用于盗版追踪的数字水印协议研究

胡玉平[1,2] 张 军[1]
(广东商学院信息学院 广州 510320)[1] (湖南人文科技学院计算机系 娄底 417000)[2]

摘 要 设计了一种用于盗版追踪的基于数字水印的买卖交易协议。协议中,为了减少可信任第三方的在线参与,引入了一个无记忆的水印认证授权中心WCA,它能为买方一次产生多个数字水印,从而不需要参与买卖双方的每次数字产品交易。为了解决买方匿名问题,WCA应加密买方的数字证书,并通过买方将其传递给卖方,使买方在购买数字作品时方能保持匿名。此外,本协议能解决其它各种已知的安全问题,如消费者权益、水印绑定问题、共谋问题、争论问题。分析结果表明,提出的协议是安全有效的。

关键词 数字水印,盗版追踪,安全协议
中图法分类号 TP391 **文献标识码** A

Watermarking Protocol for Piracy Tracing

HU Yu-ping[1,2] ZHANG Jun[1]
(Guangdong University of Business Studies, Guangzhou 510320, China)[1]
(Hunan Institute of The Humanities, Science and Technology, Loudi 417000, China)[2]

Abstract A novel buyer-seller watermarking protocol was designed for piracy tracing. In the proposed protocol, a memoryless Watermark Certification Authority (WCA) was introduced, that can produce many watermarks for a buyer at a time and is not required to participate in each transaction of digital content between the buyer and seller. In order to guarantee the anonymity of the buyer, the WCA also can encrypt the digital certificate of buyer and hand over the encrypted message to seller via the buyer. In addition, the proposed protocol also can resolve other problems, such as the customer right problem, the binding attack problem, the digital conspiracy problem, the dispute problem. The analysis indicate that the proposed protocol is secure and practical.

Keywords Digital watermarking, Piracy tracing, Securer protocol

1 引言

在网络环境下进行的数字作品交易中,若要保护数字版权,使用的数字水印算法的安全性固然很重要,但也必须考虑到版权保护过程中所采用的协议的安全性[1,2]。水印安全协议是以密码学、数字水印为基础的消息交换协议,其目的是在网络环境中提供各种安全服务。当攻击者转向攻击协议而不是数字水印算法本身时,如果协议本身存在安全漏洞,整个系统就起不到真正保护数字版权的作用。显然,通过引入完备的安全协议,可以最大限度地防范攻击者对整个系统的破坏。基于数字水印的数字版权保护安全协议,在国外开展研究的时间不长,但已经受到世界各国的重视。目前国内这方面的研究还处于起步阶段,主要是对数字水印算法应用过程中存在的一些实际问题进行了探讨,但距离形成基本实用的数字版权保护安全协议还有较大距离。

一般地,在水印协议框架内至少包含3个独立的角色[3],即买方(Buyer)、卖方(Seller)及仲裁(Arbiter)。买方作为数字内容的最终使用者,卖方作为数字内容的所有者和提供者,在交易中通过水印技术在数字内容的每个拷贝中嵌入水印,以识别买方;仲裁是可信赖的第三方(TTP),在版权纠纷出现时,通过卖方提供的相关证据进行裁决。三者间的交互主要由买卖双方交易数字产品和证据提交及仲裁两部分组成。一个安全的基于数字水印的买卖交易协议应主要解决以下6个基本的安全问题[4,5]:(1)盗版追踪问题。对非法复制和传播数字作品的盗版源进行追踪。(2)消费者权益保护问题。水印的产生及嵌入由多方参与,保证对买卖双方进行平等的约束,从而达到保护双方的利益不受侵犯,特别是保证任何一个诚实的消费(购买)者不会被恶意的卖方或其他购买者诬陷。(3)水印移植(未绑定)问题。卖方将买方的水印移植到其他数字作品中,这样可以恶意控告买方非法传播数字作品以获取更多赔偿。(4)匿名(私隐保护)问题。消费者(买方)个人信息泄露给了卖方。(5)共谋问题。第三方与交易的一方共谋来侵害另一方的利益。(6)争论问题。被指控非法复制和传播数字作品的购买者无法指控盗版是由买方或卖方的系统

到稿日期:2009-02-18 返修日期:2009-04-25 本文受国家自然科学基金课题(60873198),湖南省教育厅重点科研项目(06A031),广东省自然科学基金项目(06023961),广东省教育厅高水平科研项目(05Z013)资助。
胡玉平(1969—),男,博士,教授,主要研究方向为信息隐藏与网络安全,E-mail:okhyp@yahoo.com.cn;张 军(1966—),男,博士,教授,主要研究方向为信息隐藏与传感器网络。

安全漏洞造成的。

考虑到在互联网上买卖双方交易的实际需要，我们认为一个有效的买卖交易协议还要解决如下问题：(7)可信赖三方(TTP)的在线参与问题。TTP 必须参与买卖双方的每一次交易，买方、卖方和 TTP 的交互将成为协议走向应用的瓶颈。遗憾的是，目前还没有一个水印协议能够很好地解决以上所有的问题。Qian 和 Nahrsteds 在文献[6]中，首次提到了在用于盗版追踪的数字水印协议中存在消费者权益保护问题。Memon 和 Wong 在文献[7]中提出了一种能同时解决盗版追踪和消费者权益保护问题的基于数字水印的买卖交易协议，在此协议中，利用数字水印和认证机构功能的结合，实现了产品提供者对于包含购买者水印的拷贝的不可知，因此它无法复制包含购买者水印的拷贝。Lei 等人在文献[8]中首次讨论了水印绑定问题。在此协议中，通过 TTP(可信任第三方)的签名把一个水印和购买订单绑定，而购买订单又和本次交易的产品唯一绑定，这样卖方无法将买方的水印移植到其他数字作品中；此外，在此协议中买方通过向证书机构(CA)申请一个匿名证书，可以在交易中保持匿名性。在文献[9]中，Ju 等人提出了一个匿名的数字水印协议。在此协议中，买方可以匿名地购买一个数字作品且匿名是受控制的。在文献[4]中，J. Zhang 提出了一个安全的买卖水印协议，由于无第三方参与，可以完全避免共谋问题的发生。在文献[10]中，Chun-I Fan 提出了一个无可信第三方在线参与的买卖水印协议。在此协议中，每个销售者(买方)配置了一个防篡改的 WCA 设备来产生所需的水印和数字签名。然而，在以上提出的协议中，文献[6,7]协议存在不能解决水印未绑定、匿名及共谋的问题。文献[4,8,9] 协议中，每次交易买方还需要从认证机构获得一个匿名的数字证书，这样在网络环境下，每一次交易均需一个可信任的第三方在线参与，将成为这些协议走向应用的瓶颈。在文献[10]协议中，每个销售者(卖方)附加配置了一个防篡改的 WCA 设备，此设备也将在线参与买卖双方的每次交易，但此设备的实现成本及开销将会严重影响协议的实现。

2 同态加密技术

对于定义在代数结构$(G,*)$上的公钥加密函数 $E:G\rightarrow R$，如果给定 $E(X)$和 $E(Y)$，其中 $x,y\in G$，在没有私钥的情况下能够计算出 $E(x*y)$，则称该公钥加密系统具有同态性质[11]。例如，公钥密码算法满足乘同态性，即

$$E(x)*E(y)=E(x*y) \tag{1}$$

Paillier 公钥密码体制[12]满足加同态性，即

$$E(x)+E(y)=E(x+y) \tag{2}$$

同态公钥密码体制目前在安全投票协议、多方计算和签名等方面得到了广泛的应用。在数字水印领域中，若数字水印采用乘嵌入方式嵌入到原始的媒体数据中，并采用 RSA 公钥密码体制对其进行加密，由式(1)可得

$$E(y_i)=E(1+\alpha w_i)E(x_i) \tag{3}$$

若数字水印采用加嵌入方式嵌入到原始的媒体数据中，并采用 Paillier 公钥密码体制对其进行加密，由式(2)可得

$$E(y_i)=E(\alpha w_i)E(x_i) \tag{4}$$

在买卖双方协议中，用户水印的嵌入算法利用了加密算法的同态性：

$$E(\hat{X})=E_{PK_B}(X')\oplus E_{PK_B}(\delta(W))=E_{PK_B}(X'\oplus\delta(W)) \tag{5}$$

对含水印的作品信息进行加密，等价于对原始作品信息和水印信息分别进行加密后相乘或相加。这样就可以保证用户水印的安全性，因为一般的方案中用户水印由版权人独立嵌入，那么版权人也可以随意提取用户水印，版权人完全可以利用用户水印进行非法操作，这样对用户很不公平。而加密算法的同态性使得用户的水印是用公钥加密后传给版权人，版权人必须对原始作品用公钥加密后才能实现用户水印的嵌入。版权人在水印嵌入时不知用户水印内容，也得不到用户购买的作品的最终版本，所以不可能对用户水印进行非法操作，用户水印的安全性得到保证。

同态加密技术是买卖双方协议的基础，也是其优于一般水印协议的原因所在。本文提出的协议也是建立在这一基础之上的，且直接利用具备乘法同态性的加密技术，进行用户水印的嵌入，如式(3)。

3 协议设计

整个协议由 3 个子协议组成：水印生成子协议、交易子协议、仲裁协议。协议包含 4 个主要的角色，即买方 B，卖方 S，水印认证授权中心 WCA，仲裁 ARB。买方、卖方、仲裁前面已经介绍，这里不再重复。协议中，WCA 的主要责任是为买方生成随机有效的水印，它一次能为买方生成多个数字水印，从而不需要参与买卖双方的每次数字作品交易。为了保证买方的匿名，WCA 还对买方的数字证书进行加密，并通过买方把加密的数字证书传给卖方。协议中出现的主要符号定义如下。

(PK_I,SK_I)：用户 I 的公私钥对，其中 PK_I 是 I 的公钥，SK_I 是 I 的私钥。

$Sign_{SK_I}(M)$：用户 I 用它的私钥对信息 M 的数字签名。

$E_{PK_I}(M)$：用 I 的公钥 PK_I 对信息 M 加密。

$E_{SK_I}(C)$：用 I 的私钥 SK_I 对原始信息的加密信息 C 进行解密。

$Cert_{CA}(I,PK_I)$：用户 I 的数字证书，它包含用户的身份 I、用户所持有的公钥 PK_I 以及 CA 认证中心对(PK_I,I)的数字签名。

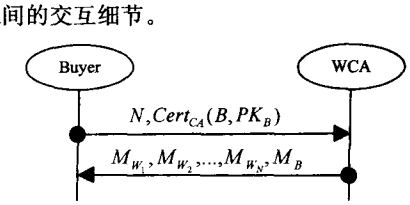
$\oplus$：水印嵌入操作算法。

σ：随机变换函数。

协议中采用的加密操作 E_{PK_I}有秘密同态性，即对任意的信息 a 和 b，有 $E_{PK_I}(a\oplus b)=E_{PK_I}(a)\oplus E_{PK_I}(b)$。

3.1 水印生成子协议

为了完成水印的生成，买方和水印认证授权中心 WCA 遵循如下的水印生成子协议，图 1 描述了水印生成子协议中两者之间的交互细节。



$$M_{W_i}=\{Sign_{SK_{WCA}}(PK_B\|E_{PK_B}(W_i)\|E_{PK_{WCA}}(W_i),E_{PK_B}(W_i),E_{PK_{WCA}}(W_i))\}$$

$$M_B=\{Sign_{SK_{WCA}}(PK_B\|E_{PK_{WCA}}(Cert_{CA}(B,PK_B)),PK_B,E_{PK_{WCA}}(Cert_{CA}(B,PK_B)))\}$$

图 1 水印生成子协议的交互细节

Step1　买方 B 向 WCA 提供包含其身份信息和公钥的数字证书 $Cert_{CA}(B,PK_B)$ 以及所需申请的水印个数 N。

Step2　水印认证授权中心 WCA 在验证申请者的身份后，为申请者随机产生多个水印 $W_1,W_2,\cdots,W_N$，并根据式(6)，式(7)生成消息 $M_{W_1},M_{W_2},\cdots,M_{W_N},M_B$

$$M_{W_i}=\{Sign_{SK_{WCA}}(PK_B\|E_{PK_B}(W_i)\|E_{PK_{WCA}}(W_i),E_{Pk_B}(W_i),E_{PK_{WCA}}(W_i))\} \quad (6)$$

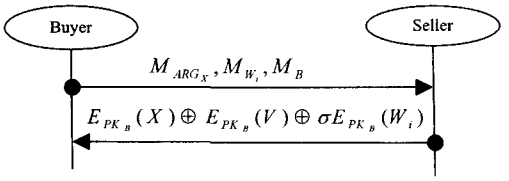
$$M_B=\{Sign_{SK_{WCA}}(PK_B\|E_{PK_{WCA}}(Cert_{CA}(B,PK_B)),PK_B,E_{PK_{WCA}}(Cert_{CA}(B,PK_B)))\} \quad (7)$$

然后，WCA 把消息$\{M_{W_1},M_{W_2},\cdots,M_{W_N},M_B\}$发送给买方 B。

Step3　买方 B 收到 WCA 的消息后，验证$\{M_{W_1},M_{W_2},\cdots,M_{W_N},M_B\}$中所有签名的正确性，如果所有的签名正确，买方 B 把$\{M_{W_1},M_{W_2},\cdots,M_{W_N},M_B\}$保存到自己的数据库中。

3.2　交易子协议

为了完成数字产品的交易，买方 B 和卖方 S 遵循如下的水印生成子协议，图 2 描述了交易子协议中两者之间的交互细节。



$$M_{ARG_X}=\{Sign_{SK_B}(E_{PK_B}(W_i)\|ARG_Y),ARG_X)\}$$

$$M_{W_i}=\{Sign_{SK_{WCA}}(PK_B\|E_{PK_B}(W_i)\|E_{PK_{WCA}}(W_i)),E_{Pk_B}(W_i),E_{PK_{WCA}}(W_i))\}$$

$$M_B=\{Sign_{SK_{WCA}}(PK_B\|E_{PK_{WCA}}(Cert_{CA}(B,PK_B)),PK_B,E_{PK_{WCA}}(Cert_{CA}(B,PK_B))\}$$

图 2　交易子协议的交互细节

Step1　卖方 S 公布将出售的所有产品的信息。如果买方 B 决定购买某数字产品 X，他首先与 S 协商并填写订单 ARG_X。ARG_X 阐述了买卖双方的权利和义务及数字产品 X 的描述，并将本次交易和 X 唯一绑定。

Step2　买方 B 从他的数据库中随机选择一个包含在 M_{W_i} 中的水印加密信息 $E_{PK}(W_i)$，并根据式(8)形成订单消息 M_{ARG_X}

$$M_{ARG_X}=\{Sign_{SK_B}(E_{PK_B}(W_i)\|ARG_X),ARG_X)\} \quad (8)$$

然后，买方 B 把消息$\{M_{ARG_X},M_{W_i},M_B\}$发送给卖方 S。

Step3　卖方 S 在收到买方 B 发来的所有消息后，验证消息 M_{ARG_X},M_{W_i},M_B 的所有数字签名。如果其中任何一个签名无效，则终止本次交易。否则 S 产生本次交易的检索水印 V，并将其嵌入数字产品 X 中，得到 $X'=X\oplus V$。卖方 S 产生一个 n 维向量的随机变换 σ，用此随机变换作用于 $E_{PK_B}(W_i)$，并计算 $\sigma(E_{PK_B}(W_i)=E_{PK_B}(\sigma(W_i))$。

Step4　由于卖方 S 从买方 B 处获得的水印信息是用买方 B 的公钥加密的 $E_{PK_B}(W_i)$，他也用相应的买方 B 的公钥对 X' 进行加密后再嵌入第二个水印 $E_{PK_B}(W_i)$，从而得到

$$E_{PK_B}(\hat{X})=E_{PK_B}(X')\oplus E_{PK_B}(\sigma(W_i))=E_{PK_B}(X'\oplus\sigma(W_i))=E_{PK_B}(X\oplus V\oplus\sigma(W_i)) \quad (9)$$

卖方 S 将计算所得的 $E_{PK_B}(\hat{X})$ 发送给买方 B。

Step5　卖方 S 把$\{V,\sigma,\oplus,M_{ARG_X},M_{W_i},M_B\}$保存在一张表格 $Table_X$ 中，每次交易在 $Table_X$ 中对应一个条目用来记录上述信息。

Step6　买方 B 收到从卖方 S 发来的 $E_{PK_B}(\hat{X})$ 后，用自己的私钥 PK_S 进行解密，得到水印化的数字品产品 $\hat{X}$

$$\hat{X}=D_{SK_B}(E_{PK_B}(X))=X\oplus V\oplus\sigma(W_i) \quad (10)$$

3.3　仲裁子协议

当卖方 S 在市场上发现数字产品 X 的盗版 Y 时，仲裁子协议将用于确定盗版者的身份，并以不可否认的证据说明就是先前交易中的买方。图 3 描述了仲裁子协议中实体之间的交互细节。

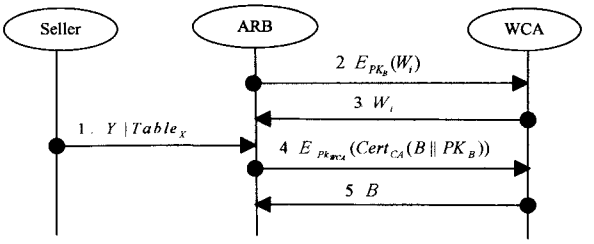


图 3　仲裁子协议的交互细节

首先，卖方 S 以 X,Y 作为输入，利用水印提取函数 $D(X,Y)$ 提取出水印 U，然后 S 用 U 检索数字产品 X 的销售记录表，查找匹配的方法视具体的水印方案而定。对于鲁棒水印技术，通常把提取的水印 U 与表 $Table_X$ 中的每个水印信息 V 进行相关检测，选择其中超过门限值 T 且相关系数值最高者为匹配项。找到匹配项 V 后，S 收集保存在该项记录中的相关信息$\{V,\sigma,\oplus,M_{ARG_X},M_{W_i},M_B\}$，并将它们和 Y 一起发送给仲裁机构 ARB，请求仲裁。

仲裁收到以上信息后，首先检查 Y 是否与消息 M_{ARG_X} 中订单 ARG_X 对 X 的描述一致，然后验证消息 M_{ARG_X},M_{W_i},M_B 中签名的有效性。如果其中任何一个无效，则拒绝诉讼。否则，请求 WCA 解密 $E_{PK_{WCA}}(W_i)$。WCA 把解密得到的 W_i 返回给仲裁，仲裁将 W_i,σ,V 和 Y 作为水印检测算法的输入，以判断 Y 中是否存在水印 V 和 σW_i。如果 Y 中检测存在水印 V 和 σW_i，仲裁要求 WCA 解密 $E_{Pk_{WCA}}(Cert_{CA}(B\|PK_B))$ 且揭示 B 的真实身份。买方的身份被揭穿后，仲裁将宣判买方有罪并结束诉讼。如果 Y 中检测不出 V 和 σW_i，则买方将被认为是无辜的，其身份依旧保密，而卖方将被认为有诬告的嫌疑。

4　有效性和安全性分析

我们提出的协议方案的安全性建立在所采用的水印技术和密码技术的安全性的基础上。与前人的工作相比，协议的实现有两个方面的特点：(1)引入了一个无记忆的水印认证中心(WCA)，它能为买方一次产生多个水印，且不需要参与买卖双方的每一次数字作品交易；(2)WCA 加密买方的数字证书，且通过买方传递给卖方。本节将从有效性和安全性的角度对我们提出的协议进行相关的分析和探讨。

4.1　协议有效性分析

(1)WCA 在交易中的参与问题：WCA 是买方和卖方之间增加的一个角色。为了减少第三方的在线参与，在我们的协议中，WCA 可根据买方的需要为买方一次生成多个水印，而买方与卖方的每一次交易只需要一个水印，这样买方与 WCA 的交换次数将大大减少，且 WCA 也不需要在线参与买卖双方的每一次交易，也就是说我们的协议能较好地解决在引言中提出的问题(7)。为了改善 WCA 的可靠性，可以使用

集群解决方案将 WCA 设置成一个单独的结点。此外，若在互联网上配置一个具有 WCA 结点的分布式系统，则可以解决由于网络故障而使买方暂时无法连接上某一特定 WCA 的问题。

(2) WCA 的存储要求：可信任第三方(TTP)的配置开销将对安全协议产生直接影响。事实上，一个无记忆的可信任第三方有利于协议在应用中的实现。在我们提出的协议中，WCA 不需要把它生成的所有水印保存在一个数据库中，因为水印 $W_i(i=1,2,\cdots,N)$ 一旦产生，就会生成 $M_{W_i}(i=1,2,\cdots,N)$ 并发送给购买者。如果 ARB 需要某一水印，WCA 再通过解密 ARB 提供的密文来恢复水印。另外，对于 ARB，它只是简单地回应 S 的请求，也不需要保存任何信息。

(3)买方和卖方的存储要求：与以往提出的协议不同，我们的协议中，每一次交易卖方需要保存一条记录 $\{V,\sigma,\oplus,M_{ARG_X},M_{W_i},M_B\}$，买方申请水印后也需要保存 WCA 发送给他的信息 $M_{W_1},M_{W_2},\cdots,M_{W_N},M_B$。我们认为这种存储要求是合理的，因为在现实世界中，买方很有可能要保存他的私人信息，卖方每次销售也需保存一个记录，而存储合理的有用信息可以看作买卖交易合理投资的一部分。随着存储设备容量的增大，价格的降低，协议中附加的存储开销在交易中实际上可以忽略不计。

由以上分析可知，本文提出的协议接近于现实情况，不会出现交易的瓶颈，且对 WCA 没有存储要求，有利于协议的实现和应用。

4.2 协议安全性分析

本文提出的协议可以解决引言中提出的 6 个基本安全问题。具体分析如下。

(1)盗版追踪：协议中，买方得到的数字产品是水印化的数字产品，但他不知道原始的数字产品 X 以及随机变换函数 σ，所以他无法从水印化的数字产品中移除水印 σW_i。另外，一旦发现盗版，协议也提供了相应的机制，确定盗版者的身份。

(2)消费者权益保护：协议中，卖方能知道 $E_{PK_B}(W_i)$ 及 $E_{PK_B}(\hat{X})$，但他无法获得原始的水印信息 W_i 及数字产品的最终形式 $\hat{X}$，所以他无法伪造 $\hat{X}$ 并诬告买方 B。

(3)绑定问题：协议中买方的消息 M_{ARG_X} 中用签名 $Sign_{SK_B}(E_{PK_B}(W_i)||ARG_X))$ 将 $E_{PK_B}(W_i)$ 和 ARG_X 绑定在一起，而 ARG_X 唯一地指定了 X，所以卖方无法将他出售给买方的数字产品 $\hat{X}$ 中的水印移植到其它数字产品中。

(4)买方的匿名问题：协议中，买方的身份信息 B 包含在其数字证书 $Cert_{CA}(B,PK_B)$ 中。卖方能获得的信息 $\{V,\sigma,\oplus,M_{ARG_X},M_{W_i},M_B\}$ 中，只有 M_B 中包含了用 WCA 公钥对买方数字证书加密的信息 $E_{PK_{WCA}}(Cert_{CA}(B,PK_B))$，但因卖方不知道 WCA 的私钥，他也就无法解密此信息而获得买方的数字证书，从而保证了买方在交易中的匿名。此外，WCA 虽然知道买方的身份信息，但他不知道买方购买的数字产品 X，因此买方的隐私相对于 WCA 也得到了保护。

(5)共谋问题：在我们的方案中，WCA 一次生成 N 个水印，且形成信息 $M_{W_1},M_{W_2},\cdots,M_{W_N}$，而卖方只是选择一个随机的 M_{W_i} 得到 $E_{PK_B}(W_i)$。因此，除买方本人外，没有任何其他人知道买方每次交易使用的唯一水印，从而共谋攻击对我们的协议是无效的。

(6)争论问题：如果一个不诚实的买方非法出售数字产品 $\hat{X}$，卖方把它保存的记录 $\{V,\sigma,\oplus,M_{ARG_X},M_{W_i},M_B\}$ 提交给 ARB，ARB 能根据这些证据确定盗版是由不诚实的购买者引起的，且不诚实的买方不可抵赖。

结束语 本文提出了一种安全的适用于盗版追踪的买卖交易协议，此协议能解决各种已知的安全问题，如消费者权益问题、水印绑定问题、买方匿名、共谋问题、争论等问题。其主要贡献如下：(1)强调了可信赖第三方(TTP)离线参与问题的重要性。为了减少可信任第三方的在线参与，提出的协议中，配置了无需记忆功能的水印认证授权中心 WCA，它不需要参与买卖双方的每次交易。(2)强调了买方的匿名控制问题。为了保证匿名控制，提出的协议中，WCA 加密买方的数字证书，且通过买方传递给卖方，从而在购买数字作品时，买方能保持匿名，且当仲裁判断买方有版权侵权罪时，买方身份可被揭穿。

参 考 文 献

[1] Frattolillo F. Watermarking Protocol for Web Context[J]. IEEE Transactions on Information Forensics and Security, 2007, 2(3):350-363

[2] 陈晓苏，刘立刚，卢正鼎. 网络环境下数字图像版权保护安全协议的设计与分析[J]. 计算机学报，2006，29(9)：1722-1728

[3] Cheung Shing-chi, Leung Ho-fung, Wang Changjie. A commutative encrypted protocol for the privacy protection of watermarks in digital contents[C]// Proceedings of the 37th Annual Hawaii International Conference on System Sciences. 2004, 1:94-103

[4] Zhang J, Kou W, Fan K. Secure buyer-seller watermarking protocol[J]. IEEE Proceedings of Information Security, 2006, 153(3):15-18

[5] Katzenbeisser S. On the design of copyright protection protocols for multimedia distribution using symmetric and public-key watermarking[C]// 12th International Workshop on Database and Expert Systems Applications. 2001:815-819

[6] Qiao L, Nahrstedt. Watermarking schemes and protocols for protecting rightful ownership and customer's rights[J]. Visual Comm and Image Representation, 1998, 23(9):194-210

[7] Memon N, Wong P W. A buyer - seller watermarking protocol [J]. IEEE Transactions on Image Processing, 2001, 10(4):643-649

[8] Lei L, Yu P L, Tsai P L, et al. An Efficientand and Anonymous Buyer-Seller Watermarking Protocol[J]. IEEE Transactions on Image Processing, 2004, 32(16):1618-1626

[9] Ju H S, Kim H J, Lee D H, et al. An anonymous buyer-seller watermarking protocol with anonymity control[C]// Lee P J, Lim C H. eds. Proc. ICISC. 2002, LNCS 2587:421-432

[10] Fan Chun-I, Chen Ming-te, Sun Wei-zhe. Buyer-Seller Watermarking Protocols with Off-line Trusted Parties[C]// International Conference on Multimedia and Ubiquitous Engineering MUE '07. 2007, 4:1035-1040

[11] Sander, Tschudin. On software protection via function hiding[C]// LNCS. 1525. 1998:111-123

[12] II PAILIER P. Public-key eryptosystems based composite degree residuosity classed[C]// Euricrypt'99. 1592:223-238