一种基于时间戳的DCT域零水印方案

刘会英,张政保,文家福,冯 帆
(军械工程学院 计算机工程系,河北 石家庄 050003)

摘 要:提出了一种新的基于时间戳的DCT域图像零水印方案。原始图像进行分块DCT变换后,选取DCT域低频系数作为重要特征,通过混沌置乱与逻辑运算生成零水印,并为生成的零水印加盖时间戳以防止攻击者通过伪造零水印信息来混淆作品版权。在检测过程中利用原始图像几何矩进行水印的二次检测,有效地提高了零水印算法抗攻击能力。实验结果表明,该方案能很好地抵抗JPEG压缩,叠加噪声,裁剪,旋转等攻击,具有较好的可行性和安全性,能很好地实现版权保护功能。

关键词:时间戳;几何矩;二次检测;零水印
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2009)09-0143-03

A DCT-Domain Zero-Watermark Scheme Based on Time Stamping

LIU Hui-ying, ZHANG Zheng-bao, WEN Jia-fu, FENG Fan
(Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract: A kind of zero-watermarking scheme in DCT domain based on time stamp is proposed. The core idea of this scheme is: firstly, select the low frequencies of the DCT domain as important feature to generate zero-watermark by logistic operation and chaos scrambling, then take advantage of time stamp mechanism to prevent the attacker from forging watermark information. Quadric-detecting is adopted by using the geometric moment of the original image, which has greatly improved the capability of the method to resist attacking. Experiment results show this scheme is robust against some usual attacks such as JPEG compression, adding noise, cropping and rotation and so on. This scheme is proved of high feasibility and security and can be used for copyright protection.

Key words: time stamping; geometric moment; quadric-detecting; zero-watermark

0 引 言

数字水印技术是信息隐藏技术领域的重要分支,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[1]。目前大多数算法都属于鲁棒性算法,该类算法始终存在着两个矛盾,也就是不可感知性与鲁棒性间的矛盾,以及不可感知性与水印嵌入量间的矛盾。零水印的提出恰好有效地解决了这两个矛盾。零水印技术是指利用原始图像的重要特征来构造水印,而不对原始图像做任何修改的水印技术[2,3]。文献[2]选取图像高阶累积量作为特征来构造零水印。该算法的主要缺点是计算量过大,对稍大一点的图片(如512×512)可行性不高,另外对乘性噪声干扰的测试效果也不够理想。针对以上缺陷,笔者选取图像DCT低频系数作为特征,并利用混沌置乱和逻辑运算来构造零水印。实验结果表明该算法安全性能好,鲁棒性强。另外,由于零水印并没有向图像作品中真正嵌入水印信息,任何人都能够根据算法从作品中构造自己的水印,因此并不能唯一标识版权。这里,为生成的零水印信息加盖时间戳,用以证明作者在某个时间之前对于某个图像作品的版权声明,从而能很好防止攻击者通过伪造零水印信息来混淆作品版权。

1 基于时间戳的零水印方案设计

时间戳扮演的角色即为数字化的邮戳,可以为任何电子文件提供准确的时间证明,以证明该文件在某一时间点就已存在,即使凭证已过期或取消,它仍具备不可否认性功能,且能验证文件或交易的内容自加上时间戳后是否曾被人修改[4]。

假设作者在将图像作品发表之前,通过时间戳权威机构TSA为生成的零水印加盖时间戳,将图像作品、作者版权水印、时间戳信息三者进行绑定,这样便

收稿日期:2008-12-23;**修回日期**:2009-03-01
基金项目:河北省科技基金项目(05213579)
作者简介:刘会英(1984-),男,硕士研究生,主要研究方向为信息安全;张政保,教授,硕士生导师,主要研究方向为信息安全、多媒体信息处理。

可以将含有时间戳的零水印作为作者在某个时间之前对图像作品的版权声明。而攻击者得到传播图像并伪造出自己的零水印的时间必然滞后于作者。这样，当发生版权纠纷时可以根据零水印中时间戳标记时间的先后来判定版权所属，从而达到解决版权争议的目的。

基于时间戳的零水印方案如图 1 所示：原始图像作品经 8×8 分块 DCT 变换处理后，选择图像 DCT 域低频系数作为重要特征生成二值特征比特 B，再将 B 和版权注册水印 W 利用逻辑运算生成零水印 Wa，最后将 Wa 发往时间戳权威机构 TSA 加盖时间戳，由作者保存含时间戳的零水印 Wa′。在水印检测过程中，首先利用同样的方式从待检测图像中提取二值特征比特 B′，并解密 Wa′得到零水印 Wa 和时间戳 T，然后将 B′和 Wa 进行相反的逻辑运算恢复出版权注册水印 W′，最后通过时间戳 T 来确定零水印生成时间，以及 W 和 W′的互相关系数 NC 值来判定水印有无。

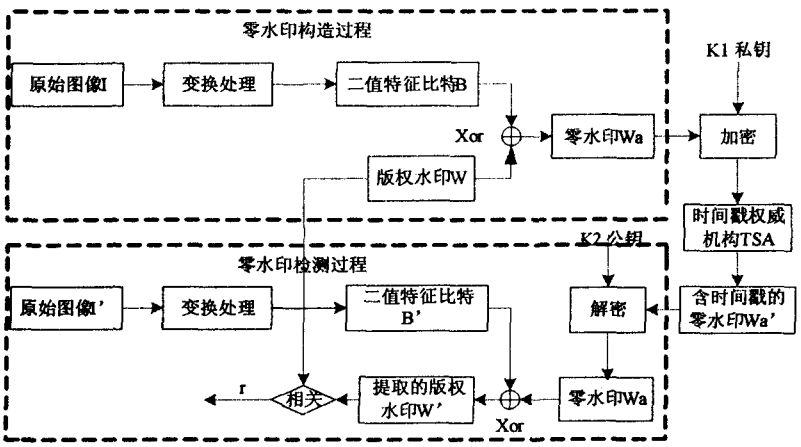


图 1 基于时间戳的零水印方案

2 基于时间戳 DCT 域零水印算法

2.1 Logistic 混沌映射

混沌现象是非线性系统中出现的确定性的类似随机的过程。Logistic 映射是典型的、广为应用的一维混沌模型，其函数如式(1)所示。式(1)中 μ 属于[0 4]，$x_k \in (0\ 1)$。当 $3.569945 < \mu < 4$ 时，Logistic 映射工作处于混沌状态，也就是说给定不同的初值 x_0 时，由式(1)生成的序列非周期，不收敛，不相关。

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

2.2 零水印构造

图像经分块 DCT 变换后，中低频系数集中了原始图像的大部分能量。根据 Watson 感知模型[5]可知人眼对于 DCT 低频系数非常敏感，低频系数的修改很有可能会引起图像视觉上 的较大改变。选取图像的低频系数作为图像的重要特征，一方面可以尽量避免有损压缩对水印信息可能带来的损失，另一方面由于人眼对于低频系数敏感度高，攻击者一般会避免较大改动低频系数，因此低频系数一般很稳定。所以文中选取低频系数作为图像重要特征来构造零水印信息。

零水印的构造过程如图 1 所示，算法步骤如下：

1)对原始图像进行 8×8 分块 DCT 变换，将空域像素矩阵转化为 DCT 系数矩阵。

2)选取分块的 DCT 低频系数构成一维序列 A。

3)根据式(2)将序列 A 转化为二值序列 B

$$B_i = \begin{cases} 0 & A_i \leqslant 0 \\ 1 & A_i > 0 \end{cases} \quad i = 1,\cdots,1024 \tag{2}$$

4)采用 Logistic 映射法对 B 进行混沌置乱，生成二值特征序列 C。混沌发生器初始值作为密钥。利用式(1)生成长度为 4096 的序列 X，与 B 序列一一对应，然后对 X 进行冒泡法排序，将无规则的混沌序列 X 按从小到大的顺序排列，同时与 X 一一对应的 B 序列也被置乱。由于序列 X 为混沌的，对于初值非常敏感，B 也被随机置乱，在没有密钥情况下很难找到置乱规律。这样可以增强水印的安全性。

5)将二值特征序列 C 和版权二值水印图像 W 进行按位异或，获得最终的零水印 Wa。

6)对零水印 Wa 和密钥信息 k_0 用作者私钥进行加密后发给 TSA，并请求加盖时间戳。作者收到 TSA 的响应后用 TSA 的公钥验证 TSA 时间戳签名真实性，若验证通过，则保存 TSA 发送来的含时间戳的版权水印 Wa′。

3 DCT 域零水印检测算法

3.1 图像旋转角度的估计

假设图像是定义在整数笛卡尔坐标系上的实值函数 $f(i,j)$，其中 $1 < i < M, 1 < j < N$，那么图像的 $p+q$ 阶几何矩 m_{pq} 定义为式(3)：

$$m_{pq} = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} i^p j^q f(i,j) \tag{3}$$

$$\theta = \arcsin \frac{m'_{01}m_{10} - m'_{10}m_{01}}{m_{10}^2 + m_{01}^2} \tag{4}$$

设 $f(x,y)$ 表示原始图像，$f(x',y')$ 表示旋转 θ 角度后的图像，定义顺时针旋转 θ 角为负，逆时针为正，图像旋转一定角度后可根据式(4)计算出其旋转角 θ。

其中，m_{10} 和 m_{01}，m'_{10} 和 m'_{01} 分别表示图像旋转前后的一阶几何矩[6,7]。

3.2 水印二次检测方案

由于 DCT 域的零水印无法抵抗旋转攻击,文中通过采用几何矩对含水印图像经过的旋转角度进行估计并校正的二次检测方案来提高算法的抗旋转攻击能力。水印的检测方案步骤如下:

1)对待检测图像进行 8×8 分块 DCT 变换,将空域像素矩阵转化为 DCT 系数矩阵。

2)选取分块的 DCT 低频系数构成一维序列 A。

3)根据式(2)将序列 A 转化为二值序列 B。

4)使用 TSA 的公钥和作者私钥对含有时间戳的版权水印 Wa′进行解密,分离出零水印 Wa,时间戳 T 以及密钥 k_0。

5) 使用 k_0 作为混沌发生器初始值,利用 Logistic 映射法对 B 进行混沌置乱,得到二值特征序列 C。

6)将二值特征序列 C 和零水印 Wa 进行按位异或操作,恢复出版权二值水印图像 W′。

7)根据 W 和 W′的相关系数 NC 值判定水印存在与否。如果 NC 值大于给定阈值,则认为水印存在,版权属于作者;否则,利用几何变换参数估计的方法进行含水印图像旋转角度的校正,对水印进行重同步,然后在此基础上进行零水印的二次检测。对校正后的图像进行零水印二次检测后,若 NC 值大于给定阈值,则认为水印存在,版权属于作者,否则认为水印不存在,版权和作者无关,水印检测结束。

4 实验结果及分析

采用 512×512 的 256 灰度级的 Lena 图像作为原始图像进行实验。在实验中选取 4096 个低频系数构造零水印,即选取 8×8 分块 DCT 变换后每块中的第一个低频系数(0,1)。用互相关系数 NC 值来衡量提取水印和原始水印之间的相似性。原始图像和版权二值水印图像如图 2a 所示。混沌发生器初值 $k_0 = 0.3256, \mu = 3.9$。设定阈值 $T = 0.7$。

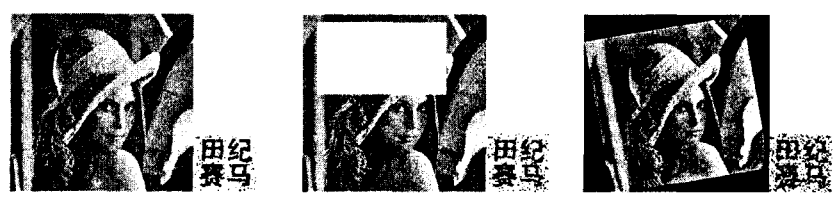
1)JPEG 压缩。不同质量因子所对应的提取出的水印图像的 NC 值如表 1 所示。采用标准 JPEG 格式对含水印图像以不同的质量因子 QF 压缩,然后进行零水印检测。从表中可看出该算法对于 JPEG 压缩鲁棒性很好。QF 为 30% 时提取的版权水印如图 2b 所示。

2) 滤波及加噪攻击。对含水印图像分别采用椒盐噪声,高斯白噪声,中值滤波进行攻击,然后进行检测,检测结果如表 2 所示。从表中可以看出该算法对于一般强度的噪声攻击和滤波处理具有较好的鲁棒性。其中对于椒盐噪声的抵抗能力强于高斯噪声。噪声密度为 0.02 的椒盐噪声攻击以及滤波器大小为 5×1 的中值滤波攻击下提取的版权水印分别如图 2c 和 2d 所示。

表 1　对含水印图像进行 JPEG 压缩后检测结果

压缩质量因子	NC
90%	0.9688
75%	0.9155
50%	0.8576
30%	0.8214

(a) 原始图像以及版权二值水印(64×64)　(b) JPEG 压缩 QF=30%　(c) 椒盐噪声 0.02



(d) 中值滤波[5,1]　(e) 剪切 35%　(f) 旋转 10 度

图 2　经过各种攻击实验后提取的水印图像对比

表 2　对含水印图像进行噪声和滤波攻击后检测结果

噪声攻击	NC	中值滤波	NC
椒盐(0.01)	0.8767	3×1	0.9683
椒盐(0.02)	0.8452	1×3	0.9641
高斯(0,0.005)	0.8076	5×1	0.9492
高斯(0,0.01)	0.7510	1×5	0.9412

3) 剪切攻击。对图像进行不同位置、不同比例的剪切后,进行检测,检测结果如表 3 所示。当剪切强度为 35% 时,NC 仍高于阈值 T,这说明算法能很好对抗剪切攻击。图像被剪切 35% 时提取的版权水印如图 2e 所示。

表 3　对含水印图像进行不同比例裁剪后检测结果

剪切强度	NC
6%	0.9783
15%	0.9246
25%	0.9024
35%	0.8642

4)旋转攻击。从一次检测结果可以看出,DCT 域零水印算法不能对抗旋转攻击。从二次检测结果可以看出,利用图像几何矩对旋转图像进行参数估计并校正,然后进行检测,能明显提高算法对旋转攻击的鲁棒

(下转第 172 页)

UART 作为系统的标准输入和输出接口，GPIO 接口外接发光 LED，用作系统的状态指示。硬件平台本身与 FC IP 的测试结果通过 UART 输出到 PC 机上显示或通过 GPIO 输出相应的信号。

最终，使用带有光电收发器的 Virtex2－Pro FPGA 开发验证板，将在 EDK 下生成的系统逻辑和测试程序通过编程器下载到 FPGA 中，进行单板光纤环绕通信或板间点到点通信验证。通过实物平台，结合 FC 分析仪，验证了 FC IP 的设计满足 FC－PH 以及 FC－FS 等标准的要求各接口功能正确。重点测试项包括了寄存器资源测试、硬件接口测试、链路管理验证、不同服务类型数据帧和控制帧收发测试、无效帧测试、信用管理测试、速度协商测试、结点(两板)互联通信测试、FC－2 层协议解析和处理流程(包括结点注册、注销)测试等。结合对应测试程序，在 FPGA 平台上进行了基于此 FC IP 核的光纤通信的性能测试，结果表明，满足 FC 通信在 1G、2G 速率配置时的性能要求。

5 结束语

光纤通道以其传输速度高、兼容性好等特点，将在未来的航空电子统一网络中得到广泛的应用[7]，将 FC－2 协议处理以及完成 FC－1 层协议和对 FC－0 层协议支持的基础硬件以 IP 核的形式实现，可对下一步设计高性能的的 FC 协议芯片奠定良好基础。对 IP 核进行验证的关键是验证 IP 内部逻辑的详尽功能以确保 IP 的正确实现。如上文所述，将功能仿真与 FPGA 验证相结合，完成了对 FC IP 核的目的性验证和等效性验证[8]，证明其实现了预定功能，符合设计要求。

参考文献：

[1] ANSI. Fibre Channel Framing and Signaling－2(FC－FS－2). Rev0.01[M]. US:ANSI,2003.

[3] ANSI. Fibre Channel Physical and Signaling Interface (FC－PH),X3[M]. US:ANSI,1994.

[2] 苏连栋. 光纤通道在综合航电系统应用中的关键技术[J]. 飞机设计,2007,27(4):66－70.

[4] 郑学仁，邓婉玲，范健明，等. An IP Simulation and Verification Platform Based on FPGA[J]. 华南理工大学学报：自然科学版,2006,34(1):38－42.

[5] 韩 霞，杨洪斌，吴 悦. 面向 SoC 的事务级验证研究[J]. 计算机技术与发展,2007,17(3):33－36.

[6] 赵文波，黄士坦. Fiber Channel 协议分析[J]. 计算机技术与发展,2006,16(12):35－38.

[7] 章宇东. SOC 技术在 FC 芯片设计中的应用[J]. 航空电子技术,2005,36(1):42－48.

[8] 信息产业部集成电路 IP 核标准工作组.《集成电路 IP 核开发与集成的功能验证分类法》概要[J]. 信息技术与标准化,2008(1－2):30－33.

(上接第 145 页)

性(见表 4)。图像旋转 10 度后，经几何矩估计并校正后提取的版权水印如图 2f 所示。

表 4 对含水印图像进行旋转后两次检测结果

旋转角度	(一次检测)NC	(二次检测)NC
－3 度	0.5136	0.9055
3 度	0.5124	0.9036
5 度	0.4963	0.8860
10 度	0.4751	0.8336

5 结束语

给出一种基于时间戳的 DCT 域零水印方案。原始图像进行分块 DCT 变换后，选择 DCT 低频系数作为图像重要特征量，通过混沌置乱和逻辑运算生成零水印，最后通过时间戳权威机构对生成的零水印加盖时间戳，以防止攻击者通过伪造水印信息来混淆作品版权。在水印检测过程中，采用几何矩对含水印图像旋转角度进行估计并校正的二次检测方案，有效地提高了算法抗攻击能力。实验结果表明，该方案对各种常见的图像操作和攻击具有很强的鲁棒性，并且算法中使用了私人密钥，具有很高的安全性，能很好地解决版权争议问题。

参考文献：

[1] 朱佳婷，吕建平. 抗旋转的整数小波变换数字水印算法[J]. 计算机技术与发展,2007,17(7):145－147.

[2] 温 泉，孙锬峰，王树勋. 零水印的概念和应用[J]. 电子学报,2003,31(2):214－216.

[3] 杨树国，李春霞，孙 枫，等. 基于小波变换的零水印方案[J]. 计算机工程与应用,2003(29):128－130.

[4] 王 勇，朱方金，史清华. PKI 中数字时间戳技术[J]. 大连理工大学学报,2003,43(S1):27－29.

[5] Watson A B. DCT Quantization Matrices Optimized for Individual Images[J]. Human Vision, Visual Processing and Digital Display IV,1993,1913:202－216.

[6] 张 力，肖薇薇，张基宏. 基于原始图像矩的仿射不变性水印算法[J]. 深圳大学学报：理工版,2003,20(2):16－21.

[7] Masound A, Ahmed H T. 图像水印技术中几何变换的校正[M]//SPIE 安全与多媒体水印技术. 美国加利福尼亚：[出版者不详],2000:381－392.