基于自适应图像块组合的无损图像认证算法

罗剑高[1]，韩国强[2]，沃焱[2]，李向阳[1]
(1. 广东农工商职业技术学院 计算机系，广东 广州 510507；2. 华南理工大学 计算机科学与工程学院，广东 广州 510006)

摘 要：现有基于分块的无损图像认证算法在图像认证块划分方面存在不足。为此，提出一种基于自适应分块组合的无损图像认证算法。算法中的认证块由基本分块根据原图像特征和水印图像保真度要求自适应组合而成，认证信息用数字签名技术产生，以无损水印方式嵌入，同时以多次嵌入方式实现图像编号的顽健传送，利用图像编号和认证块编号防止矢量量化攻击。理论分析与实验结果表明该算法篡改定位能力强于现有无损图像认证算法，且适应性强，能抗矢量量化攻击。

关键词：无损图像认证；可逆图像认证；无损图像水印；可逆图像水印；篡改定位；矢量量化攻击
中图分类号：TP391 **文献标识码**：A **文章编号**：1000-436X(2012)06-0064-09

Lossless image authentication algorithm based on adaptive combinations of image basic blocks

LUO Jian-gao[1], HAN Guo-qiang[2], WO Yan[2], LI Xiang-yang[1]
(1. Department of Computer, Guangdong AIB Polytechnic College, Guangzhou 510507, China;
2. School of Computer Science and Engineering, South China University of Technology, Guangzhou 510006, China.)

Abstract: As the existing block-wise lossless image authentication algorithms were inadequate in the division of image authentication blocks, a novel lossless image authentication algorithm based on adaptive combinations of image basic blocks was proposed. The image authentication block was composed of some basic image blocks by the source image characteristics and requirements of watermarking image fidelity, and the authentication code was generated by a digital signature algorithm and embedded into the authentication block via a lossless watermarking algorithm. Moreover, the robust transmission of the image ID was achieved via multi-embedding, and using the ID and authentication block ID the image authentication algorithm could prevent vector quantizationattack. Theoretical analyses and experimental results demonstrate that the algorithm not only improves the existing tamper localization accuracy but also has strong adaptability and can resist vector quantization attack.

Key words: lossless image authentication; reversible image authentication; lossless image watermarking; reversible image watermarking; tamper localization; vector quantization attack

---

收稿日期：2010-12-29；**修回日期**：2011-12-30
基金项目：国家自然科学基金资助项目(61070090, 61003270)；国家自然科学基金广东省联合基金资助项目(U1035004)；中央高校基本科研业务费重点基金资助项目(2012ZZ0066)；广东省重大科技专项基金资助项目(2010A080402005)
Foundation Items: The National Natural Science Foundation of China (61070090, 61003270); The National Natural Foundation of Science Guangdong Province (U1035004); Fundamental Research Funds for the Central Universities (2012ZZ0066); The Major Science and Technology Project of Guangdong Province (2010A080402005)

1　引言

现有基于数字水印具有篡改定位能力的图像认证算法[1~9]是以独立图像块为基础的，其主要思想是将原图像划分为互不重叠的块，然后对各块进行独立的认证水印生成与嵌入；认证时，逐一提取各图像块中的水印，并根据水印中所含认证信息对各块做是否被篡改的判断。需注意的是，在具体应用中，为防穷举攻击，该类算法中所取的认证水印、图像块尺寸不宜过小[1]。

在医学、军事、艺术品保存等要求高保真图像的应用中，为避免认证水印给原图像带来的噪声影响，上述图像认证技术要求采用无损水印[1]，以确保在图像通过认证后，能无损地恢复原图像。无损水印，也称可擦除水印或可逆水印，近来，因得到人们的广泛关注，出现了许多有效的算法[10~13]。

现有基于独立图像块的无损图像认证算法[5~9]，除文献[9]外，都是按大小一致的方式划分认证块。Celik 等[5]基于 64×64 图像块，采用层次结构的认证水印抗矢量量化攻击，相应的认证信息用数字签名算法（DSA）生成。Weng 等[6]基于 32×32 图像块，通过在原图像中引入定位模式，实现抗剪裁攻击。Yeo 等[7]基于 16×16 图像块，提出一种采用图像块 DCT 系数作为认证信息的认证算法，该算法中 DCT 系数除作为认证信息外，还可为篡改块的内容修复提供信息。Chen 等[8]基于 16×16 图像块，提出一种可执行 n 幅水印图交互修复被篡改块的认证算法，该算法不仅可检测并定位水印图的篡改，且能通过 n 幅水印图中完好的图像块修复对应的被篡改图像块。上述典型算法的认证信息都是以统一规格图像块为单位，采用无损水印方式嵌入的。在统一规格图像块中以无损水印方式嵌入相对定量的认证信息，如何合理确定认证块大小是一个十分关键的问题，遗憾的是，这些算法对此都没有进行分析讨论。针对无损图像认证算法中如何确定认证块大小的问题，罗等在文献[9]中进行了较系统的论述。罗等注意到，常规有损水印算法是通过与原图像相关数据进行替换达到水印嵌入目的，这种信息替换不可避免地丢失了原图像的一些信息，同时给原图像引入了噪声；为了不丢失原图像任何信息，无损水印算法[10~13]与常规有损水印算法不同，其水印嵌入是通过降低原图像编码冗余或像素间冗余来实现的，显然有效的无损水印量与原图冗余度高度相关，在平滑区，因数据冗余量较大，水印嵌入能力强，反之在纹理区，数据冗余量较小，水印嵌入能力较弱。基于这个事实，罗等[9]指出，在采用统一大小认证块的无损图像认证算法中，为保证每一认证块都能独立、完整地嵌入各自的认证信息，必然要求认证块大小由水印嵌入能力最弱的区域决定，而这不可避免地牺牲了其他水印强嵌入能力区域的篡改定位能力，且这种由嵌入能力最弱区域确定的认证块大小，不同特征的图像，通常也是不同的。

篡改定位能力通常是一个实用的无损图像认证算法最重要的性能参数。人们总是希望认证算法中所选的认证块尺寸尽可能小，以提高算法的篡改定位能力，然而，从现实世界获得的图像千差万别，不同图像区域的无损水印嵌入能力可能相差较大，因而要为一个无损图像认证算法确定一个合理的、规格统一的认证块尺寸是不太现实的。为此，罗等[9]提出一种认证块尺寸动态可调的无损图像认证算法(LIAA)。LIAA 首次提出认证块尺寸动态确定的思路，解决了之前认证块划分存在的主要缺陷，不足的是，LIAA 生成的认证块大小通常偏大，还有进一步缩小的空间，且 LIAA 在动态确定有效认证块过程中，数字签名等算法的处理次数一般较大，计算复杂度的控制有待于改进。

本文针对现有基于分块无损图像认证算法在图像认证块划分方面存在的不足，提出一种基于自适应分块组合的无损图像认证算法。该算法中自适应分块组合构成的认证块尺寸小于等于对应的 LIAA 动态认证块，且该算法在确定图像认证块的过程中，通过图像块无损水印量预估值的有效利用，较好地控制了数字签名等算法的处理次数，达到了提高认证算法计算效率的效果。

2　无损图像认证算法

与罗等[9]的 LIAA 类似，本文提出的基于自适应分块组合的无损图像认证算法（ALIAA）采用动态方式确定认证块，认证块划分基本思想是：首先选定一种适合小尺寸图像块的无损水印算法，由该无损水印算法和篡改定位精度要求等综合确定图像基本块（bb）的尺寸；把原图像 I 划分为 m 个（不足构成完整基本块的用 0 填充扩展）能够被识别的基本块 $(bb_i, 1 \leqslant i \leqslant m)$；$m$ 个 bb_i 根据某种规则自适应地生成 n 个图像认证块$(ab_j, 1 \leqslant j \leqslant n)$。在划分基本块和认证块的过程中要求满足以下基本条件。

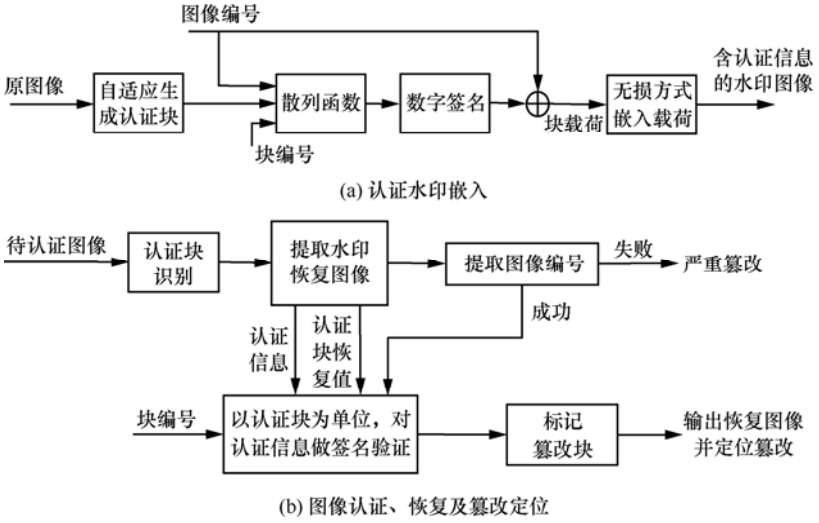


图1 ALIAA处理过程

1) $\bigcup_{i=1}^{m} bb_i = \bigcup_{j=1}^{n} ab_j = I,\ m \geqslant n$。

2) $bb_{i1} \cap bb_{i2} = \varnothing,\ ab_{j1} \cap ab_{j2} = \varnothing,$ if $i1 \neq i2,\ j1 \neq j2$。

3) $C_{vab_j} >= C_{pab_j}\quad ab_j \in \{ab_1, ab_2, \cdots, ab_n\}$。

其中，C_{vab_j}、C_{pab_j}分别表示认证块ab_j的有效水印容量和待嵌入的含认证信息的水印载荷量。

4) bb_i、ab_j在认证端能被正确地识别。

5) ab_j的平均面积尽可能小和紧凑度尽可能高。

6) 合理的计算复杂度。

文中ALIAA处理过程分为认证水印嵌入和图像认证、恢复2个阶段，主要步骤如图1所示。

在认证水印嵌入阶段，ALIAA最核心的内容为认证块的自适应生成，2.1节详细阐述了该过程；图1（a）中用于区分不同图像的图像编号用原图的摘要D表示，见2.3节；以D、认证块编号和认证块像素矩阵作为输入生成认证块水印载荷的内容，见2.3节；以认证块为单位嵌入水印载荷，形成含认证水印输出图的内容见2.2节。

在水印提取、图像认证和恢复阶段，有效地识别出候选认证块是ALIAA的关键环节，该部分内容见2.4节；图1（b）以候选认证块为单位提取水印，恢复图像的内容见2.2节；从候选认证块提取的水印中筛选出D及对候选认证块进行逐块签名验证的内容见2.5节。

2.1 认证块自适应生成及标记

文中采用一种利用图像二叉树表达的分裂合并递归算法自适应生成ab_j，该算法在保证生成的ab_j具有良好紧凑性的同时，易于ab_j标识的有效实现。

2.1.1 图像区域的分裂合并

ALIAA中图像区域的分裂合并指的是对bb_i矩阵（以bb_i为元素的矩阵）的分裂合并。

设原图I分辨率为$x \times y$，bb_i的分辨率为$u \times v$，首先用0值填充，把原图I扩展为$\hat{x} \times \hat{y}$：

$$\begin{cases} bx = \left\lceil \dfrac{x}{u} \right\rceil \\ by = \left\lceil \dfrac{y}{v} \right\rceil \\ \hat{x} = bx \times u \\ \hat{y} = by \times v \end{cases} \tag{1}$$

其中，⌈ ⌉为上取整符号。扩展后，待处理的图像I表示为$bx \times by$个$bb_i(1 \leqslant i \leqslant bx \times by)$组成的图像。

图2是bb_i矩阵分裂合并的一个示例。令$P(I_i)$代表图像区域I_i是否可执行分裂的逻辑谓词：

$$\begin{cases} P(I_i) = 0, & C_{eli} < 2 \times C_{pli} \\ P(I_i) = 1, & C_{eli} \geqslant 2 \times C_{pli} \end{cases} \tag{2}$$

其中，C_{eli}、C_{pli}分别表示区域I_i的有效水印量估计值（见2.2节）和待嵌入的水印载荷量（见2.3节）。文中分裂合并算法可递归地把I按式(3)分裂成越来越小的矩形子区域I_i，且始终使$P(I_i) = 1$，换句话说，如果$P(I_i) = 0$，结束分裂，继续后续步骤的操作。分裂与合并过程相伴，合并在认证水印嵌入可能失效(Cel_i<Cpl_i)或失效(见2.2节)时执行，且只合并那些相邻的子区域，如图2中子区域I_1与I_{21}的合并、I_{221}与I_{222}的合并。

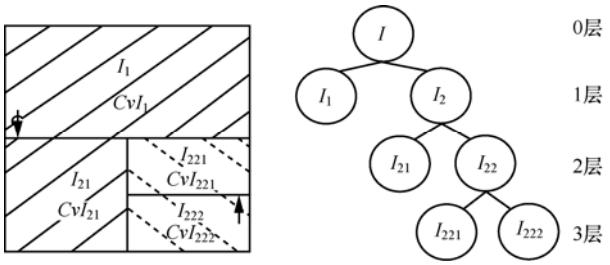


图 2　图像分裂合并的二叉树表示

$$\begin{cases} \begin{cases} I_1 = I\ (1:bx\times u, 1:\left\lfloor \dfrac{by}{2} \right\rfloor \times v) \\ I_2 = I\ (1:bx\times u, \left\lfloor \dfrac{by}{2} \right\rfloor \times v+1:by\times v) \end{cases}, bx<by、by>1 \\ \begin{cases} I_1 = I\ (1:\left\lfloor \dfrac{bx}{2} \right\rfloor \times u, 1:by\times v) \\ I_2 = I\ (\left\lfloor \dfrac{bx}{2} \right\rfloor \times u+1:bx\times u, 1:by\times v) \end{cases}, bx\geqslant by、bx>1 \end{cases} \tag{3}$$

2.1.2　图像基本块的链接与认证块生成

为了在认证端对 ab_j 逐一认证，必须建立有效的 ab_j 标记方式，确保在认证端能正确地提取各合法 ab_j。ALIAA 采用了一种可无歧义表达 ab_j 的 bb_i 链表结构来标记合法 ab_j。在 ALIAA 的 ab_j 表达中，每个 bb_i 用 4bit 表示 bb_i 序列的结构关系，其中，首比特用于标识是否是 ab_j 的首 bb_i，其他 3bit 表示后续 bb_i 的空间位置，如图 3 所示（000→右邻，001→右上邻，010→上邻，100→左邻，011→左 2 下邻，101→右下邻，110→下邻，111 表示没有后续 bb_i，即当前 bb_i 为 ab_j 的尾 bb_i）。

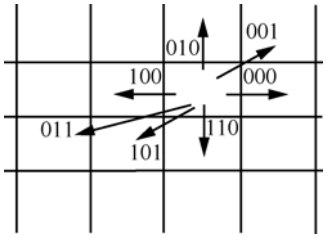


图 3　bb_i 间的空间链接关系表示

在描述认证块自适应生成算法之前，先逐一对 bb_i 组合的矩形结构($s\times t$)建立 5 种可能次序（左上→右上；左下→右下；左上→左下；右上→右下；左上→右下）、可用图 3 链接关系表示 bb_i 链表结构。

图 4 是以左上—右上次序对 bb_i 矩形结构建立链表的示意图，分 2 种情况说明。

1) bb_i 组合矩阵的列 t 为奇数：从左上 bb_i 开始，从上到下，从左到右扫描头 2 列，接着从左到右，交叉地从下到上、从上到下链接 bb_i，建立 bb_i 链表。

2) bb_i 组合矩阵的列 t 为偶数：从左上 bb_i 开始，按从左到右的次序，交叉地从上到下、从下到上地链接 bb_i ，建立 bb_i 链表。

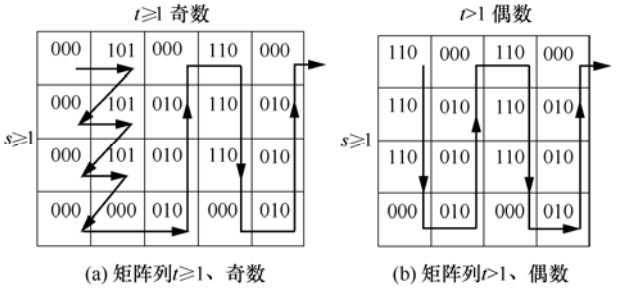


图 4　矩形区域左上—右上次序图像块链表

其他 4 种次序 bb_i 链表结构的建立过程与上述过程类似，限于篇幅，仅用图 5~8 示意其过程。

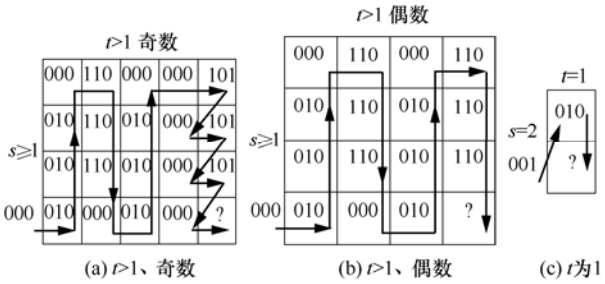


图 5　矩形区域左下—右下次序图像块链表

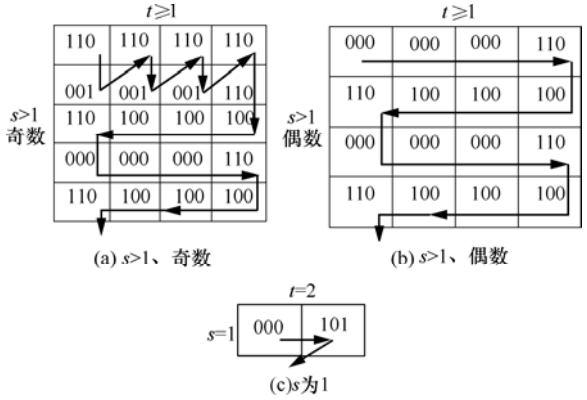


图 6　矩形区域左上—左下次序图像块链表

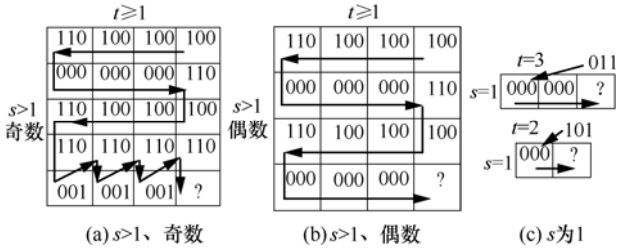


图 7　矩形区域右上—右下次序图像块链表

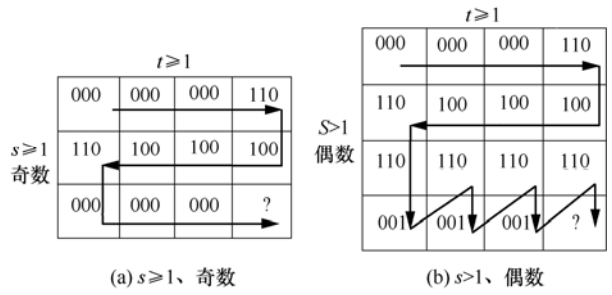


图 8　矩形区域左上—右下次序图像块链表

文中自适应生成 ab_j 的分裂合并（split-merge）递归算法描述如下：

过程 RV=SM（M, F_{lt}, E_{lt}, F_{sm},τ）

//输入参数 M 为待处理图的 bb_i 矩阵，F_{lt} 为链接在 M 左上角的 bb_i 链表，E_{lt} 为链接在 M 右下角的 bb_i 链表，F_{sm} 为是否执行分裂的标记，τ为水印图像保真门限。认证信息嵌入失败，返回值 RV 为 0，否则为 1。初始时，F_{lt}、E_{lt} 为空，F_{sm} 为 1。

if　F_{sm} ==0 或 M 的大小为1×1

按图 8 所示，建立 M 的链表结构 M_{lt}，合并 F_{lt}、M_{lt}、E_{lt}，令 L_t 为 F_{lt}+M_{lt}+E_{lt} 链表结构；

在 L_t 对应的图像区域上，执行认证块水印载荷生成及嵌入，见 2.2 节、2.3 节，把嵌入结果标记赋给 RV；

else

按式(3)，把 M 分裂成 M_1（上部分或左部分），M_2（下部分或右部分）；令 F_{lt}+M_1、M_2+E_{lt} 中 bb_i 的有效水印估计值（见 2.2 节）的和为 C_{e1}、C_{e2}，待嵌入的认证水印载荷量为 C_{p1}、C_{p2}；

if　CF(C_{e1}, C_{p1})==0

// CF(a, b)表示值 a、b 的比较函数，$a \geqslant b$ 时函数值为 1，反之为 0。

按图 4 或图 6 所示，建立 M_1 的链表结构 M_{l-1t}，合并 F_{lt}、M_{l-1t}，令 F_{lt}+M_{l-1t} 链表结构 L_{1-t} 为 M_2 的前链 $F_{2\text{-}lt}$，E_{lt} 为 M_2 的后链 $E_{2\text{-}lt}$；

//F_{lt}+M_1 中的 bb_i 组合构成的图像区域估计不能独立完成认证水印载荷的嵌入，故把 F_{lt}+M_1 记入到 F_{2-lt}，预备与 M_2 的 bb_i 结合构成认证块。

RV=SM（M_2, $F_{2\text{-}lt}$, $E_{2\text{-}lt}$, $P(M'_2)$,τ）；

// M'_2 为 $F_{2\text{-}lt}$, M_2, $E_{2\text{-}lt}$ 中 bb_i 链构成的图像。

elseif　CF(C_{e1}, C_{p1})==1 且 CF(C_{e2}, C_{p2})==0

按图 5 或图 7 所示，建立 M_2 的链表结构 M_{2-1t}，合并 M_{2-1t}、E_{lt}，令 M_{2-1t}+E_{lt} 链表结构 L_{2-t} 为 M_1 的后链 E_{1-lt}，F_{lt} 为 M_1 的前链 F_{1-lt}；

RV=SM（M_1, F_{1-lt}, E_{1-lt}, $P(M'_1)$,τ）；

// M'_1 为 $F_{1\text{-}lt}$, M_1, $E_{1\text{-}lt}$ 中 bb_i 链构成的图像。

else

令 F_{1-lt}=F_{lt}; E_{1-lt}=[]; F_{2-lt}=[]; E_{2-lt}=E_{lt};

RV_1=0; RV_2=0;

if　CF(C_{e1}, C_{e2})==0

RV_1=SM（M_1, F_{1-lt}, E_{1-lt}, $P(M'_1)$,τ）；

if　RV_1==1

RV_2=SM（M_2, F_{2-lt}, E_{2-lt}, $P(M'_2)$,τ）；

end

else

RV_2=SM（M_2, F_{2-lt}, E_{2-lt}, $P(M'_2)$,τ）；

if　RV_2==1

RV_1=SM（M_1, F_{1-lt}, E_{1-lt}, $P(M'_1)$,τ）；

end

end

if　RV_1==1 且 RV_2==1

RV=1;

elseif　RV_1==1 且 RV_2==0

按图 5 或图 7 所示，建立 M_2 的链表结构 M_{2-1t}，合并 M_{2-1t}、E_{lt}，令 M_{2-1t}+ E_{lt} 链表结构 L_{2-t} 为 M_1 的后链 E_{1-lt}，F_{lt} 为 M_1 的前链 F_{1-lt}；

RV=SM（M_1, F_{1-lt}, E_{1-lt}, $P(M'_1)$,τ）；

elseif　RV_1==0

按图 4 或图 6 所示，建立 M_1 的链表结构 M_{l-1t}，合并 F_{lt}、M_{l-1t}，令 F_{lt}+M_{l-1t} 链表结构 L_{1-t} 为 M_2 的前链 F_{2-lt}，E_{lt} 为 M_2 的后链 E_{2-lt}；

RV=SM（M_2, F_{2-lt}, E_{2-lt}, $P(M'_2)$,τ）；

end

end

end

为了简化计算，上述算法忽略 bb_i 有效水印估计量（见 2.2 节）与图像块认证水印实际嵌入量之差对 ALIAA 的性能影响。

2.1.3　认证块的标记

2.1.2 节生成的认证块是由一组两两相邻的 bb_i 组成，且由 bb_i 间的空间链接关系形成的 bb_i 链表结构可建立认证块的无歧义表达。文中认证块标记利用了这种链接关系，并借助链接符与 LSB 的交换实现了合法认证块在认证端的盲提取。认证块的标记过程为：把 4bit 的结构关系表示符保存在相应 bb_i 头 4 像素最低有效位(LSB)上，原 LSB 值作为待嵌水印载荷的一部分，用于通过认证后的图像恢复。

2.2　无损水印嵌入与提取

文中认证块的水印载荷嵌入与提取所采用的无损水印算法可以根据具体要求进行选取或设计，需注意的是，认证块尺寸一般较小，因此所采用的无损水印算法应适用于小尺寸图像。

文中采用文献[13]的无损水印算法，该算法中灰度溢出的解决方法无需无损压缩计算，较适用于小尺度图像块。无损水印嵌入过程用水印图像保真门限τ控制，在水印图像 PSNR 不小于τ的条件下，要求尽可能接近τ。

原图的有效无损水印量估计以 bb_i 为单位，用随机产生的比特作为待嵌入值，对给定门限τ，通过逐步尝试，确定文献[13]无损水印算法中满足门限τ的嵌入参数 T（出于控制辅助信息的考虑，把 T 的范围设为[0,15]，用 4bit 表示，令 E_{tbi} 为满足τ条件的 T）和此时的嵌入比特量 E_{wbi}。

认证信息的嵌入以认证块为单位。各认证块待嵌入的水印载荷参见 2.3 节。对给定门限τ，以认证块中的 E_{tbi} 均值作为初始 T，依次在各 bb_i 执行无损水印算法，通过逐步尝试不同的 T，直至满足门限τ的要求。水印嵌入参数 T 记录在认证块的首 bb_i 第 5~8 像素 LSB 中，各 bb_i 链接比特记录在各 bb_i 头 4 像素 LSB 中。认证块嵌入过程中待嵌入量不足时，用随机比特填充。

如果认证块认证信息嵌入失败（即无法在认证块中完整嵌入认证信息，或完整嵌入后，水印图峰值信噪比小于保真门限τ），认证信息嵌入结果标记值返回为 0，否则为 1。

无损水印的提取同样以认证块为单位，待处理认证块的识别参见 2.4 节。首先从认证块首 bb_i 的第 5~8 像素 LSB 上提取参数 T，以 bb_i 为单位执行水印提取并依次合并水印，然后从结果水印中截取对应的比特恢复 bb_i 头 4 像素 LSB 和首 bb_i 第 5~8 像素 LSB。如果水印提取过程出现错误，则返回出错标记，否则输出水印提取结果和图像恢复结果。

2.3　认证信息及认证块水印载荷生成

与 LIAA 类似，ALIAA 也需要解决矢量量化攻击的安全问题。现有基于分块相关[3]和基于层次结构[4]的抗矢量量化攻击方法要求图像认证块结构固定，不适用于 ALIAA。ALIAA 采用基于块编号和图像编号的方法[2,9]，其中，对图像编号 D 生成、存储与传送等问题进行如下处理：

$$D = H_{\mathrm{MD5}}(I) \tag{4}$$

其中：I 为原图像；H_{MD5} 为 MD5 散列函数；D 为 128bit 的散列值。由式（4）生成的图像编号 D 可实现图像编号的唯一性。为实现盲认证，ALIAA 把 D 作为水印载荷的一部分嵌入图像，并采用在各认证块中重复嵌入的方式来保证 D 传送的顽健性，D 在认证端的获取过程参见 2.5 节。

ALIAA 以认证块为单位生成水印载荷 W_p，W_p 由认证信息 S、认证块特定像素 LSB 和 D 合并形成：

$$W_p = S + L + D \tag{5}$$

其中，“+”表示比特串接合并，S 用式（6）生成：

$$S = S_{\mathrm{DSA}}(H_{\mathrm{SHA}}(\psi, \mathrm{D}, x, y), k) \tag{6}$$

式中：S 表示长为 320bit 的签名串；S_{DSA} 为 DSA 数字签名函数[14]；H_{SHA} 为 SHA 散列函数；ψ 为 2.1.2 节中 bb_i 链表 L_t 对应的认证块像素矩阵；(x,y) 为认证块首 bb_i 的左上角像素坐标（作为区别认证块的块编号，用于克服同一图像中不同认证块之间的替换攻击）；k 为数字签名的私钥。

L 由认证块首 bb_i 第 5~8 像素原 LSB（水印图像中，用表示水印嵌入参数 T 的比特替换）和各 bb_i 头 4 像素原 LSB（水印图像中，用认证块结构标识的比特替换，参见 2.1 节）串接形成。

令 W_p 的比特长度为 C_p，C_p 可表示为

$$C_p = 320 + 4 + 4\delta + 128 \tag{7}$$

其中，δ 表示 bb_i 组合中 bb_i 的数量。

2.4　认证端对合法认证块的识别

从水印图像起始位置开始，有效认证块的识别过程如下。

1) 扫描当前 bb_i 头 4 像素 LSB（记为 L_1、L_2、L_3、L_4），若 L_1 为 1，建立以当前 bb_i 为首块的一候选认证块，转 3）；否则，转 2)。

2) 判断当前 bb_i 是不是 bb_e，若不是，依左到右、从上到下的次序转到下一 bb_i，执行 1)；若是，结束本过程。

3) 若 $L_2L_3L_4$ 为 111，当前 bb_i 为候选认证块尾块，组装从候选认证块首块至尾块所有遍历的 bb_i，形成完整的候选认证块链，转 5)；否则，根据 $L_2L_3L_4$ 转到下一 bb_i，执行 4)。

4) 查看当前 bb_i 的 L_1，若为 1，该候选认证块识别失败，返回到该候选认证块首块，执行 2)，否则，进一步确认当前 bb_i 在当前候选认证块中是否已出现，如已出现，返回到该候选认证块首块，执

行 2)，否则转到 3)。

5) 合法认证块的结构具有与认证块生成算法相对应的某些特点（限于篇幅，不予讨论），检查候选认证块是否具有这些特点，如没有，表明该候选认证块无效，返回到该候选认证块首块，执行 2)；否则，做进一步的分析，先执行 2.2 节无损水印提取和像素恢复，该过程如出错，返回到该候选认证块首块，执行 2)，否则，把该候选认证块的结构及提取的图像编号、认证信息、图像恢复结果保存在候选认证块数组中，然后返回到该候选认证块首块，执行 2)。

2.5 认证信息签名验证

对候选认证块数组中各候选认证块执行的认证信息签名验证与 LIAA 类似。

1) 从候选认证块数组中的图像编号字段，选取出现频率最大的值作为有效图像编号 D，如果该值出现频率低于 50%，则给出已发生严重篡改的提示，结束认证，否则，执行 2)。

2) 从头到尾依次扫描候选认证块数组，如果当前候选认证块的图像编号字段的值不等于 D，标记该认证块被篡改；否则，执行式（8）的 DSA 签名验证，并标记验证的结果：

$$V_{\mathrm{DSA}}(H_{\mathrm{SHA}}(\hat{\psi},D,x,y),S',k')\in\{0,1\} \tag{8}$$

式中：V_{DSA} 为 DSA 签名的验证算法；S' 表示从当前候选认证块中提取的认证信息；$\hat{\psi}$ 为当前候选认证块 bb_i 链表对应的认证块像素恢复矩阵；k' 为 DSA 签名算法的公钥，其他符号同式（6）。

3) 输出含篡改块标记的恢复图像。

3 算法性能分析

与 LIAA 类似，ALIAA 因有效结合了数字签名、数字水印技术，具有安全性高、盲认证、篡改定位能力能较好地按需自动调整、易于扩展等优点。相比 LIAA，ALIAA 在篡改定位能力、计算效率方面取得了较大改进。

3.1 篡改定位能力

用图像二叉树表示 ab_j，2.1.2 节算法 SM 算法产生的 ab_j 可能是叶子节点，也可能是某节点和其兄弟节点或兄弟节点的若干子孙节点合并而成的组合区域。LIAA[9]中 ab_j 除了叶子节点外，组合区域只能是互为兄弟的 2 个节点合并而成。如图 2 所示，当 I_1 需与相邻区域合并时，LIAA 只能和 I_2 合并，而 ALIAA 可以根据情况与 I_2 或仅和 I_2 的子孙节点 I_{21} 合并，显然，这有助于 ALIAA 获得比 LIAA 更小区域的认证块。

3.2 计算效率

在确定有效认证块时，ALIAA 利用预先计算的有效水印估计量对候选区域做初步判定，初步判定有效后，才进行散列、签名等密码计算，并进一步作候选认证块的有效性确认。通常情况下，初步判定有效的候选区域大概率地为有效认证块，即这些区域只需进行一次认证信息的产生、嵌入操作，相比 LIAA 在确定有效认证块过程中，多次重复计算散列、签名等密码计算，计算效率有较大的提高。

4 实验及结果分析

为验证了 ALIAA 的有效性，本文在 MATLAB 平台上实现了 ALIAA 算法，并用 ALIAA 对 USC-SIPI 图像数据库[15]中各种不同性质的图像进行了多组实验，实验结果及分析如下。

文中将无损图像认证算法的篡改定位精度定义为

$$\Gamma=\sqrt{\frac{\hat{x}\times\hat{y}}{\lambda}} \tag{9}$$

式中：$\hat{x}\times\hat{y}$ 为原图像 I 的分辨率；λ 为认证块总数。

ALIAA 的篡改定位精度与所选择的无损水印算法有较大关系，现有算法中适用于小图像区域的不多，这主要是在小图像区域条件下，现有无损水印算法嵌入过程中辅助信息占总嵌入水印量的比例较大，导致有效水印量较明显下降。本文所选无损水印算法虽相对有效，但还有需改进的地方，这是下一步待研究的内容。图 9 是 ALIAA 选用 3 种不同大小基本块的实验结果对比，总体来看，16×16 下的结果最好，这主要是因为，8×8 下虽然组合元素的颗粒小了，但该尺寸下有效水印嵌入性能下降了；32×32 下主要的问题是组合元素的颗粒较大。

由图 9 的 Γ-τ 曲线可看出，ALIAA 的篡改定位精度 Γ 能根据 τ 的变化进行动态调整。ALIAA 认证块选取的有效性体现在：一方面，由于单个认证块的水印载荷只有几百比特，现实中有意义的图像 I 采用 ALIAA 中的无损水印算法时，不会出现在 $\hat{x}\times\hat{y}$ 范围内因找不到足够大小的有效认证块实现认证信息的完整嵌入而导致 ALIAA 失效的问题；另一

方面，在保证足以完整嵌入认证信息的前提下，ALIAA 会尽可能在$[u\times v,\ \hat{x}\times\hat{y}]$内自适应地获取较合适大小的认证块。

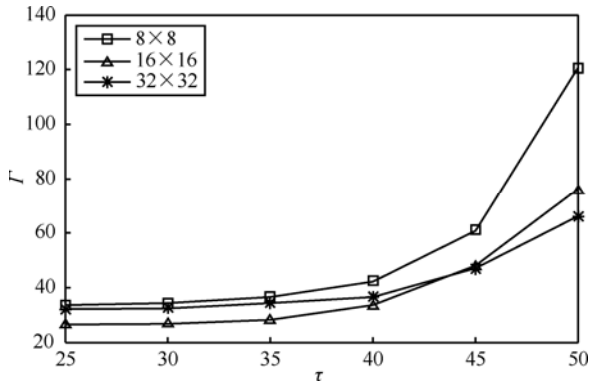


图 9　ALAA 基于不同大小基本块的 Plane 篡改定位精度-保真门限曲线

接下来，取16×16的基本块，比较 ALIAA 与 LIAA 中各自认证块动态划分算法的性能，为了便于比较，除了认证块划分算法，LIAA 其他部分选用 ALIAA 的内容，本文称这种改造算法为 LIAA*，ALIAA 和 LIAA*作用在典型测试图上的实验结果对比见图 10。结果显示，ALIAA 的认证块划分算法优于 LIAA 中的认证块划分算法。

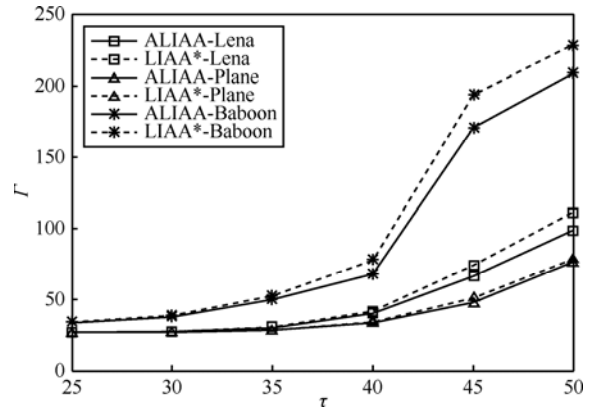
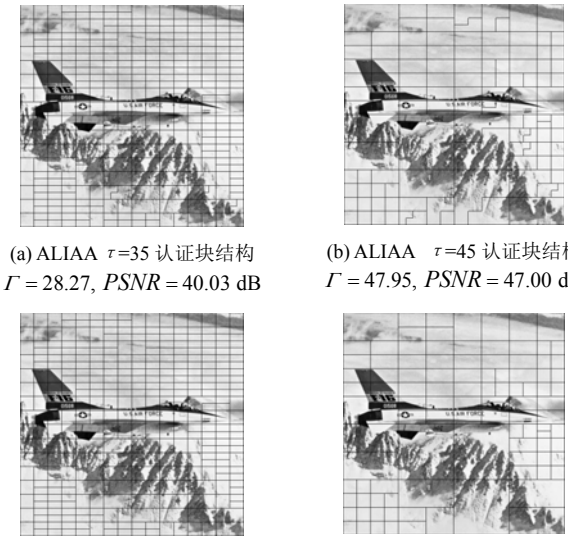


图 10　ALAA 与 LIAA*作用在典型测试图上的篡改定位精度-保真度门限曲线对比

图 11 给出了在不同τ下使用 ALIAA 和 LIAA* 处理 Plane 时的认证块结构，其中，PSNR 表示嵌入认证信息后全图 I 的峰值信噪比，Γ为式（10）定义的篡改定位精度。图 11 显示，ALIAA 和 LIAA* 都能根据图像的局部特征和τ动态地调整定位精度。通过图中结果比较不难看出，ALIAA 中由自适应分块组合构成的认证块尺寸小于等于对应的 LIAA* 动态认证块。



(a) ALIAA τ=35 认证块结构 Γ = 28.27, $PSNR$ = 40.03 dB

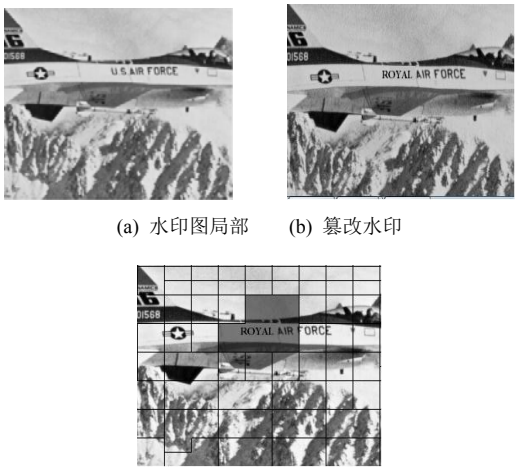
(b) ALIAA τ=45 认证块结构 Γ = 47.95, $PSNR$ = 47.00 dB

(c) LIAA* τ=35 认证块结构 Γ = 28.49, $PSNR$ = 40.24 dB

(d) LIAA* τ=45 认证块结构 Γ = 50.95, $PSNR$ = 47.45 dB

图 11　ALAA 与 LIAA *的篡改定位精度实验结果

ALIAA 的篡改检测、定位的一个实例见图 12。图 12(a)是水印图 Plane 的一个局部，使用 ALIAA 对篡改图 12(b)进行认证，认证结果不仅检测出被篡改，而且能准确地定位出篡改所在的认证块区域，如图 12(c)所示(阴影部分表示被篡改的定位区域，图中分格线实际输出时可去除)。



(a) 水印图局部　(b) 篡改水印

(c) 认证输出

图 12　ALIAA 的篡改检测、定位实例

5　结束语

本文提出一种基于自适应分块组合的无损图像认证算法 ALIAA。一方面，ALIAA 由自适应分块组合构成的认证块尺寸小于等于对应的 LIAA 动态认证块，使现有基于分块无损图像认证算法的篡

改定位能力得到较稳定提高；另一方面，ALIAA 在确定图像认证块的过程中，通过图像块无损水印量预估值的有效利用，较好地控制了数字签名等算法的处理次数，降低了认证算法的计算复杂度。与 LIAA 类似，ALIAA 采用图像编号、认证块编号来区分不同图像、不同图像区域，可防止矢量量化攻击。理论分析和实验结果表明，ALIAA 安全性高、适应性强，计算复杂度可控，篡改定位能力强于现有同类的无损图像认证算法。

参考文献：

[1] COX I J, MILLER M L, BLOOM J A, *et al*. Digital Watermarking and Steganography[M]. Burlington: Morgan Kauffman, 2008. 375-422.

[2] 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.

[3] 张鸿宾,杨成. 基于公钥和脆弱水印的图像认证算法[J]. 计算机科学,2004,31(11):218-221.
ZHANG H B, YANG C. An image authentication scheme based on public key and fragile watermar king[J]. Computer Science, 2004, 31(11): 218-221.

[4] CELIK M U, SHARMA G, SABER E, *et al*. Hierarchical watermarking for secure image authentication with localization[J].IEEE Transactions on Image Processing,2002,11(6):585-595.

[5] CELIK M U, SHARMA G, TEKALP A M. Lossless watermar- king for image authentication: a new framework and an implementation[J]. IEEE Transactions on Image Processing, 2006, 15(4):1042-1049.

[6] WENG S W, ZHAO Y, PAN J S. Reversible watermarking resistant to cropping attack[J]. IET Information Security,2007,1(2):91-95.

[7] YEO D G, LEE H Y. Block-based image authentication algorithm using reversible watermarking[A]. Computer Science and Convergence, CSA 2011 and WCC 2011 Proceedings[C]. Jeju, Korea, 2012. 703-711

[8] CHEN Y S, WANG R Z. Reversible authentication and cross-recovery of images using (*t*,*n*)-threshold and modified-RCM watermarking[J]. Optics Communications, 2011, 284(12):2711-2719

[9] 罗剑高, 韩国强, 沃焱等. 篡改定位精度可动态调整的无损图像认证算法[J]. 华南理工大学学报（自然科学版）,2011,39(7):121-126.
LUO J G, HAN G Q, WO Y, *et al*. Lossless image authentication algorithm with dynamic adjustable tamper localization accuracy[J]. Journal of South China University of Technology (Natural Science Edition), 2011, 39(7):121-126.

[10] TIAN J. Reversible data embedding using a difference expansion[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8): 890-896.

[11] THODI D M, RODRIGUEZ J J. Expansion embedding techniques for reversible watermarking[J]. IEEE Transactions on Image Processing, 2007,16(3):721-730.

[12] TAI W L, YEH C M, CHANG C C. Reversible data hiding based on histogram modification of pixel differences[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2009,19(6): 906-910.

[13] LEE C F, CHEN H L, TSO H K. Embedding capacity raising in reversible data hiding based on prediction of difference expansion[J]. Journal of Systems and Software, 2010,83(10):1864-1872.

[14] KAHATE A. 密码学与网络安全[M].北京:清华大学出版社,2005.
KAHATE A. Cryptography and Network Security[M]. Beijing: Tsinghua University Press, 2005.

[15] Signal and Image Processing Institute, University Southern California, Los Angeles. Image database[EB/OL]. http://sipi.usc.edu/database/.

作者简介：

罗剑高（1971-），男，江西金溪人，博士，广东农工商职业技术学院副教授，主要研究方向为图像处理、数字水印、信息安全等。

韩国强（1962-），男，江西临川人，博士，华南理工大学教授、博士生导师，主要研究方向为图像处理、多媒体技术等。

沃焱（1975-），女，云南昆明人，博士，华南理工大学副教授，主要研究方向为图像处理、数字水印、信息安全等。

李向阳（1966-），男，湖南湘潭人，博士，广东农工商职业技术学院副教授，主要研究方向为图像处理、数字水印、信息安全等。