第 32 卷 第 22 期 计 算 机 工 程 2006 年 11 月
Vol.32 No.22 Computer Engineering November 2006
·安全技术· 文章编号：1000—3428(2006)22—0172—03 文献标识码：A 中图分类号：TP391

基于零水印和认证水印的双水印方案

赵怀勋[1]，王丽娜[1]，季称利[2]
(1. 武警工程学院通信工程系，西安 710086；2. 武警北京总队 13 支队，北京 102607)

摘 要：为解决高值图像同时具有版权保护和内容认证需求的问题，提出了基于零水印和认证水印的双水印方案。实验表明，该方案具有篡改敏感度高和水印鲁棒性强的特性，性能可靠，可以同时实现对高值图像的版权保护和内容安全认证。
关键词：零水印；认证水印；双水印；整数小波变换

A Double Watermark Scheme for Image Based on Zero-watermark and Authentication Watermark

ZHAO Huaixun[1], WANG Lina[1], JI Chenli[2]
(1. Department of Communication Engineering, Engineering College of Armed Police Force, Xi'an 710086;
2. Thirteen Detachment of General Beijing Brigade of CAPF, Beijing 102607)

【Abstract】In order to solve the problem that some expensive images not only have the needs of protecting their copyrights but also have the needs of assuring their integrity, a new scheme is proposed. The experiments have demonstrated that this scheme has good performance; sounds robustness and can achieve the good protection of copyrights and image content authentication for the expensive color images.
【Key words】Zero-watermark; Authentication watermark; Double watermark; Integer wavelet transform

现有的绝大多数水印算法在功能上都是单项的，或者只解决图像的版权问题，或者只解决图像的内容认证问题。然而，一些高价值的图像，如法庭上的证据图像、军事中的卫星图像和重大事件的新闻图像等，既有版权保护的需要，又有保证其内容完整性和真实性的需要，所以很有必要开发能同时解决上述两类问题的水印技术。文献[3]针对这一课题向图像里嵌入两个水印，即一个鲁棒水印用以保护图像版权，一个脆弱水印用来实现图像认证。但是这样处理会导致以下两个问题：(1)同时往图像中嵌入两个水印会给图像带来过多的噪声，这是高保真图像(如卫星图像)所不能接受的；(2)两类水印标准特性差异很大，在同一图像中很可能由于协调不好而相互影响性能，从而导致算法无法有效地实现对上述高值图像的版权保护和内容认证。

针对上述问题，本文提出了基于零水印和认证水印的双水印方案。利用零水印算法实现对高值图像的版权保护，采用基于整数小波变换的认证水印算法达到对高值图像的安全认证，利用其整数加法和位移运算特性有效地提高了水印图像的重构质量，实现了对高值彩色图像的高保真水印嵌入。

1 基于零水印和认证水印的双水印方案

1.1 图像双水印形成

如图 1 所示双水印形成过程分为以下几个步骤：

Step1 对图像 I 的 R、G 和 B 空间进行整数小波变换

将原彩色图像I分成 $a\times b$ 大小的图像块并依次编号 $A_1,A_2,\ldots,A_i$，因为要在 3 个颜色通道中都嵌入各自的认证水印，所以对每一图像块 A_i 的红色、绿色和蓝色通道分别进行整数小波分解。

Step2 生成 R、G 和 B 的认证水印

为了满足彩色图像的内容认证要求，增加算法对图像处理的敏感性，设计了R、G和B的独立空间封闭水印形成算法。在 3 个空间中，初步水印信息由 3 部分构成，其中，R通道的初步水印信息由块A_i整数小波分解后的高频小波系数集 h_i^R、低频小波系数集 l_i^R 和中频小波系数LSB置零后得到的值集 n_i^R 构成，G通道和B通道与R通道类同。设 $P(X)$ 是置乱函数，$H(X)$是哈希函数，首先分别将R、G和B的 3 部分初步水印信息合并，然后用置乱函数对其置乱，再用哈希函数对置乱后的初步水印信息作运算以求取认证水印。其中，R通道的认证水印为 $mark_i^R = H(P(h_i^R \cup l_i^R \cup n_i^R))$，G通道和B通道的认证水印类同。

Step3 嵌入认证水印及生成水印图像

在密钥 key^R 的参与下，将 R 通道的认证水印 $mark_i^R$ 嵌入 A_i 的 R 通道中频小波系数 LSB 中，G 通道和 B 通道同理。然后对块 A_i 做整数小波逆变换，待所有图像块完成水印嵌入、整数小波逆变换后，合并所有块生成水印图像 I'。这一步，可以根据算法安全需要来确定 3 个通道嵌入密钥，若为了使用方便，可以选择三者等同，若为了提高算法的安全性，则令三者各不相等。

Step4 对图像 I' 进行整数小波变换和 DCT 变换

因为算法要采用 3 个颜色通道中的信息构造零水印，所以对图像的红色、绿色和蓝色通道分别进行整数小波分解，然后，分别对 3 个通道中的低频部分做 DCT 变换。

Step5 合成初步零水印

基金项目：武警部队科学技术基金资助项目
作者简介：赵怀勋(1960－)，男，教授，主研方向：网络安全，数字水印；王丽娜，硕士生；季称利，硕士
收稿日期：2005-12-24 **E-mail：**zhaowjhx@163.com

在 3 个颜色通道中，分别选择A、B和C(A、B同C之和为M)个最大的DCT变换系数并将它们合并，从而构成一维序列D。如果D中的第i个数为正，则相应的初步零水印信息中的第i个数为 1，否则为-1，这样就产生了二值初步零水印信息序列$W=\{w(i),1\le i\le M\}$，其中$w(i)\in\{1,-1\}$。设key_p与key_s分别是用户的公钥与私钥，用公钥key_p对初步零水印信息W处理得零水印$W'=\{w'(i),1\le i\le M\}$。$\sigma(sk,m)$是共享加密函数，所以利用半密钥sk_2对一维序列W进行处理得到零水印验证信息$W''=\sigma(sk_2,W)$。

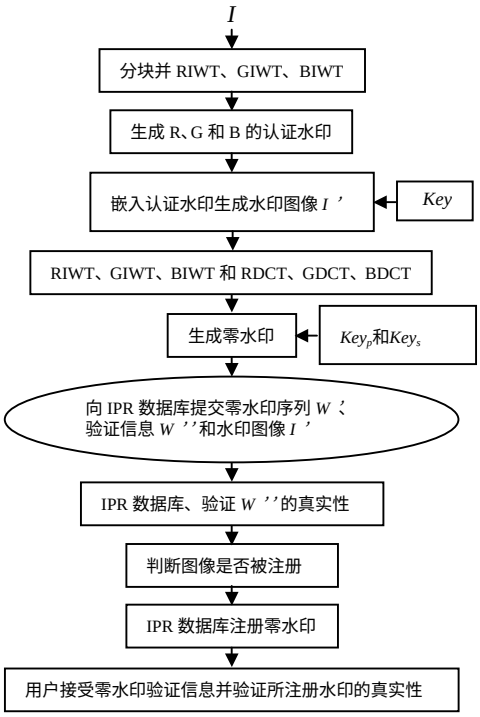

图 1 双水印形成

Step6 向 IPR 数据库提交零水印序列W'、验证信息W''和水印图像I'

Step7 IPR 数据库验证W'和W''的真实性

IPR数据库利用与Step4 和Step5 同样的方法对水印图像I'进行频域变换，得到二值初步零水印信息序列$W=\{w(i),1\le i\le M\}$。然后利用用户的公钥key_p对初步零水印信息W处理得到零水印$W_{IPR}'=\{w'_{IPR}(i),1\le i\le M\}$，IPR数据库通过判定$W'_{IPR}=?W'$来判定$W'$的真实性，若$W'_{IPR}=W'$，则认为用户提交的零水印序列为真实，否则认为该水印序列为假，于是IPR数据库拒绝零水印注册，退出程序。

IPR 数据库利用与用户同样的共享加密函数$\sigma(sk,m)$和 IPR 数据库水印半密钥$sk_1=d_1$得到零水印验证信息$W'''=\sigma(sk_1,W)$。因为有$\sigma(sk,m)=\sigma(sk_1,m)\Diamond\sigma(sk_2,m)$，所以 IPR 数据库通过利用水印公钥$VK=<e,N>$来验证$\sigma(sk,m)$的真实性，进而判定$W''$的真实性。若有$\sigma(sk,m)$为真，则认为$W''$是真实的。否则认为$W''$不是真实的，于是 IPR 数据库拒绝零水印注册，退出程序。

Step8 判断图像是否被注册

IPR 数据库为了防止非法盗版者也注册非法的零水印，所以要对注册图像及其水印进行数据库唯一性检测。IPR 数据库利用与用户相同或类似的方法提取唯一性鉴定零水印W_{ind}，然后利用公式$\mu=sim(w,w')=w.w'/\sqrt{w'w'}$对$W_{ind}$与数据库原有零水印做相关性计算，若$\mu<5$则执行 Step9，否则拒绝注册，退出程序。

Step9 IPR 数据库注册零水印

IPR 数据库接受零水印的注册，并将水印图像I'和零水印序列W'、验证信息W''统一储存。IPR 将零水印验证信息W'''发送给用户。

Step10 用户接受零水印验证信息并验证所注册水印的真实性

为了切实保证水印用户的利益，在用户收到零水印的验证信息后，计算$\tilde{W}=W''\Diamond W'''$，而后利用水印公钥$VK=<e,N>$判定$\tilde{W}$的真实性。若$\tilde{W}$为真，则认为零水印$W'$成功注册，否则认为零水印$W'$不可用并向 IPR 数据库申诉。

1.2 图像双水印的检测

1.2.1 认证水印的检测

若要鉴定高值图像内容的完整性、真实性执行以下操作:

Step1 对图像I'进行整数小波变换

将彩色水印图像I'分成$a\times b$大小的图像块并依次编号$A_1', A_2', \ldots, A_t'$，因为算法要检测 3 个颜色通道中的认证水印，所以对每一图像块A_i'的红色、绿色和蓝色通道分别进行整数小波分解。

Step2 提取水印

在图像块A_i'的红色、绿色和蓝色通道的中频小波系数 LSB 中，分别利用密钥key^R、key^G和key^B按与嵌入相反的操作提取 3 种认证水印$mark_i^{R'}$、$mark_i^{G'}$和$mark_i^{B'}$。

Step3 产生水印检测信息

用生成初步水印信息的方法计算水印检测信息。在 R 通道中将高频小波系数集$h_i^{R'}$、低频小波系数集$l_i^{R'}$和中频小波系数 LSB 置零后得到的值集$n_i^{R'}$，合并成比特流B^R，然后用与嵌入同样的置乱函数$P(X)$、哈希函数$H(X)$计算检测信息$\det_i^{R'}=H(P(B^R))$，G 通道和 B 通道中类同。

Step4 判别篡改

分别判别并比较图像块A_i'3 个通道的提取水印$mark_i^{R'}$、$mark_i^{G'}$和$mark_i^{B'}$与检测信息$\det_i^{R'}$、$\det_i^{G'}$和$\det_i^{B'}$。在R通道中，若$\det_i^{R'}=mark_i^{R'}$，则判定图像块A_i的R通道未被篡改，接受图像块A_i'；若$\det_i^{R'}=mark_i^{R'}$，则判定图像块A_i的R通道已被篡改，抛弃图像块A_i'。G通道和B通道中同理。

Step5 生成篡改标示图像

图像的 3 个颜色空间生成 3 个篡改标示图。在 R 通道中，对被接受的图像块A_i'进行整数小波反变换，将被抛弃的图像块置为零像素块。按分块相反顺序合并所有图像块A_i'以生成篡改标示图像I_R''。以同样方法生成 G 通道的篡改标示图像I_G''和 B 通道的篡改标示图像I_B''。

1.2.2 零水印的检测

Step1 对图像I'进行整数小波变换和 DCT 变换

因为算法要在 3 个颜色通道中提取零水印，所以对图像的红色、绿色和蓝色通道分别进行整数小波分解，然后，分别对 3 个通道中的低频部分做 DCT 变换。

Step2 提取零水印

在 3 个颜色通道中，分别选择A、B和C(A、B同C之和为

M)个最大的DCT变换系数并将它们合并，从而构成一维序列D^0。如果D^0中的第i个数为正，则相应的初步零水印信息中的第i个数为 1，否则为-1，这样就提取出了二值初步零水印信息序列$W^o=\{w^o(i),1\le i\le M\)$，其中$w^o(i)\in\{1,-1\}$。

Step3 仲裁方向 IPR 数据库获取注册零水印

当图像作品发生版权纠纷时，由仲裁方向 IPR 数据库提出相关图像的水印获取请求，同时由图像所有者向 IPR 数据库提交零水印验证信息$W''=\sigma(sk_2,W)$。IPR 数据库收到仲裁方的水印请求与零水印验证信息$W''=\sigma(sk_2,W)$后利用与用户同样的共享加密函数$\sigma(sk,m)$和 IPR 数据库水印半密钥$sk_1=d_1$得到零水印验证信息$W'''=\sigma(sk_1,W)$，然后 IPR 数据库通过利用水印公钥$VK=<e,N>$来验证$\sigma(sk,m)$的真实性，进而判定W''的真实性。若W''是真实的，则将零水印序列W'、零水印验证信息W'''发送给仲裁方。若W''不是真实的，于是 IPR 数据库拒绝提供零水印。

Step4 计算提取出的零水印与注册零水印的相关度

仲裁方要求水印用户利用其私钥key_s通过公式$\mu=sim(w,w')=w.w'/\sqrt{w'w'}$计算$W^o$与$W'$的相关度，若$\mu<5$则认为零水印被检测出来，否则认为水印没有被检测出来。

2 实验与分析

为测试方案的性能，在 MATLAB 实验环境下进行了多组仿真测试。下面是部分实验结果。实验用图为 512×512 的 Lena 彩色图像(图像格式为 bmp)。哈希函数选用的是经典的 MD5 算法。零水印序列长度设为 *M*=1 000。在实验中，利用 1 000 个取值为{1，-1}的随机水印序列来构造水印相关性检测图，其中第 450 个是水印序列。

图 2 中，左上部分为将 Lena 的双眼涂上黑色的图像。其余部分分别是算法生成的 RGB3 通道的水印图像篡改位置标示图。图 3 中，左上部分为 Lena 的帽缨 R 通道篡改图像。其余部分分别是算法生成的 RGB 3 通道的水印图像篡改位置标示图。


图 2 双眼篡改实验 Lena 图像 图 3 帽缨 R 通道篡改实验 Lena 图像

图 4 是经过打印-扫描处理后的 Lena 彩色图像水印检测器响应图，检测器输出 sim=25.622。由此可见，算法对打印-扫描处理具有较好的鲁棒性。

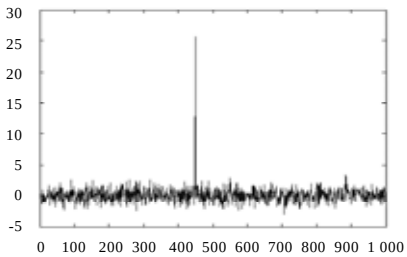

图 4 打印-扫描后的水印检测响应

图 5 是加 Specle 乘性噪声(方差为 0.5)后的 Lena 彩色图像水印检测器响应图，检测器输出 sim=23.167。

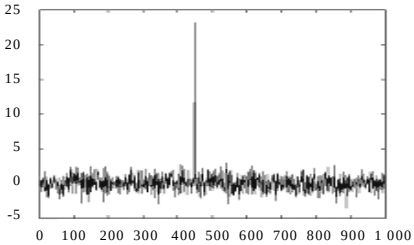

图 5 乘性噪声处理的水印检测响应

图 6 是加椒盐加性噪声(系数为 0.3)后的 Lena 彩色图像水印检测器响应图，检测器输出 sim=29.536。

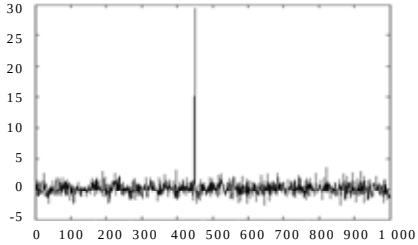

图 6 加性噪声处理的水印检测响应

图 7 是对 Lena 彩色水印图像进行 JPEG 压缩后的水印检测器响应图，检测器输出 sim=30.167。

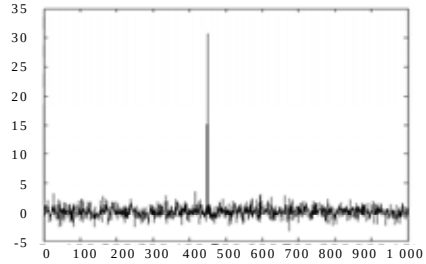

图 7 JPEG 压缩处理的水印检测响应

4 结束语

随着数字水印技术逐渐走向应用，实现版权保护，和内容认证的双水印算法的研究越来越受到重视。本文提出的基于零水印和认证水印的双水印方案，经过 MATLAB 实验环境下对认证水印和零水印的多组仿真测试，表明方案篡改敏感度高，水印鲁棒性好，性能可靠，能够很好地实现对高值图像的版权保护和内容安全认证。

参考文献

1 Pereira S, Voloshynovskiy S, Pun T. Optimized Wavelet Domain Watermark Embedding Strategy Using Linear Programming[C]. Proc. of SPIEAeroSence'00: Wavelet Applications VII, Orlando, FL, USA, 2000-04.

2 Celik M U, Sharma G. Hierarchical Watermarking for Secure Image Authentication with Localization[J]. IEEE Transactions on Image Processing, 2002, 11(6): 585-595.

3 Mintzer F, Braudaway G W. If One Watermark is Good, Are More Better?[C]. Proc. of Int. Conf. on Acoustics, Speech, Signal Processing, 1999: 2067-2070.

4 温 泉，孙锬锋，王树勋. 零水印的概念与应用[J]. 电子学报，2003, 31(2).

5 季称利，杨晓元，张 崇等. 结合空域不变量的变换域零水印二次检测方案[J]. 计算机工程, 2004, 30(14): 105-107.