一种新颖的水印密钥系统*

钟 桦, 焦李成, 刘 芳

(西安电子科技大学 雷达信号处理国家重点实验室,陕西 西安 710071)

E-mail: huazh@rsp.xidian.edu.cn

http://www.rsp.xidian.edu.cn

摘要: 水印技术作为一种有效的信息隐藏方法,发展得非常迅速.大部分水印系统都只具有一把私钥,而且不能公开,但是在某些应用中需要公钥来恢复水印.如何保证公钥的产生不会影响私钥的性能,是水印密钥系统的关键问题.构造了一种水印密钥系统,提出了一种新颖的公钥生成方法.无须原始数据即可利用公钥恢复嵌入的标识符.由于公钥的产生只涉及部分水印信息,从而成功地解决了公钥生成与私钥之间的矛盾.实验结果表明,该系统是安全、有效的.

关键词: 水印;信息隐藏;公钥;私钥;标识符

中图法分类号: TP309 **文献标识码**: A

作为电子数据版权保护的一种有效的技术,近几年水印技术在这一领域的研究发展很快[1~7].水印技术的应用包括版权保护、数据管理与跟踪、数据鉴定等方面.其中版权保护是提出水印这一技术的初始目的.水印系统的密钥分为两种,一种是私钥,由数据所有者保管;另一种是公钥,由数据接收者拥有.以版权或其他说明信息作为水印嵌入,数据所有者利用私钥可以根据嵌入的水印跟踪数据的发行或传播路径.私钥水印恢复必须非常稳定,以保证即使水印数据经历了相当程度的失真以后,数据所有者仍能正确提取数据接收者的标识符.公钥的使用是符合应用需要的[8~10],但是公钥的使用会使得数据接收者:(1) 检测或恢复出水印;(2) 破坏或删除水印;(3) 用相同的公钥嵌入不同的水印信息.这其中既有利又有弊.因此,需要一种安全、有效的密钥系统,既能满足数据接收者和数据所有者的需要,同时又能保证水印系统的有效性和安全性.

本文提出的水印密钥系统可以有效地解决这一问题.不失一般性,我们以图像为例,但是其思想对于其他类型的多媒体数据仍然适用.与文献[8]不同,水印过程在小波域里进行,以提高嵌入水印的稳定性[2],并以用户标识符作为水印,因而更具说明性.公钥水印恢复不需要原始图像,但是又利用了原始数据的信息,从而有效地克服了公钥水印恢复中原始数据不可获得的问题.较之利用滤波的方法来获得原始图像的近似版本的水印算法[8,11],本文的算法更加精确,而且无滤波误差.同时,公钥的生成并不影响私钥水印恢复.实验结果表明,该水印密钥系统是十分有效和实用的.

1 水印系统的设计

1.1 标识符水印及纠错编码

大部分水印技术都是取一个伪随机序列作为水印,利用伪随机序列在自相关和互相关以及安

* 收稿日期: 2000-12-15; 修改日期: 2001-04-18

基金项目: 国家自然科学基金资助项目(60073053);国家教育部博士点基金资助项目

作者简介: 钟桦(1976-),男,四川南充人,博士生,主要研究领域为智能信息处理,信息隐藏,数字水印;焦李成(1959-),男,陕西白水人,博士,教授,博士生导师,主要研究领域为非线性理论,人工神经网络,子波理论和应用,进化算法,数据挖掘,多用户检测,数字水印;刘芳(1963-),女,湖南华容人,副教授,主要研究领域为智能信息处理,模式识别,电子商务.

全和抗干扰方面的良好特性,从而稳定、可靠地嵌入和检测水印.但是,由于伪随机水印不具有说明性,因而其用途要远小于标识符水印.

一般来说,当二值标识符的长度 $N=30$ 时就能满足应用的需要.文献[3,6]以随机序列代表比特值,水印序列过长,嵌入水印的冗余度将减小,检测结果很不理想.因此,本文的算法直接以二值序列作为标识符.在水印恢复中一般都存在误码.由于存在标识符的唯一性,必须保证标识符的误码为零.本文以纠错编码后的序列作为水印序列,其信息位即标识符.如果能把误码率控制在纠错码的纠错范围之内,就可以准确地恢复每一个比特值.纠错码越长,纠错能力越好,但是在图像水印中纠错码会受到长度的限制,因此必须在水印序列长度和冗余度之间选取一个最佳的折衷方案.

1.2 水印嵌入算法

由于小波域水印所具有的良好性能[2],因此水印嵌入在小波域里进行.首先用 9-7 双正交小波[2,4]对原始图像进行分解.图像的 4 层小波分解如图 1 所示,其中 $l=1,2,3,4$ 表示分辨层,$f=0,1,2,3$ 分别表示最低分辨层和水平、垂直、对角频率方向.

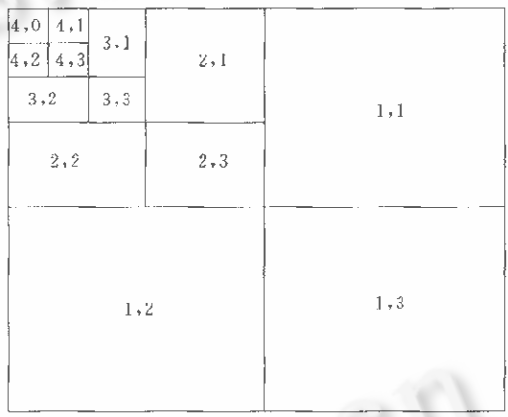


Fig. 1 Wavelet decomposition of four levels
图1 4层小波分解

水印算法基于一种简单的视觉模型.在图像压缩中,JND 门限(临界可见误差)根据人类视觉模型和图像的局部特性来确定图像的最优量化步长.在水印问题中,可以利用 JND 门限来确定水印信号嵌入的位置和最大强度[2,4,12].

在文献[2,4]中,每一子带系数,不考虑幅值大小,都具有相同的 JND 值.这显然是可以根据人类视觉模型进一步改进的[12].为了提高水印冗余度,这里采用一种双阈值嵌入策略,如式(1)所示.适当选取 T 即可在不产生感知失真的前提下增加小波系数修改的个数,从而提高嵌入水印的冗余度.

$$x^{w}_{m,n,l,f}=\begin{cases}x_{m,n,l,f}+JND_{l,f}\cdot w_i, & |x_{m,n,l,f}|>JND_{l,f}\\ x_{m,n,l,f}+T\cdot w_i, & |x_{m,n,l,f}|>T\\ x_{m,n,l,f}, & \text{其他}\end{cases} \tag{1}$$

类似于扩谱水印[5,8],水印序列循环嵌入.具体的水印嵌入算法如下:

(1) 对原始图像进行 L 层小波变换,取 $L=4$.

(2) 对小波系数块 $X_{l,f}$,$l=1,2,3,4$,$f=0,1,2,3$ 按照以下嵌入策略嵌入水印.

a) 逐行确定要修改的系数集合 $A_{l,f}$.如果 $X_{l,f,m,n}>T$,则系数坐标 $(m,n)\in A_{l,f}$,假设 $A_{l,f}$ 中共有 $M_{l,f}$ 个坐标;

b) 确定水印序列重复嵌入的次数,即码片率(chip rate) $CR_{l,f}=fix(M_{l,f}/N)$,其中函数 $fix(\cdot)$ 是朝零方向取整函数,N 是水印序列的长度;

c) 利用私钥 K 对集合 $A_{l,f}$ 中的系数进行伪随机排序,得到系数集合 $B_{l,f}$;

d) 根据式(1)对集合 $B_{l,f}$ 中的系数重复嵌入水印,

(3) 对所有的小波系数块重复以上操作.

(4) 对修改过的图像小波系数进行 L 层小波反变换,得到加水印的图像.

2 基于密钥的水印恢复

水印恢复算法分为私钥水印恢复和公钥水印恢复两种.数据所有者要求在水印数据经历了较大失真的情况下,仍能稳定地恢复出嵌入的水印,从而掌握其数据拷贝的流通路径以及其他目的.因此,私钥水印恢复必须具有较高的稳定性.而公钥水印恢复的目的是确认水印代表的信息,它只对较小失真的数据感兴趣,因此,所需的稳定性较小.在这一前提下,本文的水印密钥系统能够很好地满足这一要求.

2.1 私钥水印恢复算法

对加水印图像的任意系数块 $X_{l,f}^{w}$,根据私钥 K 可以得到集合 $B_{l,f}$.对集合 $B_{l,f}$ 中的坐标位置逐行排列,得到一个 $CR_{l,f}\times N$ 的坐标矩阵 $L_{l,f}$.

$$L_{l,f}=\begin{bmatrix} B_{l,f}(1), & B_{l,f}(2), & \cdots, & B_{l,f}(N) \\ B_{l,f}(N+1), & B_{l,f}(N+2), & \cdots, & B_{l,f}(2\cdot N) \\ \vdots & \vdots & \vdots & \vdots \\ B_{l,f}((CR_{l,f}-1)\cdot N+1), & B_{l,f}((CR_{l,f}-1)\cdot N+2), & \cdots, & B_{l,f}(CR_{l,f}\cdot N) \end{bmatrix}. \quad (2)$$

其中 $CR_{l,f}$ 是该系数块中嵌入的水印序列个数.坐标矩阵 $L_{l,f}$ 对应的系数矩阵为 $C_{l,f}$.

$$C_{l,f}=\begin{bmatrix} c_{l,f,1,1}, & c_{l,f,1,2}, & \cdots, & c_{l,f,1,N} \\ c_{l,f,2,1}, & c_{l,f,2,2}, & \cdots, & c_{l,f,2,N} \\ \vdots & \vdots & \vdots & \vdots \\ c_{l,f,CR_{l,f},1}, & c_{l,f,CR_{l,f},2}, & \cdots, & c_{l,f,CR_{l,f},N} \end{bmatrix}$$

其中 $c_{l,f,i,j}$ 表示该系数值嵌入的是系数块 $X_{l,f}$ 中第 i 个水印序列的第 j 个比特值 w_j.因此有水印的恢复公式:

$$w_{i,f,i,j}^{*}=\begin{cases} \dfrac{c_{l,f,i,j}^{*}-c_{l,f,i,j}}{JND_{l,f}}, & c_{l,f,i,j}>JND_{l,f} \\ \dfrac{c_{l,f,i,j}^{*}-c_{l,f,i,j}}{T}, & T<c_{l,f,i,j}<JND_{l,f} \end{cases}. \quad (3)$$

其中 $c_{l,f,i,j}^{*}$ 和 $c_{l,f,i,j}$ 分别是相应块的失真系数和原始系数,$w_{i,f,i,j}^{*}$ 是恢复的第 i 个水印序列的第 j 个比特值,$CR_{l,f}$ 是水印重复次数.这样就可以得到水印序列 $w_{f,i}^{*}$,$i=1,2,\ldots,CR_{l,f}$.

水印的恢复策略是自适应于失真类型的,具体为:分别列出每一分辨层、每一频率方向、最低频带以及整幅图像中水印序列的平均值,从中选取相似度最大的作为恢复的水印序列.为了客观评价水印算法的效果,定义相似度函数如下[27]:

$$\rho(w,w^{*})=\frac{\sum_{i=1}^{N}w(i)w^{*}(i)}{\sqrt{\sum_{i=1}^{N}w^{2}(i)}\sqrt{\sum_{i=1}^{N}w^{*2}(i)}}. \quad (4)$$

2.2 公钥水印恢复算法

公钥水印恢复需要两把公钥 K_1 和 K_2,其中 K_1 是某一图像小波系数块中特定坐标的位置序列,K_2 则是用于水印恢复的图像信息.公钥的产生及公钥水印恢复分以下几个步骤进行:

(1) 任取图像小波变换的一个系数块 $X_{l,f}$,其中 $l\in\{1,2,3,4\}$,$f\in\{0,1,2,3\}$.类似于文献[8],为确保安全,我们仅为数据接收者提供 $n\leqslant CR_{l,f}/2$ 个可恢复的水印序列.不失一般性,坐标矩阵可以表示为

$$L_{l,f}=\begin{bmatrix} B^1_{l,f}(1), & B^1_{l,f}(2), & \cdots, & B^1_{l,f}(N) \\ B^n_{l,f}((n-1)\cdot N+1), & B^n_{l,f}((n-1)\cdot N+2), & \cdots, & B^n_{l,f}(n\cdot N) \\ \vdots & \vdots & \vdots & \vdots \\ B^{CR_{l,f}}_{l,f}((CR_{l,f}-1)\cdot N+1), & B^{CR_{l,f}}_{l,f}((CR_{l,f}-1)\cdot N+2), & \cdots, & B^{CR_{l,f}}_{l,f}(CR_{l,f}\cdot N) \end{bmatrix}.$$

对该矩阵,$L_{l,f}$保持前 n 行不变,后$(CR_{l,f}-n)$行的坐标随机给出,以此坐标阵列作为公钥 K_1.

为了确保安全,对于每一个系数块只能取少量公钥,以防止攻击者破析公钥信息.例如,根据同一元素在同一列中的不变性来估计水印系数,从而破坏嵌入的水印.

(2) 由于公钥水印恢复不能利用原始图像,本文提出选取原始数据的一部分统计信息作为公钥 K_2,K_2 应满足条件:① 安全性,即数据接收者不能通过这一公钥推知原始数据的信息;② 稳定性,即在一定失真条件下仍能恢复出水印序列.

对于水印序列的任一个比特值 w_i,$i=1,2,\ldots,N$,假设公钥 K_1 的第 i 列元素所对应的加水印图像系数值为

$$K_{1,i}=\begin{bmatrix} c^w_{l,f,i,1} \\ \vdots \\ c^w_{l,f,i,n} \\ c^s_{l,f,i,n+1} \\ \vdots \\ c^w_{l,f,i,CR_{l,f}} \end{bmatrix}.$$

假设其中 $\begin{bmatrix} c^w_{l,f,i,1} \\ \vdots \\ c^w_{l,f,i,n} \end{bmatrix}$ 是含有 w_i 的系数值,而 $\begin{bmatrix} c^w_{l,f,i,n+1} \\ \vdots \\ c^w_{l,f,i,CR_{l,f}} \end{bmatrix}$ 是随机给出的系数值.这里,假设加水印图像没有失真.因此,

$$\sum_{j=1}^{CR_{l,f}} c^w_{l,f,i,j}=\sum_{j=1}^{n} c^w_{l,f,i,j}+\sum_{j=n+1}^{CR_{l,f}} c^w_{l,f,i,j}$$

$$=JND\cdot n_1\cdot w_i+T\cdot n_2\cdot w_i+\sum_{j=1}^{n} c_{l,f,i,j}+\sum_{j=n+1}^{CR_{l,f}} c^w_{l,f,i,j}, \tag{5}$$

其中 $n=n_1+n_2$,$c_{l,f,i,j}$是原始图像的系数值.

由式(5)可以看出,取公钥 $K_{2,i}=\sum_{j=1}^{n} c_{l,f,i,j}+\sum_{j=n+1}^{CR_{l,f}} c^w_{l,f,i,j}$,则恢复的水印为

$$w_i=sign\left(\sum_{j=1}^{CR_{l,f}} c^w_{l,f,i,j}-K_{2,i}\right),\ i=1\ldots N. \tag{6}$$

对得到的水印序列进行纠错解码,即可得到嵌入的标识符.

通过公钥 K_1 和 K_2,数据接收者即可对相应的系数块进行水印序列恢复,而其他系数块中的水印序列丝毫不受干扰.也就是说,即使该系数块中的水印序列被破坏,仍可以从其他的系数块恢复出水印,从而保证了私钥水印恢复的稳定性.

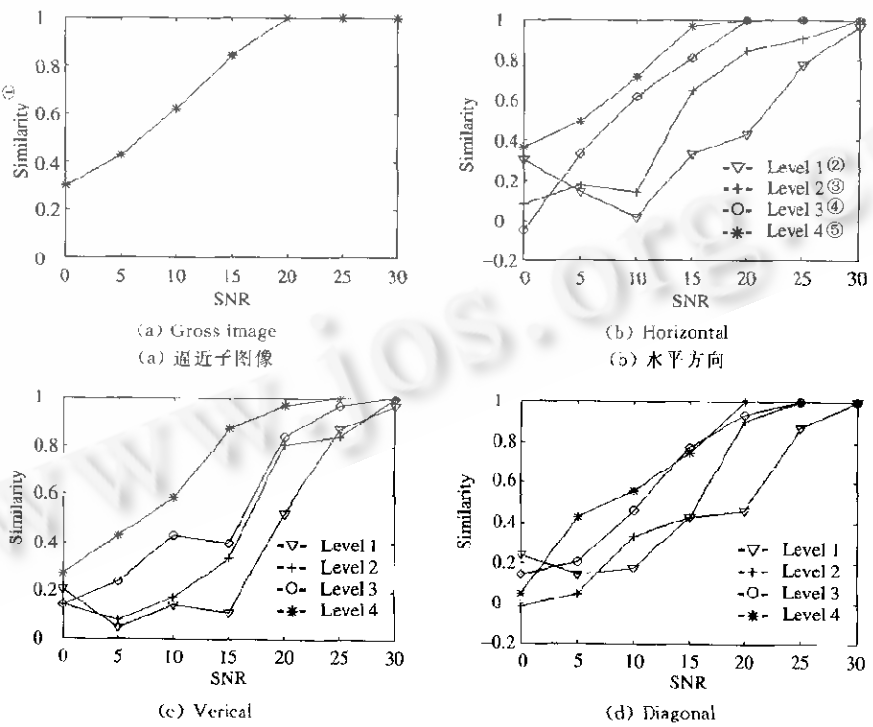
对所有系数块都可设置类似的公钥.考虑到不同系数块对图像恢复的影响以及各种失真的稳定性不同,例如,图像的第1层细节,尤其是对角细节部分,对图像的恢复影响很小,应该根据不同的应用需要来设置公钥,也可以结合多个系数块来产生一套公钥.但是必须注意的是,由于"取反"攻击的影响(见第3.2节),选取的小波系数块数目不能太大,以保证不被破坏的水印序列具有一定的冗余度.

3 实验结果

3.1 公钥性能

实验中选取典型的256×256×8的Lena图像作为主图像.标识符是随机选取的长度$N=30$的二值序列.纠错码类型选用BCH码,对标识符进行纠错编码后得到的水印序列长度为63.该码的纠错能力为6个错码.因此,当恢复的水印序列错码超过6个时,也即当相应的相似度值小于0.809 5时,BCH码将无法纠错.取可恢复的水印序列数目$n=CR_{l,f}/2$,对图像的所有系数块各设一套公钥分别测试其性能.

图2和图3分别给出了在AWGN噪声和JPEG压缩编码两种失真情况下,水平、垂直和对角这3个频率方向以及逼近图像的公钥水印恢复在各个分辨层的性能.由图2和图3可以看出,在AWGN噪声信噪比不超过15dB,或者JPEG压缩编码的质量因子Q不小于20的情况下,可以在水平、垂直或对角方向选择合适的公钥.



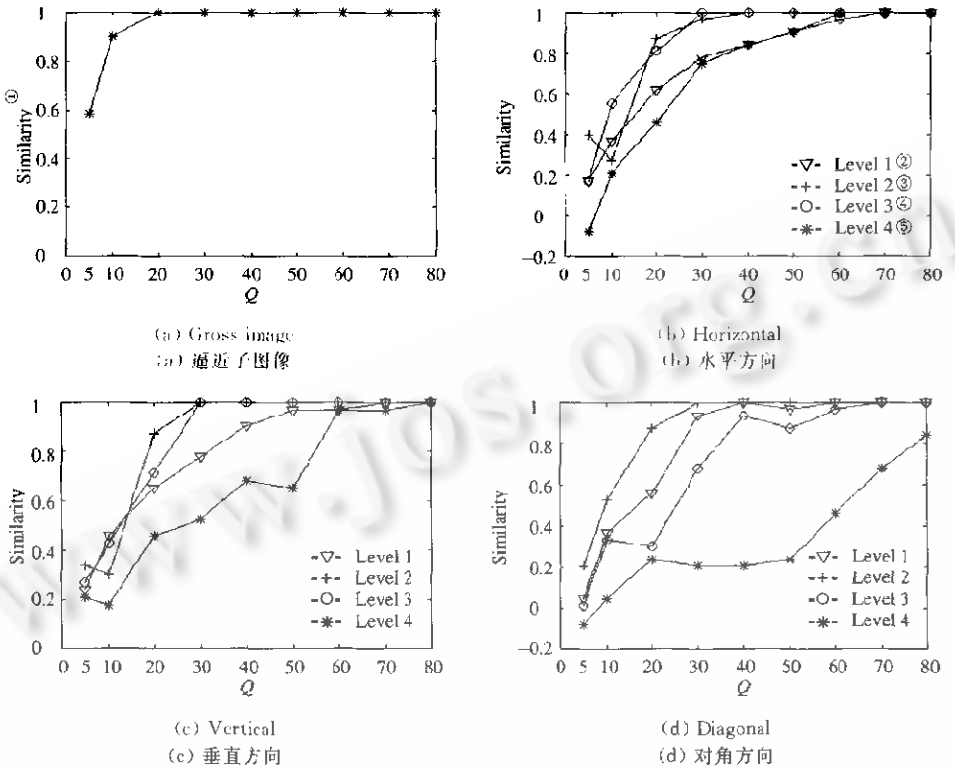
(a) Gross image (b) Horizontal
(a) 逼近子图像 (b) 水平方向

(c) Verical (d) Diagonal
(c) 垂直方向 (d) 对角方向

①相似度,②第1层,③第2层,④第3层,⑤第4层.

Fig. 2 Watermark retrieval with public keys under AWGN distortion when $n=CR_{l,f}/2$

图2 $n=CR_{l,f}/2$时AWGN失真下公钥水印恢复性能



(a) Gross image
(a) 逼近子图像

(b) Horizontal
(b) 水平方向

(c) Vertical
(c) 垂直方向

(d) Diagonal
(d) 对角方向

①相似度,②第1层,③第2层,④第3层,⑤第4层.

Fig. 3 Watermark retrieval with public keys under JPEG compression distortion when $n-CR_{1,j}/2$

图3 $n-CR_{1,j}/2$ 时JPEG压缩失真下公钥水印恢复性能

3.2 私钥性能

在不公开公钥的情况下,私钥水印恢复已经相当稳定.这里将主要讨论公钥带来的攻击可能对私钥水印恢复产生的影响.利用公钥对水印进行的典型攻击可分为两种:重构私钥和破坏水印.

(1) 重构私钥

文献[8]已经讨论过,当公钥发行过多时,水印将变得不安全,攻击者可能通过公钥来重构私钥.因此,我们只允许在各个系数块中设置少量的公钥.

公钥 K_2 涉及部分水印系数和原始系数的统计值(总和),因此是无法利用的.另一把公钥 K_1 是一个近似随机排列的坐标矩阵,每列仅对应 n 个正确的系数,且这 n 个系数在该列中的位置也是随机的.对于每一系数块,由于只发行少量的公钥,因此攻击者无法由此推测公钥 K_1 每列中这 n 个正确的系数,也就无法重构私钥.

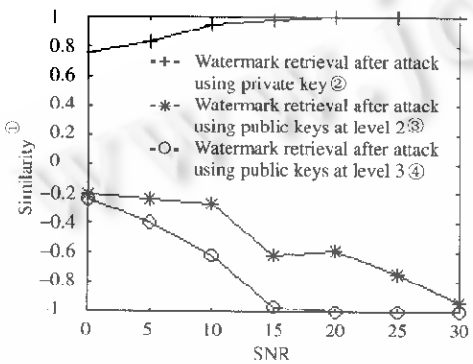
(2) 破坏水印

由于重构私钥非常困难,攻击者则倾向于破坏水印.本文提出一种"取反"攻击,即把公钥 K_1 对应的小波系数全部"取反",也就是将对应于1的列减去相应的修改值 JND 或 T,而对应于-1的列加上相应的修改值 JND 或 T,如下所示:

$$K'_{1,j}=\begin{cases}K_{1,j}+m, & \text{if } w_j=1\\ K_{1,j}-m, & \text{if } w_j=-1\end{cases}.$$

其中 m 为相应的修改值，$m=\begin{cases}JND & \text{if } c^{w}_{i,f_{i,1}}>JND\\ T & \text{if } c^{w}_{i,f_{i,1}}<JND\end{cases}$，$K_{1,j}$为公钥 K_1 的第 j 列对应的系数，$K'_{1,j}$为攻击后的相应列系数.把该列系数值分别代入其在加水印图像的原始坐标位置，就意味着公钥 K_1 每列中至少有 n 个水印序列值被破坏，本文和文献[8]中的公钥水印恢复必定失效.对于私钥水印恢复，则因为水印冗余度的减小，检测效果也会受到影响.

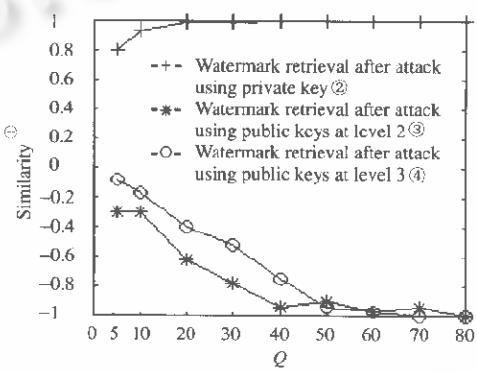
实验中取 $n=CR_{i,f}/2$，在分辨层 2 和分辨层 3 中的水平频率方向系数块中各设一套公钥.图 4 和图 5 给出了在"取反"攻击后，私钥、公钥水印恢复的性能分别与 AWGN 信噪比(SNR)和 JPEG 压缩质量因子 Q 之间的函数关系.可以看出，此时公钥已经不能恢复水印.对于 AWGN 和 JPEG 压缩这两种失真，公钥恢复的水印相似度分别随着 SNR 和 Q 的增加而下降，最后趋于 -1.这是因为在式(5)中，各列中 n 个正确的系数被删除水印，而其他系数也被减去相应的修改值 m，因此得到的水印序列比特值与嵌入的比特值相反.



①相似度，②攻击后的私钥水印恢复，③攻击后的第 2 层公钥的水印恢复，④攻击后的第 3 层公钥的水印恢复.

Fig. 4 Results of secret key watermark retrieval under AWGN distortion

图 4 AWGN 失真时，公钥、私钥水印恢复性能与 SNR 的函数关系



①相似度，②攻击后的私钥水印恢复，③攻击后的第2层公钥的水印恢复，④攻击后的第 3 层公钥的水印恢复.

Fig. 5 Results of secret key watermark retrieval under JPEG compression distortion

图 5 JPEG 压缩失真时，公钥、私钥水印恢复性能与质量因子 Q 的函数关系

虽然公钥不可恢复水印，但是私钥水印恢复的性能仍然不受影响.由图 4 和图 5 可以看出，当 SNR 不小于 5dB 和 Q 不小于 5 时，相似度不小于 0.809 5，标识符均能完全恢复.

除了 AWGN 和 JPEG 压缩两种失真以外，"取反"攻击后的加水印图像在分别经历修剪、缩放和中值滤波等失真以后，私钥水印恢复的性能也没有产生多大影响，当修剪(仅保留 0.5%)、缩放(加水印图像缩小 1/2)以及中值滤波(滤波器大小为 2×2 和 3×3)时，标识符均可无错地恢复.

4 结 论

本文构造了一种水印密钥系统，提出了一种新颖的公钥生成方法，其思想适用于图像以及其他多媒体数据.公钥水印恢复的特点是安全和稳定，能够抵制一定的失真，不需要原始数据，有效地解决了公钥生成与私钥之间的矛盾.由于公钥选取是分块独立的，私钥水印恢复非常稳定.在公钥水印恢复完全被破坏的情况下，即使经历较大的失真也能保持较高的稳定性.例如，信噪比低达 5dB 的 AWGN 失真，JPEG 压缩质量因子 $Q=5$，当修剪(仅保留 0.5%)、缩放(加水印图像缩小 1/2)以及中值滤波(滤波器大小为 2×2 和 3×3)时，标识符均可无错地恢复.实验结果证明该系统是实用

和有效的.

References:

[1] Swanson, M. D., Zhu, Bin, Tewfik, A. H. Multiresolution scene-based video watermarking using perceptual models. IEEE Journal on Selected Areas in Communication, 1998,16(4):540~550.

[2] Podilchuk, C. I., Zeng, Wen-jun. Image-adaptive watermarking using visual models. IEEE Journal on Selected Areas in Communication, 1998,16(4):525~539.

[3] Servetto, S., Podilchuk, C. I., Ramchandran, K. Capacity issues in digital image watermarking. In: Werner, B., ed. Proceedings of the 1998 International Conference on Image Processings, Vol 1. Chicago: Braun-Brum Field, Inc., 1998. 445~449.

[4] Wolfgang, R. B., Podilchuk, C. I., Delp, E. J. Perceptual watermarks for digital image and video. Proceedings of the IEEE, 1999,87(7):1108~1126.

[5] Hsu, Chicu-ting, Wu, Ja-ling. Hiding digital watermarks in image. IEEE Transactions on Image Processing, 1999,8(1): 58~68.

[6] Hartung, F., Kutter, M. Multimedia watermarking techniques. Proceedings of the IEEE, 1999,87(7):1079~1107.

[7] Cox, I. J., Kilian, J., Leighton, F. T., *et al*. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing, 1997,6(12):1674~1687.

[8] Hartung, F., Girod, B. Fast public-key watermarking of compressed video. In: Torwick, I., ed. Proceedings of the 1997 International Conference on Image Processing, Vol 1. Santa Barbara: Braun-Brum Field, Inc., 1997. 528~531.

[9] Watermarking for DVD-Call for proposals. 1997. http://www.Dvcc.com/dhsg/.

[10] Fornaro, C., Sanna, A. Public key watermarking for authentication of CSG models. Computer-Aided Design, 2000,32 (12):727~735.

[11] Marvel, L. M., Boncelet, C. G., Retter, C. T. Spread spectrum image steganography. IEEE Transactions on Image Processing, 1999,8(8):1075~1083.

[12] Watson, A. B., Yang, G. Y., Solomon, J. A., *et al*. Visibility of wavelet quantization noise. IEEE Transactions on Image Processing, 1997,6(8):1164~1175.

A Novel Secret Key Watermarking System*

ZHONG Hua, JIAO Li-cheng, LIU Fang

(*Key Laboratory for Radar Signal Processing, Xidian University, Xi'an 710071, China*)

E-mail: huazh@rsp.xidian.edu.cn

http://www.rsp.xidian.edu.cn

Abstract: Watermarking, as an effective method for information hidding, has evolved very quickly. Most watermarking systems available have only a secret key, which cannot be public. But in some applications, watermarking needs to be retrieved by public keys. How to generate public keys without weaken the performance of the private key is a key problem. In this paper, a secret key watermarking system is designed, in which a novel method of generating public keys is proposed. The identifier (ID) embedded can be reliably retrieved using public keys without resorting to the original data. Because only part of embedding information is used in public keys, the above problem is successfully solved. Experimental results show its security and validity.

Key words: watermarking; information hidding; public key; private key; identifier

* Received December 15, 2000; accepted April 18, 2001

Supported by the National Natural Science Foundation of China under Grant No. 60073053; the National Research Foundation for the Doctoral Program of Higher Education of China