数字水印的关键技术

于帅珍[1],冯丽平[2]
(1. 安徽财经大学 信息工程学院,安徽 蚌埠 233041;
2. 上海第二工业大学 电子与电气学院,上海 201209)

摘 要:随着因特网的日益普及,多媒体信息交流达到前所未有的深度和广度,但作品侵权也随之更加容易,篡改也更加方便,因此如何保护作品版权已受到人们的高度重视。数字水印是信息隐藏技术的一个重要分支,是一种全新的数字产品保护技术,它是将特定的数字信息内嵌到图像、音频、视频或软件等各种数字产品中,以达到信息安全和版权保护等目的。着重阐述了数字水印的选择、嵌入技术、提取技术、验证技术、数字水印的重要参数和变量等关键技术,提出了数字水印今后的研究方向,使人们对该技术有一个比较全面的了解。

关键词:水印选择;水印嵌入技术;水印提取技术;水印验证技术;研究方向
中图分类号:TP391 **文献标识码**:A **文章编号**:1673-629X(2010)02-0148-04

The Key Technique of Digital Watermark

YU Shuai-zhen[1], FENG Li-ping[2]
(1. School of Information Engineering, Anhui University of Finance & Economics, Bengbu 233041, China;
2. Electronic & Electrical Engineering College of Shanghai Second Polytechnic University, Shanghai 201209, China)

Abstract: The digital media has become a main way for information communication along with the popularization of internet and the development of multimedia techniques, people can get almost information through the internet. But this gives rise to serious problems including wide spread copyright violation, illegal copying, easy forging etc. How to provide copyright protection and implement covert communication has drawn extensive attention in recent years. Digital watermarking is an important branch of information hiding and a new technology to protect digital products, which is a process of embedding a watermarking into various digital works, such as images, audio, video or software and so on, to acquire information security and copyright protection. Focus on the choice of digital watermarking, embeded technology, extraction technology, verification technology, digital watermarking important parameters and variables, in addition, some possible new directions of digital watermarking research are also put forward. Aimed to provide people with a full understanding of it.

Key words: watermark selection; watermark insertion; watermark extraction; watermark verification; research direction

0 引 言

随着多媒体技术和网络技术的迅猛发展及广泛应用,对数字媒体的保护已成为一个迫在眉睫的现实问题。如何既能充分利用因特网的便利,又能有效地保护知识产权,已受到人们的高度重视。由于传统的加密方法对多媒体数据的保护能力存在一定的局限性,于是数字水印技术应运而生[1~3]。

数字水印技术是通过一定的算法将一些标志性信息——水印嵌入原始的多媒体信息(如图像、文本、音频和视频)中,成为源数据不可分离的一部分,它们不能被人的视觉系统察觉到,并可以经历一些不破坏源数据使用价值或商用价值的操作而保存下来,在需要时可以被专用的检测器或阅读器提取,起到防盗版、侵权和随意篡改的作用,弥补了密码技术的缺陷。因此,数字水印技术成为当今网络信息安全和数字媒体版权保护研究的热点。

收稿日期:2009-06-21;**修回日期**:2009-09-08
基金项目:2008年度安徽省高等学校省级自然科学研究项目(KJ2008B090)
作者简介:于帅珍(1968-),女,山东烟台人,副教授,硕士,研究方向为信息监测与信息处理、数字水印;冯丽平,副教授,硕士,研究方向为信息监检与信息处理。

1 数字水印的关键技术

1.1 水印的选择

鲁棒水印理论与算法是目前不可见水印的主要研究内容,影响水印鲁棒性的主要因素有两个:水印构造和内嵌策略。水印信号的构造是水印算法的首要工作,由于人类视觉系统对纹理具有极高的敏感性,所以水印构成纹理是不允许的,构成水印的序列应该具有

不可预测的随机性(Unpredictable Randomness)以及与噪声相同的特性。目前一般取下述随机序列作为水印信号内嵌到图像数据中。

(1)高斯白噪声序列。

一种满足均值为 μ、方差为 σ^2 的正态分布。

(2)伪随机序列。

具有类似白噪声的性质,但又有周期性和规律性,可以人为地加以产生和复制,如 m－序列或 M－序列等。

(3)有特定含义的水印信号。

选取具有特定含义的字符串或图像作为水印信号,由于其不是随机信号,所以在载体中内嵌水印信号前首先要进行预处理(如加密、随机化等),使其成为具有良好随机性的伪随机信号。

Cox 等在对水印结构进行研究之后指出,由随机序列构成的水印能够达到很好的鲁棒性。但是文献[4]指出,利用随机序列构成的水印不能提供作者本身的证明信息,不能满足版权保护的需求,所以用于版权保护的水印信号最好是二值图像或灰度图像。

1.2 水印的嵌入

水印的嵌入是将水印信号嵌入到原始图像中得到内嵌水印的图像。内嵌水印的图像与原始图像从视觉上应无明显差别。水印的嵌入是整个水印方案中的核心内容,它主要分为二块内容:

1.2.1 嵌入区域的选择

根据水印信号嵌入图像的方式,数字水印嵌入的区域可以分为两大类:空域技术和变换域技术。

(1)空间域的选择。

空域技术是直接在信号空间上内嵌水印信息。该算法实现简单,但其嵌入的信息量少,鲁棒性差,一般早期的水印采用这种算法,现在已经很少见到单独采用这种技术的算法了。

(2)变换域的选择。

变换域技术在内嵌水印前先对图像进行某种可逆的数学变换(常见的变换有离散余弦变换 DCT、离散小波变换 DWT、离散傅立叶变换 DFT、奇异值分解 SVD 等),通过修改变换域的某些系数值来内嵌水印,然后再进行逆变换得到内嵌水印的图像。研究人员普遍认为在变换域中内嵌水印有利于不可感知性,并且变换域水印比空域水印具有更好的稳健性,因而近年来的数字水印算法多集中于变换域方案。

(3)人类视觉系统在水印嵌入时的应用。

根据人类视觉系统的研究,人眼对于具有不同性质的图像区域有不同的感知特性,背景的亮度越高,纹理越复杂,人类视觉对其轻微的变化就越不敏感。因此,应该尽可能地将水印内嵌到图像中人类视觉不敏感的部位。

一个好的稳健数字图像水印算法应当结合人类的视觉特性。

1.2.2 嵌入模型的选取

在变换域中内嵌水印的效果明显要比空间域好,目前大多数数字水印嵌入模型多采用下面的两个公式:

$x' = x + \alpha w_i$(加法准则)

$x' = x + \alpha x w_i$(乘法准则)

采用这两个公式内嵌水印,在水印提取时不能采用盲检测技术,而盲检测技术具有快速、自动实现的优点,应用较广泛。为了采用盲检测技术,可以根据典型的算法构造嵌入模型,例如,根据文献[5]中的量化思想可以构造下面的内嵌水印公式:

$$x' = \begin{cases} x - \mathrm{mod}(x,Q) - Q/4 & \mathrm{mod}(x,Q) \leqslant Q/4, w_i = 1 \\ x - \mathrm{mod}(x,Q) + 3Q/4 & \mathrm{mod}(x,Q) > Q/4, w_i = 1 \\ x - \mathrm{mod}(x,Q) + 5Q/4 & \mathrm{mod}(x,Q) \geqslant 3Q/4, w_i = 0 \\ x - \mathrm{mod}(x,Q) + Q/4 & \mathrm{mod}(x,Q) < 3Q/4, w_i = 0 \end{cases}$$

其中 x 表示原始图像变换域的值,x' 表示内嵌水印后变换域的值,w_i 表示为要嵌入的水印,α,Q 为内嵌水印强度,由使用者设定。

1.3 水印的提取技术

水印提取是水印框架中最重要的部分,无论是水印生成算法,还是水印嵌入算法,最终要以能否正确可靠地提取水印为基准。

根据数字水印提取时输入和输出的不同将其分为私有水印(private watermarking)、半私有水印(semi－private watermarking)和公开水印(public watermarking)。私有水印(或称非盲水印,non－blind watermarking)在检测时至少需要原始图像(有时还需要原始水印),非盲检测可以从待检测图像中提取水印,也可以利用概率统计的方法判断水印是否存在;半私有水印(或称半盲水印,semi－blind watermarking)在检测时不需要原始图像,但需要原始水印,一般是利用概率统计的方法判断水印是否存在;公开水印(或称盲水印,blind watermarking)在检测时既不需要原始图像,也不需要原始水印,它是从内嵌水印的图像中提取水印。

非盲检测技术和半盲检测技术由于需要原始图像或原始水印的参与,因此给检测带来了不便,同时也不能抵制 IBM 攻击;而盲检测技术,由于不需要原始图像和原始水印的参与,因此其实用性得到了大大的增强,也是现在水印研究的一个热点[6]。

1.4 水印的验证技术

水印验证是数字水印技术中最为关键也是最为复

杂的技术之一,其验证方法一般分为两种[7-12]。

(1)提取并重建水印。这种方法只适用于图像水印信号。因为图像水印在提取后可直观地表达版权信息,从而直接判断版权的归属。

(2)利用概率统计的方法判断待检测图像中是否存在水印。这种方法既适用于伪随机信号(因为伪随机信号不能直观表达版权信息,只能通过概率统计的方法判断是否存在所检测水印),又适用于图像水印。其大致包括两类方法:

①利用假设检验判断是否存在水印。利用统计学中的假设检测,构造假设检验统计量,通过计算该统计量的值得到是否存在水印的判断,比较典型的有 patchwork 算法。

②利用相关检验(相似性检测)判断是否存在水印,它是目前水印检测中最常用的方法。将提取的水印信号和原始水印信号作相关运算,或直接使用原始水印信号与待检验图像进行相关运算,判断待检测图像中是否存在参与运算的原始水印。

a. 提取信号与原始水印作相关运算。

设 w' 是从待测图像中提取的水印信号,w 是原始水印信号,则相关系数为:

$$\mathrm{Cor}(w',w)=\frac{w'*w}{\sqrt{w'*w'}}=\frac{\sum_{i=1}^{N}(w'_i*w_i)}{\sqrt{\sum_{i=1}^{N}(w'_i*w'_i)}}$$

这个公式还有如下几种变化形式:

$$\mathrm{Cor}(w,w')=\frac{1}{N}(w*w')=\frac{1}{N}\sum_{i=1}^{N}(w_i*w'_i)$$

$$\mathrm{Cor}(w,w')=(w*w')=\sum_{i=1}^{N}(w_i*w'_i)$$

其中 N 为信号序列长度。预先设定一检测阈值 T_r(此值可通过理论分析或实验确定),若 $\mathrm{Cor}>T_r$,则待测图像中存在此水印,否则不存在。

b. 直接使用待检测图像与原始水印作相关运算。

若水印验证时不进行水印信号的提取,而是直接将待检测图像或者其中的一部分系数 x'(空间域或变换域)与原始水印 w 作相关运算,验证方法同上。

c. 利用检测响应图判断水印信号是否存在。

选择包括正确信号在内的若干个(一般为 1000 以上)独立的随机信号,作相关检验,正确信号的响应远远大于其余信号的响应,因而可以判断水印信号是否存在。

d. 位错误率度量方法。

在检测有含义的二值水印图像时,一般不采用前面的方法,而是采用位错误率的度量公式:

$$\mathrm{BCR}=\frac{\text{正确比特数}}{\text{总比特数}}\times 100\%=\frac{1}{N}\sum_{i=1}^{N}\overline{w_i\oplus w'_i}\times 100\%$$

其中⊕表示数字逻辑中的异或操作,若提取的水印与原始水印对应位置的值相同,则结果为 1,否则为 0。BCR 取值在 0 到 1 之间,BCR 越大,则表明提取的水印与原始水印越相似。

2 数字水印的重要参数和变量

数字水印系统中的参数和变量影响和限制系统的性能,一般来说,数字水印系统的性能主要依赖于四种因素:内嵌信息量、内嵌强度、载体图像尺寸和特性、秘密信息。

(1)内嵌信息量。这是一个重要的参数,它直接影响水印的鲁棒性。对同一种图像水印方法而言,内嵌信息越多,水印的鲁棒性就越差,而内嵌的信息量取决于不同的应用场合。

(2)内嵌强度。水印的内嵌强度需要在水印的鲁棒性和不可感知性之间进行折衷。提高鲁棒性就要增大水印的内嵌强度,而这必然会降低水印的不可感知性。

(3)载体图像尺寸和特性。载体图像尺寸对数字水印的鲁棒性有直接影响。尽管非常小的含水印图像可能没有多少商业价值,但一个水印软件程序应该能够从该图像中恢复出水印信息。除了载体图像尺寸以外,载体图像特性也对数字水印的鲁棒性产生重要影响,如对扫描的自然图像具有高鲁棒性的数字水印方法在应用于合成图像时,其鲁棒性可能会大大削弱。一个好的水印系统应适用于广泛的图像尺寸范围,以及不同类型的图像。

(4)秘密信息(如密钥)。尽管秘密信息的数量不会直接影响到数字水印的不可感知性和鲁棒性,但它对整个水印系统的安全性起了重要作用。密钥空间(秘密信息允许取值的范围)必须足够大,以使袭击耗时而失效。许多安全系统不能够抵御一些简单的攻击往往是因为系统设计者在设计系统时没有遵循基本的密码学原理。

3 结束语

数字水印技术的研究涉及不同学科研究领域的思想和理论,是近几年来国际学术界兴起的一个前沿研究领域,得到了迅速的发展。但数字水印仍然是一个未成熟的研究领域,还有很多问题需要解决,其理论基础仍然薄弱。

(1)基本原理和评价方法。目前数字水印技术研

究中的模型和基础理论尚处于雏形阶段,现有的水印算法和对水印系统的评价方法大多是经验性的,未来需要继续修改和完善水印系统的基本理论。

(2)算法分析及新算法。重点研究现有数字水印技术算法的稳健性、安全性和抗攻击性,并融合数字信号处理技术,找出它们之间的关系,从而发现更好的算法。

(3)与密码学结合。在有关版权的应用中,数字水印技术必须与像密码之类的其他机制相结合,尤其是与数字签名技术结合,才能构造综合的数据安全系统,才能提供可靠的保护。

(4)对水印攻击的研究。水印攻击与水印算法是矛盾关系,二者相互制约又相互促进,只有能够经受住各种攻击的算法才是最鲁棒的算法,加强对水印攻击的研究可以极大地促进水印技术的发展。

参考文献:

[1] 张冠男,王树勋,温　泉.一种嵌入可读水印的自适应盲水印算法[J].电子学报,2005,33(2):308-312.

[2] 钮心忻,杨义先,吴志军. 信息隐藏理论与关键技术研究[J].电信科学,2004,20(12):28-30.

[3] 蒋建国,宣　曼,齐美彬.数字水印技术的研究现状及进展[J].计算机应用,2006,26(12):60-62.

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

[5] 谢荣生.盲检测图像数字水印技术研究[D].哈尔滨:哈尔滨工程大学,2002:75-78.

[6] 费伦科,丁振凡.数字水印技术的研究[J].华东交通大学学报,2006,23(1):78-81.

[7] Cox I J, Kilian J, Leighton F T, et al. Secure spread spectrum watermarking for multimedia[J]. IEEE Transactions on Image Processing, 1997, 6(12): 1673-1687.

[8] Voyatzis G, Pitas I. Digital image watermarking using mixing systems[J]. Computer & Graphics, 1998, 22(4): 405-416.

[9] Kutter M, Jordan F, Bossen F. Digital signature of color images using amplitude modulation[C]// Proc. of SPIE: EI'97. [s. l.]: [s. n.], 1997: 518-526.

[10] Podilchuk C I, Zeng W. Image-adaptive watermarking using Visual models[J]. IEEE Journal on Selected Areas in Communications, 1998, 16(4): 525-539.

[11] Barni M, Bartolini F, Piva A. Improved wavelet based watermarking through pixel-wise masking[J]. IEEE Transactions on Image Processing, 2001, 10(5): 783-791.

[12] Huang J W, Yun Q S, Shi Y. Embeding Image Watermarks in DC Components[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2000(10): 974-979.

(上接第 147 页)

的能量耗费,可以更加有效地利用各个节点的能量。该算法在无线传感器网络中具有一定的应用价值。后续的研究可以进一步考虑簇内节点的数目以及各簇头的分布均衡以及改选簇头时如何进行数据传递的问题。

参考文献:

[1] Heinzelman W R, Chandrakasan A, Balakrishnan H. Energy-efficient communication Protocol for wireless microsensor networks[C]//System Sciences. 2000. Proceedings of the 33rd Annua Hawaii International Conference. Hawaii: [s. n.], 2000.

[2] Bandyopadhyay S, Coyle E J. An energy efficient hierarchical clustering algorithm for wireless sensor networks[C]//INFOCOM 2003. Twenty Second Annual Joint Conference of the IEEE Computer and Communications Societies. [s. l.]: IEEE, 2003: 1713-1723.

[3] Younis O, Fahmy S. HEED: a hybrid, Energy-Efficient, distributed clustering approach for ad hoc sensor networks[J]. Mobile Computing, IEEE Transactions on, 2004, 3(4): 366-379.

[4] Moussaoui O, Ksentini A, Naimi M, et al. A novel clustering algorithm for efficient energy saving in Wireless Sensor Networks[C]//7th International Symposium on Computer Networks (ISCN'06). Istanbul, Turkey: [s. n.], 2006: 66-72.

[5] 胡　静,沈连丰,宋铁成,等.新的无线传感器网络分簇算法[J].通信学报,2008,29(7):20-26.

[6] Cheng Lu, Qian Depei, Wu Weiguo. An Energy Efficient Weight-clustering Algorithm in Wireless Sensor Networks [C]//Proceedings of 2008 Japan-China Joint Workshop on Frontier of Computer Science and Technology (FCST'08). [s. l.]: IEEE Computer Society, 2008: 30-35.

[7] Bouhafs F, Merabti M, Mokhtar H. A Semantic Clustering Routing Protocol for Wireless Sensor Networks [C]//3rd IEEE Consumer Communications and Networking Conference (CCNC 2006). Las Vegas, Nevada, USA: [s. n.], 2006: 351-355.

[8] 杜胜永,柴乔林.基于最大连通度的生成簇优化算法[J].计算机应用,2006,26(6):186-189.

[9] Akyildiz I F, Su W, Sankarasubramaniam Y, et al. A survey on sensor networks [J]. IEEE Communication Magazine, 2002, 40(8): 102-114.

[10] 芦东昕,侯晓东.无线传感器网络路由协议成簇算法研究[J].华北电力大学学报,2006,33(4):51-54.