零知识数字水印检测协议研究*)

周四清[1,2] 余英林[1] 陈潮填[2]

(华南理工大学电子与通信工程系 广州510641)[1] (广东职业技术师范学院计算机系 广州510665)[2]

Research on Zero Knowledge Proof Protocol of Watermark Detection

ZHOU Si-Qing[1,2] YU Ying-Lin[1] CHEN Chao-Tian[2]

(Dept of Electronic Engineering & Communication ,South China University Technology,Guangzhou510641)[1]

(Dept. of Computer Science, Guangdong Polytechnic Normal University, Guangzhou 510665, China)[2]

Abstract The advent of the Web, electronic commerce and the creation of electronic distribution channels for content have brought new challenges regarding the protection of intellectual property. Digital watermarking is a new information security technique. Using zero knowledge proofs in the cryptography we propose a watermark detection based on zero knowledge, of solving that the existence of a watermark without revealing what the watermark is , of providing the security when we apply watermarking.

Keywords Digital watermark, Zero knowledge proof, Security

1 引言

数字媒体(数字图像、数字视频、数字音频等)的版权保护已成为一个迫切需要解决的问题。传统的加密系统在数据传输过程中虽有保护作用,但数据一旦被接收并解密,其保护作用也随着消失,因此只能满足有限的要求。

近几年来发展起来的数字水印技术作为多媒体信息安全问题的一种解决方案已引起了人们的极大关注,它是在数字信息产品(如图像、声音、视频等)中通过某种算法嵌入不可感知的标记信息(即水印)。数字水印技术在数字知识产权保护、DVD版权保护、电子商务、数码相机、认证授权的证明及文化遗产继承与现代文化艺术等领域都有潜在的应用,它正是国内外的学术界和产业界研究的热点之一[1,2]。

在设计新的数字水印算法或检测上至今已进行了大量的研究,对数字水印的鲁棒性和不可感知性研究得比较多,而对数字水印系统的安全性研究得还不够,版权所有者掌握了水印的嵌入与检测的密钥。特别在使用它来解决实际问题时(如版权保护等)如何保证其安全可靠性。

数字水印按照水印算法经受攻击的能力可分为鲁棒性水印与脆弱性水印,鲁棒性水印经过图像运算或蓄意攻击仍然能够检测水印的存在性,而脆弱性水印则是能够直接反映对水印的操作运算。前者用于版权保护等应用中,而后者则可用于认证等。按照水印是否可见可分为可视水印与隐形水印;按照检测水印时是否使用密钥分为私钥水印与公钥水印,密钥水印就是嵌入和检测水印时都需要用同一种密钥。它隐藏了水印的嵌入位置,仅密钥拥有人才知道。而公钥水印则是每一个都知道水印的隐藏位置。两者的安全性能不一样,就安全来就说,前者比后者要好,但使用方便来说,后者比前者则要好。在Internet网络上的应用更需要公钥水印。因此,希望研究如何在使用时保证具有私钥水印一样安全性能的公钥水印。

如图1是一个数字产品网络发布模型,它由三个部分组成,数字产品的所有者即版权人、消费者即用户及发布数字产品的网络,与此相应存在有关的安全和版权问题有:1)网络环境的安全性;2)所有者的版权;3)用户的消费权益。

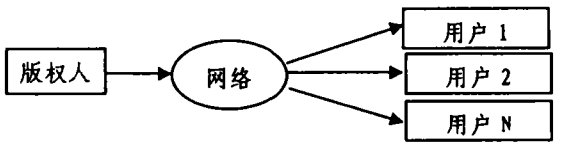

图1 数字产品网络发布模型

网络环境的安全可以使用加密技术和网络协议保证。数字水印就是向欲被保护的多媒体数据嵌入某种信息(即水印)以保护所有者的权益。但在使用水印方法时,为了验证数字水印的存在性,版权所有者不可避免地要泄露水印的有关信息,这样一来就无法保证攻击者不破坏水印或自制水印,用户使用的水印化数字产品的合法性不能得到保证,从而妨碍了水印化数字产品在Internet上的应用和所有者的版权保护,因此需要解决实际使用水印中的安全性问题。我们需要的水印方法应该是不需要泄露有关水印信息就能证明水印的存在性,利用加密技术中的零知识证明协议来解决在不泄露水印信息就能证明水印存在的问题,从而保证了水印应用中的安全性。

2 零知识证明协议

零知识证明是一种协议(即完成一项任务的一系列步骤,它包括两方或多方),这种协议的一方称为证明者 $P(Alice)$,它试图使被称为验证者 $V(Bob)$ 的另一方相信某个论断是正确的,却不向验证者提供任何有用的信息。零知识证明分交互式和非交互式两种,交互式零知识证明就是证明者 P 和验证者 V 之间必须进行双向对话,才能实现零知识性;而非交互式零知识证明双方不需要任何交互,从而任何人都可以将 P

*)基金项目:国家自然科学基金(NO.60074039)。周四清 副教授,博士生,研究方向:数字水印、电子商务与网络安全等。余英林 教授,博士导师,研究方向:图像处理,模式识别,模糊神经技术等。陈潮填 教授,博士,研究方向:广义系统理论,控制与优化等。

公开的信息进行验证。

1)基于离散对数的零知识证明协议

证明者 P 要向验证者 V 证明他知道 x 满足 $A^x=B \bmod p$，p 是素数，A、B 和 p 是公开的，x 是秘密的且 V 不知道。证明协议如下：

(1)P 随机选择数 $r<p-1$，计算 $h=A^r \bmod p$ 并将 h 发送给 V；

(2)V 随机选择比特 b 并将 b 发送给 P；

(3)P 计算 $s=(r+bx)\bmod(p-1)$并将 s 发送给 V；

(4)V 验证是否有 $A^s=hB \bmod p$；

(5)重复步骤(1)～(4)t 次。

P 欺诈 V 成功的概率为2^{-t}。这个协议对模 $n=pq$(p,q 均为素数)也是可行的，此时，P 随机选择数 $r<(p-1)(q-1)$，并计算 $s=(r+bx)\bmod(p-1)(q-1)$。

2)基于图同胚的零知识证明协议

Alice 拥有两个图 H_1和 H_2的同胚信息，为了向 *Bob* 证明知道这个秘密信息，

(1)*Alice* 置乱 H_1或 H_2产生 H_3，并将 H_3传送给 *Bob*。

(2)*Bob* 知道三个图 H_1、H_2和 H_3，根据掷硬币结果，要求 *Alice*：或者公开 H_1和 H_3的同胚，或者公开 H_2和 H_3的同胚。

(3)*Alice* 利用 H_1和 H_2的同胚信息回答 *Bob* 的问题。

(4)抛弃 H_3，每一轮构造新的图，重复 t 次。

这些协议的重要特点之一就是利用盲化，将一个问题变为另一个相关的问题，保持原问题的重要特点，而不泄露敏感信息。另一个特点就是它们是“请求-响应”协议，通常必须实现盲化才能保证证明方的诚实性。

非交互式零知识证明就是用单向散列函数代替验证者 V。

有关零知识证明的详细内容可参考文[4]。

3 零知识水印检测协议

零知识协议提供了一种证明数据中信息存在而不泄露其信息的方法，从而自然猜想可以应用于数字水印检测，但不能直接应用于数字水印检测，这是由数字水印的特点所决定的。在数字水印中，假设 Web 站点有用于认证的某些数据，但这些数据要嵌入多媒体中，如果这些数据在网站上公开的话，别人就可以利用它来消除此数据，从而失去了保护作用。

以图像水印算法为例，研究零知识水印检测协议。假设图像 I 中嵌入一个水印 W，得到一个水印化图像 I_w。如果应用零知识证明协议，首先第一步需要用同一个扰动运算 ρ 盲化图像 I 和水印 W，从而能够证明 $\rho(W)$在 $\rho(I_w)$中存在，而不泄露有关水印 W 的信息。

1)基于随机扰动的零知识水印检测协议

假设公开水印空间 Ω，所有的合法水印都是 Ω 的合法扰动。为了证明 I_w 中包含水印 W：

(1)*Alice* 选择一个合法的随机扰动 ρ，计算 $J_w=\rho(I_w)$，将 J_w 传送给 *Bob*。

(2)*Bob* 知道 I_w 和 J_w，根据掷硬币规则，要求 *Alice*：或者公开 ρ，证明 J_w 是 I_w 的合法扰动；或者公开 $\rho(W)$，证明 $\rho(W)$在 J_w 中存在。

(3)*Alice* 回答 *Bob* 的问题，证明 $\rho(W)$是合法构造水印，用合法扰动 σ，使得 $\sigma(\Omega)=\rho(W)$。

(4)抛弃扰动 ρ，构造新的扰动，重复 t 次。

在实现这个协议时使用 Pitas 水印算法[3]，但存在的问题是随机扰动可能使原图像和水印化图像不匹配。

2)基于难解问题的零知识检测协议

将水印 W 信息编码成一个图 G，从而利用水印嵌入方法将此图 G 隐藏于图像 I 中，要实现零知识水印检测，利用基于图同胚的零知识证明协议，可以达到此目的。

(1)*Alice* 将 I_w 和 G_w 扰乱成 J_w 和 F_w，G_w 和 F_w 同胚，将 J_w、F_w 和生成水印图的密钥 K 传送给 *Bob*。

(2)*Bob* 知道 K、I_w、G_w、J_w 和 F_w，根据掷硬币规则，要求 *Alice*：或者公开生成水印图的密钥 K，或者证明 G_w 和 F_w 同胚。

(3)*Alice* 回答 *Bob* 的问题。

(4)抛弃 J_w 和 F_w，*Alice* 和 *Bob* 双方重复多次。

在实现这个协议时使用图像频域水印算法[5]，在实现过程中，先将水印排成一个图，按照遍历图的方法将它嵌入图像频域中。在水印检测时，*Alice* 公开水印构成的图 G 和水印化图像 I_w，利用图的同胚性，来实现零知识水印检测。

小结 在数字图像水印的版权保护应用中，最重要的是验证水印的存在而不泄露有关水印的信息。本文所提出的零知识水印检测协议，就是一个能够证明图像中水印的存在性而不泄露有关水印信息的安全方法，一旦这种协议应用于具体水印系统中，水印的检测就能公开进行，这种方法能够解决在应用水印时所发生的版权纠纷等问题。

参 考 文 献

1 Hartung F, Kutter M. Multimedia Watermarking Techniques. Proceeding of the IEEE, 1999, 87(7): 1079～1107

2 Brassil J T, Low S, Maxemchuk N F. Copyright Protection for the Electronic Distribution of Text Documents. Proc. of the IEEE, 1999, 87(7): 1181～1196

3 Pitas I. A Method for Signature Casting on Digital Images. In: Processings of ICIP, vol 3, IEEE press, 1996. 215～218

4 Schneier B. Applied Cryptography Second Edition: protocols, algorithms, and source code in C. John Wiley & Sons, Inc. 1996

5 Craver S, et al. Resolving Rightful Ownership With Invisible Watermarking Techniques: Limitions, Attacks, and Implications. IEEE Journal on Selected Areas of Communications, special issue on Copyright and Privacy Protection, April 1998 (IBM Research Report, RC 20755, March 1997)