用于图像认证的半脆弱数字水印的设计与实现①

Design and Implementation of Semi-Fragile Watermark for Image Authentication

尹　柳　(桂林电子科技大学 计算科学与数学学院 广西 桂林 541004)
易招师　(桂林电子科技大学 信息与通信学院 广西 桂林 541004)
陈光喜　(桂林电子科技大学 计算科学与数学学院 广西 桂林 541004)

摘　要： 为了更好地实现半脆弱水印,避免对图像变换造成的舍入误差，采用整数提升小波变换技术对图像进行小波变换。并根据人眼视觉特性设计量化步长，自适应的嵌入水印以提高水印的不可见性和相应的鲁棒性。并设计了半脆弱水印的篡改认证和定位的方案。实验结果表明水印具有良好的不可见性，能较好的实现图像认证。

关键词： 整数提升小波变换 混沌加密 自适应量化 图像认证 半脆弱

1　引言

随着计算机网络的普及和多媒体技术的迅猛发展，数字产品(图像、文本、音频、视频等)的安全问题、盗版问题和版权纠纷愈发成为严重的社会问题。因此，对数字产品的版权保护和认证迫在眉睫。数字水印技术应运而生，它与信息安全、信息隐藏、数据加密等均密切相关。目前应用于图像认证水印技术的研究相对较少。所谓图像认证 ，指能有效检测对图像数据的修改。脆弱水印用于精确认证，它对图像内容进行完全保护，图像的任何修改都视为非法；而半脆弱水印用于选择性认证，它同时具有鲁棒水印和脆弱水印的特性，要求能容忍一定程度的某些常规信号处理，而对恶意篡改具有脆弱性。考虑到实际应用中，数字图像数据量大，需要以压缩的方式存储及传输，且最终用户需要的通常是经过压缩或其它保持图像内容的操作处理后的图像，因此半脆弱水印技术具有更重要的应用价值。针对量化水印的均匀量化和篡改定位问题，本文设计了一种用于图像认证的自适应量化的半脆弱水印方案。

2　嵌入策略

由于小波变换良好的空间－频率局部特性和与人眼视觉特性相符的变换机制，在新一代静止图像压缩标准(JPEG 2000)和运动图像压缩标准 MPEG-4 中占据了重要位置。因此研究 DWT(discrete wavelet transform)域水印算法具有十分良好的前景。小波变换是将信号分成低频和高频信息。低频部分集中了信号的大部分能量，高频部分集中了信号的大部分细节。对低频部分进行多级分解，分出更低频率的低频信号和高频信号，从而实现多分辨率分析。小波变换还能很好的进行空间到频率的定位。考虑到整数提升小波[1]比传统小波运算复杂度低，时间快，占内存少(见表 1[2])，本文采用有利于图像变换的 harr 小波基对图像进行整数提升小波变换。

为了使水印嵌入后的图像达到很好的不可见性，同时使其具备一定程度的脆弱性(这里的一定程度指能抵抗一些常规的图像处理操作，如压缩、亮度增强等)。就需要根据小波系数的幅值自适应量化修改。现有图像水印嵌入方案[3,4]普遍采用了均匀量化策略，即对整幅图像采用一个相同的量化步长 q。如果 q 取

① 基金项目:国家自然科学基金项目(10501009,10661005);广西教育厅科研项目(200807LX112)
收稿时间:2008-09-24

表 1　DWT 变换和提升变换处理时间比较

小波(%)	三级 DWT 变换	三级提升变换	提高速度
Haar	0.3208	0.1720	47.56
db2	0.3600	0.2180	39.44
db4	0.3910	0.3430	12.28
9/7	0.4220	0.2970	29.63

值较小，则会影响水印的抗攻击性；而如果 q 取值较大，会给图像质量带来较大影响。选取确定量化步长 q 应充分考虑图像自身特点和人眼视觉特性。水印的嵌入过程可以看作是在载体图像叠加噪声[5]。图像的高频系数从小到大分别对应了空域上的平滑区域、纹理区域、边缘区域，从而具有了不同的噪声掩蔽性。同一邻域内纹理越复杂，对噪声的掩蔽性就越大。基于人眼视觉特性知，人眼对于纹理复杂区域不敏感，故可采取较大量化。对于同一子带内部的各个系数的重要性来说，系数的模代表了能量的大小，并且反映了该位置的纹理特征。因此可以用相同分解级的其它几个子带相同位置的小波系数块来预测该系数上嵌入的量化步长 q 值[6]。为了实现认证的灵活性，本文设计了灵敏性参数(取值可作为密钥 1)，以便用户可以根据需要通过设置灵敏性参数来实现图像的不同灵敏度等级的认证。

$$q(i,j) = a \times ln \frac{\Sigma\left|f_L^{LH}\right| + \Sigma\left|f_L^{HH}\right|}{2} \qquad (1)$$

式中(i,j)表示所选子块位置，L 为小波分解级数，f_L^{LH}、f_L^{HH} 为子带 LH、HH 对应的子块小波系数。

3　数字水印嵌入

3.1　水印的混沌加密

设数字水印是一副 m×n 的二值图像 W。为了消除二值水印图像的像素空间相关性，加强数字水印的安全性，在水印嵌入前对其进行置乱加密。目前被广泛应用研究的混沌序列，具有对初值敏感性高，安全性强，有普通伪随机序列没有的低通性，以抵抗 JPEG 压缩。本文采用 Logistic 映射，即 $s_{i+1}=\mu s_i(1-s_i)$ $s_0 \in (0,1)$，$\mu \in [1,4]$，$i=0,1,2,\cdots$当 μ 取接近 4 的实数时，系统处于混沌状态。由 Logistic 映射生成的混沌序列转化为二值序列，并升维成二维掩蔽模板:key={key(i,j)(0,1),i=1,2,…m,j=1,2,…n}。

3.2　水印嵌入算法的具体步骤

① 对载体图像做 L 级整数提升小波变换；

② 根据经过 key 调制的水印的大小把 HL 子带分成 $\frac{M}{2^L \times m} \times \frac{N}{2^L \times n}$ 大小的子块($M \times N$ 为载体图像的大小，$m \times n$ 表示水印 W_t 的大小，L 表示小波分解级数)，即每小块嵌入 1 比特水印信息。根据公式(1)计算每子块的量化步长 q；

③ 在每个子块中任意选取一个系数(作为密钥 2)，用 q(i,j)量化，并根据量化结果 $Q(f_L^{HL})$ 把系数调整到区间中心，这样该水印比特具备了一定的抗干扰能力，确保水印数据被正确检测出来。首先定义量化函数：

定义 1．定义量化函数 $Q(f)$，将小波系数映射到集合{0，1}，

$$Q(f) = \begin{cases} 0, & rq \le f < (r+1)q, \quad r = 0, \pm 2, \pm 4, \ldots \\ 1, & rq \le f < (r+1)q, \quad r = \pm 1, \pm 3, \pm 5, \ldots \end{cases}$$

具体嵌入规则如下：

IF $Q(f_L^{HL}(i,j)) == W_t(i,j)$

$f_L^{HL}(i,j)' = D\_C + 0.5 * q\ (i,j)$

ELSE

IF $r > q/2$

$f_L^{HL}(i,j)' = D\_C + 1.5 * q\ (i,j)$

ELSE $f_L^{HL}(i,j)' = D\_C - 0.5 * q\ (i,j)$

其中 D_C=floor($f_L^{HL}(i,j) / q$)$*q\ (i,j)$，floor 表示向下取整，$r = f_L^{HL}(i,j) - D\_C$ 。

④ 逆整数提升小波变换，得到含水印信息的图像。

3.3　水印的提取

水印的提取基本上是水印嵌入的逆过程，整个水印提取过程不需要原始图像，具体步骤如下:

① 将含水印图像做 L 级整数提升小波变换；

② 如 2.2 中步骤(2)选取 HL 子带分块，结合密钥 1，计算量化步长 q'

③ 利用密钥 2 选取子块内的系数，根据如下公式提取水印

$W_t'(i,j)=\mathrm{mod}(\mathrm{floor}(f_L^{HL}(i,j)/q'(i,j)),2)$

④ 利用密钥 key 解调 W_t'，即可还原出两个水印。

4　水印的篡改检测与定位分析

为了进行篡改的认证，定义篡改矩阵 G，$G=W\oplus W'$（$\oplus$ 表示异或，W 为原始水印，W' 为从含水印图像中提取的水印)。若 $G(i,j)=0$ 判定该点位置在空域上的对应位置 N×N 子块内容未发生变化；若 $G(i,j)=1$，则判定当前子块内容发生了变化。但直接使用上述篡改矩阵 G 无法区分常规图像处理与恶意篡改。事实上，对于 JPEG 压缩、图像增强和图像滤波等常规处理引起的图像变化是全局性的，即使 G 中出现非零点，这些非零点也是均匀分布在整个 G 矩阵中；而恶意篡改常常带有一定的目的性，通常是对图像某些局部内容的篡改，这种篡改必将引起中出现集 G 中分布的非零点。根据 G 求解图像全局比特错误率 TAF：

$$\mathrm{TAF}=\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}G(i,j)}{m\times n}$$

然后考查 G 中一个包含多点(如 8×8 点)的局部，计算该局部的比特错误率 TAF_1（该局部 G 取值为 1 的点数/该局部的总点数)。如果 $TAF_1>T\times TAF$，认为该区域内的篡改为恶意篡改，对该局部的 G 值不作处理；否则，认为该局部的变化为常规处理改变，将该局部的 G 值改为 0。T 为通过实验得到的一个阈值。设修正后的篡改矩阵为 G_1，然后按照 G_1 对图像重新认证。若 $G_1(i,j)=0$，图像的第(i,j)个 N×N 子块认证通过；否则，判定该 N×N 子块发生了篡改。据此可以将发生篡改的子块标记出来。因此有效地区分了一般常规图像处理与恶意篡改，并解决了篡改定位问题。按照预处理后的篡改矩阵 G_1 计算比特错误率 TAF，若 TAF=0，则整个图像内容认证通过；若 TAF>0，判定图像内容发生了恶意篡改，TAF 值越大，篡改程度越大。

5　实验结果与分析

实验以 256×256 的灰度图像为载体图像(如图 1)，提取的水印与原水印的相似性用归一化互相关数 NC 来度量，$NC=\frac{\sum_{m,n}W_{m,n}\times W'_{m,n}}{\sum_{m,n}W_{m,n}^2}$ 式中 W 表示原始水印，W' 表示提取的水印。由于 haar 小波的优良特性适合图像，本文采用 haar 整数提升小波，分解层数 L=3，水印嵌入到第二层 HL 子带。下面以 baboon 载体图像为例，给出实验结果。

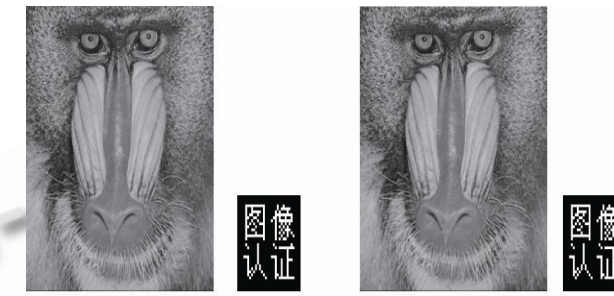


图 1 载体图像和原始水印　图 2 含水印图像和提取的水印

含水印图像的峰值信噪比(PSNR)达到了 45.99dB，从含水印图像提取的水印图像的 NC 值为 1(如图 2)。可见，本文提出的水印方法的峰值信噪比明显优于文献[3]，嵌入的水印具有很好的透明性。不经过攻击，对图 2 直接进行水印检测和认证，可以得到 TAF=0。

为了测试对一些常规图像处理的鲁棒性，使用 JPEG 压缩、叠加噪声和亮度增强等常规操作对水印进行处理，实验结果如图 3。

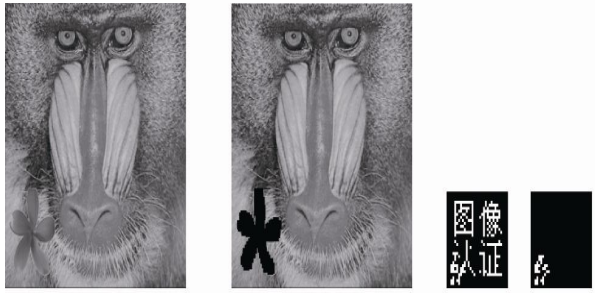
(a)　(b)　(c)　(d)　(e)　(f)　(g)

图 3　经常规图像处理后提取的部分水印图像

(a)JPEG 压缩，品质因子为 90,NC=0.986
(b)JPEG 压缩，品质因子为 80,NC=0.948
(c)JPEG 压缩，品质因子为 70,NC=0.888
(d)加入 0.3%的椒盐噪声，NC=0.946
(e)加入 1%的椒盐噪声，NC=0.837
(f)亮度增强 40%，MC=1.000
(g)亮度增强 50%，NC=1.000

从实验中可以得出，本算法能够抵抗某种程度的常规图像处理，具备一定的鲁棒性，同时对图像叠加噪声的实验也证明了本算法对噪声有一定的容忍度。

为了说明本算法的脆弱性，并进行篡改认证，首先在含水印图像中添加物体，再进行 50%的 JPEG 压缩。篡改检测矩阵预处理阈值 T=3.5。图 4(a)为篡改图像，图 4(b)为定位出的篡改图像，图 4(c)、(d)分别为由图 4(a)提取的水印和篡改检测矩阵。



(a) (b) (c) (d)

图 4 篡改检测与定位

6 结束语

本文提出的用于图像认证的半脆弱数字水印方案，考虑人眼视觉特性，采用自适应量化，提高了不可见性，用户可根据需要调节灵敏度参数来实现不同程度的认证，在保护数字图像版权的同时，有效地区分常规图像处理和恶意篡改，并解决了篡改定位问题。

参考文献

1 SWELDENSW. The Lifting Scheme: A Construction of Second Generation Wavelets. SIAMJ Math Anal, 1997, 29:511 − 546.

2 杨娟,杨丹,雷明,等.基于二代小波和图像置乱的数字图像盲水印算法.计算机应用, 2007,27(2):295 − 298.

3 Kundur D, Hatzinakos D. Digital Watermarking for Telltale Tamper Proofing and Authentication. Proceedings of the IEEE, 1999,87 (7):1167 − 1180.

4 Eggers JJ, Girod B. Informed watermarking, the Kluwer international series in engineering and computer science 685. Kluwer A cademic Publishers, Boston, April 2002.

5 Cox IJ, Killian J, Leighton FT. Secure spread spectrum watermarking for multimedia. IEEE Trans on Image Processing, 1997,6(12):1673 − 1687.

6 王向阳,陈利科.一种新的自适应半脆弱水印算法.自