一种基于模运算的数字水印隐藏算法

宋 琪[1],朱光喜[1],容太平[1],罗航建[2]
(1. 华中科技大学电信系,湖北武汉 430074;2. 武汉长通公司,湖北武汉 430070)

摘 要: 数字水印技术是进行数字产品版权保护的一种手段. 本文提出了一种基于模运算的数字水印隐藏方法,该方法具有以下性能: ①水印的隐藏效果较好; ②在水印的嵌入和提取过程中需个人的密钥,因此不知该密钥的用户无法正确恢复水印; ③在计算嵌入水印的位置时,采用了具有不可逆性质的方法,因而非法用户无法获得水印的嵌入位置; ④水印的提取无需原始图像; ⑤可以抵抗 LSB 进攻、BIT-COMPLEMENT[4] 进攻和剪切进攻.

关键词: 版权保护; 数字水印; 模运算; 数据隐藏
中图分类号: TP309 **文献标识码**: A **文章编号**: 0372-2112 (2002) 06-0890-03

A Kind of Digital Watermarking Algorithm Based on Modulo

SONG Qi[1], ZHU Guang-xi[1], RONG Tai-ping[1], LUO Hang-jian[2]
(1. *Dept. of Electronics & Information, Huazhong University of Sci & Tech, Wuhan, Hubei* 430074, *China*;
2. *Wuhan Changjiang Communications Industry Group Limited-Liability Co., Wuhan, Hubei* 430070, *China*)

Abstract: Digital watermarking technology is a kind of method to protect digital products. This paper proposes a new watermarking algorithm based on integer modulo. The features of presented method to embed the watermark are: ①the difference between the watermarked and the original image is perceptually invisible; ②using a secret key in the procession of embedding and retrieving the watermark; ③the position for embedding is random and calculation procession for the position is irreversible; ④retrieval of the embedded watermark does not need the original image; ⑤the watermark is robust against LSB, BIT-COMPLEMENT[4] and cut attack.

Key words: copyright protection; digital watermarking; modulo; data hiding

1 引言

随着以微电子技术为代表的信息产业的飞速发展和网络的迅速普及,快捷廉价的数字传输手段面临着新的挑战——数字产品(如电子出版物,数字视频、音频产品等)的侵权、盗版和任意篡改. 现有的一些先进技术已被用于防止非法盗版,例如密码技术,但仅靠密码技术并不能完全解决这一问题,因为密钥加密只能在数据的传输过程中对数据进行保护,一旦数据被接收并进行解密后,产品将不再受到保护. 数字水印就是在这样一种需求下产生的. 数字水印技术是一种新型的数字产品版权保护技术,它利用数据隐藏技术将特定的信息隐藏在数字产品中,从而达到标识和保护数字产品的著作权、版权的目的,或证明产品的真实可靠性.

目前,国际上已出现了许多数字水印方案[1~5],但由于数字水印的研究是基于信号处理、数字通信、密码学等多学科领域的思想,一种数字水印方法总是不可避免地存在着这些领域的一些固有缺点. 文献[3]提出了一种基于单向哈希函数的数字水印方法,但遭到了文[4]的攻击. 本文借鉴了文[3]的采用不可逆运算可提高算法安全性的思想,提出了一种基于模运算的,采用私人密钥的数字水印算法,该算法不仅隐藏效果好,而且安全性也较好,既可抵抗 LSB 进攻,又可抵抗 BIT-COMPLEMENT(以下简称 B-C) 进攻和剪切进攻.

收稿日期:2001-02-12;修回日期:2002-01-31
基金项目:国家教育部科技重点项目(No. 200175)

2 基于模运算的数字水印算法

2.1 水印隐藏算法

将原始灰度图像表示为 $m_x \times m_y \times m_z$,这里,$m_x \times m_y$ 是图像的大小,m_z 代表计算机要用多少位来表示一个像素的灰度级. 例如,若某图像的灰度级为 256,则由于 $256 = 2^8$,因此 $m_z = 8$. 水印图像是一 $n_x \times n_y$ 二值图像.

水印的隐藏分以下几步进行:

(1)随机选取一大素数 n,输入私钥 K,通过以下方法获得种子 X, Y, Z:

$$X = K \bmod n$$
$$Y = K^2 \bmod n$$
$$Z = K^4 \bmod n$$

这里,n 可公开,而私钥 K 保密,这样即使算法公开亦能保证其安全性.

(2)利用以下算式计算得到嵌入水印的第一个位置:

$$x = X \bmod m_x$$
$$y = Y \bmod m_y$$
$$z = Z \bmod m_z$$

⑶将水印图像中的 1 比特嵌入到 (x, y, z) 中;

⑷先利用下面两个算式计算出两个量,再由这两个量得到下一嵌入位置 (x, y, z):

$$dir = (dis + pix\_num + K) \bmod 8 \quad (1)$$

$$dis = (dir + pix\_num) \bmod m_x + 1 \quad (2)$$

其中,dir 表示下一嵌入位置的方向,即由现在的嵌入位置往何方向移动才可到达下一位置,dis 表示移动的步长(见图 1 和图 2 及相关说明),pix_num 则表示已隐藏的水印比特数. 式(1)中的 8 代表着 8 个邻域,式(2)中加 1 是为了防止出现距离等于 0 的情况.

⑸重复 ⑶、⑷,直至水印图像中的每个比特都被嵌入到原始图像中.

可以看出,在此算法中,除水印信息的第一个比特的嵌入位置由私钥及任选的大素数决定以外,其余位置皆由上一位置处像素的灰度值及已嵌入的比特数决定(即第(4)步). 具体是这样确定的:

选取八邻域,方向如图 1 所示. 若此时隐藏位置为图 1 中的 # 处,且通过(1)、(2)分别计算得到 $dir = 3$, $dis = 4$,则下一隐藏位置处于方向在 # 的左上方,距离 # 有 $dis - 1$ 个像素远的那个像素,如果已到达图像的左边缘或上边缘,则循环到右边或下边,如图 2 所示,# 的下一位置在 * 处.

3	2	1
4	#	0
5	6	7

图 1

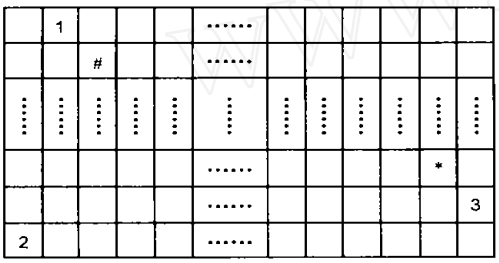

图 2

2.2　水印提取算法

水印的提取与水印的隐藏基本上是两个对称的过程:

⑴输入密钥 K,计算种子 X, Y, Z;

⑵计算第一个隐藏位置 (x, y, z);

⑶从 (x, y, z) 处提取一个比特;

⑷计算下一隐藏位置;

⑸重复 ⑶、⑷,直至水印图像的每个比特都被提取出来.

2.3　关键技术

在以上的水印隐藏与提取过程中,有两个问题需要解决:第一,计算出的隐藏位置 (x, y, z) 可能出现冲突;第二,计算出的 z 可能位于像素的最高比特,若修改此位,则嵌入水印后的图像就会出现较严重的失真.

实验中,分别采用了以下解决办法:

(1)建立一个临时表来记录已嵌入了水印信息的位置 (x, y, z),每计算出一组 (x, y, z) 后就到表中查找,如果在表中能找到一组相同的 (x, y, z),则表明产生冲突,这时就放弃该组 (x, y, z),再计算下一组;否则,将该组 (x, y, z) 放入临时表中,并在该 (x, y, z) 处嵌入一个比特的水印信息.

(2)为了解决第二个问题及有效抵抗 LSB 进攻,每当计算出一组 (x, y, z) 后,我们检查的 z 值,若 $z = 1$ 或 $z = 8$,则放弃该组 (x, y, z);否则,检查 (x, y) 处像素的第 z 位,若该位与所需嵌入的水印比特相同,则不做任何修改,继续计算下一隐藏位置,若二者不同,则修改该比特. 由于仅修改该位可能造成此像素的灰度值与原图像中该像素的灰度值相差很大,从而嵌入水印后的图像与原始图像相比变化太大,因此不仅要改变该像素的第 z 位,而且其余各位也要相应变化,以使改动过的像素,其灰度值与原图像中该像素的灰度值相差最小. 值得注意的是,如果该像素的其它位上已隐藏有水印信息,则不能修改这些位. 举个例子,某像素为 $(b_8\, b_7\, b_6\, b_5\, b_4\, b_3\, b_2\, b_1)$,其中 b_3 为已嵌入了水印信息的位,现计算得 $z = 6$,那么我们只能修改 $b_8, b_7, b_5, b_3, b_2, b_1$ 这些位,(假设修改为 $p_8, p_7, p_5, p_4, p_2, p_1$)以使 $(p_8\, p_7\, b_6\, p_5\, p_4\, p_3\, p_2\, p_1)$ 与 $(b_8\, b_7\, b_6\, b_5\, b_4\, b_3\, b_2\, b_1)$ 之间相差最小.

3　实验结果

实验中采用的原始图像为标准图像 Lena(256 ×256),水印图像为写有"华中科技"四个字的二值图像(64 ×64). 为了评价嵌入水印后的图像的质量,我们仍沿用了文献[3]中的指标 PSNR. PSNR 值越大,图像的质量就越好.

图 3 为嵌入水印后的图像 wmLena(PSNR = 55.67)及从中提取出的水印.

图 3　嵌入水印后的图像 wmLena(PSNR = 55.67)及从中提取出的水印

图 4　遭受剪切攻击后的 wmLena(PSNR = 33.20)及从中提取出的水印

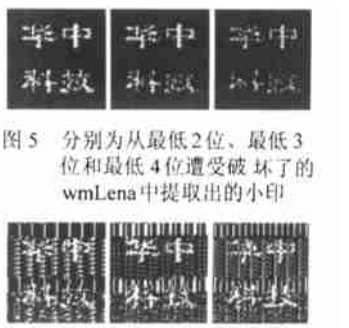

图 5　分别为从最低 2 位、最低 3 位和最低 4 位遭受破坏了的 wmLena 中提取出的小印

图 6　分别为从最低 2 位、最低 3 位和最低 4 位遭受 B-C 进攻的 wmLena 中提取出的水印

图 4 为遭受剪切攻击后的 wmLena (PSNR = 33.20) 及从中提取出的水印.

图 5 中的三个图像分别为从最低 2 位、最低 3 位和最低 4 位遭受破坏了的 wmLena 中提取出的水印.

图 6 中的三个图像分别为从最低 2 位、最低 3 位和最低 4 位遭受 B-C 进攻的 wmLena 中提取出的水印.

实验结果表明,本算法对于破坏其最低 4 位的进攻是鲁棒的,虽然有噪声干扰,但提取出的水印能分辨出来,同时,它也能有效抵抗 B-C 进攻. 其实,B-C 进攻与 LSB 进攻本质上是一致的,比较图 6 中的几个图像,提取出的水印的质量并没有因遭受进攻的位数增加而明显恶化,这说明这种进攻受各种条件影响,如原始图像、水印图像、大素数 n 及密钥 K. 同时,由于嵌入位置的随机性,此算法还可抵抗剪切进攻.

4 结论

本文提出了一种基于模运算的数字水印隐藏方法,通过实验可以看出,嵌入水印后的图像的 PSNR 为 55,这说明原始图像与嵌入水印后的图像,其视觉效果基本一致,即水印的隐藏效果好. 除此之外,我们的算法还具有以下特点:

⑴在水印的提取过程中利用了私钥 K,因此不知 K 的人无法正确提取出水印;

⑵水印的嵌入位置是随机地,不可逆地计算出来的,因此非法用户不可能获得准确的水印嵌入位置;

⑶水印的提取无需原始图像,只要掌握 K 即可;

⑷水印信息仅隐藏到每个像素的第 2 到第 7 位,因此可抵抗 LSB 进攻. 实验表明,它也可有效抵抗 B-C 进攻.

⑸可以有效抵抗剪切进攻.

数字水印技术的发展虽然只经历了短短的几年,但国际上已出现了相当多的水印产品,今后随着社会的进一步电子化和网络化,数字水印产品必将发挥更大的作用.

参考文献:

[1] C H Lee, Y K Lee. An adaptive digital image watermarking technique for copyright protection [J]. IEEE Trans on Consumer Electronics, 1999, 45(4): 1005 - 1015.

[2] F Hartung, M Kutter. Multimedia watermarking techniques [J]. Proc IEEE Int Conf on Digital Watermarking, 1999, 87(7): 1079 - 1107.

[3] M S Hwang, C C Chang, K F Hwang. A watermarking technique based on one-way hash function [J]. IEEE Trans on Consumer Electronics, 1999, 45(2): 286 - 294.

[4] Chi-Kwong Chan, L M Cheng. An attack on the HWANG-CHANG-HWANG watermarking scheme [J]. IEEE Trans on Consumer Electronics, 2000, 46(1): 40 - 43.

[5] 孙圣和,陆哲明. 数字水印处理技术 [J]. 电子学报, 2000, 28(8): 85 - 90.

作者简介:

宋 琪 女,1970 年出生于湖北省,1992 年获得西南交通大学计算机及应用专业学士学位,1995 年获得华中理工大学通信与电子系统专业硕士学位,现为华中科技大学电子与信息工程系信息与通信工程专业博士研究生,同时为该系讲师,主要研究方向有:数字图像处理,数字信号处理和信息安全.

朱光喜 男,1945 年出生于广西,1969 年毕业于华中工学院无线电工程系,现为电子与信息工程系系主任,信息与通信工程教授,博士生导师,国家信息产业部通信技术专家组成员,国务院特殊津贴专家. 长期从事计算机图像、图形处理,多媒体信息处理和信息网络系统等领域的工作,获得多项研究成果,在国内外发表论文 100 余篇,其中进入国际四大索引的 18 篇,现主要从事多媒体通信、CSCW、数字电视等工作.