安全数字水印体系的研究 [1]

毛 琼 陈明奇 夏光升 杨义先 谭铁牛 *

(北京邮电大学信息安全中心 北京 100876)
*(模式识别国家重点实验室 北京 100080)

摘 要 数字水印是用于保护网络多媒体产品版权的一门热门新兴技术. 随着对数字水印技术研究的深入, 水印技术日趋成熟. 但是算法的改进和优化仍然很难抵御五花八门的攻击方法, 因此必须建立一套安全的数字水印体系标准来规范水印的加载和检测. 该文基于 IPR 保护和认证体系 IMPRIMATUR 和 AQUARELLE 商业模型, 提出了一个新的安全数字水印体系, 该体系弥补了 IMPRIMATUR 和 AQUARELLE 所采用的 DHWM 水印协议的缺陷, 而且更加简洁实用.

关键词 知识产权保护, 数字水印, 水印攻击, 水印协议, 安全数字水印体系
中图号 TN918.1, TP391.4

1 引 言

多媒体产品的传播给人们生活带来了巨大的变化。迅速兴起的 Internet 电子印刷出版、电子广告、数字仓库和数字图书馆、网络视频和音频、电子商务等新的服务和运作方式孕育着极大的商机, 已经为人们普遍接受。同时, 通过提供这些服务盈利的商业结构也面临着巨大的挑战: 如何保护数字产品不被非法拷贝、再次传播和盗用? 如何确定是否有人恶意篡改了数字产品的内容? 如何控制监视非授权用户? 数字水印 (Digital Watermarking) 是迄今为止最有效的数字产品版权保护技术, 它可以在数字产品中嵌入作者、所有者、发行者、使用者的标识, 携带版权保护信息和认证信息. 通过检验水印的存在与否能够鉴别出非法复制和盗用的数字产品.

2 数字水印技术及其应用

数字水印是永久镶嵌在其它数据 (宿主数据) 中具有可鉴别性的的数字信号或模式, 而且并不影响宿主数据的可用性. 现在有很多种数字水印技术. 针对不同的应用, 采用的技术也不一样. 数字水印的应用方向及相应采用的技术主要有以下几类:

(1) *数字产品的所有权和版权保护* 当数字水印应用于版权保护时, 潜在的应用市场在于: 电子商务, 在线或离线地分发多媒体内容以及大规模的广播服务. 这种水印对稳健性的要求比较高, 一般采用变换域水印来实现. 其原理一般基于常用的图像变换, 基于局部或是全部的变换, 这些变换包括: 离散余弦变换 (DCT) 、小波变换 (WT) 、傅氏变换 (FT 或 FFT) 以及哈达玛变换 (Hadamard Transform) 等等. 其原理主要是通过改变频域系数的方法来加载水印. 水印加载在图像的视觉敏感部分, 因而具有较强的稳健性. 例如 E. Koch, J. Zhao[1] 提出的基于分块 DCT 的水印技术; Cox 等人在文献 [2,3] 中提出的基于图像全局变换的水印方法.

(2) *认证和完整性校验*(Authentication and integrity verification) 在许多应用中, 需要验证数字内容未被改变, 修改或造假. 这时可以在数字产品中加载水印, 通过检验水印的存在与否来判断内容是否被改动, 为法庭判决提供证据. 这与密码学中的数字签名类似. 它们的不同点在于: 该类水印是不可见的, 不易引起攻击者的怀疑.

[1] 1999-11-01 收到, 2000-03-28 定稿
国家自然科学基金资助项目 (批准号 60073049, 69882002), 国家重点基础研究发展规划项目 (批准号 G1999035805), 模式识别国家重点实验室资助项目, 高等学校骨干教师资助计划项目

这种情况一般采用脆弱的不可见水印。该水印的特点是图像像素的改变极易破坏水印。同时，该水印还必须满足在图像改变后不可能掩盖改变或再生出水印，即使是知道了水印加载过程，或者知道了水印本身。例如，改变图像像素的最低位比特 (LSB) (L.F.Turner[4] 和 R.G.van Schyadel[5] 等先后利用此方法将特定的标记隐藏于数字音频和数字图像内。) 来加载水印是不安全的，因为，在保持图像的外观几乎不变的同时，只要在改变图像像素时保持 LSB 不变即可保持水印不变。

(3) 内容保护(Content protection) 在一些特定应用中，数字产品内容的所有者可能会希望要卖的多媒体内容能被公开自由地预览，以尽可能地多招徕潜在的顾客，但也需要防止这些预览的内容不被其他人用于商业目的，因此，这些预览内容被自动加上可见的但同样难以除去的水印。

3 安全数字水印体系

数字水印技术为数字产品的知识产权保护提供了一种工具，但是仅技术的成熟还远远不能达到目的。其中制定水印加载和检测环节的实施方案是关键。是否需要水印密钥来控制水印的生成？加载水印应由谁来进行？由谁鉴别水印的存在与否？这些问题都直接关系着水印的安全。总的来说，存在以下几种情况：

(1) 水印的加载和检测可由任何用户进行，无须水印密钥。最早的水印的加载和检测过程无须密钥，但这类水印的安全依赖于水印算法的秘密性。一旦水印算法公开，水印便极易被擦除。

(2) 水印的加载和检测都由所有者进行，所有者选择并且保存密钥。这会给人造成黑匣子的感觉，很难让局外人相信。

(3) 水印的加载由所有者进行，所有者选择并保存水印密钥。检测则由公众进行。当发生版权纠纷时，由所有者出示水印密钥来检验水印的存在。但是水印密钥一旦公开，就会被人用来除去水印。所以每次验证后，还需更换密钥，重新加载水印。这给所有者带来极大不便。

(4) 水印的加载和验证由可信任第三方进行。水印密钥的选择由可信任的第三方和所有者共同决定并保存。当采用这种方案时，攻击者会在已加载水印的数字产品中再加入自己的水印。这样，原来的数字产品中就叠加了两个水印。对第三方来说，这两个水印都有效。这就造成了判决的混乱。此类攻击方法，在文献 [6] 中有详细的描述。

(5) 不同的数字产品所有者对所加载的水印有不同的要求。例如，有的所有者目的是保护版权，需要加载稳健性强的水印；有的所有者要保护数字产品的真实性，需要加载脆弱的不可见水印。这些水印算法将由谁提供才能让公众信服，让所有者放心？

综上所述，在 Internet 网这样的开放环境里，保护数字产品的版权必须采用一套严密完整的体系标准，规定网络上利益联系的实体、可信任第三方、加载和检验水印的实体、各个实体的责任、应遵守的协议等，即安全数字水印体系。

4 多媒体产权保护和认证体系结构的范例—— IMPRIMATUR

4.1 IMPRIMATUR 体系结构

IMPRIMATUR[7] 是由欧洲委员会 DGIII 计划制定的网络数字产品的知识产权保护 IPR (Intellectual Property Rights) 认证和保护体系标准。 IMPRIMATUR 系统定义了电子商务环境下的若干重要角色，描述了角色间的关系。如图 1 所示。

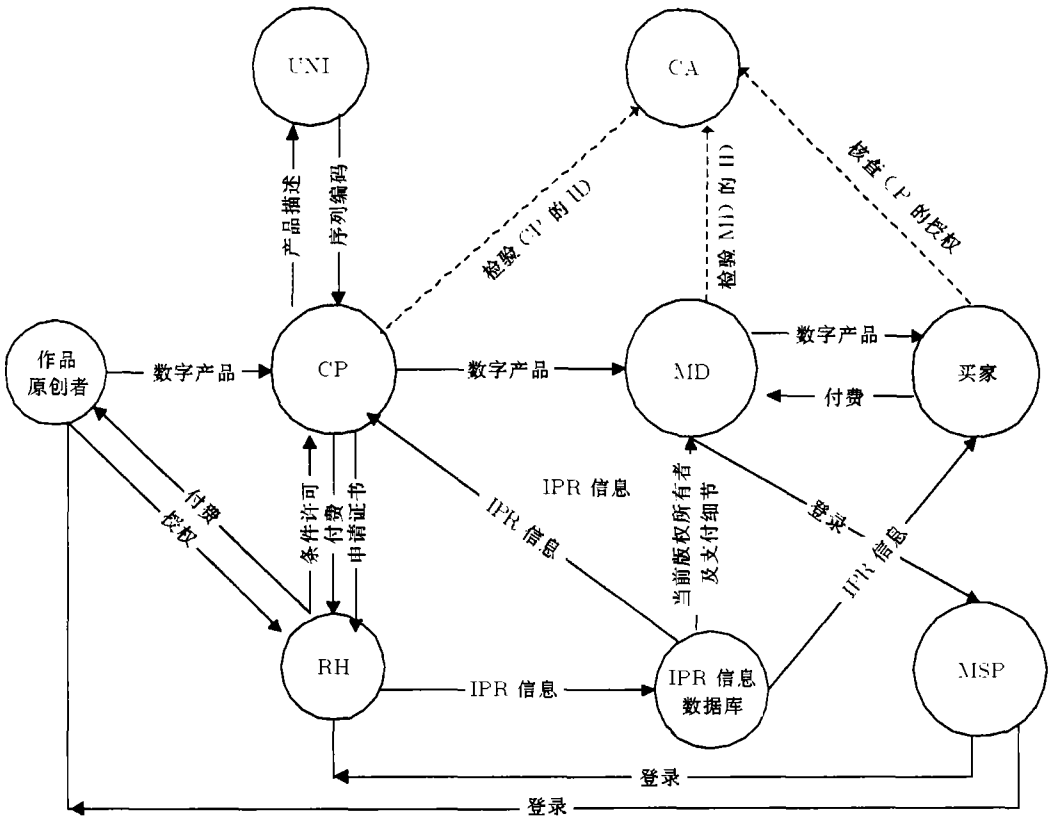

图 1　IMPRIMATUR 体系结构模型

图 1 中的角色定义如下：

(1) 作品原创者：如作者，电影制造商，音像产品制造商等.

(2) RH(Rights Holder)：版权所有者.

(3) CP(Creation Provider) 和 MD(Media Distributor)：网络多媒体产品的提供商. CP 和 MD 必须从版权所有者那里得到发行许可才能提供服务. MD 是从 CP 得到授权的合法数字产品提供商. 为了简化模型，可以认为 CP 和 MD 是一个机构，执行同样的功能，统称为网络多媒体产品的提供商.

(4) UNI (Unique Number Issuer)：产品序列号分发机构. 主要负责为数字产品产生唯一标识的序列号.

(5) CA(Certification Authority)：认证中心，是数字水印的检验机构，同时负责提供水印算法和分发水印密钥.

(6) IPR 信息数据库：IPR 信息数据库，是法律授权的权威机构，负责登记产品的版权信息、版权所有者的信息、经过版权所有者许可的网络多媒体产品提供商的信息.

(7) 买家：数字产品的购买者.

(8) MSP(Monitoring Service Provider)：监视数字产品的非法拷贝工作可以由法定部门进行，也可以由服务提供商提供. 该机构的细节问题超出了本文的讨论范围，这里不再赘述. 其中存在商务关系的角色有作品原创者，版权所有者，网络多媒体产品提供商，中间分发商和购买者. 作品原创者将从版权所有者获取版税，版权所有者向网络多媒体产品提供商和中间分发商提供发行许可. 网络多媒体产品提供商，和购买者之间是买方和卖方的关系. 其中的可信任

第三方有产品序列号分发机构，认证中心， IPR 信息数据库。从这三个机构的职能及其与其它各角色的关系可以了解整个体系的运行过程。

4.1.1 IPR 信息数据库 IPR 信息数据库是经过政府授权的 IPR 信息数据库。任何版权所有者想将产品数字化，通过网络发布数字产品，必须找到合适的网络多媒体产品提供商为他完成这些工作。当然版权所有者也可以自己同时做为网络多媒体产品提供商。版权所有者必须在 IPR 信息数据库中注册登记，提供产品的 IPR 信息、版权所有者的信息、版权所有者所许可的网络多媒体产品提供商的信息、注册日期、注册期限等。版权所有者将这些信息存放在自己的数据库中。

4.1.2 UNI 版权管理机构主要是通过国际标准序列号来管理 IPR 。例如 (ISBN)ISO2108, (ISSN)ISO3297 等. 数字产品的版权保护也需要一个产品序号标准来标识其唯一性。有些网络多媒体产品提供商想自己定义序号标识，而不是由权威机构来统一管理。这将会给数字产品监测和认证带来很大困难。因为没有人能够保证其唯一性。目前比较著名的序号标识体系是 DOI[8] 。DOI 机构独立于任何商家企业，是获得官方授权的可信任第三方。产品序列号的定义有两种方法：智能型和非智能型。前者不同的序列位代表不同的含义，如 ISRC ，可以根据序列号确定有关产品的信息，如产品种类、生产日期、地理位置等。其缺点是不利于扩充。后者则是一系列无意义的数字，如 ISWC 。虽然方便扩充，但不易于分类管理。

4.1.3 CA CA 是经过官方授权的机构，主要控制水印的加载和鉴定。 CA 和网络多媒体产品提供商之间的交互必须遵守一定的协议，称之为水印协议，这是 IMPRIMATUR 体系实施的关键环节。

4.2 AQUARELLE 商业模型及其水印协议

水印协议规定了 CA 和网络多媒体产品提供商之间传递的信息以及交互方式。协议中定义的主要角色有：

(1) TTP ： 可信任第三方，即 IMPRIMATUR 中的 CA 。

(2) CO ： 数字产品版权所有者，即 IMPRIMATUR 中的 CP 和 RH 。

(3) CO-ID ： CO 自定义的标识，用来唯一标明身份。

(4) IM ： 原始图象。未加载水印的数字多媒体产品。

(5) IM-ID ： 唯一标识 IM 的序列。在 IMPRIMATUR 中， IM-ID 应由 UNI 统一发布。

(6) D ： 水印加载的日期。

(7) IM* ： 加载水印后的 IM 。 IM** ： 加载水印后的 IM ，可能已经被篡改或遭到攻击。

(8) K-ID ： 用来加载和检测水印的密钥，不同的数字产品有不同的 K-ID 。

(9) User: AQUARELLE 的用户。

最初的水印协议采取三个步骤：

(10) CO 向 TTP 发送 IM ， IM-ID ，和 CO-ID 。

(11) TTP 产生随机密钥 K-IM, 对 IM 加载水印，将 IM-ID ， CO-ID ， D 保留在数据库中。

(12) TTP 将加载水印后的 IM* 返回给 CO ，同时返回的还有 CO-ID 和 IM-ID 。

上面三个步骤将水印的加载和检测交给 TTP 完成，由 TTP 负责分发水印密钥，区分不同的 CO ，提供统一可靠的水印算法。 TTP 提供的检测结果可以作为法庭判决的强有力证据。这样一个规范的过程避免了仲裁水印过程中不必要的纠纷。虽然如此，该协议仍然存在缺陷。首先， CO 必须向 TTP 发送 IM ，从 TTP 接收 IM* 。往返过程将占用很大带宽，消耗大量网络资源。而且 IM 和 K-ID 在发送的途中很有可能被人窃取。

经过改进的 DHWM 协议克服了最初水印协议的缺陷。 DHWM 协议由欧洲文化数据库 AQUARELLE 所提出并已被 AQUARELLE 采用。 DHWM 结合了数字水印技术和密码学领域的认证体制，为用户提供了一个较完善的 IPR 保护机制。协议模型如图 2 所示。

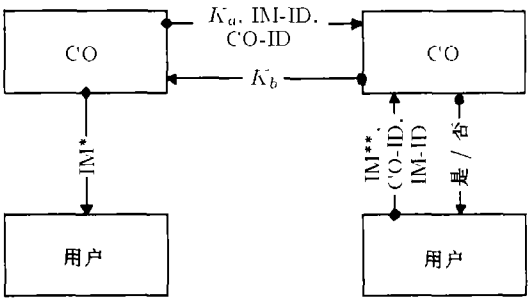

图 2　DHWM 协议模型

协议的交互过程如下：

(1) CO 和 TTP 共同产生一个公共密钥 K-IM。K-IM 的生成采用 DH[9] 公钥密码体制，通过通信双方 Alice 和 Bob 的交互产生公共的会话密钥。其原理如下：

两个公开的整数 p, g。其中 $p < g$，且 p 是大素数。从代数式 $g^{X_a} \bmod p$ 很难确定 X_a 的值。其难度依赖于 p 的二进制比特位长度 n，算法复杂度为 $O\{\exp(n \log\log n)^{1/3}\}$。

当 p 足够大时，我们可以认为从中解出 X_a 是不可能的。公共会话密钥的生成过程如下：

步骤 1　Alice 随机产生自己的密钥 X_a，计算

$$K_a = g^{X_a} \tag{1}$$

将 K_a 传送给 Bob;

步骤 2　Bob 随机产生自己的密钥 X_b，计算

$$K_b = g^{X_b} \tag{2}$$

将 K_b 传送给 Alice;

步骤 3　公共会话密钥

$$K_{ab} = (g^{X_b})^{X_a} = g^{X_a X_b} = (g^{X_a})^{X_b} = K_{ba} \tag{3}$$

现在 Alice 和 Bob 共同分享一个会话密钥。即使 K_a 和 K_b 在传输过程中分别为攻击者 C 所截获，C 也不能得到会话密钥。根据上述原理，CO 随机产生 X_a，计算出 DH 半密钥 K_a，将 K_a、IM-ID、CO-ID 传给 TTP。TTP 随机生成 X_b，计算出 K_b 作为 TTP 对所有 CO 提供的 DH 公钥，传给 CO。

(2) TTP 计算出 K_{ab} 将 IM-ID、CO-ID、D 和 K-IM 存在数据库中。

(3) CO 用 K-ID 加载水印。

DHWM 协议将密码学中的密钥分配体制与数字水印技术结合在一起，通过 TTP 和 CO 的安全交互产生公共的水印密钥，控制水印的加载和检测。发生版权纠纷时，用户向 TTP 提供 IM*、IM-ID 和 CO-ID，TTP 查询数据库得到相应的 K-ID，用 K-ID 检测是否存在水印。如果存在，将检测到的水印与 CO 出示的水印比较，相同则证明 CO 具有版权或合法许可。

变量 D(日期) 的引入是为了防止多重水印的攻击。在 IMPRIMATUR 体系中，CO-ID 是由 CO 自己产生的。IM-ID 是向产品序列号分发机构申请的，这个申请过程不需要对申请人进行版权许可的验证。因此，任何非法 CO 都可以获得其 CO-ID 和 IM-ID。假设一个非法数字产品提供商 CO1，盗用了 CO 的数字产品 IM*(已加载了 CO 的水印)。他可以通过 DHWM 协议和 TTP 共同生成一个水印密钥 K-ID1，用 K-ID1 在 IM* 中再加入自己的水印。同时向

TTP 提供 CO-ID1 和 IM-ID1 。结果，在 IM** 中重叠了两个水印。这两个水印经 TTP 检验均有效。这时， TTP 就通过数据库中记录的时间先后来判定 CO 的真实性。

5 IMPRIMATUR 体系的改进

5.1 IMPRIMATUR 体系及 DHWM 协议的缺陷

IPR 认证和保护体系和 DHWM 协议提供了一个比较完善的机制。但是仍存在漏洞和不足。主要有以下几个方面。

(1) DHWM 的安全性： DHWM 协议采用了密码学中的 DH 密码算法为通信双方产生一个公共的水印密钥 K-ID 。K-ID 为双方秘密保存，作为水印验证的依据。该协议的安全性是建立在 DH 算法的安全性基础上的。即使攻击者分别得到 K_a 和 K_b ，也不能算出 K-ID(K_{ab}) ，也就无法除去水印。然而攻击者可以在不用得到 K-ID 的情况下，采用中间人攻击法成功地达到攻击目的。具体做法如下：攻击者 C 随即选择一个密钥 X_c ，计算出 $K_c = g^{X_c} (\mathrm{mod} p)$ 。

同时， C 分别截获来自 A 和 B 的 K_a 和 K_b ，然后分别向 A 和 B 发送 K_c 。这样，在 A 端计算出来的密钥： $K - \mathrm{ID1} = g^{X_a X_c} (\mathrm{mod} p)$ 。

B 端计算出的密钥： $K - \mathrm{ID2} = g^{X_b X_c} (\mathrm{mod} p)$ 。

A 端用 K-ID1 作为水印密钥加载水印，而在 B 端保存的用来验证的水印密钥是 K-ID2 ，不可能检验出 A 的水印的存在。

(2) TTP 对 CO 的身份认证： IMPRIMATUR 中的 CA(TTP) 和产品序列号分发机构并没有采取对 CO 的身份验证。也就是说，任何 CO ，不管合法还是非法都可以向产品序列号分发机构申请 IM-ID ，产品序列号分发机构并不知道该 CO 提供的 IM 是否是盗版的。CO 将该 IM-ID 和自己定义的 CO-ID 提交给 CA(TTP) 后，就可以和 CA 交互得到公共水印密钥 K-ID ，加载自己的水印。虽然 D(时间登记) 可以抵御加载多重水印的攻击方法，但是如果攻击者结合上述 DHWM 的漏洞，就完全可以达到颠倒是非，混淆黑白的目的。除此之外， CA(TTP) 和产品序列号分发机构对 CO 不加鉴别地提供服务也将浪费它们的数据库资源，给管理带来不便。

(3) 水印算法的发布：这是该协议中遗漏的一个环节。 TTP 和 CO 必须采用同一水印算法，才能检测出 CO 加载的水印。 TTP 应负责提供统一的安全水印算法。为了防止攻击者替换水印算法，应建立一个安全的获取水印算法的途径。

5.2 改进

针对上述 3 个问题，我们在 IMPRIMATUR 体系结构和 DHWM 协议的基础上作了相应的改进，建立一个更加简洁实用的安全数字水印体系。如图 3 所示。

(1) 设立 DPLI 机构：为了防止任何 CO 不加限制地申请 IM-ID ，可以将产品序列号分发机构和 IPR 信息数据库的功能结合在一起，由一个机构统一管理，称为 DPLI(Digital Product License Issuer) 。 DPLI 对申请 IM-ID 的 CO 进行身份验证。同时， DPLI 机构将负责登记版权所有者的版权信息、版权所有者所授权的 CO 的信息、授权日期、授权期限等。对于每个 CO ， DPLI 还保存了该 CO 的数字产品的信息，如产品名称、类别、生产日期等。 DPLI 接着为每个 CO 和版权所有者 (如果版权所有者自己发布产品的话) 生成一个序列号即 IM-ID 。为了防止攻击者通过直接与 CA 交互加载水印来寻找漏洞， DPLI 将对所有合法 CO 和版权所有者发布许可证书，该证书将作为 CO 和版权所有者同 CA 交互的许可。具体实现上，可以采用数字签名技术。 DPLI 将 IM-ID 、有关 CO 的公开信息、许可说明、许可日期等用其私钥做数字签名，用 CO 的公钥加密后传给 CO 。 CO 必须向 CA 出示经 DPLI 签名的许可才能得到 CA 提供的水印服务。在 CO 向 CA 提供许可证书前，先用 CA 的公钥加密，再进行传输。这里，两次用到了公钥加密体制，这是因为许可证书的作用至关重要，如果不加密传送，容易被人截取来冒充合法 CO 。

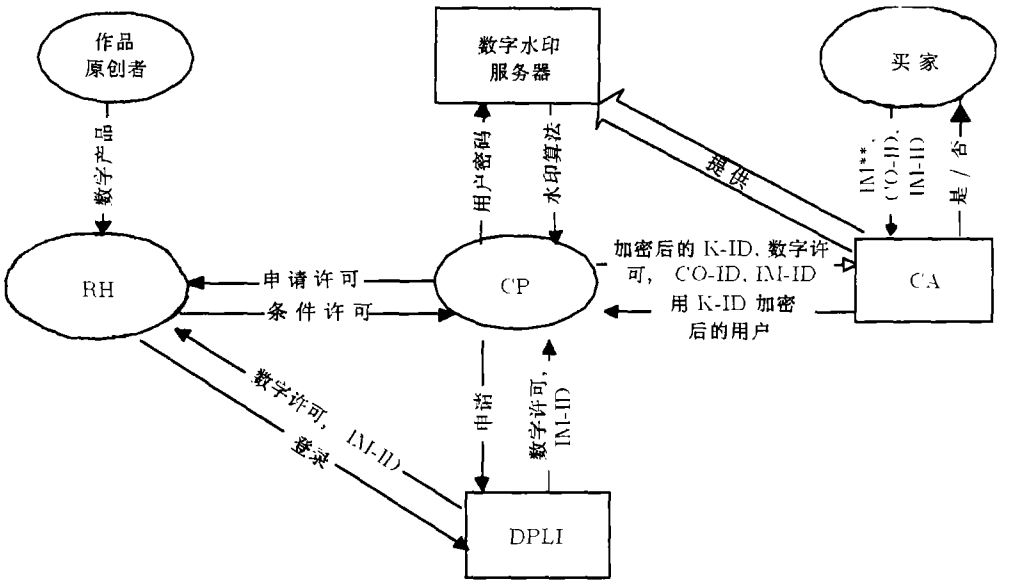

图 3　安全数字水印体系模型

(2) 水印密钥的传递：采用 DHWM 水印协议来解决水印密钥的传输是存在漏洞的。因此，必须改用其它的加密体制。公钥加密体制 (如 RSA) 是个很好的选择。CO 选定 K-ID 后，将 K-ID，CO-ID 用 CA 的公钥加密再传给 CA。当然，同时传给 CA 的还有经签名和加密后的许可证书。CA 收到后，用自己的私钥解开，核查无误后保存在数据库中。然后生成一个确认信息，用 K-ID 加密后回送给 CO。

(3) 水印算法的分发：为了防止水印算法被攻击者替换，可以采取以下方法。CA 提供一个水印算法服务器，该服务器上存放的水印算法都是经过 CA 认定的安全算法。只有合法用户才能从该服务器上下载水印算法。这些合法用户就是经 CA 核查无误的 CO。CA 为每个合法的 CO 提供一个帐号和密码，以便该 CO 登录水印服务器。CA 在向 CO 传递帐号和密码前可以先用该 CO 的 K-ID 加密。这时的 K-ID 相当于一次性密码。水印服务器可以根据 CO 要求的多样性，提供多种水印算法，如用于验证版权的稳健性水印、用于验证真实性的脆弱性水印、用于标识数字产品的可见水印、用于提供侵权证据的不可见水印等。

6 结　论

数字水印技术是数字产品产权保护的强有力保证。然而，技术的进步必须配合安全体制的制定和完善才能真正发挥作用。IMPRIMATUR 体系规范了数字水印的加载和检测过程，为 IPR 保护提供了较完善的模型。但是该体系仍有潜在的安全问题。另外，DHWM 水印协议也存在安全漏洞。经过改进的数字水印体系更加简化，弥补了原来的安全缺陷，必将推进数字水印技术的应用，为 IPR 的保护和认证提供了有力保障。

参　考　文　献

[1] E. Koch, J. Zhao, Towards robust and hidden image copyright labeling, Proc. of 1995 IEEE Workshop on Nonlinear Signal and Image Processing, Neos Marmaras, Halkidiki, Greece, June 20-22, 1995, 452-455.

[2] I. J. Cox, J. Kilian, T. Leighton, T. Shamoon, Secure spread spectrum watermarking for images audio and video, IEEE Proc. Int. Conf. Image Processing(ICIP'96), Lausanne, Switzerland, Vol.III, 1996, 243–246.

[3] I. J. Cox, J. Killian, F. T. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Trans. on Image Processing, 1997, 6(12), 1673–1687.

[4] L. F. Turner L F, Digital data security system, Patent IPN WO89/08915, 1989.

[5] R. G. Schyndel, A. T. Tirkel, C. F. Osborne, A digital watermark, Int. Conf. on Image Processing, Vol.2, 1994, 86–90.

[6] Scott Craver, Nasir Memon, Boon-Lock Yeo, Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications, IEEE J. on Selected Areas in Communications, 1998, 16(4), 573–586.

[7] Daniel Augot, Jean-Marc. Jean-Francois, Secure delivery of image over open networks, Proc. IEEE, 1999, 87(7), 1251–1266.

[8] Keith Hill, A Perspective: The role of identifiers in managing and protecting intellectual property in the digital age, Proc. IEEE, 1999, 87(7), 1228–1238.

[9] W. Diffie, M. W. Hellmann, New directions in cryptography, IEEE Trans. on Info. Theory, 1976, IT-22(5), 644–645.

THE RESEARCH OF SECURE DIGITAL WATERMARKING ARCHITECTURE

Mao Qiong Chen Mingqi Xia Guangsheng Yang Yixian Tan Tieniu*

(*Info. Security Center, Beijing Univ. of Posts and Telecom., Beijing* 100876, China)

*(*National Laboratory of Pattern Recognition, Beijing* 100080, China)

Abstract Watermarking, as a new technique mainly used for IPR protection and authentication, has become a research hotspot not long after its appearance. Many effective watermarking algorithms have been proposed. But the mature of watermark technology is not enough for IPR protection. Confronted with current various attack method, a secure watermarking architecture must be built to standardize the whole process, from watermark insertion to detection. The AQUARELLE system is a good example for showing how IMPRIMATUR —an architecture for IPR protection is operated. The secure flaws of IMPRIMATUR and AQUARELLE system watermarking protocol will also be pointed out. Further, a new secure watermarking architecture will be proposed. Its effectiveness will make up for the flaws mentioned above.

Key words Intellectual property right protection, Digital watermarking, Watermarking attack, Watermarking protocol, Secure digital watermarking architecture

毛 琼: 女, 1975 年生, 硕士生, 研究方向为密码学, 计算机网络与信息安全, 信息隐藏, 数字水印等.

陈明奇: 男, 1973 年生, 博士生, 研究方向为密码学, 计算机网络与信息安全, 信号处理, 信息隐藏, 数字水印等.

夏光升: 男, 1974 年生, 博士生, 研究方向为密码学, 计算机网络与信息安全, 叠像术, 信息隐藏, 数字水印等.

杨义先: 男, 1961 年生, 教授, 博士生导师, 全国政协委员, 研究方向为密码学, 计算机网络与信息安全等.