软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(9):2510−2521 [doi: 10.3724/SP.J.1001.2012.04169]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于邻域比较的 JPEG 脆弱水印算法及性能分析*

霍耀冉, 和红杰+, 陈 帆

(西南交通大学 信号与信息处理四川省重点实验室,四川 成都 610031)

Fragile Watermarking Algorithm for JPEG Images Based on Neighborhood Comparison and its Performance Analysis

HUO Yao-Ran, HE Hong-Jie+, CHEN Fan

(Sichuan Key Laboratory of Signal and Information Processing, Southwest Jiaotong University, Chengdu 610031, China)

+ Corresponding author: E-mail: hjhe@home.swjtu.edu.cn

Huo YR, He HJ, Chen F. Fragile watermarking algorithm for JPEG images based on neighborhood comparison and its performance analysis. *Journal of Software*, 2012,23(9):2510−2521 (in Chinese). http:// www.jos.org.cn/1000-9825/4169.htm

Abstract: To improve the tamper detection performance and harmonize the conflict between security and invisibility, this paper proposes a fragile watermarking algorithm for JPEG images, in which the authenticity of image blocks is determined by neighborhood comparison. This scheme divides the original image into 8×8 image blocks. For each block, four bits watermarks are generated based on the DCT coefficients to be protected. Next, the watermarks are randomly embedded in the least significant bit (LSB) of DCT coefficients with smaller quantization step in other four blocks. The authenticity of each block is determined by comparison between the number of inconsistent image blocks in the eight-neighborhood of each block and its four corresponding mapping blocks. Then, this paper derives the probability of false acceptance and false rejection under general tampering and collage attack and validates the theoretical analysis results by statistical experiments. Theoretical analysis and statistical experiments show that comparing the number of inconsistent image blocks in the eight-neighborhood of each block with its four corresponding mapping blocks improves the tamper detection performance. Embedding watermarks in the LSB of DCT coefficients with less quantization step efficiently solves the conflict between the number of DCT coefficients to be protected and invisibility.

Key words: fragile watermarking; JPEG image; tamper detection; neighborhood comparison; inconsistent image block; theoretical analysis

摘 要: 为提高篡改检测性能和协调安全性与不可见性之间的矛盾,提出一种利用邻域比较判定图像块真实性的 JPEG 脆弱水印算法.该算法将原始图像分成 8×8 的图像块,基于图像块保护 DCT 系数生成的 4 比特水印基于密钥随机嵌入到其他 4 个图像块量化步长较小的 DCT 系数最低位.通过比较该图像块与相应 4 个水印嵌入块 8 邻域中不一致图像块个数来判定该图像块的真实性,推导给出一般篡改和拼贴攻击下算法的虚/漏警率,并

* 基金项目: 国家自然科学基金(60970122, 61170226); 国家教育部博士点基金(20090184120021); 中央高校基本科研业务专项基金(SWJTU09CX039, SWJTU10CX09); 北京市"现代信息科学与网络技术"重点实验室基金; 铁道部"铁路信息科学与工程"开放实验室基金(XDXX1007)

收稿时间: 2011-05-04; 修改时间: 2011-10-08; 定稿时间: 2011-12-31

利用统计实验对理论分析结果进行验证.理论分析和实验统计结果表明,通过比较图像块与其相应水印嵌入块8邻域中不一致图像块个数能够提高篡改检测性能,在量化步长较小DCT系数的最低位嵌入水印,解决了保护DCT系数个数与不可见性之间的矛盾.

关键词: 脆弱水印;JPEG图像;篡改检测;邻域比较;不一致图像块;理论分析

中图法分类号: TP309 **文献标识码:** A

随着计算机与图像处理技术的发展,数字图像的易伪造性使图像内容的完整性和真实性受到了严重威胁,认证水印技术是解决该问题的有效途径之一[1].根据水印承受图像改变的程度,认证水印分为[2]选择性认证[3,4]和精确认证[5−11].精确认证不允许任何改变,包括去噪、压缩等常规处理,通过脆弱水印实现;选择性认证在保证图像内容完整性和真实性的同时能够区分恶意篡改和无意操作,通过半脆弱水印实现.实际应用中,考虑到传输容量和图像质量,不可避免地要对数字图像进行一些处理,如压缩、去噪、增强等.同时,JPEG压缩标准在数字图像的存储和传输中的广泛应用,使JPEG脆弱水印成为研究热点.

不可见性和篡改定位性能是脆弱水印算法的重要指标.由于JPEG图像水印容量较小,如何保证在较小失真的条件下尽可能提高JPEG脆弱水印算法的篡改定位性能显得尤为重要[7].通过同时修改JPEG Huffman表和比特流嵌入水印,文献[8]提出了一种零失真水印(zero-error watermarking,简称ZEW)算法.由于没有改变图像的DCT系数,该算法的含水印图像没有失真.但是文献[8]只能认证图像的真实性,不能定位篡改区域.在每个8×8图像块中可逆地嵌入2比特水印信息,文献[7]提出了一种高定位精度的可逆JPEG脆弱水印算法.该算法通过比较提取和基于恢复图像重构的水印信息,能够精确定位小区域篡改,但是不能区分内容与水印篡改.因此,文献[9]通过比较彩色图像*Y*分量的每个块的63比特水印中不一致比特的比率来区分内容与水印篡改.但是该算法只利用*Y*分量生成和嵌入水印,无法有效保护*U*,*V*分量.

根据数字图像JPEG压缩前后,其相应*DWT*的*LH*和*HL*子带系数大小关系变化概率较小的特性,文献[3]提出通过调整*LH*或*HL*子带系数的大小关系,实现二值水印图像嵌入的半脆弱数字图像水印算法,并利用形态学处理来提高篡改检测性能.文献[3]虽然能够有效抵抗JPEG压缩,但不能抵抗Fridrich等人[12]提出的拼贴攻击.结合JPEG压缩标准,文献[10]将图像分成8×8的图像块,对每个图像块,将基于密钥和该图像块内容生成的4比特水印嵌入到该图像块的4个非零DCT中频系数.为引入图像块之间的相关性,结合与该块相邻图像块中随机选取的部分DCT系数嵌入水印[10].由于该算法只建立了图像块与其相邻图像块之间的相关性,因此当拼贴区域较大时,该算法只能检测出拼贴区域的边界,而拼贴区域内的篡改块依然能通过认证[11].此外,余淼等人[11]指出,文献[10]将水印嵌入在非零系数,不能有效保护平滑区域.为引入图像块之间的随机相关性且保护平滑区域,余淼等人[11]将基于图像块的前h'个DCT系数(经ziag排序,下同)生成的4比特水印分别随机嵌入在其他4个图像块的第h'+1~h'+4个量化DCT系数,通过与该块相邻图像块中不一致块的个数来判定该图像块的真实性.该算法通过水印嵌入建立了图像块之间的随机相关性,极大地提高了算法抵抗拼贴攻击的能力.然而,块间随机相关性的引入也增加了判定图像块真实性的难度.文献[11]仅根据图像块和与其相邻图像块的不一致性来判定该图像块的真实性,该算法的篡改检测性能有待进一步提高.当篡改比例较大时,该算法的误检率(probability of false decision,简称PFD)[13]较高.另一方面,DCT域中水印嵌入位置既影响水印的稳健性,也影响不可见性[14].文献[11]将水印嵌入在第h'+1~h'+4个系数上,待保护DCT系数越多(即h'越大),嵌入水印的DCT系数位置越靠后.由JPEG量化表可知,DCT系数的位置靠后,其量化步长较大,则反量化引起的误差也相对较大.因此,在文献[11]的算法中,不可见性随着待保护DCT系数个数的增加而降低.

为提高算法的篡改检测性能和解决待保护DCT系数个数与不可见性之间的矛盾,本文提出一种基于邻域篡改特性比较的JPEG图像脆弱水印算法.首先将原始图像分成8×8的图像块,基于待保护DCT系数和密钥生成4比特水印,并随机嵌入到其他4个图像块量化步长较小的量化DCT系数最低位(least significant bit,简称LSB),既引入了图像块之间的随机相关性,又解决了待保护系数个数与不可见性之间的矛盾.检测时,通过比较图像块与对应4个水印嵌入块的8邻域中不一致图像块个数来判定该图像块的真实性,以提高算法的篡改检测

性能.为验证算法的篡改检测性能,推导给出一般篡改和拼贴攻击下算法的漏警率(probability of false acceptance,简称 PFA)[13]和虚警率(probability of false rejection,简称 PFR)[13],并利用统计实验验证了理论分析的正确性.理论分析和实验仿真结果表明,相同条件下,本文算法的不可见性和篡改检测性能优于现有算法.

1 邻域特性比较 JPEG 脆弱水印算法

设 I 表示大小为 $m\times n$(假设 m 和 n 均能被 8 整除)的原始图像,Q 为给定压缩因子的量化表,h 为图像块保护 DCT 系数个数.水印算法包括水印嵌入、邻域篡改特性比较检测.

1.1 水印嵌入

水印嵌入算法框图如图 1 所示,包括以下 5 个步骤:

Step 1. 分块 DCT:将原始图像 I 分为 8×8 互不重叠的图像块 $I_i(i=1,2,\ldots,N)$,其中,N 为图像块个数.利用公式(1)和 JPEG 量化表 Q 生成量化 DCT 系数矩阵 $X_i=\{x_{ij}|j=1,2,\ldots,64\}$($i$ 是图像块索引,j 是图像块量化 DCT 系数 zigzag 排序后的索引).

$$X_i=round(DCT(I_i)/Q) \tag{1}$$

其中,$round(\cdot)$是四舍五入操作,$DCT(\cdot)$是 DCT 变换.

Step 2. 水印生成:对每个图像块 I_i,首先将其量化 DCT 系数矩阵 X_i 的第 2、第 3、第 5、第 6 个量化 DCT 系数 $x_{ij'}(j'=2,3,5,6)$的 LSB 置 0,然后将前 h 个量化 DCT 系数分别转换为 8 位二进制,生成大小为 8×h 的二值矩阵 B_i.基于密钥 Key_1 生成两个二值矩阵 C_i 和 C_i',其大小分别为 1×8 和 h×4.按公式(2),生成图像块 I_i 的 4 比特水印信息 $W_i=\{w_{ik}|k=1,2,3,4\}$.

$$W_i=\mathrm{mod}(C_iB_iC_i',2) \tag{2}$$

其中,$C_iB_iC_i'$ 表示 C_i,B_i,C_i' 这 3 个矩阵相乘运算,随机二值矩阵 C_i 和 C_i' 的生成方法与特性分析见文献[4,6].

Step 3. 水印嵌入块索引:基于密钥 Key_2 生成大小为 N×4 的随机矩阵 $S=\{s_{ik}|i=1,2,\ldots,N,k=1,2,3,4\}$.将 S 按列排序得到矩阵 S 的列索引有序矩阵 $A=\{a_{ik}|i=1,2,\ldots,N,k=1,2,3,4,a_{ik}\in[1,N]$的整数$\}$作为水印嵌入块索引,即将图像块 I_i 的第 k 比特水印嵌入到第 a_{ik} 个图像块中.

Step 4. 水印嵌入:对每个图像块 I_i,将其第 $k(k=1,2,3,4)$比特水印 w_{ik} 嵌入到量化 DCT 系数 $x_{i'j'}$的 LSB 中,生成含水印 DCT 系数 $x'_{i'j'}$.

$$x'_{i'j'}=\left\lfloor x_{i'j'}/2\right\rfloor\times 2+w_{ik} \tag{3}$$

其中,$\lfloor\ \rfloor$表示向下取整;$i'=a_{ik}$ 表示水印比特 w_{ik} 嵌入图像块的索引;j'表示待嵌入水印 DCT 系数的位置,其取值依赖于 k.

$$j'=\begin{cases}k+1, & \text{if } k=1,2\\ k+2, & \text{if } k=3,4\end{cases} \tag{4}$$

Step 5. 含水印图像生成:将上一步生成的含水印量化 DCT 系数矩阵 X_i' 反量化、反 DCT 变换生成含水印图像 I_w.

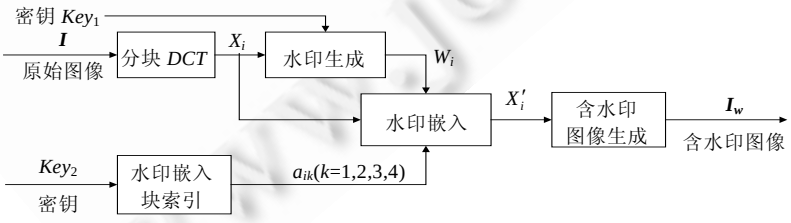


Fig.1 Schematic diagram of watermark embedding

图 1 水印嵌入算法框图

1.2 邻域篡改特性比较检测

设 Y 为被测图像,按照水印嵌入将其分为 N 个图像块 $Y=\{Y_i|i=1,2,\ldots,N\}$.对每个图像块 Y_i,其篡改检测包括以下步骤:

Step 1. 水印重构:根据密钥 Key_1,按照公式(2)计算每个被测图像块 Y_i 的重构水印信息:

$$W_i'=\{w_{ik}' \mid k=1,2,3,4\}$$

Step 2. 水印提取:根据密钥 Key_2 生成水印嵌入块索引矩阵 $A=\{a_{ik}|i=1,2,\ldots,N,k=1,2,3,4\}$,则第 i 个图像块的提取水印信息 $W_i^*=\{w_{ik}^* \mid k=1,2,3,4\}$ 根据公式(5)得到:

$$w_{ik}^*=\mathrm{mod}(x_{i'j'},2) \tag{5}$$

其中,$x_{i'j'}$为被测图像第 i'个图像块 $Y_{i'}$的第 j'个量化 DCT 系数,$i'=a_{ik}$,j'由公式(4)计算得到.

Step 3. 不一致块标识:利用 w_{ik}^* 和 $w_{ik}'(k=1,2,3,4)$ 生成图像块不一致块标识矩阵$\Lambda=\{\lambda_i|i=1,2,\ldots,N\}$.

$$\lambda_i=\begin{cases}0, \text{ if } w_{ik}^*=w_{ik}', k=1,2,3,4\\ 1, \text{ otherwise}\end{cases} \tag{6}$$

$\lambda_i=1$ 表示图像块 Y_i 的重构水印信息与提取水印信息不一致,称图像块 Y_i 为不一致图像块.

Step 4. 邻域不一致块个数统计:设 d_i 为与第 i 个图像块相邻的 8 个图像块中不一致块的个数:

$$d_i=\sum_q \lambda_q, q\in E_i \tag{7}$$

其中,E_i 表示被测图像块 Y_i 的 8 邻域块索引集合[5].

Step 5. 邻域篡改特性比较检测:对每一个图像块 Y_i,如果该图像块为不一致图像块,且与其相邻的 8 个图像块中至少有一个块是不一致块,同时,该图像块邻域不一致块个数不小于其 4 个相应水印嵌入块的邻域不一致块个数的最大值,则判定该图像块 Y_i 被篡改;否则,判定 Y_i 是真实的.用 $T=\{t_i|i=1,2,\ldots,N\}$表示篡改标识矩阵,则

$$t_i=\begin{cases}1, \text{ if } \lambda_i=1 \,\&\, d_i>0 \,\&\, d_i \geqslant \max(d_{i'})\\ 0, \text{ otherwise}\end{cases} \tag{8}$$

其中,max(·)表示最大值,$i'=a_{ik}(k=1,2,3,4)$.

2 篡改检测性能分析

本节对算法的篡改检测性能进行理论分析,利用公式(8)和概率论的相关知识分别推导出一般篡改和拼贴攻击下算法的漏警率[13]P_{fa}(篡改图像块判定为真实的概率)和虚警率[13]P_{fr}(真实图像块被判定为篡改的概率),并利用统计实验对理论分析结果进行验证.统计实验中漏/虚警率的计算公式如下:

$$P_{fa}=\frac{N_T-N_{TD}}{N_T} \tag{9}$$

$$P_{fr}=\frac{N_{VD}}{N-N_T} \tag{10}$$

则误检率[13]P_{fd},即误判图像块(包括两部分:判定为真实的篡改块和判定为篡改的真实块)占整个图像的比例为

$$P_{fd}=\frac{(N_T-N_{TD})+N_{VD}}{N}=p\times P_{fa}+(1-p)\times P_{fr} \tag{11}$$

其中,N_T 为被篡改图像块个数;N_{TD} 为被判定为篡改的篡改图像块个数;(N_T-N_{TD})即为判定为真实的篡改图像块个数;N_{VD} 为被判定为篡改的真实图像块个数;N 为图像块总个数,p 为篡改比例,即被篡改图像块个数占图像块总个数的比例.

水印嵌入时,每个图像块的 4 个比特水印分别随机的嵌入在其他 4 个图像块.设 H_0,H_1 分别表示篡改图像块和真实图像块的集合,则根据水印嵌入位置的随机性可知,每个水印嵌入块分别位于篡改区域内、外的概率为

$$P\{Y_{i'}\in H_0\}=p \tag{12}$$

$$P\{Y_{i'}\in H_1\}=1-p \tag{13}$$

由公式(8)可得:

$$P\{t_i=1\}=P\{(\lambda_i=1)\cap(d_i>0)\cap(d_i\geqslant\max(d_{i'}))\} \tag{14}$$

则算法的漏警率 P_{fa} 和虚警率 P_{fr} 为

$$P_{fa}=P\{t_i=0|Y_i\in H_0\}=1-P\{\lambda_i=1|Y_i\in H_0\}P\{d_i>0|Y_i\in H_0\}P\{d_i\geqslant\max(d_{i'})|Y_i\in H_0\} \tag{15}$$

$$P_{fr}=P\{t_i=1|Y_i\in H_1\}=P\{\lambda_i=1|Y_i\in H_1\}P\{d_i>0|Y_i\in H_1\}P\{d_i\geqslant\max(d_{i'})|Y_i\in H_1\} \tag{16}$$

由公式(15)、公式(16)可以看出,只要计算出不同条件下被测图像块 Y_i 对应的 3 个概率值:$P\{\lambda_i=1\}$,$P\{d_i>0\}$ 和 $P\{d_i\geqslant\max(d_{i'})\}$,将其代入公式(15)和公式(16)即可求出算法在相应条件下的漏/虚警率 P_{fa} 和 P_{fr}.

下面推导给出一般篡改和拼贴攻击下,被测图像块 Y_i 分别为篡改块和真实块 $P\{\lambda_i=1\}$,$P\{d_i>0\}$ 和 $P\{d_i\geqslant\max(d_{i'})\}$ 的计算公式.推导过程中,$P_{fa|G}$,$P_{fr|G}$ 分别表示一般篡改下的漏/虚警率,$P_{fa|C}$,$P_{fr|C}$ 分别表示拼贴攻击下的漏/虚警率. $P_{\beta|H_0}$,$P_{\beta|H_1}$ 表示 Y_i 位于篡改区域内、外,其重构的 4 个水印比特改变的个数为 β(=0,1,2,3,4)时 $\lambda_i=0$ 的概率.设独立随机变量 Z_1 和 Z_2 分别服从参数为 (n,p_1) 和 (n,p_2) 的二项分布.$P_{=z}(n,p_1)$ 表示 Z_1 等于 z($z\in[0,n]$ 的整数)的概率,$P_{<z}(n,p_1)$ 表示 Z_1 小于 z 的概率,$P_{<}(n,p_1,p_2)$ 表示 Z_1 小于 Z_2 的概率.

2.1 一般篡改

根据一般篡改的特点可知,由篡改块重构的每比特水印 w'_{ik} 改变的概率为 1/2,真实块重构的水印不改变.

因此,

$$P\{w^*_{ik}=w'_{ik}\,|\,Y_i\in H_0\cup Y_{i'}\in H_0\}=1/2 \tag{17}$$

$$P\{w^*_{ik}=w'_{ik}\,|\,Y_i\in H_1\cap Y_{i'}\in H_1\}=1 \tag{18}$$

当图像块 Y_i 为篡改块时,则

$$\begin{aligned}P\{\lambda_i=1\,|\,Y_i\in H_0\}=1-\sum_{\beta=0}^{3}P_{\beta|H_0}-P_{=4}(4,P\{w^*_{ik}=w'_{ik}\,|\,Y_i\in H_0\cup Y_{i'}\in H_0\})\\(P\{Y_{i'}\in H_0\}P\{w^*_{ik}=w'_{ik}\,|\,Y_i\in H_0\cup Y_{i'}\in H_0\})^4\end{aligned} \tag{19}$$

其中,$P_{\beta|H_0}$ (β=0,1,2,3)的计算公式为

$$\begin{aligned}P_{\beta|H_0}=P_{=\beta}(4,P\{w^*_{ik}=w'_{ik}\,|\,Y_i\in H_0\cup Y_{i'}\in H_0\})(P\{Y_{i'}\in H_0\}P\{w^*_{ik}=w'_{ik}\,|\,Y_i\in H_0\cup Y_{i'}\in H_0\})^{\beta}\\\sum_{\alpha=0}^{4-\beta}P_{=\alpha}(4-\beta,P\{Y_{i'}\in H_0\})(P\{w^*_{ik}=w'_{ik}\,|\,Y_i\in H_0\cup Y_{i'}\in H_0\})^{\alpha}\end{aligned} \tag{20}$$

当图像块 Y_i 为真实块时,则

$$P\{\lambda_i=1\,|\,Y_i\in H_1\}=1-\sum_{\beta=0}^{4}P_{\beta|H_1} \tag{21}$$

其中,β取不同值时,$P_{\beta|H_1}$ 的计算公式为

$$P_{\beta|H_1}=P_{=0}(4,P\{Y_{i'}\in H_0\}),\ \beta=0 \tag{22}$$

$$P_{\beta|H_1}=(P\{w^*_{ik}=w'_{ik}\,|\,Y_i\in H_0\cup Y_{i'}\in H_0\})^{\beta}P_{=\beta}(4,P\{Y_{i'}\in H_0\}),\ \beta=1,2,3,4 \tag{23}$$

2.1.1 漏警率

为简便起见,忽略图像块 Y_i 及其水印嵌入块 $Y_{i'}$ 位于篡改区域边界的情形.

当 $Y_i\in H_0$ 时,$d_i\sim B(8,P\{\lambda_i=1|Y_i\in H_0\})$.所以,

$$P\{d_i=0|Y_i\in H_0\}=P_{=0}(8,P\{\lambda_i=1|Y_i\in H_0\})=(1-P\{\lambda_i=1|Y_i\in H_0\})^8 \tag{24}$$

$$P\{d_i>0|Y_i\in H_0\}=1-(1-P\{\lambda_i=1|Y_i\in H_0\})^8 \tag{25}$$

同时,对于水印嵌入块 $Y_{i'}$ 的邻域不一致块数 $d_{i'}$,有

$$d_{i'}\sim\begin{cases}B(8,P\{\lambda_i=1\,|\,Y_{i'}\in H_0\})=B(8,P\{\lambda_i=1\,|\,Y_i\in H_0\}),\ \text{if } Y_{i'}\in H_0\\B(8,P\{\lambda_i=1\,|\,Y_{i'}\in H_1\})=B(8,P\{\lambda_i=1\,|\,Y_i\in H_1\}),\ \text{if } Y_{i'}\in H_1\end{cases} \tag{26}$$

比较不同篡改比例下的 $P\{\lambda_i=1|Y_i\in H_0\}$ 和 $P\{\lambda_i=1|Y_i\in H_1\}$ 可知,$P\{\lambda_i=1|Y_i\in H_0\}>P\{\lambda_i=1|Y_i\in H_1\}$.根据二项分布的期望值,$d_{i'}\sim B(8,P\{\lambda_i=1|Y_i\in H_0\})$ 的期望值要大于 $d_{i'}\sim B(8,P\{\lambda_i=1|Y_i\in H_1\})$ 的期望值.所以,当 4 个水印嵌入块中既

有篡改块又有真实块时,可以近似认为 $\max(d_{i'})\sim B(8,P\{\lambda_i=1|Y_i\in H_0\})$.若 4 个水印嵌入块均为真实块或均为篡改块时,可以认为 $\max(d_{i'})\sim B(8,P\{\lambda_i=1|Y_i\in H_1\})$或 $\max(d_{i'})\sim B(8,P\{\lambda_i=1|Y_i\in H_0\})$.因此,

$$\begin{aligned}P\{d_i\geqslant\max(d_{i'})\,|\,Y_i\in H_0\}=1-[1-(1-p)^4]P_<(8,P\{\lambda_i=1\,|\,Y_i\in H_0\},P\{\lambda_i=1\,|\,Y_i\in H_0\})-\\(1-p)^4P_<(8,P\{\lambda_i=1\,|\,Y_i\in H_0\},P\{\lambda_i=1\,|\,Y_i\in H_1\})\end{aligned}\tag{27}$$

将公式(19)、公式(25)、公式(27)代入公式(15),即可得到一般篡改下的漏警率 $P_{fa|G}$.

2.1.2 虚警率

若图像块 Y_i 未被篡改而λ_i=1,则 Y_i 对应的 4 个水印嵌入块中至少有一个块位于篡改区域 H_0.因为与篡改区域相邻的非篡改点较少,所以仅考虑被测图像块 Y_i 与篡改区域不相邻的情况,则 $d_i\sim B(8,P\{\lambda_i=1|Y_i\in H_1\})$.所以对于 $Y_i\in H_1$ 有,

$$P\{d_i=0|Y_i\in H_1\}=P_{=0}(8,P\{\lambda_i=1|Y_i\in H_1\})=(1-P\{\lambda_i=1|Y_i\in H_1\})^8\tag{28}$$

$$P\{d_i>0|Y_i\in H_1\}=1-(1-P\{\lambda_i=1|Y_i\in H_1\})^8\tag{29}$$

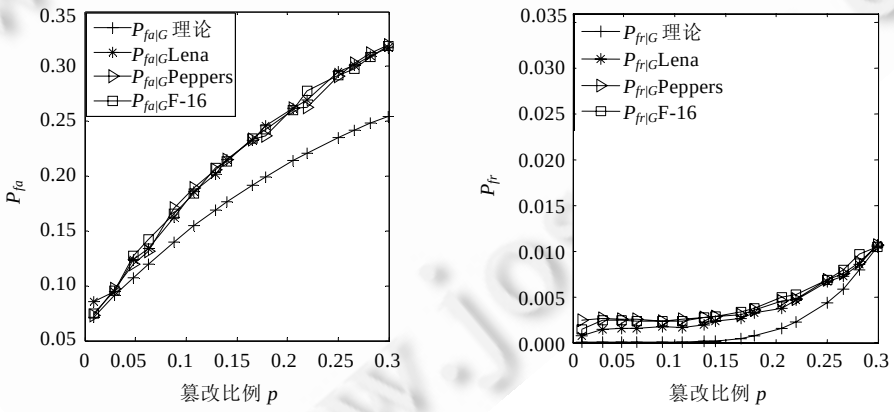
按照第 2.1.1 节对 $\max(d_{i'})$分布的分析,可得 $\max(d_{i'})\sim B(8,P\{\lambda_i=1|Y_i\in H_0\})$,则

$$P\{d_i<\max(d_{i'})|Y_i\in H_1\}=P_<(8,P\{\lambda_i=1|Y_i\in H_1\},P\{\lambda_i=1|Y_i\in H_0\})\tag{30}$$

$$P\{d_i\geqslant\max(d_{i'})|Y_i\in H_1\}=1-P\{d_i<\max(d_{i'})|Y_i\in H_1\}=1-P_<(8,P\{\lambda_i=1|Y_i\in H_1\},P\{\lambda_i=1|Y_i\in H_0\})\tag{31}$$

将公式(21)、公式(29)、公式(31)代入公式(16),即可求得一般篡改下的虚警率 $P_{fr|G}$.

为验证理论推导的正确性,分别以 Lena,Peppers 和 F-16 等 3 幅图像为测试图像,在量化因子为 70、h 为 18 时分别生成它们的含水印图像.随机选取不同大小的正方形区域对含水印图像进行不同比例的篡改,在 JPEG 压缩因子为 80 的条件下对篡改图像进行篡改检测.结合原始图像、篡改图像和检测结果统计出 N_T,N_{TD},N_{VD} 和 N 的值,根据公式(9)和公式(10)计算实验统计的漏/虚警率,如图 2 所示.其中,$P_{fa|G}$Lena,$P_{fa|G}$Peppers,$P_{fa|G}$F-16 分别为一般篡改下,被测图像 Lena,Peppers 和 F-16 得到的 P_{fa} 实验统计曲线;$P_{fr|G}$Lena,$P_{fr|G}$Peppers,$P_{fr|G}$F-16 为一般篡改下,被测图像 Lena,Peppers 和 F-16 得到的 P_{fr} 实验统计曲线.同时,根据被测图像的统计值 N_T 和 N,可计算得到篡改比例 $p=N_T/N$.根据公式(19)、公式(25)、公式(27)和公式(21)、公式(29)、公式(31),即可分别计算出被测图像中篡改块和真实块的 3 个概率 $P\{\lambda_i=1\}$,$P\{d_i>0\}$和 $P\{d_i\geqslant\max(d_{i'})\}$的值.将其代入公式(15)和公式(16),计算出特定篡改比例下漏/虚警率理论值.图 2 中的 $P_{fa|G}$ 理论和 $P_{fr|G}$ 理论分别是一般篡改下 P_{fa} 和 P_{fr} 理论曲线.理论推导过程中没有考虑篡改区域边界,所以理论值略小于实际值.实验结果也验证了理论推导的正确性.



(a) 一般篡改下的 P_{fa} (b) 一般篡改下的 P_{fr}

Fig.2 Theoretical and experimental detection results under general tampering

图 2 一般篡改下,检测性能的理论值和实验值

2.2 拼贴攻击

拼贴攻击首先由相同密钥和相同算法生成的大小相同的两幅含水印图像,然后将其中一幅含水印图像的

某一区域替换另一幅含水印图像的相同位置区域得到拼贴攻击图像.

根据拼贴攻击的特点得出:由篡改图像块重构的每比特水印发生变化的概率为 1/2,真实块重构的水印不发生变化.因此,

$$\begin{cases} P\{w_{ik}^{*}=w'_{ik}\mid (Y_i\in H_0\cap Y_{i'}\in H_0)\cup (Y_i\in H_1\cap Y_{i'}\in H_1)\}=1 \\ P\{w_{ik}^{*}=w'_{ik}\mid (Y_i\in H_1\cap Y_{i'}\in H_0)\cup (Y_i\in H_0\cap Y_{i'}\in H_1)\}=1/2 \end{cases} \tag{32}$$

其中,$i'=a_{ik}(k=1,2,3,4)$.

所以,在拼贴攻击下,

$$\begin{aligned} &P\{\lambda_i=1\mid Y_i\in H_0\}=1-P\{\lambda_i=0\mid Y_i\in H_0\}= \\ &1-\sum_{\beta=0}^{4}P_{=\beta}(4,P\{w_{ik}^{*}=w'_{ik}\mid (Y_i\in H_1\cap Y_{i'}\in H_0)\cup (Y_i\in H_0\cap Y_{i'}\in H_1)\})(P\{Y_{i'}\in H_0\})^{\beta} \end{aligned} \tag{33}$$

$$\begin{aligned} &P\{\lambda_i=1\mid Y_i\in H_1\}=1-P\{\lambda_i=0\mid Y_i\in H_1\}= \\ &1-P_{=0}(4,P\{Y_{i'}\in H_0\})[P\{w_{ik}^{*}=w'_{ik}\mid (Y_i\in H_0\cap Y_{i'}\in H_0)\cup (Y_i\in H_1\cap Y_{i'}\in H_1)\}]^4- \\ &\sum_{\beta=1}^{4}P_{=\beta}(4,P\{Y_{i'}\in H_0\})[P\{w_{ik}^{*}=w'_{ik}\mid (Y_i\in H_1\cap Y_{i'}\in H_0)\cup (Y_i\in H_0\cap Y_{i'}\in H_1)\}]^{\beta} \end{aligned} \tag{34}$$

2.2.1 漏警率

为简便起见,忽略被测图像块 Y_i 及其水印嵌入块 $Y_{i'}$ 位于篡改区域边界的情形.

当 $Y_i\in H_0$ 时,$d_i\sim B(8,P\{\lambda_i=1|Y_i\in H_0\})$,所以,

$$P\{d_i=0|Y_i\in H_0\}=P_{=0}(8,P\{\lambda_i=1|Y_i\in H_0\})=(1-P\{\lambda_i=1|Y_i\in H_0\})^8 \tag{35}$$

$$P\{d_i>0|Y_i\in H_0\}=1-(1-P\{\lambda_i=1|Y_i\in H_0\})^8 \tag{36}$$

拼贴攻击下,对于水印嵌入块 $Y_{i'}$ 的邻域不一致块数 $d_{i'}$,有

$$d_{i'}\sim\begin{cases} B(8,P\{\lambda_i=1\mid Y_{i'}\in H_0\})=B(8,P\{\lambda_i=1\mid Y_i\in H_0\}),\ \text{if } Y_{i'}\in H_0 \\ B(8,P\{\lambda_i=1\mid Y_{i'}\in H_1\})=B(8,P\{\lambda_i=1\mid Y_i\in H_1\}),\ \text{if } Y_{i'}\in H_1 \end{cases} \tag{37}$$

比较拼贴攻击下不同篡改比例时的 $P\{\lambda_i=1|Y_i\in H_0\}$ 和 $P\{\lambda_i=1|Y_i\in H_1\}$ 可知,$P\{\lambda_i=1|Y_i\in H_0\}>P\{\lambda_i=1|Y_i\in H_1\}$.根据二项分布的期望值,$d_{i'}\sim B(8,P\{\lambda_i=1|Y_i\in H_0\})$ 的期望值要大于 $d_{i'}\sim B(8,P\{\lambda_i=1|Y_i\in H_1\})$ 的期望值.所以,当 4 个水印嵌入块中既有篡改块又有真实块时,可以近似认为 $\max(d_{i'})\sim B(8,P\{\lambda_i=1|Y_i\in H_0\})$;若 4 个水印嵌入块均为真实块或均为篡改块时,可以认为 $\max(d_{i'})\sim B(8,P\{\lambda_i=1|Y_i\in H_1\})$ 或 $\max(d_{i'})\sim B(8,P\{\lambda_i=1|Y_i\in H_0\})$.因此,

$$\begin{aligned} &P\{d_i\geqslant\max(d_{i'})\mid Y_i\in H_0\}=1-P\{d_i<\max(d_{i'})\mid Y_i\in H_0\}= \\ &1-[1-(1-p)^4]P_{<}(8,P\{\lambda_i=1\mid Y_i\in H_0\},P\{\lambda_i=1\mid Y_i\in H_0\})-(1-p)^4P_{<}(8,P\{\lambda_i=1\mid Y_i\in H_0\},P\{\lambda_i=1\mid Y_i\in H_1\}) \end{aligned} \tag{38}$$

将公式(33)、公式(36)、公式(38)代入公式(15),即可求得拼贴攻击下的漏警率 $P_{fa|C}$.

2.2.2 虚警率

由以上分析可得,虚警率时:

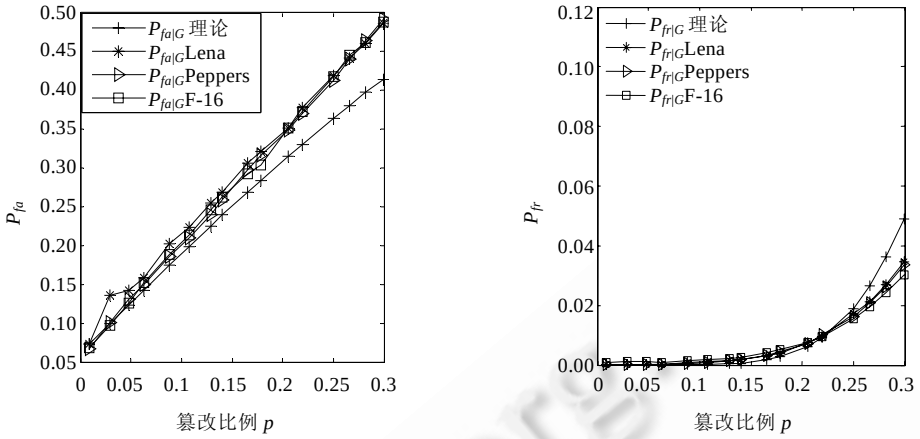
$$P\{d_i>0|Y_i\in H_1\}=1-(1-P\{\lambda_i=1|Y_i\in H_1\})^8 \tag{39}$$

$$P\{d_i\geqslant\max(d_{i'})|Y_i\in H_1\}=1-P\{d_i<\max(d_{i'})|Y_i\in H_1\}=1-P_{<}(8,P\{\lambda_i=1|Y_i\in H_1\},P\{\lambda_i=1|Y_i\in H_0\}) \tag{40}$$

将公式(34)、公式(39)、公式(40)代入公式(16),即可求得拼贴攻击下的虚警率 $P_{fr|C}$.

为验证理论推导的正确性,分别以 Lena,Peppers 和 F-16 这 3 幅图像为测试图像,在量化因子为 70、h 为 18 时分别生成它们的含水印图像.随机选取不同大小的正方形区域对含水印图像进行不同比例的篡改,在 JPEG 压缩因子为 80 的条件下对篡改图像进行篡改检测.结合原始图像、篡改图像和检测结果统计出 N_T,N_{TD},N_{VD} 和 N 的值.根据公式(9)和公式(10)计算实验统计的漏/虚警率,如图 3 所示.其中,$P_{fa|C}$Lena,$P_{fa|C}$Peppers,$P_{fa|C}$F-16 分别为拼贴攻击下,被测图像 Lena,Peppers 和 F-16 得到的 P_{fa} 实验统计曲线;$P_{fr|C}$Lena,$P_{fr|C}$Peppers,$P_{fr|C}$F-16 为拼贴攻击下,被测图像 Lena,Peppers 和 F-16 得到的 P_{fr} 实验统计曲线.同时,根据被测图像的统计值 N_T 和 N,可计算得到篡改比例 $p=N_T/N$.根据公式(33)、公式(36)、公式(38)和公式(34)、公式(39)、公式(40),即可分别计算出被测图像中篡改块和真实块的 3 个概率 $P\{\lambda_i=1\}$,$P\{d_i>0\}$ 和 $P\{d_i\geqslant\max(d_{i'})\}$ 的值.将其代入公式(15)和公式(16),计算出

特定篡改比例下漏/虚警率理论值.图 3 中的 $P_{fa|C}$ 理论和 $P_{fr|C}$ 理论分别是拼贴攻击下 P_{fa} 和 P_{fr} 理论曲线.理论推导过程中没有考虑篡改区域边界,所以理论值略小于实际值.实验结果也验证了理论推导的正确性.



(a) 拼贴攻击下的 P_{fa} (b) 拼贴攻击下的 P_{fr}

Fig.3 Theoretical and experimental detection results under collage attack

图 3 拼贴攻击下篡改检测性能理论值和实验值

3 性能比较

本节从篡改检测性能和不可见性两方面分别比较本文算法和现有算法的性能.为公平起见,本文和参与对比的文献都采用相同的水印容量,本文和文献[11]嵌入水印时均采用相同的量化因子和保护系数个数.仿真实验中,本文、文献[11]和文献[3]的水印容量均为 0.0625 bpp (bit per pixel),本文和文献[11]嵌入水印时均采用 70 的量化因子和保护前 22 个系数,文献[3]中嵌入阈值 g=1.

3.1 篡改检测性能

为比较本文算法与现有同类算法的篡改检测性能,利用误检率[13]P_{fd} 评估算法的篡改检测性能,其计算公式见公式(11).

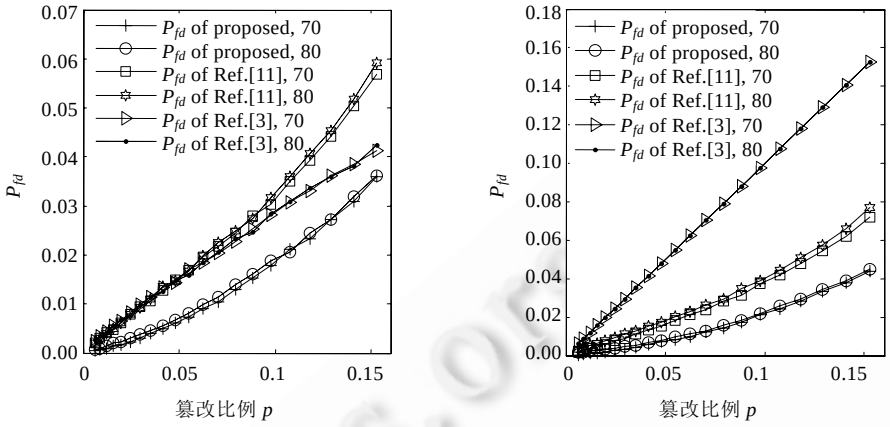
分别利用本文、文献[11]和文献[3]的算法生成含水印图像,对含水印图像进行相同方式、相同比例的篡改,利用原始图像、篡改图像和检测结果得到 N_T,N_{TD},N_{VD} 和 N,从而利用公式(11)计算 P_{fd},最后得到本文算法、文献[11]和文献[3]的误检率统计结果如图 4 所示.其中,每条曲线名称中的 70,80 分别表示含水印图像在 JPEG 压缩因子为 70,80 的条件下对篡改图像进行篡改检测.

图 4(a)是一般篡改下的篡改检测统计结果.由图 4(a)看出:3 种算法均能检测出此类篡改;且随着篡改比例的增大,3 种算法的误检率均增大,而本文算法的误检率最低.不同篡改比例时,本文算法的误检率均优于文献[11]和文献[3].图 4(b)是拼贴攻击下的篡改检测统计结果.由于文献[3]不能检测出拼贴攻击,其漏警率为 1,虚警率为 0,所以根据公式(11)可知,其误检率与篡改比例相等,如图 4(b)中右三角实线、点虚线所示.本文算法和文献[11]均能检测出拼贴攻击,随着篡改比例的增大,两种算法的误检率也随之增大.但是本文算法的误检率要小于文献[11],因此拼贴攻击下,不同篡改比例时,本文算法的篡改检测性能均优于文献[11]和文献[3].

单篡改区域下,本文算法在保证安全性的前提下,利用相同的水印容量提高了篡改检测性能.下面,图 5 以 Lena 图像为例给出多种攻击、多篡改区域条件下的篡改检测比较结果.图 5(a)为原始图像;图 5(b)为含水印图像;图 5(c)为篡改图像,篡改比例约为 13%,包括一般篡改和拼贴攻击区域.其中,一般篡改区域为将 Lena 图像右上角斜放木板截取一部分粘贴到 Lena 帽子上部(区域 1);将 Lena 帽子上的头花复制粘贴到帽子的另一部位(区域 2);将 Peppers 图像中的一个辣椒复制粘贴到 Lena 图像的左下角(区域 3),拼贴攻击区域为将基于相同算法相

同密钥生成大小相同的含水印 Peppers 图像的右下角长方形区域(293:512,425:512)粘贴到含水印 Lena 图像的相同位置(区域 4).

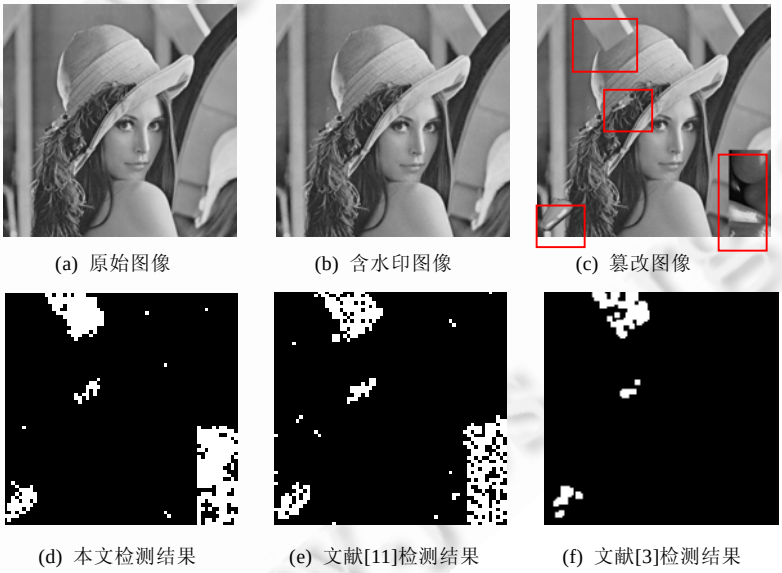
图 5(d)~图 5(f)分别为本文、文献[11]和文献[3]的篡改检测结果,其中,白色点为检测出的篡改区域.由图 5 可以看出,图 5(d)篡改区域内的白色点多于图 5(e)和图 5(f);而图 5(d)篡改区域外的白色点少于图 5(e)和图 5(f),且图 5(f)没有检测出拼贴区域 4.



(a) 一般篡改下的 P_{fd} (b) 拼贴攻击下的 P_{fd}

Fig.4 P_{fd} of proposed, Ref.[3] and Ref.[11] under different types of tampering

图 4 不同篡改方式下,本文、文献[3]和文献[11]的 P_{fd}



(a) 原始图像 (b) 含水印图像 (c) 篡改图像

(d) 本文检测结果 (e) 文献[11]检测结果 (f) 文献[3]检测结果

Fig.5 Detection results under different attacks and different tampered regions

图 5 多种攻击、多篡改区域的篡改检测结果

根据原始图像、篡改图像和检测结果计算得出,本文、文献[11]和文献[3]的漏警率分别为 0.25,0.292,0.752,虚警率分别为 0.004,0.012,0.002;由公式(11)计算得到的误检率分别为 3.59%,4.83%,9.48%.由于文献[3]没有引入图像块之间的相关性,不能抵抗拼贴攻击,因此文献[3]的漏警率较高,且利用形态学操作对定位结果处理,存

在较低的虚警率;而文献[11]只利用图像块的九邻域块的水印不一致性来判断图像块的真实性,其虚警率较高.本文算法利用图像块及其水印嵌入块的邻域块特性定位篡改区域,漏警/误检率均低于文献[11]和文献[3].因此,在一般篡改、拼贴攻击和多攻击、多篡改区域下,利用相同水印容量本文算法的篡改检测性能均优于文献[11]和文献[3].

3.2 不可见性

DCT 域中水印嵌入位置不但影响水印的稳健性,还影响水印的不可见性[14].图 6 给出了 JPEG 压缩因子为 50 的量化表,其他量化因子的量化步长与图 6 的值呈线性关系[15].由图 6 可知,第 2、第 3、第 5、第 6 个系数(深色阴影部分所示)对应的量化步长分别为 11,12,12,10,量化步长最小.若量化 DCT 系数变化量相同,反量化引入的失真较小.所以,本文选择图像块的第 2、第 3、第 5、第 6 个系数作为水印嵌入位置.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

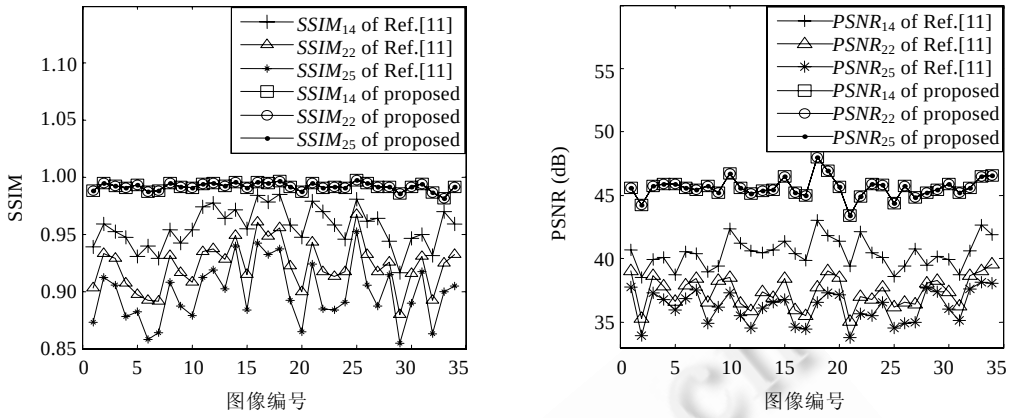
Fig.6 Quantization table corresponding to quality factor 50

图 6 量化因子为 50 的量化表

为考察不同水印嵌入位置对不可见性的影响,取 34 幅不同结构的图像分别采用本文和文献[11]在不同保护系数个数时嵌入水印,并采用基于 HVS(Human visual system)的度量标准 SSIM(structural similarity)[16]和 PSNR(peak signal to noise ratio,峰值信噪比)评估水印的不可见性,实验统计结果如图 7 所示.其中,$SSIM_{14}$ of proposed,$SSIM_{22}$ of proposed,$SSIM_{25}$ of proposed 表示待保护系数个数为 14,22,25 时,本文算法的 SSIM 曲线;$SSIM_{14}$ of Ref.[11],$SSIM_{22}$ of Ref.[11],$SSIM_{25}$ of Ref.[11]表示待保护系数个数为 14,22,25 时,文献[11]的 SSIM 曲线.$SSIM(\in[0,1])$越接近于 1,水印的不可见性越好.$PSNR_{14}$ of proposed,$PSNR_{22}$ of proposed,$PSNR_{25}$ of proposed 表示待保护系数个数为 14,22,25 时,本文算法的 PSNR 曲线;$PSNR_{14}$ of Ref.[11],$PSNR_{22}$ of Ref.[11],$PSNR_{25}$ of Ref.[11]表示待保护系数个数为 14,22,25 时,文献[11]的 PSNR 曲线.PSNR 值越高,含水印图像的不可见性越好.

由图 7(a)可以看出,随着待保护 DCT 系数个数的增加,本文算法的 SSIM 曲线保持不变,且 $SSIM(\in[0.9820, 0.9979])$值较高;文献[11]的 SSIM 随着待保护 DCT 系数个数的增加而逐步减小,且 SSIM 值较低.由图 7(b)也可以看出:随着待保护 DCT 系数个数的增加,本文算法的 PSNR 曲线保持不变,且 PSNR 值较高;文献[11]的 *PSNR* 随着待保护 DCT 系数个数的增加而逐步减小,且 PSNR 值较低.这是因为随着待保护 DCT 系数个数的增大,水印嵌入位置越靠后,相应量化步长较大,则水印嵌入引起的失真更大.所以,文献[11]存在待保护 DCT 系数个数与不可见性之间的矛盾.而本文算法的水印嵌入位置不再依赖于保护系数个数,而是固定嵌入在第 2、第 3、第 5、第 6 个 DCT 系数的 LSB,保证了较好的不可见性.所以,本文算法解决了待保护 DCT 系数个数与不可见性之间的矛盾,且相同容量下引入的失真较少,改善了水印的不可见性.

由图 4、图 5、图 7 的仿真和统计结果可以看出,本文算法检测时,比较图像块与其水印嵌入块的 8 邻域中不一致图像块个数来判定图像块的真实性,提高了算法的篡改检测性能;将基于图像块保护系数生成的水印固定嵌入在量化步长较小 DCT 系数的 LSB,不仅解决了保护系数个数与不可见性的矛盾,还改善了水印的不可见性.



(a) 本文和文献[11]的 SSIM (b) 本文和文献[11]的 PSNR

Fig.7 Invisibility of proposed and Ref.[11] with different embedding positions

图 7 不同嵌入位置时,本文和文献[11]的不可见性

4 结束语

JPEG 图像脆弱水印算法中,虽然引入图像块之间的随机相关性能有效抵抗拼贴攻击,但也使篡改检测变得相对困难.本文从提高认证水印算法的篡改检测性能和降低水印嵌入引起的图像失真出发,提出了一种高定位精度且抗拼贴攻击的 JPEG 脆弱水印算法.该算法基于图像块的重要 DCT 系数和密钥生成 4 比特水印信息,随机嵌入到其他图像块量化步长较小量化 DCT 系数的最低有效位,通过比较图像块与其水印嵌入块的 8 邻域中不一致图像块个数来判定图像块的真实性.推导给出本文检测算法在一般篡改和拼贴攻击下的虚/漏警率,并用统计实验验证了推导的正确性.理论分析和实验结果表明,通过邻域比较判定图像块的真实性,能够提高块随机相关认证水印算法的篡改检测性能,将水印嵌入在量化步长较小的量化 DCT 的最低有效位,改善了含水印图像的不可见性,解决了待保护 DCT 系数的个数与不可见性之间的矛盾.下一步的工作是将算法推广到彩色图像中,并研究如何提高篡改区域边界的篡改检测性能.

References:

[1] Zhu BB, Swanson MD, Tewfix AH. When seeing isn't believing. IEEE Signal Processing, 2004,21(2):40−49. [doi: 10.1109/MSP.2004.1276112]

[2] Haouzia A, Noumeir R. Methods for image authentication: A survey. Multimedia Tools and Applications, 2008,39(1):1−46. [doi: 10.1007/s11042-007-0154-3]

[3] Li C, Huang JW. A semi-fragile image watermarking resisting to JPEG. Journal of Software, 2006,17(2):315−324 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/315.htm [doi: 10.1360/jos170315]

[4] Huo YR, Chen F, He HJ, Yin ZK. A digital image authentication watermarking algorithm combined with compression factor. Journal of Sichuan University (Natural Science Edition), 2010,47(Supplementary Issue 1):112−116 (in Chinese with English abstract).

[5] He HJ, Zhang JS, Chen F. A self-recovery fragile watermarking scheme for image authentication with superior localization. Science in China (Series F—Information Sciences), 2008,51(10):1487−1507. [doi: 10.1007/s11432-008-0094-1]

[6] Zhang XP, Wang SZ, Feng GR. Fragile watermarking scheme with extensive content restoration capability. In: Ho A, Shi Y, Barni M, eds. Proc. of the Int'l Workshop on Digital Watermarking (IWDW 2009). Berlin: Springer-Verlag, 2009. 268−278. [doi: 10.1007/978- 3-642-03688-0_24]

[7] Zhang XP, Wang SZ, Qian ZX, Feng GR. Reversible fragile watermarking for locating tampered blocks in JPEG images. Signal Processing, 2010,90:3026−3036. [doi: 10.1016/j.sigpro.2010.04.027]

[8] Wu, YD, Deng RH. Zero-Error watermarking on JPEG images by shuffling Huffman tree nodes. In: Yang JF, Hang HM, Tanimoto M, Chen T, eds. Proc. of the IEEE Int'l Conf. on Visual Communications and Image Processing (VCIP 2011). New York: IEEE Press, 2011. 1–4. [doi: 10.1109/VCIP.2011.6115939]

[9] Wang HX, Liao CX. JPEG images authentication with discrimination of tampers on the image content or watermark. IETE Technical Review, 2010,27(3):244–251. [doi: 10.4103/0256-4602.62787]

[10] Li CT. Digital fragile watermarking scheme for authentication of JPEG images. IEEE Proc.—Vision, Image and Signal Processing, 2004,151(6):460–466. [doi: 10.1049/ip-vis:20040812]

[11] Yu M, He HJ, Zhang JS. A digital authentication watermarking scheme for JPEG images with superior localization and security. Science in China (Series F—Information Sciences), 2007,50(3):491–509. [doi: 10.1007/s11432-007-0024-7]

[12] Fridrich J, Goljan M, Memon N. Cryptanalysis of the Yeung-Mintzer fragile watermarking technique. Electronic Imaging, 2002, 11(4):262–274. [doi: 10.1117/1.1459449]

[13] He HJ. Digital Image secure authentication watermarking algorithm and their performance analysis of statistical detection [Ph.D. Thesis]. Chengdu: Southwest Jiaotong University, 2009 (in Chinese with English abstract).

[14] Huang JW, Shi YQ, Cheng WD. Image watermarking in DCT: An embedding strategy and algorithm. Acta Electronica Sinca, 2000, 28(4):57–60 (in Chinese with English abstract).

[15] Yu M. Research on digital fragile watermarking scheme for authentication of JPEG images [MS. Thesis]. Chengdu: Southwest Jiaotong University, 2007 (in Chinese with English abstract).

[16] Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. Image quality assessment: From error visibility to structural similarity. IEEE Trans. on Image Processing, 2004,13(4):600–612. [doi: 10.1109/TIP.2003.819861]

附中文参考文献:

[3] 李春,黄继武.一种抗 JPEG 压缩的半脆弱图像水印算法.软件学报,2006,17(2):315−324. http://www.jos.org.cn/1000-9825/17/315.htm [doi: 10.1360/jos170315]

[4] 霍耀冉,陈帆,和红杰,尹忠科.结合压缩因子的数字图像认证水印算法.四川大学学报(自然科学版),2010,47(增刊 1):112−116.

[13] 和红杰.数字图像安全认证水印算法及其统计检测性能分析[博士学位论文].成都:西南交通大学,2009.

[14] 黄继武,Shi YQ,程卫东.DCT 域图像水印:嵌入对策和算法.电子学报,2000,28(4):57−60.

[15] 余淼.用于 JPEG 图像认证的数字水印算法研究[硕士学位论文].成都:西南交通大学,2007.

霍耀冉(1987－),男,河南民权人,硕士生,主要研究领域为数字水印,图像处理.

陈帆(1971－),男,副教授,主要研究领域为网络技术,信息安全.

和红杰(1971－),女,博士,副教授,CCF 会员,主要研究领域为图像处理,信息隐藏.