

# 基于 JPEG 压缩的水印算法

赵金凤<sup>1</sup>, 李陶深<sup>1,2</sup>, 兰红星<sup>1,2</sup>

(1. 广西大学 计算机与电子信息学院, 广西 南宁 530004;

2. 中南大学 信息科学与工程学院, 湖南 长沙 410083)

**摘要:**提出了一种基于 JPEG 压缩的盲水印算法。在算法中首先对水印图像进行纠错编码和置乱变换双重预处理技术, 提高水印自身抵御攻击的能力。水印嵌入是在量化的过程中进行, 并根据各块的特征确定嵌入强度, 以保证嵌入图像后的视觉效果; 水印的提取不需要原始图像的参与, 实现了盲水印检测。实验结果表明: 该算法有很好的抵御 JPEG 压缩的性能, 对于噪声等也有较好的鲁棒性。

**关键词:**数字水印; JPEG; 置乱变换; 量化嵌入; 盲水印

**中图分类号:**TP391

**文献标识码:**A

**文章编号:**1673-629X(2006)12-0247-03

## A Digital - Watermark Algorithm Based on JPEG

ZHAO Jin-feng<sup>1</sup>, LI Tao-shen<sup>1,2</sup>, LAN Hong-xing<sup>1,2</sup>

(1. School of Computer, Electronics and Information, Guangxi University, Nanning 530004, China;

2. School of Information Science and Engineering, Central South University, Changsha 410083, China)

**Abstract:** A new blind digital - watermark algorithm is proposed in this paper. This algorithm uses correct - encode technique and scrambling technique in the pre - procession of the watermark to improve the capability of resisting attacks. The watermark is inserted parallel with qualification, and the embedding strength factor is adaptive for each selected image block to make sure the visualization of the image. The watermark does not need origin image so that can implement blind watermark detection. The experimental results show that it has good ability to withstand JPEG compression and better robust to noises.

**Key words:** digital watermark; JPEG; scrambling changes; qualified insertion; blind watermark

## 0 引言

数字水印技术作为实现版权保护的有效方法, 近几年来已成为多媒体信息安全研究领域的一项重要技术。它通过在原始数据中嵌入秘密信息——水印来证实该数据的所有权, 被嵌入的水印可以是一段文字、标识、序列号等。水印信息与媒体内容集成在一起, 不需要额外的存储空间, 并且可以经历一些不破坏原数据的操作而存在。数字水印与信号处理、编码理论、加密技术、检测理论等领域的不断结合<sup>[1,2]</sup>, 使之得到了飞快发展。

在对数字水印技术的研究过程中, 人们发现它和压缩技术在许多方面有着相同或者相似的特点, 借鉴压缩技术 (JPEG) 的研究成果, 可以进一步推动水印技术的研究。由于存储资源和网络带宽的限制, 多媒体数据通常都是以压缩形式存储和传输的, 因此研究直接与压缩过程相结合

的水印算法将更有实际意义。近几年来, 对压缩域的水印的研究已经引起了业界人士的广泛关注<sup>[3,4]</sup>, 但目前基于 JPEG 压缩的水印算法还少有文献报道。

文中提出了一种基于 JPEG 压缩的盲水印算法。该算法的基本思想是通过对水印进行预处理 (纠错编码和置乱变换) 提高水印自身的抵御攻击的能力, 再将其嵌入到原始图像的分块 DCT 的部分系数中, 并利用各块的特征自适应地嵌入水印, 嵌入过程与量化过程是同步进行的。这种基于量化的方法, 能够实现盲水印检测。

## 1 水印的预处理

为了提高水印的鲁棒性, 采用了双重预处理技术, 首先对水印进行纠错编码, 来提高其自纠错能力; 然后再进行置乱变换, 以进一步提高水印的稳健性。

### 1.1 纠错编码

纠错编码的基本思想<sup>[5]</sup>是: 通过对原信息序列进行某种变换, 使原来彼此独立、互不相关的信息码元变成具有一定的相关性和规律性的数据序列, 从而在接收端能够根据这种规律检错, 并纠正码元在信道传输中所造成的差错。将纠错编码的原理引入水印算法进行差错控制, 可以提高水印的稳健性。

收稿日期: 2006-02-22

基金项目: 广西留学回国人员科学基金项目 (桂科回 0342001); 广西科技攻关项目 (桂科攻 033008-9)

作者简介: 赵金凤 (1980-), 女, 河南许昌人, 硕士研究生, 研究方向为数字水印、信息安全; 李陶深, 教授, 研究方向为分布式工程数据库、网络安全、网络路由算法; 兰红星, 研究员, 研究方向为网络安全。

目前用于水印的纠错编码主要有汉明码、BCH 码、卷积码、turbo 码等。考虑到水印简单易用的要求和效率性,采用了(7,4)汉明码。这是一种可以纠正所有单个随机错误的高效率分组码,其中信息码元位: $b=4$ (记为  $b_3, b_2, b_1, b_0$ ),监督码元位: $r=3$ (记为  $r_2, r_1, r_0$ ),码字总长  $m=7$ (记为  $b_3, b_2, b_1, b_0, r_2, r_1, r_0$ )。根据异或关系与多重监督原则,有:

$$\begin{aligned} r_2 &= b_3 \oplus b_2 \oplus b_1 & r_1 &= b_3 \oplus b_2 \oplus b_0 & r_0 &= b_3 \oplus b_1 \oplus b_0 \end{aligned} \quad (1)$$

其纠错原理为:由于分组码是通过附加监督码元来实现对信息码元的监督,两者之间通过监督方程组建立相互约束关系。当信息码元或监督码元在传输过程中发生错误时,方程组与这些码元对应的相互制约关系就会被破坏,接收端通过校验监督方程来发现错误,且当只有单个错误时,就能知道错误的位置并给以纠正。由(1)式可知原信息码元与监督码元满足下列偶校验关系:

$$\begin{aligned} s_1 &= b_3 \oplus b_2 \oplus b_1 \oplus r_2 = 0 & s_2 &= b_3 \oplus b_2 \oplus b_0 \oplus r_1 = 0 \\ s_3 &= b_3 \oplus b_1 \oplus b_0 \oplus r_0 = 0 \end{aligned} \quad (2)$$

根据一致监督关系,如果接收的码组没有错误,则  $s_1 = s_2 = s_3 = 0$ ;当码组在传输过程中发生单个错误时,则在  $s_1, s_2, s_3$  的计算结果中至少有一个不为零。这样,根据结果就可以惟一地确定错误的位置并给与纠正。

通过以上的分析可以看出,纠错编码是通过增加冗余信息来提高水印的鲁棒性的。

## 1.2 置乱变换

图像置乱变换是通过数字图像的位置或灰度级等作变换,来扰乱图像,以达到在一定程度上迷惑第三者的目的。现有的图像置乱加密技术有 Arnold 变换、Hilbert 曲线变换、Fibonacci 变换、幻方变换,等等。文中采用的是 Arnold 变换,Arnold 变换方法将原来的  $(x, y)$  处像素对应的灰度值移动至变换后的点  $(x', y')$  处,重复迭代则可以得到比较满意的置乱效果。

## 2 水印的嵌入过程

### 2.1 量化嵌入

#### (1) 量化嵌入的基本思想。

基于量化的水印算法<sup>[3]</sup>的主要思想是:根据水印信息的不同将原始载体数据量化到不同的量化区间,检测时根据数据所属的量化区间来识别水印信息。目前,基于量化的方法主要有两种:QIM(Quantized Index Modulation)方法和 SCS(Scalar Cost Scheme)方法,前一种方法是鲁棒的,用于版权保护;后一种方法是脆弱的,用于内容认证。

#### (2) 块自适应的嵌入强度。

嵌入强度自适应方法<sup>[6,7]</sup>是指在加法、乘法或非线性嵌入规则的嵌入因子随着像素局部特征、块空域特征或者变换域特征变化而变化的方法。文中采用基于图像块特征的方法,它根据照度掩蔽特征和纹理掩蔽特征将图像进

行分类,不同类别的嵌入强度不同,以此来适应图像不同区域的变化。把图像大致分为以下几类:

第一类照度较低,且灰度变化比较平滑,HVS 对其中像素值改变较为敏感,叠加的水印分量的强度敏感性最弱。

第三类照度较高,纹理复杂,且是边缘,HVS 对其中像素值的改变敏感性较小。

第四类照度较高,纹理复杂,且不是边缘,HVS 对其中像素值的改变敏感性最弱,叠加的水印的轻度应最大。

余下的为第二类。通过大量实验,将 1,2,3,4 类的系数分别定为 0.4,3,4,6。

### 2.2 嵌入过程

算法中水印嵌入的流程如图 1 所示。

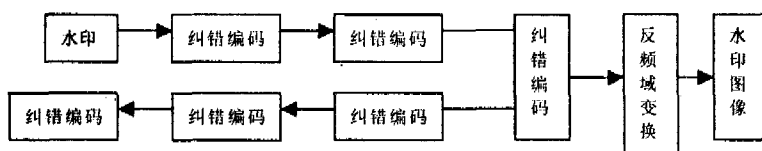


图 1 水印嵌入的流程图

嵌入水印具体步骤如下:

① 按照上面提到的置乱变换方法和纠错编码方法把水印信息进行预处理。

② 对原图像进行 DCT,并选择出图像块方差比较小的图像块嵌入水印信息。

③ 将水印自适应地嵌入到所选择的块的中频系数当中。

④ 将得到的系数进行 IDCT,即得到嵌入水印后的图像。

之所以水印嵌入的位置选择在经过 DCT 变换后的中频系数当中,是因为在压缩过程中高频的信息容易损失掉,不易嵌入水印,而低频集中了图像的主要能量,嵌入水印容易引起图像的视觉效果。

设  $X_i$  是所要嵌入水印信息的图像块 DCT 后按之字形排列得到的第  $i$  个系数,则有:

$$X_i^w = Q_i(X_i, w_j) + (1 - \alpha)E_i(X_i, w_j)$$

其中

$$Q_i(X_i, w_j) = \text{div}(X_i - d(w_j), \text{Qua}(i)) \times \text{Qua}(i) + d(w_j)$$

$$E_i(X_i, w_j) = X_i - Q_i(X_i, w_j)$$

$$d(w_j) = \begin{cases} \frac{\text{Qua}(i)}{4}, & w_j = 0 \\ -\frac{\text{Qua}(i)}{4}, & w_j = 1 \end{cases}$$

其中,Qua 是 JPEG 压缩标准中推荐的压缩量化表,Qua( $i$ ) 是量化表中之字形排列的第  $i$  个量化阶距; $w_j$  是水印信息的第  $j$  个系数; $X_i$  是嵌入水印后的 DCT 系数; $\alpha$  是各块的自适应嵌入强度。

### 3 水印的提取过程

水印的提取算法流程如图 2 所示。算法中水印嵌入

的流程如图 1 所示。

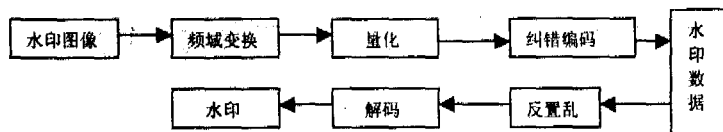


图 2 水印提取的流程图

水印的提取过程是一个盲水印提取的过程,处理过程比较简单。具体的水印步骤如下:

① 对水印图像进行 DCT 变换。

② 提取的具体算法为:

$$w_j = \text{mod}(\text{round}(Q_i(X_i, w_j) - \text{Qua}(i)/4, \text{Qua}(i)/2), 2)$$

③ 对得到的水印信息进行纠错解码和反置乱变换即得到了提取的水印。

#### 4 算法的实验结果

实验采取的原始图像是  $256 \times 256$  的灰度级 Lena 图像,水印采用的是  $48 \times 48$  的二值 mark 图像。实验结果如图 3 所示。



图 3 实验结果示意图

对水印图像进行各种常见的攻击后提取水印的实验结果如图 4 所示。

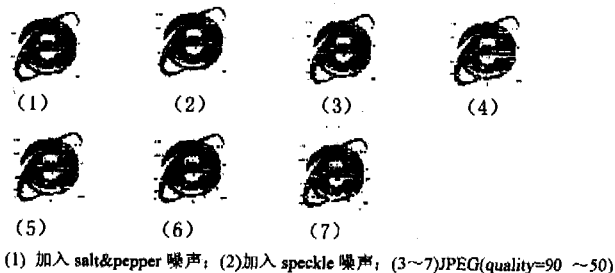


图 4 各种常见的攻击后提取水印的实验结果图

由图 3、图 4 的实验结果可以看出,文中提出的算法对 JPEG 压缩有很强的抵御能力。

表 1 给出了算法和参考文献[8]所提出的相关算法的对比结果。从对比结果可以看出,该算法抵御 JPEG 压缩的能力比文献[8]中提出的算法强:文献[8]的算法在质量因子为 70 时,提取的水印已经无法辨认;而文中的算法在质量因子为 50 时提取的水印仍然比较清晰,提取的水印

和原水印  $NC = 0.9445$ ,即两图像的相关系数仍然较大。同时,直接提取水印时,嵌入水印的图像的视觉效果更好,质量更佳(由 PSNR 参数得出)。

表 1 文中算法与其他算法的对比结果

	直接提取		加 salt & pepper 噪声		加 speckle 噪声	
	PSNR	NC	PSNR	NC	PSNR	NC
文献[8]的算法	101.6205	0.9889	79.8039	0.9453	79.7640	0.9546
文中算法	76.8889	0.9874	91.0603	0.9882	88.9137	0.9823
	JPEG(90)		JPEG(70)		JPEG(50)	
	PSNR	NC	PSNR	NC	PSNR	NC
文献[8]的算法	87.9312	0.9327	83.0190	0.6594	81.0860	0.6.22
文中算法	76.4658	0.9763	75.8942	0.9672	75.7190	0.9445

表 2 给出的是文中算法与参考文献[9]提出的算法的实验比较结果。由表 2 可以看出:文中算法在 JPEG 压缩质量因子较大(即压缩比较小)时,与文献 11 的算法性能相当;而随着质量因子逐渐减小(即压缩比逐渐增大后),文中算法提取出的水印和原水印的 NC(相关性)明显比文献[9]中的算法要大。当质量因子为 50 时,文献[9]的算法中的 NC 为 0.653,此时提取出的水印视觉效果明显较差,而文中算法 NC 仍然为 0.955,视觉效果仍然较好。

表 2 文中算法与其他算法的对比结果

JPEG 质量因子		100%	90%	80%	70%	60%	50%
NC	文献[9]的算法	0.999	0.988	0.960	0.908	0.852	0.653
	文中算法	0.999	0.985	0.978	0.972	0.963	0.955

#### 5 结束语

提出了一种新的基于 JPEG 压缩的盲水印算法。算法首先对水印进行多重预处理操作,提高了水印自身的修复和抗攻击能力。在嵌入水印之前,首先对图像本身进行分析,将水印嵌入到方差较小的那些块中,以保证嵌入水印图像的视觉效果。在量化的过程中根据各块的特征自适应地决定水印的嵌入强度,利用了图像块的局部特征,更进一步保证了图像的视觉效果,同时由于这些所选择的分析特征是图像所有者所知的,更保证了其鲁棒性。水印提取的过程则不需要原始图像的参与,实现了盲水印检测。从实验的结果中可以看出,文中提出的水印算法有很好的抵御 JPEG 压缩的能力,与其他算法相比,其视觉效果更好。

#### 参考文献:

- [1] Cox I J, Miller M L, Bloom J A. 数字水印[M]. 王颖,黄志蓓,等译. 北京:电子工业出版社,2003.
- [2] Kutter M, Winkler S. A Vision - Based Masking Model for Spread - Spectrum Image Watermarking[J]. IEEE, Transactions on Image Processing, 2002(1):16 - 25.

(下转第 252 页)

是标准的 XML 文件,它们存于安全服务器上且在整个集群内可见。

安全模块一旦加载,系统内主客体需要赋予安全标识,在本实现中,主体就是进程。

#### 1) 主体。

(1) 模块初始化时,扫描所有进程,为每个进程赋予安全标识;

(2) 父进程执行 fork() 系统调用创建子进程,首先判断父进程有没有 fork() 权限,如果有,子进程将自动获取父进程的安全标识,除非显式地为这个子进程指定一新的安全标识;

(3) 如果子进程执行了 exec 类的系统调用,首先判断进程有没有 exec 类系统调用权限,如果有,将依据 exec 调用的客体(文件)安全属性重新赋予安全标识。

2) 客体。标识是动态创建的,在每次访问时,由安全模块检查该客体是否有安全标识,如没有就赋予一默认标识。默认标识的创建方法由配置文件和规则文件给出,利用原有的 Linux 传统访问控制标记的权限设定(文件属主、同组用户、其他用户),通过简单的换算关系得到。

3) 网络标识。当一个节点上的主体(进程)访问另一节点的客体时,它首先要取得本地 socket 的访问权限,在得到本地 socket 后,SnID(security node identifier, 节点安全标识)和 SID(subject identifier, 主体标识)将被添加到 IP 包的包头中(通过 LSM 在 IP 协议栈中的 hook)。在接收端,SnID 和 SID 将从包头中取出,然后创建一唯一的网络安全标识 NSID(network security ID), $NSID = \text{Function}(\text{SnID}, \text{SID})$ ,在当前的实现中,NSID 通过查找表换算得到,然后 NSID 就可以用于本地访问控制。

图 3 给出了跨节点的 MAC 的工作过程。假设节点 SnID2 上的主体 2(678# 进程,拥有标识 SID2)想要访问位于节点 SnID1 上的文件。那么首先主体 2 访问本地的通信资源(本地 socket),得到标识对(SnID2, SID2),然后写到 IP 包头中传递给远端节点。在远端节点 SnID1,这些标识从包头中取出,然后映射成唯一的 NSID。根据 NSID 将在本地得到主客体非等级类别和等级分类以及节点间的访问控制关系,最后依据安全判定规则裁决本次访问。当本次访问得到允许,主体 1(123# 进程)将成为主体 2 的代理执行本次访问。

### 3 结 论

经过测试,基于 LSM 的分布式强制访问控制可以用于 Linux 的集群环境中,可以有效抵御“木马”、“缓冲区溢出”等恶意程序的攻击。但某些情况下,性能会有比较大的损失,比如远程(跨节点的)UDP 访问时间效率大约损失 30% 左右(限于篇幅省略了详细的测试过程),系统的优化以及其他安全策略的实现将留待将来实现。

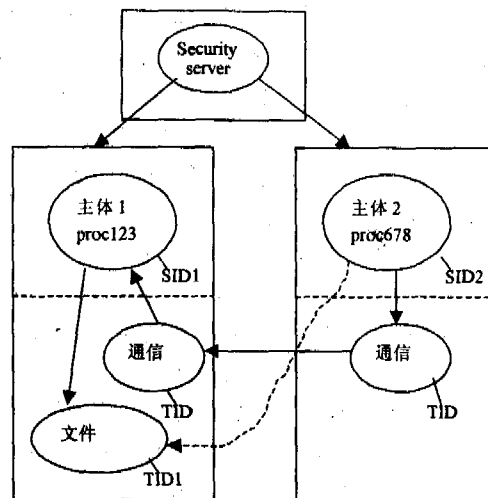


图 3 跨节点的 MAC

#### 参考文献:

- [1] Wright C, Cowan C, Morris J, et al. Linux Security Module Framework[EB/OL]. 2002. <http://www.immunix.org>.
- [2] Loscocco P, Smalley S. Integrating Flexible Support for Security Policies into the Linux Operating System[EB/OL]. 2001. <http://www.nsa.gov/selinux>.
- [3] Bell D E, LaPadula L J. Secure Computer System: Unified Exposition and MULTICS Interpretation [M]. MTR - 2997 Rev. 1. Bedford, MA: The MITRE Corporation, 1976.
- [4] 阮越, 王成耀. 基于 LSM 的安全访问控制实现[J]. 计算机工程, 2004, 30(1): 4-5.
- [5] ISO 10181-3 Security Frameworks for Open Systems: Access Control Framework[S]. 1996.
- [6] Zakrzewski M, Haddad I. A Distributed Security Infrastructure for Carrier Class Linux Clusters[R]. Canada: Open Systems Lab, Ericsson Research Canada, 2003.
- [3] Suhai M A, Obaidat A M S. A comparative study of digital watermarking in JPEG and JPEG2000 environments[J]. ELSEVIER, Information Sciences, 2003, 151: 93-105.
- [4] LI C T. Digital fragile watermarking scheme for authentication of JPEG images[J]. IEE Proc. - Vis. Image Signal Process, 2004, 151: 460-465.
- [5] Loo P, Kingsbury N. Watermark Detection Based on the Properties of error control codes[J]. IEE, - Vis: Image Signal Process, 2003, 150: 115-121.
- [6] Delaigle J F, De Vleeschouwer C, Macq B. Watermarking Algorithm Based on A Human Visual Model[J]. ELSEVIER, Signal Processing, 1988, 66: 319-335.
- [7] 孙鑫, 易开祥, 费敏. 一种基于图像特征区域的数字水印系统[J]. 计算机工程与应用, 2002(23): 88-91.
- [8] 丁玮, 闫伟齐, 齐东旭. 基于离散余弦变换的数字水印图像[J]. 北方工业大学学报, 1999, 11(9): 71-75.
- [9] 牛夏牧, 陆哲明, 孙圣和. 彩色数字水印嵌入技术[J]. 电子学报, 2000, 28(9): 10-12.

(上接第 249 页)