基于小波变换的自适应公钥数字水印

张 洪，刘晓云

(电子科技大学自动化学院 成都 610054)

【摘要】利用小波变换良好的时频局部特性，提出了一种基于小波变换的自适应公钥数字水印设计方案。数据的所有者利用私钥向数据中嵌入版权信息，任何数据使用者可以利用公钥从接收到的数据中提取版权信息。水印的嵌入强度可根据原始图像自身的特点自适应调节，水印的提取也不需要原始图像。实验结果表明该算法具有良好的不可视性和抗联合图像专家组压缩、剪切、滤波等攻击的能力。

关 键 词 公钥数字水印； 小波变换； 公钥； 私钥
中图分类号 TP391 文献标识码 A

A Wavelet Based Adaptive Public Key Watermarking Algorithm

ZHANG Hong，LIU Xiao-yun

(School of Automation Eng., Univ. of Electron. Sci. & Tech. of China Chengdu 610054)

Abstract A wavelet-based adaptive public key watermarking algorithm is presented in the paper. Data owner can use his private key embed the identification into the local image and retrieve it from the watermarked image. The data users can use the public key detect the identification from the watermarked image. How much the embedding strength is adjusted adaptively to the local image characteristics. The experimental results have shown that the proposed watermark is invisible to human eyes and very robust to joint photographic experts group compression attack, crop attack and so on.

Key words public key digital watermark; discrete wavelet transform; private key; public key

1 公钥数字水印

传统的数字水印技术，一般采用对称密钥，即用于水印嵌入和检测的密钥相同。公钥数字水印，又称为非对称数字水印，就是用于水印嵌入的密钥，不同于用于水印检测的密钥。近年来，一些学者在公钥水印算法方面作了不少的研究工作，提出了扩频公钥数字水印、Legendre水印等技术，在文献[1]中对这些方案进行了详细讨论。文献[2]提出了一种基于离散余弦变换(Discrete Cosine Transform，DCT)的扩频公钥数字水印算法，取得了较好的效果。本文借鉴文献[3-4]，提出了一种基于小波变换的自适应扩频公钥数字水印。本算法采用扩频技术，用户用公钥提取的水印信息是某一次嵌入的，即使用户利用公钥破坏或删除了该信息，也并不影响其他位置的水印信息，数据所有者仍可以利用私钥正确提取出其他位置的水印信息。水印的嵌入强度与阈值S密切相关，S的选取依赖于原始图像自身的特点，所以水印的嵌入强度可根据原始图像自身的特点自适应调节。水印的提取也仅依赖于相应的阈值而并不需要原始图像。

2 密钥的构成

2.1 密钥的产生

本文利用logistic映射产生水印系统的密钥，其定义为：

$$x_{k+1} = ux_k(1 - x_k) \tag{1}$$

当$u = 4$，$x \in [0, 1]$时，此映射产生混沌现象。水印的生成过程见文献[2]。下面叙述中的key_1、key_2、key_3分别对应文献[2]中的key_p、key_{in}、key_{DCT}。

2.2 私钥和公钥的选取

由于所使用的密钥都可由key生成，因此将其作为私钥。数据所有者可利用此私钥实现水印信息的嵌入和提取。水印信息是随机且重复嵌入到原始图像中，选择某一次嵌入时嵌入块的索引值key_public作为公钥。由于嵌入水印前对分块进行了随机洗牌，嵌入时又对分块进行随机选择，所以作品使用者不可能利用公钥重构私钥。使用者可以利用此公钥来

收稿日期：2005 - 01 - 29
作者简介：张 洪(1981 –)，女，硕士，主要从事信息安全与数字水印方面的研究.

提取某一次嵌入的水印信息。但即使作品使用者破坏或删除了此位置的水印信息，也不可能影响到其他位置的水印信息，作品所有者仍然可以正确提取出其他位置的水印信息。

3 水印的嵌入和提取

3.1 水印的嵌入

(1) 利用haar小波对原始图像I进行三级小波分解。为了水印同时具有良好的鲁棒性和不可视性，选择DWT变换后图像的中低频系数作为水印信息位的载体。所以利用第二级小波分解的系数CH_2,CV_2,CD_2形成一个新的系数矩阵$\boldsymbol{C}_{mn}$=[CH_2,CV_2, CD_2]，其中m, n分别表示矩阵的行数和列数。(2) 将系数矩阵$\boldsymbol{C}_{mn}$分成n_1块。利用密钥key$_2$生成的整数索引向量Index_sequence对n_1块进行随机洗牌。(3) 水印信息位嵌入位置的选取。在n_1块中，利用密钥key$_3$生成的随机向量Index_chose随机选取n_2个系数块嵌入水印信息。(4) 水印信息的嵌入。设嵌入的水印信息位为W，按(3)确定要嵌入的系数块系数记为$C_i(u,v)$。令$\delta(u,v)=|C_i(u,v)| \bmod S(u,v)$，如果$W(i,j)=0$或$C_i(u,v)\geq 0$，则$C_i(u,v)=C_i(u,v)-\delta(u,v)+T_a(u,v)$。否则，$C_i(u,v)=C_i(u,v)+\delta(u,v)-T_a(u,v)$。如果$W(i,j)=1$或$C_i(u,v)\geq 0$，则$\boldsymbol{C}_i(u,v)=C_i(u,v)-\delta(u,v)+T_b(u,v)$，否则，$C_i(u,v)=C_i(u,v)+C_i(u,v)+\delta(u,v)-T_b(u,v)$。其中$T_a$=$S$/4；$T_b=\frac{3}{4}S$。令$S(u,v)=\alpha(|C_i(u+1,v)|+|C_i(u,v+1)|+|C_i(u+1,v+1)|)$。这样可根据原始图像自身的特点自适应地调节嵌入水印信息的强度。α取值越大，鲁棒性越好；取值越小，不可视性越好。

为了提高水印的鲁棒性，在嵌入过程中引入扩频的概念。设水印是一个长度为b的二值序列，把每一位重复嵌入n_3次，这样每块嵌入水印容量为bn_3，n_2块嵌入的水印容量为bn_3n_2。每块中水印序列重复嵌入4次，设其中一位嵌入在点(u,v)上，则与它相同的重复位嵌入在点$(u+2,v)$，$(u,v+2)$，$(u+2,v+2)$上。

3.2 水印的提取

3.2.1 用私钥提取

(1) 对加入了水印的图像I′进行三级小波分解。用其第二级小波变换系数矩阵CH_2', CV_2', CD_2'构成新的系数矩阵$\boldsymbol{C}'_{mn}$=[CH_2' CV_2' CD_2']，并将其分成n_1块。

(2) 利用私钥生成解调混沌序列，生成随机排列整数索引向量Index_sequence，生成水印嵌入块的随机选择向量Index_chose 。

(3) 确定嵌入了水印序列的系数矩阵块，系数矩阵块中水印信息的提取策略如下：

设嵌入了水印的系数矩阵为$C_i'(u,v)$，利用与3.1中同样的方法计算水印强度$S'(u,v)$。假定检测位置点(u,v)处水印为$W^*(u,v)$，令$\delta'(u,v)=|C_i'(u,v)| \bmod S'(u,v)$。如果$\delta'(u,v)\geq (T_a(u,v)+T_b(u,v))/2$，则$W^*(u,v)=1$，否则$W^*(u,v)=0$。假设$W_i^*(k)$为第$k$ bit的第i次重复，n_3表示在某块中总的嵌入次数，如果$\sum_{i=1}^{n_3}W_i^*(k)\geq n_3/2$，则$W_i^*(k)$=1，否则$W_i^*(k)$=0。

重复以上步骤直到将水印信息全部提出。假设在n_2个块中重复嵌入水印，则最终将得到n_2个版本的水印信息。设W_i'为第i个版本的水印信息，如果$\sum_{i=1}^{n_2}W_i'(k)\geq n_2/2$，则$W'(k)=1$，否则$W'(k)=0$。水印信息的检测采用归一化相关系数。设原水印为$W$，提取的水印为$W'$，则：

$$\rho=\sum_{i=1}^{b}W(i)W'(i)\Big/\left(\sqrt{\sum_{i=1}^{b}(W(i))^2}\sqrt{\sum_{i=1}^{b}(W'(i))^2}\right) \qquad (2)$$

ρ大于等于某一阈值T，说明此图像中含有水印信息。T的具体值根据多次实验决定。

3.2.2 公钥水印的提取

公钥提取水印比私钥简单，根据密钥key_public确定水印信息嵌入的位置，提取方法及后期处理与私钥相同。

4 实验与结论

采用256级灰度、256×256的标准‘lena’图像作为原始图像，随机生成64 bit二值序列作为水印序列，α取值为1。实验结果如图1所示。水印图像从主观视觉上，与原始图像非常一致，达到了水印的不可视性要求。峰值信噪比$PSNR$ = 37.406 2。

a. 原始图像 b. 水印图像

图1 原始图像和水印图像

水印提取阈值经多次实验，公钥提取选为0.6，私钥提取为0.7。实验表明水印的提取能达到很高的准确率。提取结果如图2所示。表1显示了水印图像抗攻击的结果。从攻击实验结果来看，本文算法对线性、非线性滤波、联合图象专家组(Joint Photographic Experts Group，JPEG)压缩、剪切等都具有较强的抵抗力，但对于噪声攻击的抵抗力较差。

表1　水印图像抗攻击实验结果

攻击方法	参数	公钥检测相关值	私钥检测相关值
JPEG压缩	80	0.903 2	0.954 9
	50	0.754 2	0.924 1
	25	0.721 4	0.900 5
滤波	低通滤波	0.705 5	0.950 9
	高斯滤波	0.935 5	0.984 3
剪切	1/4	0.954 9	0.954 9
加噪声	0.005随机噪声	0.737 5	0.720 0

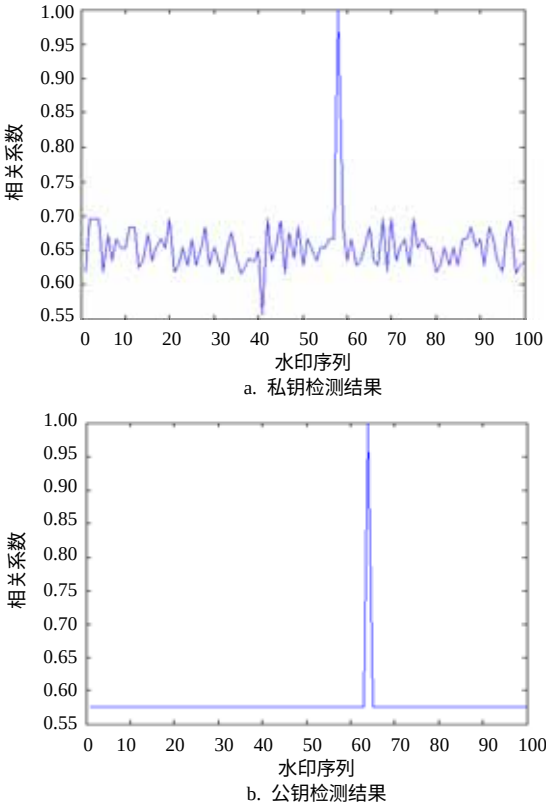

图2　水印检测结果

为了测试私钥的安全性，本文也利用公钥对私钥进行了攻击测试。因为公钥与私钥毫无关系，用公钥重构私钥根本不可能，本文主要是利用公钥删除水印信息。经过这种攻击后，公钥已无法提取水印信息，但私钥提取的水印信息几乎没什么影响。

从实验结果可看出，本文算法具有良好的不可视性、鲁棒性、安全性。总体来看，本文算法具有如下的特点：

(1) 水印强度能根据原始图像自身的特点自适应地进行调节；

(2) 采用扩频公钥算法，具有良好的安全性和鲁棒性；

(3) 水印的提取不需要原始图像。

参　考　文　献

[1] 邹潇湘, 李锦涛, 彭　聪. 非对称数字水印技术研究[J]. 计算机工程与应用, 2002, 16: 7-10.

[2] 孙　鑫, 易开祥, 石教英, 等. 公开钥数字水印系统研究[J]. 计算机辅助设计与图形学报, 2003, 15(7): 875-885.

[3] SHAO Ya-fei, WU Guo-wei, LIN Xing-gang. A wavelte based adaptive watermrking algorithm[C]//Info-Tech and Info-Net, Proceedings, ICII 2001-Beijing 2001 International Conferences on, IEEE 2001, 3(29): 384-389.

[4] TSAI Min-jin, YU Kuang-yao, CHEN Yi-zhang. Joint wavelet and transformation ROR ditital watermarking[J]. Consumer Electronics, IEEE Transactions on, 2000, 46(Issue: 1): 237-241.

本文的研究工作得到了电子科技大学青年科技基金(YF021405)的资助，在此表示感谢！

编　辑　漆　蓉