DOI:10.7544/issn1000-1239.2014.20130440
51(11):2505-2512, 2014

一种变容量的自嵌入图像易碎水印算法

巩道福[1,2]　刘粉林[1,2]　罗向阳[1,2,3]
[1](解放军信息工程大学　郑州　450001)
[2](数学工程与先进计算国家重点实验室(解放军信息工程大学)　郑州　450001)
[3](信息安全国家重点实验室(中国科学院信息工程研究所)　北京　100093)
(gongdf@aliyun.com)

A Variable-Payload Self-Embedding Fragile Watermarking Algorithm for Image

Gong Daofu[1,2], Liu Fenlin[1,2], and Luo Xiangyang[1,2,3]
[1](*PLA Information Engineering University*, *Zhengzhou* 450001)
[2](*State Key Laboratory of Mathematical Engineering and Advanced Computing* (*The PLA Information Engineering University*), *Zhengzhou* 450001)
[3](*State Key Laboratory of Information Security* (*Institute of Information Engineering*, *Chinese Academy of Sciences*), *Beijing* 100093)

Abstract The existing fragile watermarking algorithms based on blocks can't drastically avoid the independence between the blocks. A novel variable-payload self-embedding fragile watermarking algorithm is proposed. Firstly, the original image is divided into blocks with the size of 2×2 and the average value of each block is calculated. Then a new image called average-image can be composed of the obtained average values. The watermark is not generated for every signal block, but encoded statistically according to the correlation between the pixels of average-image. The watermark is embedded into 2-LSB (least significant bit) of the original image. As a result, the length of the watermark is variable due to the correlation of the image. That is to say, for a texture complex image the watermark is longer, but for a smooth image the watermark is shorter. And moreover, the independence of the blocks can be broken, so it has a better ability to resist attacks. As the authentication, string matching is used to match the blocks and the watermark. For the blocks which are not matched, group matching is used to re-match. The theoretic analysis and the simulation results show that the proposed algorithm can not only thwart the collage attack and locate tampered blocks accurately, but also has better non-visibility.

Key words variable-payload; self-embedding; fragile watermarking; tamper detection; recovery

摘　要 为了减小图像自嵌入水印的长度,降低水印对载体图像质量的影响,同时为消除基于分块的图像认证算法中图像块之间的独立性,提出了一种变容量的自嵌入易碎水印算法:首先对图像进行2×2的分块,根据各分块灰度均值生成原始图像的均值图像;根据均值图像各像素之间的相关性进行游程编码;将编码信息作为水印嵌入在图像像素的最低两位中;篡改检测时首先使用字符串匹配的思想进行图像块和水印之间的匹配,对于未匹配成功的块,使用分组的方式进行再次匹配,以完成认证和恢复.

收稿日期:2013-03-29;**修回日期**:2013-09-30
基金项目:国家自然科学基金项目(61401512,61272489,61379151,61302159);河南省科技攻关计划基金项目(122102210516);郑州市领军人才计划基金项目(10LJRC182);中国博士后基金项目(2012T50842,201104911838)

该算法进行一次的水印嵌入,同时用于篡改检测与恢复,水印长度依赖于均值图像相邻像素之间的相关性,可有效缩短水印长度,减小对载体图像质量的影响.理论分析和实验仿真表明,算法在不可见性、篡改定位和恢复、抗拼贴攻击、漏检率等方面具有较好的效果.

关键词 变容量;自嵌入;易碎水印;篡改检测;恢复图像

中图法分类号 TP391

数字图像作为获取及传播信息的主要载体,给人们的生活带来极大的便利,但其易被编辑、修改的特点也带来一系列的安全隐患.如何能够对数字图像进行真实性鉴别、篡改区域定位和原始信息恢复,进而达到还原事实真相的目的,已成为信息安全领域的重要研究内容.

根据识别篡改的能力和容忍图像被修改的程度,基于数字水印的图像认证技术可分为精确认证和模糊认证2类.前者主要基于易碎水印技术,能够检测出改变图像数据或破坏图像完整性的操作,能够定位图像被篡改的区域;后者主要基于半易碎水印技术,在保证图像内容真实的条件下,允许对图像进行一般的处理操作(如压缩或格式转换等).自嵌入水印是将图像自身信息编码为水印信息的技术,是基于数字水印的图像认证技术的重要研究内容.

1 相关工作

在自嵌入的图像认证技术方面,基于分块的方法是其中的一个研究热点.该类方法对图像进行分块,根据每个分块分别生成认证水印及恢复水印,可将篡改定位到每个分块,并可以通过控制分块的大小平衡篡改定位精度和算法安全性之间的关系.

文献[1]提出一种基于分块的多级易碎水印算法,该算法首先对原始图像进行4×4的分块,并选取每个分块的偏移子块,然后再对每个分块进行2×2的分块,并分别计算认证水印和恢复水印,嵌入在其所在4×4分块的偏移子块中.然而文献[2-3]指出,该方法由于偏移值密钥空间较小,存在偏移值被估算出的安全隐患,并分别给出了伪造攻击方法.文献[4]基于混沌映射选择偏移子块,提出一种能够区分水印或内容被篡改的脆弱水印算法,首先对图像进行8×8的分块,并通过混沌映射确定每个子块所对应的偏移子块,然后由子块的主要离散余弦变换(discrete cosine transform, DCT)系数生成恢复水印并嵌入在偏移子块的次低位,最后将认证水印嵌入在子块的最低位,该方法能够区分水印或图像内容被篡改,并在一定条件下能够对被篡改区域进行恢复.文献[5]提出一种基于Slant变换的可恢复脆弱水印算法,该算法基于独立分块技术将用于认证的水印嵌入到每个块的Slant变换域的中频区域,并将图像压缩后的数据作为恢复水印嵌入在像素的最低位,该方法的篡改定位和恢复的精度均为8×8的图像块.文献[6]提出一种基于分块的可恢复的脆弱水印算法,该算法首先对图像进行2×2的分块,并对每个分块的高6位进行奇异值分解,并使用文献[4]的方法对分块进行混沌置乱,将恢复水印嵌入在图像块的次低位,将认证水印嵌入在图像块的最低位,该方法篡改定位和恢复的精度均为2×2的图像块.文献[7]提出一种基于中国剩余定理的自嵌入水印算法,首先对每个8×8分块的图像进行DCT变换,并对DCT系数进行量化生成恢复水印信息,嵌入在偏移子块的低位中,认证时通过比较重构的图像块和压缩的图像块之间的均值误差,判定图像块的篡改情况,但是该算法的认证和恢复精度为8×8的图像块,且误判率较高.但这些算法分别对每个分块生成认证和恢复水印.而文献[8]将图像块的内容信息进行5 b的量化后作为水印,同时用于篡改检测和恢复,因此降低了水印的长度,认证时通过比较图像块8邻域的特征和水印的匹配情况进行篡改检测.该文作者又分别在文献[9]和文献[10]中对该方法进行了改进,其中文献[8]提出一种变容量的自嵌入水印算法,使得对较平滑的图像生成的水印信息有明显减小,其实验中给出每个像素平均嵌入的信息量在1.8~2.62 b之间;文献[10]对算法判定篡改进行了多种优化,提高了算法的性能.

上述算法仍然是对每个图像的分块独立生成水印,因而使得水印信息的长度较长,且分块之间的独立性并没有得到根本的改变.为了减小水印信息的长度,并消除图像分块间的独立性,本文提出一种变容量的自嵌入水印算法.首先将图像进行2×2分块,并计算每个分块高6位的均值,作为图像的均值

图像;根据均值图像相邻像素之间的相关性进行游程编码,并作为水印信息嵌入在原始图像的低位;认证时通过比较水印信息与待检测图像的均值图像之间的对应关系判断图像块的真实性;该算法只进行一次的水印嵌入,同时完成对图像的篡改检测和恢复.理论分析以及与文献[9-10]的比较表明,本文算法极大地缩短了水印信息的长度.此外,本文对算法的虚检概率和漏检概率进行了较详细的分析,通过实验验证了分析的正确性.通过与文献[7]的对比,本文算法具有更好的篡改定位精度和恢复质量.

2 算法描述

2.1 水印生成

设原始图像 $\boldsymbol{X}$ 的大小为 $M\times N$,将其无重叠地分割为大小为 2×2 的图像块,并按行优先顺序排列,则图像 $\boldsymbol{X}$ 可表示为

$$\boldsymbol{X}=(\boldsymbol{B}_1,\boldsymbol{B}_2,\cdots,\boldsymbol{B}_i,\cdots,\boldsymbol{B}_r), \tag{1}$$

其中,$\boldsymbol{B}_i=\begin{pmatrix} b_{i1} & b_{i2} \\ b_{i3} & b_{i4} \end{pmatrix}$ 为 2×2 的图像块,$r=M\times N/4$ 为图像块的总个数.

令 $B_i^{\text{avg}}=\left\lfloor \dfrac{b_{i1}+b_{i2}+b_{i3}+b_{i4}}{4}\Big/4 \right\rfloor$ 表示图像块 $\boldsymbol{B}_i$ 的灰度均值高 6 位信息.对所有的 $\boldsymbol{B}_i$ 求 B_i^{avg},则可得到图像 $\boldsymbol{X}$ 在 2×2 分块下的均值图像 $\boldsymbol{X}^{\text{avg}}$,表示为

$$\boldsymbol{X}^{\text{avg}}=(B_1^{\text{avg}},B_2^{\text{avg}},\cdots,B_i^{\text{avg}},\cdots,B_r^{\text{avg}}). \tag{2}$$

在自然图像中,$\boldsymbol{X}^{\text{avg}}$ 中各相邻元素之间存在较大的相关性,即存在大量相邻元素的值相等的情况.因此,本文通过对 $\boldsymbol{X}^{\text{avg}}$ 的各元素进行游程编码生成水印.所构建的水印如式(3)所示:

$$\boldsymbol{W}=(\boldsymbol{V},\boldsymbol{N}), \tag{3}$$

其中,$\boldsymbol{V}=(v_1,v_2,\cdots,v_k)$,$\boldsymbol{N}=(n_1,n_2,\cdots,n_k)$,$v_i$ 为 $\boldsymbol{X}^{\text{avg}}$ 中元素的值,n_i 为值等于 v_i 的相邻元素的个数,则 $n_i\in\{1,2,\cdots,r\}$,且 $\sum_{x=1}^{k} n_x = r$.

2.2 水印嵌入

水印嵌入前,为了提高算法的安全性,首先对图像 $\boldsymbol{X}$ 进行像素级置乱,将生成的水印信息以替换的方式嵌入在置乱后图像的最低两位中,然后进行逆置乱,得到含水印图像.具体的嵌入过程如下:

Step1. 使用文献[4]的混沌置乱方法,在密钥 K_1 的控制下对原始图像 $\boldsymbol{X}$ 进行像素级置乱,得到置乱后的图像 $\boldsymbol{X}^{\text{P}}$.

Step2. 以替换的方式将水印信息 $\boldsymbol{W}$ 平均地嵌入在图像 $\boldsymbol{X}^{\text{P}}$ 的次低位和最低位.

Step3. 对嵌入水印后的图像 $\boldsymbol{X}^{\text{P}}$ 进行逆置乱,得到含水印的图像 $\boldsymbol{X}^{\text{W}}$.

2.3 篡改检测与恢复

由水印的生成可知,其中 $\boldsymbol{N}=(n_1,n_2,\cdots,n_k)$ 表示 $\boldsymbol{X}^{\text{avg}}$ 的结构信息,其将 $\boldsymbol{X}^{\text{avg}}$ 的各像素分成 k 组 $(G_1,G_2,\cdots,G_k)$;$\boldsymbol{V}=(v_1,v_2,\cdots,v_k)$ 表示各组元素所对应的值,即分组 G_i 中共包含 n_i 个元素,其值均等于 v_i.因此,对含水印图像的恶意篡改将引起分组中这种对应关系的改变,本算法将利用这种严格的对应关系对图像进行篡改检测和恢复.设 $\hat{\boldsymbol{X}}$ 为可能遭受到篡改的含水印图像,具体的认证及恢复步骤如下:

Step1. 对图像 $\hat{\boldsymbol{X}}$ 进行 2×2 的分块,并计算 $\hat{\boldsymbol{X}}$ 的均值图像:

$$\hat{\boldsymbol{X}}^{\text{avg}}=(\hat{B}_1^{\text{avg}},\hat{B}_2^{\text{avg}},\cdots,\hat{B}_i^{\text{avg}},\cdots,\hat{B}_r^{\text{avg}}). \tag{4}$$

Step2. 按照 2.1 节中的水印生成方法,生成图像 $\hat{\boldsymbol{X}}$ 的参考水印:

$$\hat{\boldsymbol{W}}=(\hat{\boldsymbol{V}},\hat{\boldsymbol{N}})=((\hat{v}_1,\hat{v}_2,\cdots,\hat{v}_{\hat{k}}),(\hat{n}_1,\hat{n}_2,\cdots,\hat{n}_{\hat{k}})), \tag{5}$$

可知 $\sum_{x=1}^{\hat{k}} \hat{n}_x = r$.

Step3. 由密钥 K_1 对图像 $\hat{\boldsymbol{X}}$ 进行置乱,得到置乱后的图像 $\hat{\boldsymbol{X}}^{\text{P}}$.

Step4. 从 $\hat{\boldsymbol{X}}^{\text{P}}$ 的最低两位平面中提取所嵌入的水印信息:

$$\boldsymbol{W}'=(\boldsymbol{V}',\boldsymbol{N}')=((v'_1,v'_2,\cdots,v'_{k'}),(n'_1,n'_2,\cdots,n'_{k'})). \tag{6}$$

Step5. 利用字符串最大子串匹配的方式,将 $\hat{\boldsymbol{N}}$ 与 $\boldsymbol{N}'$ 进行匹配,令 $M(\hat{n}_i,n'_j)$ 表示字符 $\hat{n}_i$ 与 n'_j 匹配成功.

Step6. 对于匹配成功的元素 $M(\hat{n}_i,n'_j)$,若 $\hat{v}_i=v'_j$,则表明 $\hat{n}_i$ 对应的图像块均没有被修改,通过认证;否则若 $\hat{v}_i\neq v'_j$,表明 $\hat{n}_i$ 对应图像块的像素值被篡改.

Step7. 对于 $\hat{\boldsymbol{N}}$ 与 $\boldsymbol{N}'$ 中未匹配成功的元素,设子串 $(\hat{n}_{i+1},\hat{n}_{i+2},\cdots,\hat{n}_o)$ 与 $(n'_{j+1},n'_{j+2},\cdots,n'_p)$ 未匹配

成功,且存在 $M(\hat{n}_i,n'_j)$ 和 $M(\hat{n}_{o+1},n'_{p+1})(o>i,p>j)$,则可根据命题 1 判断是否因水印$(n'_{j+1},n'_{j+2},\cdots,n'_p)$被篡改而引起匹配不成功;若水印$(n'_{j+1},n'_{j+2},\cdots,n'_p)$未被篡改,则根据$(n'_{j+1},n'_{j+2},\cdots,n'_p)$对 $\hat{\boldsymbol{X}}^{\text{avg}}$ 所对应的元素进行分组,共可得到 $p-j$ 组:$(G_1,G_2,\cdots,G_{p-j})$,设各组元素所对应的值为$(v'_{G_1},v'_{G_2},\cdots,v'_{G_{p-j}})$,若 $\hat{B}_x^{\text{avg}}\in\hat{G}_l$,且 $\hat{B}_x^{\text{avg}}=v'_{G_l}$($l\in\{1,2,\cdots,p-j\}$),则 $\hat{B}_x^{\text{avg}}$ 所对应的图像块通过认证,否则若 $\hat{B}_x^{\text{avg}}\neq v'_{G_l}$,则 $\hat{B}_x^{\text{avg}}$ 所对应的图像块被修改,不能通过认证,并使用 $v'_{G_l}\times 4$ 代替该图像块中的所有像素进行恢复;若水印$(n'_{j+1},n'_{j+2},\cdots,n'_p)$被篡改,则$(\hat{n}_{i+1},\hat{n}_{i+2},\cdots,\hat{n}_o)$所对应的图像块无法进行认证.

命题 1. 若 $\sum_{x=i+1}^{o}\hat{n}_x\neq\sum_{x=j+1}^{p}n'_x$,则说明水印$(n'_{j+1},n'_{j+2},\cdots,n'_p)$被篡改.

证明. 不妨证其逆反命题,即若水印$(n'_{j+1},n'_{j+2},\cdots,n'_p)$未被篡改,则存在 $\sum_{x=i+1}^{o}\hat{n}_x=\sum_{x=j+1}^{p}n'_x$.

在 $o=\hat{k},p=k'$ 时,使用递归法证明 $\sum_{x=i+1}^{\hat{k}}\hat{n}_x=\sum_{x=j+1}^{k'}n'_x$:

当 $i=0,j=0$ 时,因为$(n'_{j+1},n'_{j+2},\cdots,n'_p)=(n'_1,n'_{j+2},\cdots,n'_{k'})$,则有 $\sum_{x=1}^{k'}n'_x=r$,因为$\sum_{x=1}^{\hat{k}}\hat{n}_x=r$,可得 $\sum_{x=j+1}^{k'}n'_x=\sum_{x=i+1}^{\hat{k}}\hat{n}_x$.

设当 $i=m,j=n$ 时,有 $\sum_{x=m+1}^{k'}n'_x=\sum_{x=n+1}^{\hat{k}}\hat{n}_x$ 成立,则当 $i=m+1,j=n+1$ 时,有:

$$\sum_{x=i+1}^{k'}n'_x=\sum_{x=m+1+1}^{k'}n'_x=\sum_{x=m+1}^{k'}n'_x-n'_{m+1},$$

$$\sum_{x=j+1}^{\hat{k}}\hat{n}_x=\sum_{x=n+1+1}^{\hat{k}}\hat{n}_x=\sum_{x=n+1}^{\hat{k}}\hat{n}_x-\hat{n}_{n+1}. \tag{7}$$

由于 $M(n'_{m+1},\hat{n}_{n+1})$,则 $n'_{m+1}=\hat{n}_{n+1}$,且由 $\sum_{x=m+1}^{k'}n'_x=\sum_{x=n+1}^{\hat{k}}\hat{n}_x$,可得 $\sum_{x=i+1}^{k'}n'_x=\sum_{x=j+1}^{\hat{k}}\hat{n}_x$.

同理,在 $i=0,j=0$ 时,使用递归法可证得:$\sum_{x=1}^{p}n'_x=\sum_{x=1}^{o}\hat{n}_x$.

由上述两个证明相结合,容易证得:

$$\sum_{x=i+1}^{o}\hat{n}_x=\sum_{x=j+1}^{p}n'_x.$$

证毕.

注:本算法的认证分为两个步骤,其中 Step5 使用字符串匹配思想,防止因 $\hat{\boldsymbol{N}}$ 和 $\boldsymbol{N}'$ 中的某些元素被修改而引起后续块的认证失败;Step7 对未通过认证的子串中的图像块进行逐一匹配,使得本算法的认证精度可以达到 2×2 的图像块.

3 算法分析

3.1 水印长度分析

本文算法中对 $\boldsymbol{X}^{\text{avg}}$ 中值相等的相邻元素进行游程编码,因此水印的长度依赖于 $\boldsymbol{X}^{\text{avg}}$ 中元素之间的相关性.有命题 2 成立:

命题 2. 设 $\boldsymbol{X}^{\text{avg}}$ 中共有 r 个元素,p_0 为 $\boldsymbol{X}^{\text{avg}}$ 的行中任取两个相邻像素,其像素值相等的概率,即

$$\forall i\in\{1,2,\cdots,r-1\},p_0=P\{B_i^{\text{avg}}=B_{i+1}^{\text{avg}}\}, \tag{8}$$

设共生成 k 组水印,即

$$\boldsymbol{W}=(\boldsymbol{w}_1,\boldsymbol{w}_2,\cdots,\boldsymbol{w}_k)=((v_1,n_1),(v_2,n_2),\cdots,(v_k,n_k)), \tag{9}$$

则 k 满足:

$$k=\frac{r}{\sum_{i=1}^{r}p_0^{i-1}}. \tag{10}$$

证明. 对于所构造的水印 $\boldsymbol{W}=(\boldsymbol{w}_1,\boldsymbol{w}_2,\cdots,\boldsymbol{w}_k)=((v_1,n_1),(v_2,n_2),\cdots,(v_k,n_k))$,$n_i\in\{1,2,\cdots,r\}$在不同取值下的概率分别为

$$P_{\{n_i=j\}}=\begin{cases}p_0^{j-1}(1-p_0), & 1\leqslant j<r,\\ p_0^{j-1}, & j=r,\end{cases} \tag{11}$$

则 $n_i=j$ 的水印组的个数为

$$num_{(n_i=j)}=P_{\{n_i=j\}}k, \tag{12}$$

则分块的个数 r 为

$$r=\sum_{j=1}^{r}j\times num_{(n_i=j)}=1\times k\times(1-p_0)+2\times k\times p_0(1-p_0)+\cdots+r\times k\times p_0^{r-1}=k\times(1+p_0+p_0^2+\cdots+p_0^{r-1}), \tag{13}$$

即 k 满足:$k=\frac{r}{\sum_{i=1}^{r}p_0^{i-1}}$. 证毕.

对于 $\boldsymbol{w}_i=(v_i,n_i)$,其中 v_i 的长度为 $len(v_i)=6$ b,n_i 的长度为 $len(n_i)=\lfloor \text{lb}\, n\rfloor+1$ b,则 w_i 的长度为

$$len(\boldsymbol{w}_i)=len(n_i)+len(v_i)=\lfloor \mathrm{lb}\, n_i \rfloor+7\ \mathrm{b}, \quad (14)$$

则根据命题 2,水印的长度可由式(15)计算得到:

$$len(\boldsymbol{W})=\sum_{j=1}^{r} num_{(n_i=j)}\, len(\boldsymbol{w}_i)=\sum_{j=1}^{r} P_{(n_i=j)}\, k(\lfloor \mathrm{lb}\, j \rfloor+7). \quad (15)$$

图 1 给出了 p_0 由 0～1 变化的情况下,256×256 的图像(共有 $r=128\times128$ 个图像块)生成的水印长度的大小.从图 1 可以看出,水印长度 $len(\boldsymbol{W})$ 随 p_0 的增大而减小,即相邻图像块之间的相关性越强则水印的长度越小.因此,本文算法对于相对平滑的图像,水印的长度将越小.对于纹理复杂的图像,即使 $p_0=0$,那么水印的长度为 $r\times7$ b,而图像的最低两位共可嵌入 $r\times8$ b 的水印信息,因此也可满足水印嵌入的需求,且相对于文献[9]和文献[10]中的算法(对图像最低两位进行满嵌,即水印长度为 $r\times8$ b),具有更小的水印长度.

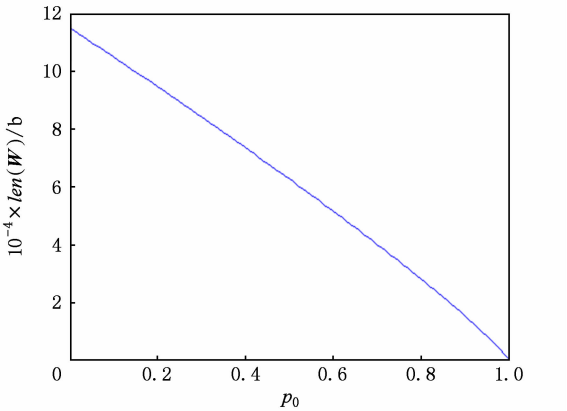


Fig. 1 The curves of $len(\boldsymbol{W})$ in the case of p_0.

图 1 水印长度 $len(\boldsymbol{W})$ 随 p_0 的变化情况

3.2 虚警概率和漏检概率

根据本文算法,由命题 1,当$(\hat{n}_{i+1},\hat{n}_{i+2},\cdots,\hat{n}_o)$所对应的水印$(n'_{j+1},n'_{j+2},\cdots,n'_p)$被篡改,且恰好使得 $\sum_{x=i+1}^{o}\hat{n}_x=\sum_{x=j+1}^{p}n'_x$ 时,将会产生虚警的情况.设 $\sum_{x=i+1}^{o}\hat{n}_x=\sum_{x=j+1}^{p}n'_x=\Gamma$,此时被修改后,$(n'_{j+1},n'_{j+2},\cdots,n'_p)$中各元素可能的取值范围为

$$\Theta(n'_{j+1})=[1,\Gamma],$$
$$\Theta(n'_{j+1+1})=[1,\Gamma-n'_{j+1}],$$
$$\vdots$$
$$\Theta(n'_p)=\Big[1,\Gamma-\sum_{x=j+1}^{p-1}n'_x\Big], \quad (16)$$

则恰好使得 $\sum_{x=i+1}^{o}\hat{n}_x=\sum_{x=j+1}^{p}n'_x$ 的概率,即虚检概率为

$$P_{\mathrm{fa}}=\frac{|\Theta(n'_{j+1})|}{r}\times\frac{|\Theta(n'_{j+1+1})|}{r}\times\cdots\times\frac{\Theta(n'_p)}{r}=\frac{\Gamma}{r}\times\frac{\Gamma-n'_{j+1}}{r}\times\cdots\times\frac{\Gamma-\sum_{x=j+1}^{p-1}n'_x}{r}, \quad (17)$$

其中,r 为图像块的个数,由于本文算法在水印嵌入时使用混沌散列进行图像的置乱,水印的嵌入类似于随机嵌入,连续修改到 $o-i$ 个元素所对应的水印信息的概率非常低,因此 $r\gg\Gamma$,即 $P_{\mathrm{fa}}\ll1$.

漏检是指图像被恶意篡改、检测器并未检测到的情况.对于本算法而言,由命题 1 可知,当$(\hat{n}_{i+1},\hat{n}_{i+2},\cdots,\hat{n}_o)$与$(n'_{j+1},n'_{j+2},\cdots,n'_p)$同时被篡改时将引起漏检的情况.设攻击者的攻击强度,即对每个像素篡改到的概率为 p,则 $\hat{n}_{i+1}$ 所对应的水印被篡改的概率为 $\lceil \mathrm{lb}\,\hat{n}_{i+1} \rceil p$.因此$(\hat{n}_{i+1},\hat{n}_{i+2},\cdots,\hat{n}_o)$和$(n'_{j+1},n'_{j+2},\cdots,n'_p)$同时被篡改的概率,即漏检概率为

$$P_{\mathrm{fr}}=\prod_{x=i+1}^{o}(\lceil \mathrm{lb}\,\hat{n}_x \rceil p)=p^{o-i}(\lceil \mathrm{lb}\,\hat{n}_{i+1} \rceil\times\lceil \mathrm{lb}\,\hat{n}_{i+2} \rceil\times\cdots\times\lceil \mathrm{lb}\,\hat{n}_o \rceil). \quad (18)$$

由式(18)可知,由于 $0\leqslant p\leqslant1$,因此 P_{fr} 随 $o-i$ 的增大而减小,即本文算法不会产生大片区域发生漏检的情况.

4 实验仿真

本文在 Windows 环境下实现仿真了本算法,所测试的图像为 256×256 的标准灰度图像,像素值介于 0～255 之间,混沌置乱的密钥同文献[4].下面分别从含水印图像质量、篡改定位及恢复、抗量化攻击、漏检率 4 个方面的实验来验证本文算法的有效性.

4.1 图像质量测试

含水印图像的质量受原始图像所产生的水印长度的影响,由 3.1 节的分析可知,水印长度受到概率 p_0 的影响,p_0 值越大则水印的长度越小,含水印图像的质量也越好.表 1 给出了一组不同的图像使用本算法所生成的水印的长度、其对应的 p_0 值及由式(15)计算得到的理论水印长度.由表 1 可以看出,水印长度和 p_0 值之间的关系与理论分析结论基本一致.由于文献[10]的水印长度为 256×256×2=131 072 b,

而文献[9]的水印长度根据图像的纹理复杂度不同而不同,因此表 2 列出了本文算法与文献[9]的水印容量(单位为 bpp,bit per pixel)对比. 从表 2 可以看出,本文算法的水印容量有明显减小. 表 3 列出了使用本文算法和文献[9-10]算法嵌入水印后图像的峰值信噪比(peak signal to noise ratio, PSNR),可见,使用本文的算法嵌入水印后,图像的质量要明显好于文献[9-10]的算法.

Table 1 The Length of Watermark Generated by the Proposed Scheme for Different Images

表 1 本文算法生成的水印长度

Images	p_0	Theoretical Length/b	Experimental Length/b
Lena	0.25	90 325	89 232
Airplane	0.32	82 980	80 880
Bird	0.54	59 223	59 128
House	0.41	73 391	72 544
Pepper	0.22	93 443	92 808
Boat	0.38	76 606	76 584

Table 2 The Watermarking Payload Comparison Between the Proposed Scheme and Ref [9]

表 2 本文算法与文献[9]的水印容量对比 bpp

Images	Proposed	Ref [9]
Lena	1.36	1.83
Airplane	1.23	1.86
Bird	0.90	1.59
House	1.11	1.73
Pepper	1.42	1.91
Boat	1.17	1.83

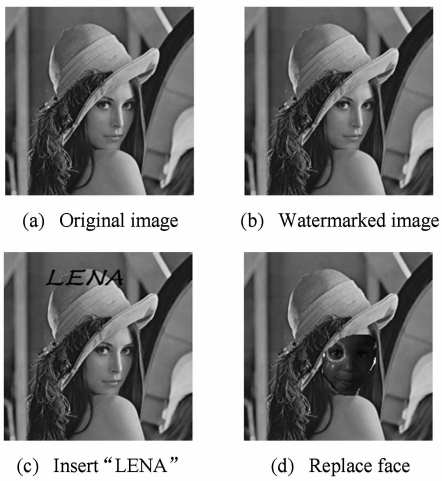
Table 3 The PSNR Comparison Between the Proposed Scheme and Ref [9-10]

表 3 本文与文献[9-10]算法含水印图像的峰值信噪比 dB

Images	Proposed	Ref [9]	Ref [10]
Lena	47.31	45.67	44.31
Airplane	47.23	45.16	44.08
Bird	48.90	46.48	44.16
House	48.22	45.80	44.23
Pepper	47.23	44.52	44.34
Boat	48.17	45.88	44.27

4.2 篡改定位及恢复

图 2 给出了原始图像和含水印图像,以及对含水印图像的篡改图像,其中分别对含水印图像添加文字"LENA"和进行内容的篡改. 图 3 给出了本文算法针对篡改攻击的认证结果和恢复结果. 由认证结果可以看出,本文算法的篡改定位精度可以达到 2×2 的图像块,且能够较高质量地恢复被篡改位置. 图 4 给出了文献[7]算法的认证结果和恢复结果,该文的篡改定位和恢复的精度为 8×8 的图像块. 且通过比较恢复结果图像和含水印图像的 PSNR 可以看出,本文算法针对添加文字和内容篡改的恢复结果图像的 PSNR 分别为 43.85 dB 和 25.41 dB,而文献[7]的恢复结果分别为 25.43 dB 和 21.08 dB,表明本文算法具有更好的恢复质量.

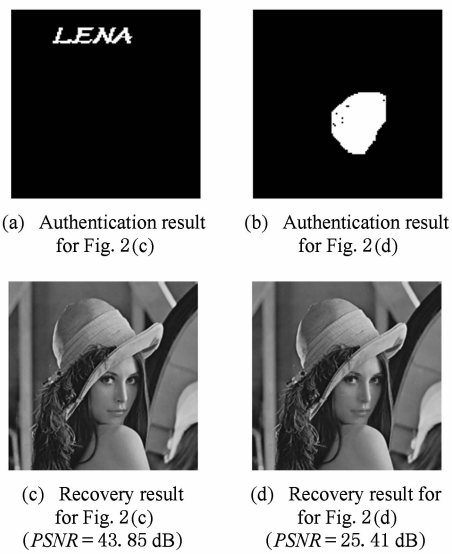


(a) Original image (b) Watermarked image

(c) Insert "LENA" (d) Replace face

Fig. 2 The watermarked image and it's tempered images.

图 2 含水印图像及篡改图像



(a) Authentication result for Fig. 2(c) (b) Authentication result for Fig. 2(d)

(c) Recovery result for Fig. 2(c) ($PSNR$ = 43.85 dB) (d) Recovery result for for Fig. 2(d) ($PSNR$ = 25.41 dB)

Fig. 3 The authentication and recovery results of proposed scheme.

图 3 本文算法的认证及恢复结果

(a) Authentication result for Fig. 2(c) (b) Authentication result for Fig. 2(d)

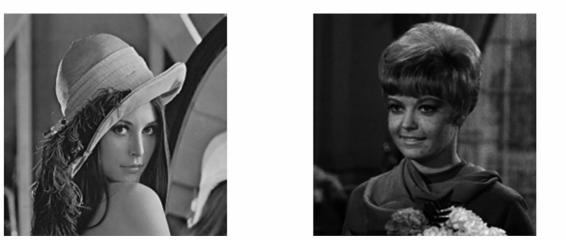
(c) Recovery result for Fig. 2(c) ($PSNR$ = 25.43 dB) (d) Recovery result for for Fig. 2(d) ($PSNR$ = 21.08 dB)

Fig. 4 The authentication and recovery results of Ref [7].

图 4 文献[7]算法的认证及恢复结果

4.3 抗拼贴攻击测试

拼贴攻击是对脆弱水印算法威胁最大的攻击之一. 图 5(a)和图 5(b)分别是使用相同密钥生成的含水印图像“Lena. bmp”和“Girl. bmp”;图 5(c)是将 Girl 图像中央 10%的区域拼贴到 Lena 图像的相同位置生成的篡改图像;图 5(d)为认证结果图像. 图 6(a)是将含水印图像 Lena 的两个图像块复制并拼贴到该图像的其他位置;图 6(b)是认证结果图像. 可见,本文算法可有效检测出在不同图像之间和一幅图像内部进行拼贴攻击的篡改位置. 这是由于本文的水印生成方式消除了图像分块间的独立性,认证时通过提出的水印信息重构的均值图像判断图像块的篡改情况,因此任何不符合水印信息的图像块均被认证为篡改图像块,即能够完全抵抗拼贴攻击.



(a) Watermarked image Lena. bmp (b) Watermarked image Girl. bmp

(c) Image under collage attack (d) Authentication result for (c)

Fig. 5 Experimental results against collage attack between different images.

图 5 抵抗图像间拼贴攻击

(a) Image under collage attack (b) Authentication result for (a)

Fig. 6 Experimental results against collage attack in the same image.

图 6 抵抗图像内部拼贴攻击

4.4 漏检测试

图 7 是针对漏检的测试结果,其中图 7(a)、图 7(c)分别为剪切图像中央 5%和 15%的区域;图 7(b)、图 7(d)分别为针对图 7(a)和图 7(c)的认证结果,其中黑色小点为漏检的图像块. 从图 7 可以看出,即使连读大面积地对图像进行篡改,本文算法漏检的概率也在可接受的范围内.

(a) Shearing 5% of the image (b) Authentication result for (a)

(c) Shearing 15% of the image (d) Authentication result for (c)

Fig. 7 Experimental results of false acceptance.

图 7 漏检测试结果

5 结束语

本文提出了一种自嵌入的易碎水印算法,可用于图像完整性认证和篡改恢复. 该算法通过对图像进行游程编码有效缩短了所生成水印的长度,因此水印的嵌入对图像质量的影响相对较小,且篡改定

位和恢复的精度均可达到 2×2 的图像块.本文通过实验验证了算法在不可见性、篡改定位精度和恢复的质量、漏检率等方面均具有较好的效果.然而,本文只是在基于图像结构信息进行认证方面的一种尝试,所选取的恢复水印编码方式有待进一步探讨,同时针对水印信息被篡改而引起漏检和影响恢复的可信性问题还需要进一步研究.

参 考 文 献

[1] Lin P L, Huang C K. A hierarchical digital watermarking method for image tamper detection and recovery [J]. Pattern Recognition, 2005, 38(11): 2519-2529

[2] He Hongjie, Chen Fan. On the security of the self-embedding watermarking scheme [J]. Acta Electronica Sinica, 2007, 35(3): 557-562 (in Chinese)
(和红杰, 陈帆. 自嵌入水印算法的安全性分析[J]. 电子学报, 2007, 35(3): 557-562)

[3] Chang C C, Fan Y H, Tai W L. Four-scanning attack on hierarchial digital watermarking method forimage tamper detection and recovery [J]. Pattern Recognition, 2008, 41(2): 654-661

[4] Wang Guodong, Liu Fenlin, Liu Yuan, et al. An image authentication scheme with discrimination of tampers on watermark or image [J]. Acta Electronica Sinica, 2008, 36(7): 1349-1354 (in Chinese)
(王国栋, 刘粉林, 刘媛, 等. 一种能区分水印或内容篡改的脆弱水印算法[J]. 电子学报, 2008, 36(7): 1349-1354)

[5] Duan Guiduo, Zhao Xi, Li Jianping, et al. A novel semi-fragile digital watermarking algorithm for image content authentication, localization and recovery [J]. Acta Electronica Sinica, 2010, 38(4): 842-847 (in Chinese)
(段贵多, 赵希, 李建平, 等. 一种新颖的用于图像内容认证、定位和恢复的半脆弱数字水印算法研究[J]. 电子学报, 2010, 38(4): 842-847)

[6] Yang Weimin, Cai Jian. Image fragile watermarking algorithm of self-embedding [J]. Journal of Chinese Computer System, 2011, 32(1): 169-172 (in Chinese)
(杨卫民, 蔡键. 一种自嵌入的图像脆弱水印算法[J]. 小型微型计算机系统, 2011, 32(1): 169-172)

[7] Patra B, Patra J C. CRT-based self-recovery watermarking technique for multimedia applications [C] //Proc of IEEE Int Conf on Acoustics, Speech, and Signal Processing. Piscataway, NJ: IEEE, 2012: 1761-1764

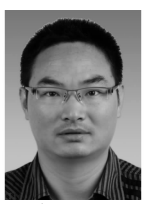
[8] He H J, Zhang J S, Chen Fan. A self-recovery fragile watermarking scheme for image authentication with superior localization [J]. Science China: Series F Information Sciences, 2008, 51(10): 1487-1507

[9] Chen Fan, He Hongjie, Wang Hongxia. Variable-payload self-recovery watermarking scheme for digital image authentication [J]. Chinese Journal of Computers, 2012, 35(1): 154-162 (in Chinese)
(陈帆, 和红杰, 王宏霞. 用于图像认证的变容量恢复水印算法[J]. 计算机学报, 2012, 35(1): 154-162)

[10] He H J, Chen F, Tai H M, et al. Performance analysis of a block-neighborhood-based self-recovery fragile watermarking scheme [J]. IEEE Trans on Information Forensics and Security, 2012, 7(1): 185-196

Gong Daofu, born in 1984. PhD of the PLA Information and Engineering University. His current research interests include digital watermarking and network information security.

Liu Fenlin, born in 1964. Professor and PhD supervisor in the PLA Information and Engineering University. Member of China Computer Federation. His current research interests include digital watermarking, steganography technology and network information security.



Luo Xiangyang, born in 1978. Associate professor and PhD supervisor in the PLA Information and Engineering University. Member of China Computer Federation. His current research interests include digital watermarking, steganography technology and network information security.