32}	315.780 000 0	−285.090 000 0	8.124 400 0	75.873 000 0	0.750 000 0	
c_{f31}	194.780 000 0	−248.720 000 0	−0.614 100 0	47.425 000 0	0.290 000 0	
c_{f23}	252.190 000 0	−237.310 000 0	0.957 800 0	43.062 000 0	0.240 000 0	
c_{f22}	149.440 000 0	−187.690 000 0	−1.424 900 0	28.642 000 0	0.110 000 0	0.390 000 0
c_{f21}	129.310 000 0	−116.750 000 0	0.248 700 0	18.267 000 0	0.043 132 0	
c_{f13}	114.630 000 0	−131.380 000 0	−0.192 700 0	16.599 000 0	0.035 621 0	
c_{f12}	116.880 000 0	−105.380 000 0	0.628 800 0	13.193 000 0	0.022 550 0	0.064 533 0
c_{f11}	52.375 000 0	−6 800.000 000 0	−0.033 000 0	7.015 700 0	0.006 352 5	

4 水印算法

算法密钥key=(置乱密钥k_1、排序密钥k_2、选择密钥k_3和k_4、基密钥base_key)。

4.1 水印生成和嵌入过程

把图像O划分为M个不重叠的16×16的子块b_{k_m} (m=1,2,⋯,M)，按照从左到右、从上到下的顺序依次将各子块编号为(1,2,⋯,M)。用k_1对图像子块进行Arnold置乱后，当前子块b_{k_m} (m=1,2,⋯,M)与偏移子块$b_{k_{m'}}$ (m'=1,2,⋯,M)一一对应；根据base_key产生一个二维正交基A_{ijkl}，对每个子块b_{k_m}进行基函数为A_{ijkl}的两层二维CAT变换，得到变换系数，f_m^1和f_m^2分别

表示第一层和第二层低频系数。以块号为m的子块b_{k_m}作为当前子块，依次对M个子块进行如下的操作：

(1) 生成认证水印：计算f_m^2的均值 av=mean(f_m^2)；用k_2对f_m^2随机排序后，按照式(5)生成b_{k_m}的特征水印$w_m=\{w_j,1\leqslant j\leqslant 16\}$：

$$w_j=\begin{cases}0 & \text{if} \quad f_{mj}^2>\text{av}\\ 1 & \text{if} \quad f_{mj}^2\leqslant\text{av}\end{cases} \tag{5}$$

特征水印和子块号组合成子块认证水印$w_{d_m}=w_m+m$。

(2) 嵌入认证水印：f_m^1的前 16 个系数组成认证水印嵌入区 area1，以k_3作为 Logistic 映射的初始值，将生成的混沌序列转换成长度为 16 位长，[1,16]间的不重复排序序列 index_1，用 index_1对 area_1中的系数$f_{m'}^1$排序，并将认证水印w_{d_m}嵌入 area_1中每个$\left\lfloor\left|f_m^1\right|\right\rfloor$的 2 个 LSB。用嵌有水印的系数代替原系数后，与其他系数一起 ICAT，得到了含水印的当前子块$b_{k'_m}$。

(3) 嵌入恢复水印：对应偏移子块$b_{k_{m'}}$的$f_{m'}^1$中的后 48 个系数组成恢复水印嵌入区 area_2，以k_4作为 Logistic 映射的初始值，将生成的混沌序列转换成长度为 48 位长、[1,48]间的不重复排序序列 index_2，用 index_2对 area_2中的系数$f_{m'}^1$排序；对当前子块b_{k_m}的f_m^2进行量化得到$qf_m^2=\left\lfloor\left|f_m^2\right|/\Delta\right\rfloor$，将量化值表示成最长 7 位二进制编码$qf^2{}_m=b_7b_6b_5b_4b_3b_2b_1$，由于二进制编码中高位信息比低位信息重要，所以将$f_m^2$的符号位$s$和$qf_m^2$的 6 个最高有效位作为当前子块$b_{k_m}$的恢复水印$w_{h_m}=sb_7b_6b_5b_4b_3b_2$嵌入 area_2中，嵌入方法如图 3 所示。用嵌有水印的系数代替原系数后，与其他系数一起进行 ICAT，得到了含水印的偏移子块$b_{k_{m'}}$。

bit	…	7	6	5	4	3	2	1
$\left\lfloor\left\|f_{m'}^1(1)\right\|\right\rfloor$						s	b_7	b_4
$\left\lfloor\left\|f_{m'}^1(2)\right\|\right\rfloor$							b_6	b_3
$\left\lfloor\left\|f_{m'}^1(3)\right\|\right\rfloor$							b_5	b_2

图3　恢复水印的嵌入

重复步骤(1)～(3)，完成M个子块的水印生成和嵌入后得到含水印图像U。

4.2　水印认证过程

将含水印图像U分割成M个不重叠的16×16的子块$b_{k_{m'}}$ (m=1,2,…,M)，用k_1对图像子块进行Arnold置乱；用base_key产生二维正交基A_{ijkl}；对每个子块$b_{k_{m'}}$进行基函数为A_{ijkl}的两层二维CAT变换，得到变换系数，$f_m^{1'}$和$f_m^{2'}$分别表示第一层和第二层低频系数。以块号为n的子块$b_{k_{m'}}$作为当前子块，依次对各子块进行如下操作：

(1) 认证水印提取：按照水印生成和嵌入过程的步骤(1)，从当前子块$b_{k_{m'}}$的$f_m^{2'}$生成子块的特征水印w'_m；从$f_m^{1'}$的 area_1中提取子块认证水印w_{d_m}，从中取出w_m。

(2) 子块认证：定义一个篡改检测矩阵$\boldsymbol{D}_m$和一个篡改度T_m，$\boldsymbol{D}_m=w'_m\oplus w_m$定位子块被篡改的位置；$T_m=\dfrac{\boldsymbol{D}_m}{L}$反映子块被篡改的程度，其中$L$表示$\boldsymbol{D}_m$的长度。认证过程为：从提取的认证水印$w_{d_m}$中取出块号$m$，与当前子块$b_{k'_m}$的块号$n$进行比较，如果$m\neq n$，表示当前子块受到恶意篡改，将$\boldsymbol{D}_m$和$T_m$都置1；如果$m$=$n$，则从$w_{d_m}$中取出特征水印$w_m$，再与生成的特征水印$w'_m$进行比较，用$\boldsymbol{D}_m$和$T_m$检测当前子块$b_{k'_m}$的篡改位置和篡改度。

重复步骤(1)、(2)，完成M个子块的水印认证，得到M个$\boldsymbol{D}_m$和T_m(m=1,2,…,M)。

(3) 篡改度修正：本文算法借鉴空域的LSB算法在CAT变换域中实现。原始图像的CAT变换系数变化后重构的图像与原始图像会有一定的误差，反映在原始图像的特征水印与重构图像的特征水印有细小差异，经实验测定它们之间的差异很小(NC≥0.97，BER≤0.015)。认证时必须区分这种算法引起的轻微篡改和恶意篡改，因此，对$\boldsymbol{D}_m$和T_m进行如下修正：如果T_m<0.2，则不认为该子块受到恶意篡改，将$\boldsymbol{D}_m$和T_m都置0；否则认为该子块受到恶意篡改，不作处理。修正后得到最终的认证结果。

4.3　篡改图像的恢复

根据图像认证结果，对篡改内容进行恢复。以子块$b_{k_{m'}}$作为当前子块，依次对 M 个子块进行如下操作：

(1) 篡改度检测：检测$b_{k'_m}$的篡改度T_m，判断当前子块$b_{k_{m'}}$是否受到恶意篡改：如果T_m=0，表示$b_{k_{m'}}$未受到恶意篡改，不作处理；如果T_m>0，表示$b_{k_{m'}}$受到恶意篡改。再检测对应偏移子块$b_{k'_{m'}}$的篡改度$T_{m'}$：如果$T_{m'}$>0，表示$b_{k'_{m'}}$也遭到了恶意篡改，不能对当前子块进行恢复；如果$T_{m'}$=0，表示$b_{k'_{m'}}$没有受到恶意篡改，可以利用$b_{k'_{m'}}$中的恢复水印对当前子块$b_{k'_m}$进行恢复。

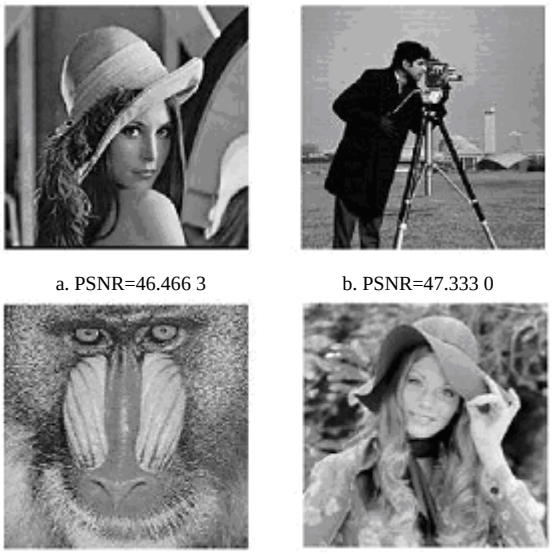
(2) 子块恢复：从偏移子块 $b_{k'_m}$ 的 area$_2$ 中提取当前子块 $b_{k'_m}$ 的恢复水印 w_{h_m}，进行反量化 $f_m^{2\prime} = w_{h_m} \times \Delta$，得到当前子块的近似低频系数 $f_m^{2\prime}$，ICAT 后得到恢复的当前图像子块。

重复步骤(1)、(2)，完成所有能够被恢复的篡改图像子块的恢复后，得到恢复的近似原始图像O'。

5 算法分析及实验结果

用 256×256 的灰度图像对本算法进行检测。

(1) 不可见性检测：图4是本算法生成的几幅含水印图像，它们的峰值信噪比，(PSNR)都大于40。实验结果表明，含水印图像与原始图像很接近，视觉上难于区分，说明本文算法的水印有很好的不可见性。



a. PSNR=46.466 3　b. PSNR=47.333 0

c. PSNR=47.111 5　d. PSNR=47.480 4

图4　含水印图像

(2) 篡改定位及恢复检测：对本算法生成的含水印图像进行几种恶意篡改，再进行篡改恢复，对各种篡改的定位用篡改检测矩阵表示，用PSNR表示恢复图像的视觉质量，实验结果如图5所示。当图像的某些部分被替换或改变，图像的低频分量会发生变化，这就使图像内容及其主要特征发生变化，从含水印图像提取和生成的特征水印将明显不一致，有利于对篡改的检测和定位。另外图像子块的块号是每个子块认证水印的一部分，可很好地抵抗VQ攻击。但是当图像被大面积裁剪时，由于有的子块及其偏移子块都同时被裁剪掉，因此会出现有子块无法被恢复的情况，即图5e中的灰色方块。实验结果表明，本文算法能够检测并精确定位恶意篡改，且恢复的图像能较好地反映图像的真实信息。

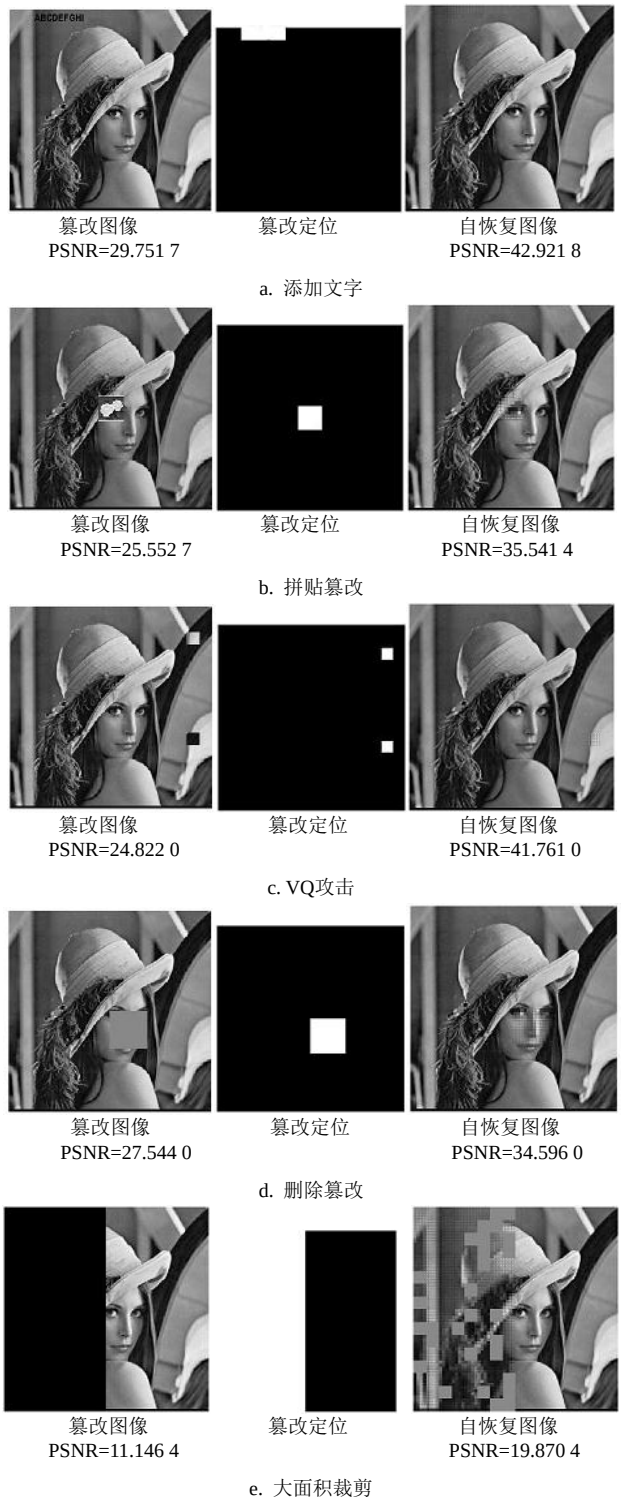


图5　部分篡改定位和自恢复检测实验结果

(3) 算法的安全性：本文算法比一般的空域LSB算法的安全性高，因为认证水印是嵌入在CAT系数中的，要移去水印，需要根据基密钥对图像进行CAT和ICAT，代价较高；基密钥的使用将CAT丰富复杂的性质引入算法中，算法的各个过程都需要密钥，在检测端各步骤的密钥时必须与嵌入端对应步骤的

(下转第1056页)