

# 抗旋转的整数小波变换数字水印算法

朱佳婷,吕建平

(西安邮电学院 计算机系,陕西 西安 710061)

**摘 要:** 现有的大多数基于小波变换的水印算法没有抵抗几何攻击的能力,例如将图像旋转微小的角度即可导致水印检测的失败。为了提高基于小波变换的水印算法抵抗图像旋转攻击的能力,提出了一种抗旋转的整数小波变换盲水印算法。该算法通过在嵌入水印后的图像中嵌入一个模板,在图像遭到旋转攻击后,利用模板能有效地恢复图像,达到水印提取同步,从而准确地提取出水印。实验结果表明,0到360度的旋转攻击均能被准确监测到,从而证明了该方法是一种鲁棒的能有效抵抗旋转攻击的图像水印算法。

**关键词:** 数字水印;整数小波变换;傅里叶变换;模板

**中图分类号:** TP393.08;TP301.6

**文献标识码:** A

**文章编号:** 1673-629X(2007)07-0145-03

## Digital Watermarking Algorithm Resistant to Rotation Based on Integer Wavelet Transform

ZHU Jia-ting, LÜ Jian-ping

(Computer Department, Xi'an Institute of Post and Telecommunication, Xi'an 710061, China)

**Abstract:** Most of the proposed watermarking algorithms based on wavelet transform are not resistant to geometric attack. For instance, the detection of watermark fails if the watermarked image is rotated by a very small angle. In order to add the ability of rotation resistance to wavelet based on watermarking algorithms, a blind digital watermarking algorithm which is resistant to rotation and based on integer wavelet transform is proposed. In this algorithm, a template is embedded into the watermarked image. Using the template, the image can be correct after the rotation attack to make the watermarking detection and embedding course be synchronization again. In this way the watermark could be extracted exactly. The experiment results show that the rotation attack from 0 to 360 degrees can be detected. It is also proved that this algorithm is robust and effective to rotation attack.

**Key words:** digital watermarking; integer wavelet transform; Fourier transform; template

## 0 引 言

随着 Internet 和多媒体技术的飞速发展,数字作品的获得和使用变得越来越容易,如何有效保护数字作品作者的版权成为一个迫切的研究课题。数字水印技术作为一种有效的版权保护技术发展了起来。数字水印技术是信息隐藏学的一个分支,它将具有特定意义的标志嵌入到原始数据中,从而达到对原始数字作品的版权保护和防篡改目的。

根据水印嵌入域的不同,水印技术分为空域水印算法和频域水印算法。由于空域水印算法通过直接修改图像像素值来隐藏信息,所以鲁棒性较差,现在的大多数水印算法为频域水印算法。小波变换因为具有良

好的局部时频分析特性,已成为新的压缩标准 JPEG2000 的核心,基于小波变换的水印算法继而成为频域水印算法的主流算法。由于小波变换不具有几何不变性,因此能抵抗几何攻击的小波变换算法不多。对于大多数利用小波变化算法嵌入水印后的图像,只需旋转小角度即可使水印检测失去同步性,达到破坏水印的目的。文献[1]指出对抗几何攻击的盲检测水印算法主要有三类:第一类是利用原始图像中具有几何不变性的量来嵌入水印;第二类是利用辅助信息来纠正受几何攻击后的图像;第三类是通过提取原始图像适合于水印的特征来嵌入水印或恢复图像达到抗几何攻击目的。小波变换不具有几何不变性,因此抵抗几何攻击只能采用第二类或第三类方法,现有的第二类算法中基于整数小波变换的算法很少。文中针对第二代小波变换中的整数小波变换,首先提出了一种鲁棒的盲检测水印算法,在原始图像中嵌入的水印是一个有意义的二值图像,然后设计出一个实用的傅氏变

收稿日期:2006-10-06

**作者简介:** 朱佳婷(1982-),女,湖南邵阳人,硕士研究生,研究方向为信息安全与数字水印;吕建平,教授,主要研究方向为图像处理与模式识别。

换域中的模板。当图像遭到旋转攻击后,首先利用模板纠正图像,然后再提取水印。

## 1 水印算法

### 1.1 整数小波变换及傅里叶变换

第一代传统小波变换是建立在傅里叶变换基础上的,而基于提升方案的第二代小波变换<sup>[2]</sup>实现了原位运算,节省了存储空间,运算较第一代小波变换更为简单。利用小波变换的提升方案可以实现整数到整数的变换,便于计算机存储和计算,而且不会引入量化误差,可以实现无损压缩。整数小波提升算法的变换过程如下:

Step1:分解。将输入信号  $s_i$  分解为  $s_{i-1}$  和  $d_{i-1}$ ;最简单的分解方法为将  $s_i$  分解为一组偶数序列  $s_{i-1}$  和一组奇数序列  $d_{i-1}$ 。

$$\text{Split}(s_i) = (s_{i-1}, d_{i-1}) \quad (1)$$

Step2:预测。用偶数序列  $s_{i-1}$  的值去预测奇数序列  $d_{i-1}$ ,用它们的差值代替  $d_{i-1}$ 。

$$d_{i-1} = d_{i-1} - P(d_{i-1}) \quad (2)$$

Step3:更新。为了使原信号集的某些全局特性(如均值)在其子集  $s_{i-1}$  中继续保持,必须找到一个更新算子  $U$  来更新子集  $s_{i-1}$ 。

$$s_{i-1} = s_{i-1} + U(s_{i-1}) \quad (3)$$

利用不同的预测算子和更新算子可以构造出不同的小波。从以上过程可以看出,提升过程的小数部分是在预测和更新过程中引入的,对这两个过程中引入的小数部分进行取整操作就可实现整数小波变换<sup>[3]</sup>。整数小波变换的三步归纳如下:

$$\begin{cases} (1) \text{Split}(S_i) = (s_{i-1}, d_{i-1}) \\ (2) d_{i-1} = d_{i-1} - [P(d_{i-1})] \\ (3) S_{i-1} = S_{i-1} + [U(s_{i-1})] \end{cases} \quad (4)$$

整数小波逆变换是正变换的反过程,过程如下:

$$\begin{cases} (1) S_{i-1} = S_{i-1} - [U(s_{i-1})] \\ (2) d_{i-1} = d_{i-1} + [P(d_{i-1})] \\ (3) S_i = \text{cinbube}(s_{i-1}, d_{i-1}) \end{cases} \quad (5)$$

图 1 是三层小波变换的示意图。 $LL_n$  为第  $N$  层的低频系数,它包含着图像的主要内容。 $HL_n, LH_n, HH_n$  分别对应第  $N$  层的垂直、水平和对角的高频信息,它们主要包含图像的细节部分。

整数小波变换具有诸多优点,但是其很大的一个缺点是不具有几何不变性。因此采用小波变换的水印算法很难抵抗几何攻击。但是图像处理中常用的傅里叶变换<sup>[4]</sup>具有很好的几何不变性。图像旋转后的傅里叶谱图等于源图像的谱图旋转同样的角度后的图像。

为了使水印能抵抗旋转攻击,算法引入了一个在傅里叶变换域中嵌入的模版。

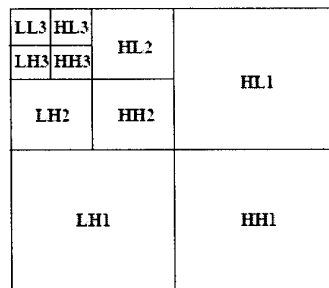


图 1 三层小波变换示意图

### 1.2 嵌入过程

#### 1.2.1 有意义二值图像的嵌入

文中提出的水印算法采用有意义的二值图像作为水印,具有容易被人理解、易辨识的优点。首先将图像做  $N$  层整数小波变换, $N$  的大小由源图像及水印图像的尺寸决定。根据文献<sup>[5]</sup>,小波变换的最佳水印嵌入位置为低频带,为了保证水印的稳健性和不可见性,算法将水印二值图像嵌入小波变换的第  $N$  层低频子带中。

嵌入方法如下:

$$LL'(x, y) = \begin{cases} LL(x, y) + Q & \text{if } \{ (W(x, y) = 0 \& \text{ODD}([LL(x, y)/Q])) \text{ OR } (W(x, y) = 1 \& \text{EVEN}([LL(x, y)/Q])) \} \\ LL(x, y) & \text{if } \{ (W(x, y) = 0 \& \text{EVEN}([LL(x, y)/Q])) \text{ OR } (W(x, y) = 1 \& \text{ODD}([LL(x, y)/Q])) \} \end{cases} \quad (6)$$

$LL'(x, y)$  为修改后的第  $N$  层低频子带系数,  $LL(x, y)$  为源图像的第  $N$  层低频小波系数,  $W(x, y)$  为水印图像。分解后的第  $N$  层低频系数矩阵大小应大于水印图像大小。 $[ ]$  表示向下取整操作,  $\text{EVEN}([LL(x, y)/Q])$  表示  $LL(x, y)/Q$  向下取整后的结果为偶数。 $\text{ODD}([LL(x, y)/Q])$  表示  $LL(x, y)/Q$  向下取整后的结果为奇数。 $Q$  为量化间隔。修改后的结果使得对应水印 0 的低频系数对量化间隔  $Q$  的商值为偶数,对应水印 1 的低频系数对量化间隔  $Q$  的商值为奇数。提取水印时根据低频系数对量化间隔  $Q$  的商值即可提取出水印,不需要源图像的参与,因此这是一种盲水印算法。量化间隔  $Q$  的选择由实验得出,取使得嵌入水印后的图像质量和水印的鲁棒性具有最佳平衡值的  $Q$  值。对变换后的图像进行  $N$  层整数小波逆变换,形成嵌入水印后的图像。

1.2.2 模板的嵌入

设原始图像尺寸为  $N \times N$ 。将嵌入水印后的图像做傅里叶变换,为了得到一个具有完整周期的傅里叶谱图<sup>[5]</sup>,将谱图中心平移到 $(\frac{N}{2}, \frac{N}{2})$ 处。以  $R$  为半径在频谱的中频区域搜索模板点。搜索到的模板点在四个象限内对称分布。取以  $R1$  为半径的区域作为局部区域大小,将模板点的幅值改为局部极大值。对图像做傅氏反变换得到嵌入模板后的图像。半径  $R$  和  $R1$  作为密钥保存。

1.3 提取过程

1.3.1 图像纠正

首先对载体图像做傅氏变换。在环形区域  $S(R1 < R < R2)$  内搜索所有局部极大值。记下极大值点的位置  $(X, Y)$ , 将其转换为极坐标  $(\rho, \theta)$ 。将得到的  $\theta$  值按从小到大的顺序排列, 记为  $(\theta_1', \theta_2', \theta_3', \dots, \theta_n')$ 。根据密钥  $R$  计算出所有模板点的极坐标, 将  $\theta$  值从小到大排列为  $(\theta_1, \theta_2, \theta_3, \dots, \theta_t)$ 。由于在环形区域中搜索范围大于模板点的搜索范围, 所以  $n \geq t$ 。对所有模板点从 1 到 360 度进行匹配, 即让  $i$  从 1 到 360 度对模板点执行以下操作:

Step1: 将所有模板点  $(\theta_1, \theta_2, \theta_3, \dots, \theta_t)$  加上  $i$  度得到  $(\theta_1 + i, \theta_2 + i, \theta_3 + i, \dots, \theta_t + i)$ , 记为  $(u_1, u_2, u_3, \dots, u_t)$ 。如果  $\theta$  与  $i$  相加结果超过 360 度, 则需减去 360 度。

Step2: 将  $(u_1, u_2, u_3, \dots, u_t)$  与  $(\theta_1', \theta_2', \theta_3', \dots, \theta_n')$  进行匹配。若在  $(\theta_1', \theta_2', \theta_3', \dots, \theta_n')$  中找到这样的值, 使得其与  $u_1$  的差值小于阈值  $T$ , 则认为  $u_1$  找到了匹配点。对  $u_2$  至  $u_t$  执行同样的操作, 记下模板匹配点总数。

Step3: 从 1 到 360 度, 取具有最多匹配点个数的度数为图像受到旋转攻击的角度。

Step4: 对图像进行反旋转校正。

1.3.2 水印二值图像的提取

对校正后的载体图像做  $N$  层整数小波变换。提取第  $N$  层的低频系数。对于嵌入水印的系数利用公式 (2) 提取水印比特。

$$W(x, y) = \begin{cases} 0 & \text{if (EVEN([LL(x, y)/Q]))} \\ 1 & \text{if (ODD([LL(x, y)/Q]))} \end{cases} \quad (7)$$

2 实验结果与讨论

按照上述方法, 实验采用将一幅  $16 \times 16$  的二值水印图像嵌入一幅  $256 \times 256$  的男孩图像中, 嵌入时利用图像处理中最常用的整数  $9/7$  小波对图像做四层整数小波变换后, 用公式 (1) 修改小波系数嵌入水印图像。

水印嵌入前后及提取的水印图像如图 2 所示。对旋转角度测试的结果如表 1 所示。图 3 是旋转 15 度得到校正后提取的水印图像。由于旋转和反旋转过程对图像质量有一定影响, 因此校正后的图像提取出的水印会产生一些噪声点, 但是不影响有意义水印图像的阅读。可以对提取后的水印图像采取形态学中的开运算以及去除孤立点操作使水印图像更加清晰易读。

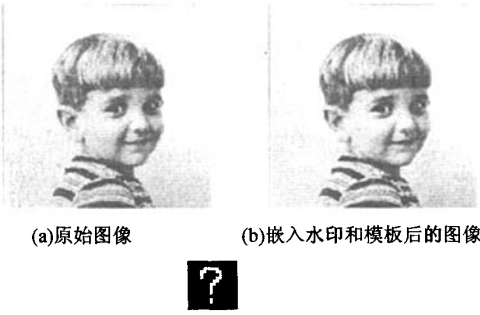


图 2 水印的嵌入及提取图像

表 1 旋转校正效果

旋转攻击度数	1	5	10	22	55	90	170
检测到的度数	1	5	10	22	55	90	170



(a) 旋转 15 度后的图像



(b) 未校正时提取的水印 (c) 校正后提取的水印

图 3 旋转图像及校正后提取的水印

基于小波变换的水印算法已成为频域水印算法的主流算法, 但是其抵抗几何攻击的能力差成了水印技术发展的一个瓶颈。文中提出了一种能抵抗旋转攻击的基于整数小波变换的数字图像盲水印算法。首先通过整数小波变换在低频系数中嵌入有意义的二值水印图像, 然后通过傅氏变换域嵌入模板来检测图像受到的旋转攻击角度, 模板点和水印互不干扰。实验证明, 该算法能有效地纠正受到旋转攻击后的图像, 使水印提取过程达到重同步后准确地提取出水印, 所以该算法是可行的。

(下转第 151 页)

部网(Intranet),企业客户与企业总部及其分公司形成企业外部网(Extranet),OPC XML 客户端通过由 IPSec 和 MPLS 构成的网络与 OPC XML 服务器进行通信,MPLS 作为网络主干部分,根据预留资源,按照标记快速转发。IPSec 与各种用户直接相连,IPSec 模块实施在 CE 路由器上,实施的方式可以采用与操作系统集成,也可以使用堆栈中的块,实施 IPSec 模块的路由器称为安全路由器。

OPC XML 客户端通过 CE 路由器进行 IPSec 安全加密时,根据用户的安全要求不同,可以分为三个级别:

①不作安全要求,无需 IPSec 加密,通过 CE 路由器的 Internet 接口,连接 MPLS 网络,进行快速转发;

②一般安全要求,可以通过 IPSec 的传输模式,保护传输层协议头,实现点到点或端到端的一般安全功能;

③较高安全要求,利用 IPSec 的隧道模式,保护整个 IP 数据包,实现较高级别的安全功能。

下面分析数据在 OPC XML 的安全模型的转发过程。在企业内部网中,企业总部作为 OPC XML 的客户端,访问分公司的 OPC XML 服务器时,通过 OPC XML 客户端发送数据到 CE1 路由器上,根据安全级别,进行加密,保护数据传输的安全性,加密后的数据到达 MPLS 网络的边缘标记路由器 PE1,数据包分配一个转发等效类(FEC),打下标签,然后按照标记在 MPLS 网络中进行快速转发,到达 MPLS 网络另一端边缘后,去掉标签,发送连接目标主机相连的 CE 路由器,进行数据解密后,发送到具体的 OPC XML 服务器,OPC XML 服务器接收数据并处理。在企业外部网中,如企业客户(OPC XML 客户端)与分公司(OPC XML 服务器)访问流程与上述过程相似。

### 3.2 性能分析

(1)满足数据传输的安全性要求。在 CE 路由器设置 IPSec 模块,同时根据安全要求的不同,实行三级分类。因此支持按照用户需求的不同的安全级别保障。

(2)保证数据传输的实时性。在 MPLS 网络实施包括 InterServ,DiffServ 和流量工程等技术,可以提供

比较高的服务质量保证<sup>[5]</sup>。

(3)具有很强的网络扩展能力。该方案业务实施支持多运营商提供端到端的业务。能支持多种用户连接接入,随着企业网点的增多可以通过 ISP 网络服务提供商实施网络的配置和管理。

(4)支持多种实施模式。可以实现企业内部(Intranet)的安全传输,如企业总部与分公司,也可以实现企业外部(Extranet)安全访问,如企业客户与分公司。支持企业内部网、企业外部网和移动用户等多种组网方式。

(5)支持多协议传输和多种用户信息流。MPLS 承载的信息流允许采用多种协议如 IPX、IP,在整个网络中用户信息流可以是 IPv4、IPv6、单播和组播。

## 4 结束语

IPSec 与 MPLS 结合,有利于把 IPSec 的高度安全、可靠的优势与 MPLS 的高速交换、服务质量保证、流量控制以及灵活性、可扩展性发挥出来,提供设计优良、运行正常和综合性的 OPC XML 数据通信安全模型。通过现有的公用网络,建立企业各级安全互连的企业内部网和企业外部网,不仅会节省网络的建设和运行维护费用,而且增强了网络的可靠性和安全性。同时也为 OPC XML 规范的安全部分提出了自己的设计方案。

### 参考文献:

- [1] OPC Foundation. OPC XML - DA Specification Version 1.0 [EB/OL]. 2003 - 07 - 12. <http://www.opcfoundation.org/>.
- [2] 胡越明. Internet 技术及其实现[M]. 北京:高等教育出版社,2003.
- [3] Doraswamy N, Harkins D. IPSec Implementation[EB/OL]. 2004 - 08. <http://www.microsoft.com/technet/itsolutions/network/security>.
- [4] Rosen E, Viswanathan A, Callon R. Multi protocol Label Switching Architecture[S]. RFC3031. 2001.
- [5] Le Faucheur F. Multi Protocol Label Switching(MPLS) Support of Differentiated Services[S]. RFC3270. 2002.

(上接第 147 页)

### 参考文献:

- [1] 刘九芬,黄达人,黄继武. 图像水印抗几何攻击研究综述[J]. 电子与信息学报,2004,26(9):1496 - 1503.
- [2] 飞思科技产品研发中心. 小波分析理论与 MATLAB7 实现[M]. 北京:电子工业出版社,2005:363 - 364.

- [3] 吴永宏,潘 泉,张鸿才,等. 基于提升框架的整数小波变换[J]. 电子与信息学报,2004,26(4):659 - 663.
- [4] Gonzalez R C, Woods R E, Eddins S L. 数字图像处理(英文版)[M]. 北京:电子工业出版社,2004:108 - 112.
- [5] 台莉春,高 珍,张志浩. 基于小波变换的数字水印最佳嵌入位置的研究[J]. 微型电脑应用,2005,21(4):11 - 14.