北京大学学报(自然科学版),第 37 卷,第 5 期,2001 年 9 月
Acta Scientiarum Naturalium
Universitatis Pekinensis, Vol.37, No.5 (Sep,2001)

非对称数字水印[1)]

崔晓瑜　程乾生
(北京大学数学学院,北京,100871)

摘　要　针对当前的数字水印实施架构中存在的低效问题,提出了一种新的架构——非对称数字水印。该体制以第三信任方为中心,通过使用二次水印(秘密水印和公开水印)和‘水印浏览器’,使版权信息的提取与显示均可在用户端独立完成。在版权信息‘公开化’的同时,极大地提高了整个架构运作的效率。该体制既保护了商家的版权利益,又使用户避免了非授权使用的问题,同时对版权的认证和管理也起到了规范化的作用。

关键词　数字水印;对称体制;非对称体制;第三信任方;秘密水印;公开水印
中图分类号　TN 911.76

0　引　言

人们在受益于先进科技带来的各种便利的同时,也面临着许多严峻的问题,其中一个就是数字媒体的安全性问题。

起初,人们使用传统的加密技术来解决这个问题。但是一旦所传输数据在接收端被解码后,数据就处于无保护状态,人们也就无从跟踪它的使用情况。因此,加密对所传输数据的保护极其有限,而数字水印正是为了弥补加密技术的不足提出来的。

“数字水印”的概念提出于 90 年代初,它一出现就引起了科学家和工业界的浓厚兴趣,而它的特性也决定了它在网络时代的广泛应用前景。

1　数字水印技术的发展与现状

所谓数字水印,从本质上讲,是一种数字信号。它可以应用于:1) 确认数据的来源;2) 跟踪用户,检查其是否有盗版行为;3) 检查数据是否被修改过。

1.1　分　类

可以说数字水印的分类五花八门,各有各的标准。其实从上述数字水印的定义来看,数字水印根据应用目的可以分为 3 类:

1) 基于来源的数字水印:使用时是把唯一的一个水印加到所有的电子信息版本中去,因此它主要应用于确认数据来源和版权的实际问题。

2) 基于目标的数字水印:它是每一个版本中所嵌入的数字水印都不一样,所以它的作用是可以确认盗版用户。

1) 国家自然科学基金资助项目(69872003)
收稿日期:2000-07-13

3）防篡改的数字水印：它也叫做“Fragile Watermarking”。它的技术特性是：水印易于发现和删除，但在删除的同时，原始数据的质量也遭到了严重的破坏，所以它主要应用于检查数据是否被攻击过。

其实，有的文献根据 1)、2)相应的特性分别称其为：Watermarking 和 Fingerprinting。

此外，根据存在方式的不同，数字水印又可分为两种：可见水印和不可见水印。目前研究比较多的是不可见水印，因为可见水印有许多缺陷，比如它会影响媒体的保真度，而且更容易被攻击等等。

1.2　性　质

对一个数字水印而言，它有以下性质：

1）不可见性：是指一个水印从感知上讲是不可见的，即数字水印是透明的，它的嵌入不会引起原始数据质量的明显下降，从而增加攻击者的“发现和删除水印”的困难程度。

2）普遍性：指设计的数字水印技术最好对任何数字媒体都适用。

3）明确性：抽取出来的数字水印应当能明确确定作者的身份，不能模棱两可。而且水印的精确度应不随攻击明显改变。

4）鲁棒性：水印的最重要性质。它是指水印应当难以去掉，而且随着攻击程度的加大，整幅图像的质量会受到严重破坏。

到目前为止，尚没有一种水印技术能够完全满足上述要求。为方便起见，本文均以图像作为数字媒体对象进行数字水印技术的探讨。

1.3　已有的数字水印技术

根据嵌入图像的方式，数字水印技术可以分为两大类：

1）空域技术：这种技术通过直接改变图像数据来嵌入数字水印，属于早期研究。典型的例子有 LSB 方法：把水印加到图像的最不显著位上，这种方案保证了水印的不可见性，但鲁棒性却很差，普通的图像压缩和低通滤波器就可以把大部分水印去掉；还有 block-mean 方法，这种方法是把图像先分成一定大小的块，然后通过改变块均值的方法加入水印。它对同谋攻击比较脆弱。

总体而言，空域技术的优点是能够有效地利用人类视觉系统特性[1]，且复杂度不高；但它的缺陷是：(1) 本质上对图像的纹理敏感；(2) 对图像的尺寸变换、JPEG 压缩的鲁棒性很差；(3) 水印容量，即能够携带的信息量不大。

2）变换域技术：改变图像变换域数据，然后进行反变换得到加水印的图像。两种最常用的变换是 DCT 和 DFT。典型的例子有 Ingemar 等人提出的“Spread Spectrum Watermarking”方法[3]。它利用通信理论上的频谱扩展思想，将水印在图像的频谱上扩展以达到不可见性和鲁棒性的目的。但它的最大缺点是在抽取水印时必须利用原图；还有人利用通信理论的调制思想(2-维多脉冲调幅)加入水印[4]。用数学公式可以表示为：

$$w(m,n) = \sum_{i=0}^{L-1} b_i p_i(m,n), \quad y(m,n) = x(m,n) + w(m,n)。$$

其中 $b_0, b_1, \cdots b_{L-1}$ 是要隐藏的信息。抽取水印时，将加过水印的电子信息同各个脉冲做相关分析来得到水印。这个方法的缺点是计算量比较大。

现在已有文献把小波变换应用到水印技术中，这种技术使变换域技术同时具有良好的空

间局部化特性。它将图像在独立的频带和不同方向上进行分解,能够更好地与人类视觉系统特性相结合[1]。

总之,目前水印技术研究的热点在于水印的具体嵌入方法上,而对它的另一重要问题——实施架构,却论之甚少。而一个甚好的方法如果没有好的实施架构,同样不能充分体现出它应有的作用来。本文就着眼于水印技术的实施架构这一问题,深入探讨目前水印实施当中所存在的主要问题,并提出一种新的实施架构——非对称数字水印。

2 非对称数字水印

人们知道,对于密码技术,非对称体制(双钥体制)与对称体制(单钥体制)相比[2],主要具有以下优点:

1) 密钥数量大大减少;2) 彻底消除了经特殊保密的密钥信道分送密钥的困难;3) 便于实现数字签名。

对于数字水印而言,已有的技术绝大多数都是对称体制:水印的加入和提取只有发送一方掌握,接收方只有通过特殊保密渠道获得原图和具体加入水印的算法才能看到隐藏的数字信息——水印。虽然该体制对发送方的鲁棒性很好,但对于接收方(在电子商务中通常为最终用户)却由于无法看到数字媒体中嵌入的有关信息而处于被动的地位,譬如说不经意中使用了非授权的数字媒体而被追究。那么,能否使用非对称的数字水印呢?

非对称数字水印,某些文献又称为公钥水印,是指任何用户能够看见但又去不掉的水印。但是前面已经提过,可见水印有许多缺陷。那么,如何实现即让用户"看见"而又隐藏于数字媒体的数字水印呢?

文献[5]中提到两种实际商业模型中的水印实施架构,它有两个主要特性:

1) 能够防止版权拥有者黑箱操作;

2) 能够跟踪用户的使用情况,确认盗版用户。

但它同时也存在一个很大的缺陷:用户想了解一幅图像的版权情况,则必须上传该图像和有关信息,这在目前拥挤的 Internet 上而言,效率非常低;此外,用户的查询结果必须要通过访问一个庞大的"版权信息数据库",势必造成低效率和数据库的不安全性。

下面提出一种非对称数字水印的可行性方案,为了说明该方案的实际意义,发送方用商家(Creator)来代替,接收方用用户(User)来代替。

在商家和用户之间设立一个第三信任方(Trusted Third Party,简称为 TTP),它们之间的具体联系分为以下 3 个阶段(图 1):

(1) 注册申请阶段。

如果商家要在网上发布数据,则首先要向第三信任方注册申请,将自己的有关版权信息发送给第三信任方;第三信任方经过一系列的检查工作后,发送回是否认可的信息。这里的认可检查问题超出本文范围,这里不做讨论。

(2) 水印加入阶段。

商家向第三信任方成功注册后,再向其发送人们称之为秘密水印的分密钥(以下用 K_U 代替)。秘密水印是商家要加入的第一个水印,它之所以称为秘密水印是因为用户无法浏览到它,人们用它来保护商家的版权利益,版权纠纷时起到明确版权的作用。它的算法可以是公开

的，但鲁棒性要很高；第三信任方在接受到 K_U 后，发送另一部分密钥 K_T 给商家。秘密水印的密钥只掌握在商家和第三信任方手中，这种 Diffie-Hellman 密钥传送方案既解决了密钥传送的困难，又避免了商家的黑箱操作[5]。第三信任方除了发送 K_T 外，同时还要发送一个“水印写入器”(Watermark Writer，简记为 WmW)，它用来加入第二个水印——公开水印，它是用户可以“浏览”的水印。内容包括商家和产品(Creation)的版权信息。由于水印的提取是在用户端，所以公开水印的算法要采用不需要原图的方法。它的具体算法掌握在第三信任方手中，商家只拥有水印加入程序。它的鲁棒性可以低于秘密水印；商家收到 K_T 和 WmW 后，在图像中分别加入秘密水印和公开水印，然后进行发布。

(3) 浏览阶段。

在商家发布图像后，若用户想了解它的版权信息，则要到第三信任方购买或免费下载一个“水印浏览器”(Watermark Browser，简记为 WmB)。通过该“水印浏览器”，用户可以方便地察看图像中的公开水印信息，从而避免了图像的非法使用。由于“水印浏览器”只是一个水印提取的可执行程序，与图像本身无关，可以重复使用，所以用户不必多次向第三信任方发送“浏览申请”。这就解决了文献[5]中的低效率问题。另一方面，由于用户可以“浏览”图像随身携带的版权信息，所以就不需要访问“版权信息数据库”(Intellectual Property Rights Database 简记为 IPR Database)，从而提高了效率和数据库的安全性问题。

另外，第三信任方和商家、第三信任方和用户之间可以通过数字签名增加信息传输的安全性。

3　非对称数字水印的主要优点

(1) 从用户角度上讲，非对称数字水印可以使用户方便、高效地辨别网上数字媒体的合法性。这一点对于电子商务的发展具有重要意义；

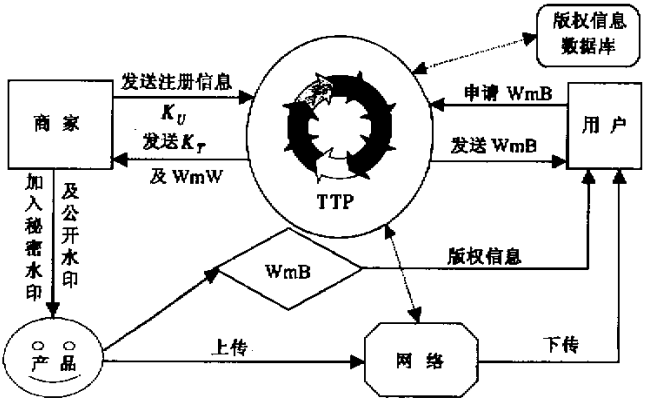

图 1　商家、第三信任方和用户之间的联系

Fig. 1　The relation among Creator, User and TTP

(2) 从第三信任方角度上讲，非对称数字水印有着良好的规范性。在传统体制中，商家与

用户直接接触,不管是在管理体制上还是在水印认证上都存在混乱性和不易管理性。而本文提出的非对称数字水印就可以很好地解决这些问题,并提高了 IPR 数据库的安全性;

(3) 从商家角度上讲,非对称数字水印大大增加了自身的利益,并起到了两层保护作用:一是利用公开水印公开声明了商家的版权,二是可以利用商家加入的秘密水印来认证版权。

4 结束语

数字水印做为密码技术的后继者正日益得到人们的青睐。当然,任何一种技术都不是万能的,它的实施是否成功与商业模式、市场定位等都有很大的关系。数字水印技术并非绝对安全,它本身也有局限性和弱点。本文提出的非对称数字水印实质上是数字水印的一种实施方案,对数字水印的具体算法并没有探讨。但是,公开水印的出现,使得在数字媒体中可以集成另外形式的多媒体信息。这就为人们提供了一条新的思路:由于公开水印对用户可见,因此在公开水印里,不仅可以加入商家的版权信息,还可以加入商家的广告信息,甚至是因特网址信息等。

参考文献

1 陈青 王延平. 数字水印——知识产权保护的新技术. 中国图像图形学报,1999(A):800~804

2 卢铁城. 信息加密技术. 成都:四川科学技术出版社,1989

3 Ingemar J Cox, Joe Kilian, Thomson Leighton F, et al. Secure Spread Spectrum Watermarking for Multimedia. IEEE Transaction on Image Processing, 1997, 6(12): 1 673~1 687

4 Joshua R Smith, Barrett 0 Comiskey. Modulation and Information Hiding in Images. Information Hiding. Springer: Lecture Notes in Computer Science, 1996, 1174: 207~225

5 Daniel Augot, Jean-Mark Boucqueau, Jean-Francois Delaigle, et al. Secure Delivery of Images over Open Networks. Proceedings of IEEE, 1999, 87(7): 1 251~1 266

6 Liu R Z, T N Tan. Watermarking for Digital Images. Proceedings of ICSP '98: 944~947

Asymmetric Digital Watermark

CUI Xiaoyu CHENG Qiansheng

(*School of Mathematical Science, Peking University, Beijing, 100871*)

Abstract Aiming at the low efficiency in current architectures of digital watermarking, it provides a new architecture—asymmetric digital watermark. This architecture has the third trusted party as the center. And by using two watermarks (secret watermark and public watermark) and "watermark browser", users can independently extract and display the intellectual property information hidden in the digital multimedia. It not only makes the intellectual property information public, but also highly improves the efficiency. In the results, this architecture can protect the intellectual property of creators, avoid users from unauthorized use, and regular the authentication and the management of the intellectual property.

Key words digital watermark; symmetric system; asymmetric system; third trusted party; secret watermark; public watermark