基于移动设备的匿名可追踪版权保护协议

姜 堃 王晓明
(暨南大学信息科学技术学院计算机科学系 广州 510000)

摘 要 提出了基于移动设备的匿名可追踪的版权管理协议。首先,它使用不断变换的临时身份来代替用户的真实身份,使其他人不可能跟踪到用户,它关注用户动态,具有匿名性;其次,使用一次口令申请一个水印的方法来抵抗假冒攻击;再次,采用单向哈希函数的认证方法对用户身份、数字内容进行验证;协议中的一些计算由可信中心完成,以减少移动用户的计算量,提高效率。另外在数字产品中嵌入版权水印和指纹水印,当发现非法副本时,它可以对叛逆者进行追踪,具有可追踪性。分析表明,该协议是安全有效的。

关键词 版权水印,指纹水印,叛逆者追踪,版权保护
中图法分类号 TP309.2 **文献标识码** A

Anonymous and Traceable Copyright Protection Protocol Based on Mobile Devices

JIANG Kun WANG Xiao-ming
(Department of Computer Science, College of Information Science and Technology, Jinan University, Guangzhou 510000, China)

Abstract Anonymous and traceable copyright protection protocol based on mobile devices was put forward in this paper. Firstly, others can not track the user by using the changing identity to replace user's true identity in the protocol. The anonymous nature exists in the protocol. Secondly, the protocol uses the method that one password only applies one fingerprint watermark so that the protocol resists the fake attack. Thirdly, while using one-way hash function to verify the identity of participators and the digital content, the protocol transfers the calculating works to the trusted center RA with enough computing ability from mobile users. The two behaviors reduce the mobile's calculating works, and improve efficiency. In addition, the copyright watermark and fingerprint watermark embedded in the digital product are used to trace the traitor when finding one or more illegal copies of the digital product. So the protocol has the ability of traitor tracing. The analysis indicates that the protocol is secure and practical.

Keywords Copyright watermark, Fingerprint watermark, Traitor tracing, Copyright protection

1 引言

随着计算机技术的快速发展,数字产品在网络中的传播越来越多,数字版权的保护成为人们关注的焦点。数字版权保护是采取信息安全技术手段,在保证具有使用权限的合法用可以正常使用数字产品的同时,保护数字产品创作者或拥有者的版权,根据版权产品获得合法收益,在版权受到侵害时能够鉴别数字产品的版权归属及版权信息的真伪,以及追踪到版权侵害人,对其进责任追究。文献[1]给出了数字版权管理系统安全性评价指标。根据现实需求,一个安全的数字版权管理系统要达到以下基本要求:

(1)安全性:安全性是数字版权管理的基本要求;

(2)匿名性:为了保护用户的隐私,将用户的真实身份隐藏起来;

(3)完整性:要保证用户得到的数字产品的完整性与正确性;

(4)认证性:确保攻击者不可能冒充用户、版权所有者及参与版权管理的其他方中的任意一方;

(5)不可否认性:用户不可否认购买过数字产品,版权所有者也不可否认出售过数字产品;

(6)可追踪性:若发现非法副本,则能够追踪到叛逆用户,并提取出不可否认的证据,追究其责任。

在学术界,很多文献提出了不同的版权管理方案。文献[5]提出了一个应用于企业的E-DRM,从而保证了安全性、完整性、认证性。文献[6]提出了一个轻量级、可匿名版权保护协议,协议嵌入水印的过程简单,计算量小,提出了有效的追踪方案。文献[2-4]将同态加密技术嵌入水印,使数字签名技术及数字证书实现了数字版权管理。在移动设备领域,许多公司组织提出了DRM标准,如苹果公司推出了在其音乐下载平台中使用的DRM私有Apple iTunes DRM;微软公司推出了Windows Media DRM;Open Mobile Alliance(OMA)在2002年先后发布了OMA数字版权保护1.0和2.0标准草案。

到稿日期:2011-10-31 返修日期:2011-12-15 本文受国家自然科学基金(61070164),广东省自然科学基金(8151063201000022),广东省科技计划项目(2010B010600025)资助。

姜 堃(1988—),女,硕士,主要研究方向为信息安全,E-mail:jk_jiangkun@126.com;王晓明(1960—),女,博士,教授,主要研究方向为密码学、信息安全。

OMA 数字版权保护 1.0 标准草案，在其禁止转发和组合发送模型中，数字内容以原始内容传输，攻击者可以截获禁止转发和组合发送包，并从中解析出原始数字内容；在其分别发送模型中，数字内容被加密，但是解密密钥以明文的形式存放，若版权对象离开终端，非法用户有可能获得解密密钥，从而获得原始内容，这两种情况中，数字内容很容易被盗版。在 2.0 标准草案中，引入了 PKI 机制，需要建设 CA、证书的管理和发放等，部署和实施的难度较大；而且终端的数字签名对手机的运算能力要求高，硬件和软件资源占用非常大，耗电量也大，普通的 3G 终端难以实现；文献[2-4]提出的方案在隐藏用户身份的同时，需要的存储空间小，但这些方案均涉及了数字签名、数字证书，需要终端有较强的计算能力；文献[5]提出的 E-DRM 没有考虑到用户的隐私问题，及获得数字产品后的盗版追踪问题；文献[6]在计算量和追踪方面都提出了合理的方案，但其需要很大的存储空间；文献[7]中介绍了一种使用临时身份隐藏真实身份的方法，但临时身份的固定性容易受到攻击者的跟踪。

针对以上问题，本文提出了一个基于移动设备的匿名可追踪的版权管理方案。与目前提出的数字版权管理方案相比，本方案具有以下优点：

(1)为了更好地保护用户的隐私，本方案采取了不断变换的临时身份来代替用户的真实身份，使得其他人不可能跟踪用户、关注用户的动态。

(2)使用一次口令申请一个水印的方法，更有效地保证了用户的不可仿冒性。

(3)认证过程通常会采用计算量较大的数字签名技术，本方案考虑了计算量和高效率问题，采用了单向哈希函数的方法对身份等进行验证，减少了计算量，提高了效率。

(4)用户向版权所有者提供的水印有效性的验证，是由可信中心计算的，这样将用户的计算量转嫁给了计算能力强的可信中心。

(5)在数字产品中嵌入了版权水印和指纹水印[8-10]，当发现法副本时，可以有效追踪到叛逆者。

2 数字版权保护协议

针对现有数字版权管理方案中存在的身份隐藏、计算量、存储空间等问题，本文提出了基于移动设备的匿名可追踪的版权管理协议。该协议由买方(B)、卖方(S)、可信中心(RA)、仲裁机构四方组成。其中卖方为数字版权的所有方，买方为想得到数字产品的合法用户，可信中心是买方和卖方要进行注册的机构，是可信的第三方，同时负责买方指纹水印的生成，向买方提供指纹水印，并协助买方和卖方之间进行交易。本协议使用了防篡改机 TRM，买方和卖方注册之后会得到各自的防篡改机 TRM_B 和 TRM_S，防篡改机内部嵌入了一个单向哈希函数 $H()$、用户的密钥对，买方和卖方交易过程由防篡改机完成，最终的数字内容也是在防篡改机中解密后输出。本协议中随机数的长度均设为 n，n 为所使用单向哈希函数输出序列的长度。若买方私钥丢失，要求买方及时发布密钥丢失时间。

具体协议分为 4 个部分：(1)注册阶段；(2)水印申请阶段；(3)交易阶段；(4)叛逆者追踪阶段，下面是对各个阶段的详细介绍。

2.1 相关名词及参数的介绍

N_i：它在第 $i-1$ 次水印申请过程中由 RA 产生，发送给买方的随机数，用于第 i 次水印申请过程中一次性口令的产生、参数的传递、认证等；

ID_{B_i}：买方 B 第 i 次申请水印时的临时身份，与 $IMEI_B$ 有关；

w_i：只属于买方的指纹水印，i 表示第几次申请的水印。

2.2 协议具体设计

2.2.1 注册阶段

在数字产品交易之前，买卖双方均要在可信中心 RA 注册。

(1)买方注册

①买方(B)填写注册信息，下载插件 TRM_B；

②TRM_B 提取出 B 的国际移动设备身份码 $IMEI_B$，使用 RA 的公钥加密后，发送给 RA；

③RA 收到后，产生一个随机数 N_1，计算：

$$ID_{B_1}=H(IMEI_B)\oplus N_1 \tag{1}$$

$$V_{N_1}=H(IMEI_B \| N_1) \tag{2}$$

将 N_1，$IMEI_B$，ID_{B_1} 保存到买方数据表中，将 ID_{B_1} 和 V_{N_1} 发送给 B；

④B 收到 RA 发送的消息后，TRM_B 根据 $IMEI_B$ 提取出 N_1，并验证 N_1 是否被篡改，验证成功则将 N_1，ID_{B_1} 保存到数据表中，用于第一次申请水印；否则重新注册。

(2)卖方注册

①卖方(S)填写注册信息，下载插件 TRM_S；

②TRM_S 提取出 S 的国际移动设备身份码 $IMEI_S$，并安全发送给 RA；

③RA 产生一个随机数 R_S，计算

$$R_{R_S}=H(IMEI_B)\oplus R_S \tag{3}$$

$$V_{R_S}=H(IMEI_S)\oplus R_S \tag{4}$$

其中 $ID_S=H(IMEI)$，将 R_{R_S} 和 V_{R_S} 发送给 S；

④S 收到后，TRM_S 提取出 R_S，并验证接收到的内容是否被篡改，若验证成功，则存储 ID_S 和 R_S，否则，重新注册。

2.2.2 水印申请阶段

在水印申请阶段使用 RSA 公钥加密算法，利用买方的公钥对指纹水印加密，在传输过程中，传输的是加密后的水印，而不是水印的原始内容。

B 要向卖方 S 购买一件数字产品前，先向 RA 申请一个仅属于自己的水印，称为指纹水印。在该阶段中一次口令只能申请一个水印。

(1)TRM_B 计算本次水印申请使用的口令：

$$P_i=H(N_i \| ID_{B_i}) \tag{5}$$

将 (i, ID_{B_i}, P_i, ID_S) 发送给 RA；

(2) RA 收到后，根据 ID_{B_i} 找到自己存储的 N_i，验证一次性口令 P_i，如果口令不通过，则拒绝本次指纹水印申请，否则生成本次指纹水印 w_i，并使用 B 的公钥加密得到 $E_{PK_B}(w_i)$，根据 ID_S 找到 S 对应的随机数 R_S，并产生一个随机数 R_{BS}，进一步计算：

$$N=H(N_i)\oplus N_{i+1} \tag{6}$$

$$R=H(N_i)\oplus R_{BS} \tag{7}$$

$$V_B=H(N_i \| E_{PK_B}(w_i) \| T \| N_{i+1} \| R_{BS}) \tag{8}$$

$$V_S=H(E_{PK_B}(w_i) \| T \| ID_{B_i} \| R_S) \tag{9}$$

其中，T 为本次申请的指纹水印的有效期。RA 将 $(E_{PK_B}(w_i), w_i, ID_S, R_{BS})$ 保存在买方的数据表中，并添加 N_{i+1}，$ID_{B_{i+1}}$，将 $(i, E_{PK_B}(w_i), T, N, R, V_B, V_S)$ 发送给 B；同时 RA 将 ID_{B_i}，$H(R_S)\oplus R_{BS}$ 和 $H(R_S \| R_{BS})$ 发送给 S；

(3) B 收到后，TRM_B 提取出 R_{B-S} 和 N_{i+1}，验证 V_i 和 V_B，若验证失败，则不采用本次指纹水印，请求水印中心重新发送水印，如果 B 请求重发水印的次数超过 3 次，RA 停止为 B 提供水印，将 $H(IMEI_B)$ 公布出来，并删除关于 B 的记录。B 需要重新注册。若采纳本次指纹水印，返回 $H(N_{i+1} \| ID_{B_{i+1}})$，$ID_{B_{i+1}}$ 更新数据表；

(4) RA 若收到重发信息，则重新发送本次申请的指纹水印，若收到 $H(N_{i+1} \| ID_{B_{i+1}})$，$ID_{B_{i+1}}$ 验证返回来的数据，验证通过则更新数据表。若 RA 没有收到返回信息或验证不通过，则要求 B 重新发送返回信息。如果 3 次要求 B 重新发送返回信息、没有收到回复或验证仍旧不通过，RA 停止为 B 提供水印，将其公布出来，并删除关于 B 的记录，需要重新注册；

(5) S 收到后提取出 R_{BS}，并验证，若验证失败，则请求 RA 重新发送；否则保存 ID_{B_i} 和 R_{BS}。

2.2.3 交易阶段

本阶段借鉴了文献[2-4]中使用的版权水印和指纹水印的嵌入方法，本协议中利用 RSA 所具有的乘同态性质在数字中嵌入指纹水印。

(1) 假设 B 要购买数字产品 X，先写订单 L_X，订单中涉及了数字产品 X 的相关信息，以及 B 和 S 的权利和义务。TRM_B 将 $(ID_{B_i}, L_X, E_{PK_B}(w_i), T, V_s, H(IDB_i \| R_{BS}))$ 发送给 S；

(2) S 收到后，TRM_S 根据发送来的消息和存储的信息验证 V_S 和 $H(ID_{B_i} \| R_{BS})$，若验证失败，则终止本次交易，若成立，TRM_S 将以上信息保存起来，执行以下操作：

①生成只与本次交易有关的版权水印 w_X，将其嵌入到数字产品 X 中：$X\otimes w_X$，其中，$\otimes$ 为水印嵌入算法；用 B 的公钥加密得到：$E_{PK_B}(X\otimes w_X)$；

②使用随机变换函数 $\alpha()$ 对 B 发送的 $E_{PK_B}(w_i)$ 进行变换：

$$\alpha(E_{PK_B}(w_i))=E_{PK_B}(\alpha(w_i)) \tag{10}$$

③使用同态加密技术计算：

$$\begin{aligned} C&=E_{PK}(X\otimes w_X)\otimes E_{PK}(\alpha(w_i)) \\ &=E_{PK_B}(X\otimes w_X\otimes\alpha(w_i)) \end{aligned} \tag{11}$$

④将 $(C, H(C \| R_{BS}))$ 发送给 B；

(3) B 收到后，TRM_B 验证 $H(C \| R_{BS})$，若不通过，交易终止，若通过，则使用 B 的私钥解密，得到 $\overline{X}=X\otimes w_X\otimes\alpha(w_i)$。

2.2.4 叛逆者追踪阶段

如果卖方 S 在网络等公共场所发现数字产品的副本 Y，S 使用水印提取技术提取出版权水印 $\overline{w}_X$，与销售记录中的所有版权水印进行匹配，找超过门限值且匹配系数最高的 w_X，该版权水印找到买方发送来的信息，连同数字产品 X、版权水印和随机变换函数一起发给仲裁机构，请求仲裁机构仲裁。仲裁机构将根据这些信息，使用水印嵌入方法进行验证，若不通过，则驳回仲裁请求，若通过，则进一步要求 RA 给出 B 的真实身份 IMEI，对 B 进行控诉。

3 安全及功能分析

3.1 功能分析

本文中使用的认证方法的思想为：

假设用户 P 想要用户 Q 传送秘密 M（本文中 M 的长度设为 m 摘要的长度），用户 P 计算：

$$C=H(m)\oplus M$$

$$V=H(m \| M)$$

式中，m 是认证双方都已知的秘密参数，M 是用户 P 要传递给用户 Q 的内容。C 和 V 直接在信道中传递；Q 收到后，根据自己存储的 m，提取出 M，进行验证。

若使用数字签名的方法来实现，用户 P 计算：

$$h=H(M)$$

$$S=Sig_{SK_P}(h)$$

$$C=E_{PK_Q}(M)$$

式中，Sig_{SK_P} 表示使用 P 的私钥签名，E_{PK_Q} 表示用 Q 的公钥加密，P 将 S 和 C 发送给 Q，Q 收到后用自己的私钥解密得到 M，对 M 进行一次哈希，用 P 的公钥对数字签名解密，比较两个哈希值。完成一次单向认证后进行统计及比较，见表 1。

表 1 计算统计及比较

方法	计算			
	哈希(次)	异或(次)	加密/解密(次)	比较(次)
哈希认证	4	2	0	1
签名认证	2	0	4	1

考虑到 Q 方的认证过程与 P 方的计算过程基本相似，采用 MD5 算法计算摘要，RSA 算法计算签名及加密，实验得到哈希认证中 P 方的计算时间约为 10ms，而签名认证中 P 方的计算时间为 70ms，由此证明哈希认证的计算要小于签名认证的计算。

在存储方面，哈希认证双方只需存储秘密参数 m，而签名认证双方要存储自己的密钥对，及对方的公钥。对于多用户参与而言，明显哈希认证的存储量要少得多。

3.2 性能及安全分析

3.2.1 抵抗假冒攻击

没有攻击者可以假冒可信中心：注册过程中，注册用户（买方和卖方）时使用可信中心的公钥将身份传输给可信中心，只有可信中心能解密得到用户的真实身份，对于买方，可信中心计算了 $ID_{B_1}=H(IMEI_B)\oplus N_1$，并将 N_1 和 ID_{B_1} 安全发送给用户，除了合法用户外没有人能得到 N_1 和 ID_{B_1}，根据哈希函数的单向性，用户可以有效验证该信息是否是可信中心给出的，以及 N_1 是否被篡改。在水印申请阶段中，买方根据可信中心发送来的信息，以及自己存储的信息验证 $H(N_i \| E_{PK_B}(w_i) \| T \| N_{i+1} \| R_{BS}) \stackrel{?}{=} V_B$，即可验证可信中心的身份。卖方根据注册阶段存储的 R_S，提取出 R_{BS}，计算 $H(R_S \|$

R_{BS})是否与可信中心发送的相等，即可验证信息是否为可信中心发送来的，是否被篡改。

没有人可以假冒买方：水印申请阶段，买方计算本次水印申请使用的口令 $P_i=H(N_i \| ID_{B_i})$，其中的 N_i 为秘密随机数，水印中心可以验证一次性口令来对买方进行认证。交易阶段，买方计算 $H(ID_{B_i} \| R_{BS})$，其中 R_{BS} 为秘密随机数，发送给卖方，卖方通过自己存储的 R_{BS}，计算 $H(ID_{B_i} \| R_{BS})$ 是否与发送来的一致，以对买方进行认证。

没有人可以冒充卖方：交易阶段中，卖方将 $(C, H(C \| R_{BS}))$ 发送给买方，买方根据自己存储的 R_{BS}，即可对卖方进行认证。

3.2.2 匿名性

在注册阶段，水印中心利用买方的真实身份和随机数 N_1，计算买方的匿名身份，买方在第一次申请水印时使用该身份，第一次申请水印的过程中，水印中心在返回水印的同时，也安全返回了随机数 N_2，用于买方计算第二次申请水印时的临时身份，这样每次买方的临时身份都会不一样，不会被恶意跟踪者追踪。

3.2.3 抵抗伪造攻击

交易阶段卖方将 $(C, H(C \| R_{BS}))$ 发送给买方，买方根据自己存储的 R_{BS}，既可以对卖方的身份进行认证，在认证的同时也验证了数字产品的正确性与完整性。

3.2.4 不可诬告性

协议采用了同态加密技术，买方的指纹水印是使用其公钥加密的，只有买方自己能得到水印，卖方不知道买方的具体水印，交易过程中填写了订单，卖方不可能将买方的水印应用到其他的数字产品中，恶意诬告买方。

3.2.5 不可否认性

在数字产品中，嵌入了变换后买方的指纹水印，买方得到数字产品后不可能从中提取出自己的指纹水印，若发现非法副本，其中必定含有买方的指纹水印，买方无法否认。

3.2.6 可追踪性

在数字产品中，嵌入了唯一的只与本次交易相关的版权水印，如果恶意买方非法得到数字产品，或将其公开发布出来，卖方发现非法副本后，能过通过版权水印找到叛逆者，再根据数字产品中的指纹水印确定以上信息后，将自己存储的信息提交给仲裁机构进行仲裁，并要求 CA 给出恶意买方的真实身份，对其进行起诉。

结束语 本文提出了一种基于移动设备的匿名的、可追踪版权保护协议，它借鉴了已有方案中的同态加密技术嵌入指纹水印和版权水印，做到了可追踪性。该协议在保证数字版权管理系统的基本要求的同时，进一步解决了用户的身份隐藏问题，设计了计算量小的高效认证方案，亦即将一些计算量大的计算从移动用户转嫁给了计算能力较强的可信中心，适应了移动设备计算能力和存储能力相对较弱的特点。

参 考 文 献

[1] 李润峰，马兆丰，杨义先，等. 数字版权管理安全性评测模型研究[J]. 计算机科学，2011，38(3)：24-27

[2] Fan Chu-ni, Chen Ming-te, Sun Wei-zhe. Buyer-seller watermarking protocols with off-line trusted parties[C]// MUE'07. International Conference on Multimedia and Ubiquitous Engineering. Secul: Kaoksiurg, 2007(4): 1035-1040

[3] Phan R C-W, Goi B-M, Poh G-S, et al. Analysis of a Buyer-Seller Watermarking Protocol for Trustworthy Purchasing of Digital Contents [J]. Wireless Pers Commun, 2011, 56: 73-83

[4] 胡玉平，张军. 用于盗版追踪的数字水印协议的研究[J]. 计算机科学，2010，37(1)：91-94

[5] Chen Chin-ling. A secure and traceable E-DRM system based on mobile device[J]. Expert Systems with Applications, 2008, 35: 878-886

[6] Chen T-h, Horng G. A lightweight and anonymous copyright-protection protocol[J]. Computer Standards & Interfaces, 2007, 29: 229-237

[7] Li M-J, Juan J S-T, Tsai J H-C. Practical electronic auction scheme with strong anonymity and bidding privacy[J]. Information Sciences, 2011, 181(12): 2550-2570

[8] Zhao Xing-wen, Zhang Fang-guo. A New Type of ID-based Encryption System and Its Application to Pay-TV Systems[J]. International Journal of Network Security, 2011, 13(3): 161-166

[9] Lin Shi-guo, Chen Xi. Secure and tracing multimedia distribution for convergent Mobile TV services [J]. Computer Communications, 2010, 23(3): 1664-1673

[10] Tomas-Buliart J, Fernandez M, Soriano M. Traitor tracing over YouTuBe video service-proof of concept[J]. Telecommun Syst, 2010(45): 47-60

(上接第 48 页)

[6] Erman J, Arlitt M, Mahanti A. Traffic classification using clustering algorithms [C]// Proc of the SIGCOMM Workshop on Mining Network Data. Pisa, Italy, 2006: 281-286

[7] Erman J, Mahanti A, Arlitt M, et al. Offline/realtime traffic classification using semi supe-rvised learning[C]// 26th International Symposium on Computer Performance, Modeling, Measurements, and Evaluation. 2007, 64(9-12): 1194-1213

[8] Qian Feng, Hu Guang-min, Yao Xing-miao. Semi-supervised Internet network traffic classification using a Gaussian mixture model[J]. Electronics and Communications, 2008(62): 557-564

[9] Lin Guan-zhou, Xin Yang, et al. Network traffic classification based on semisupervised clustering [J]. China University of Posts and Telecommunications, 2010(17): 84-88

[10] Lu W, Rammidi G, Ghorbani A A. Clustering botnet communication traffic based on n-gram feature selection[J]. Computer Communications, 2010: 1-13

[11] 唐伟，周志华. 基于 Bagging 的选择性聚类集成[J]. 软件学报，2005，16(4)：496-502

[12] Strehl A, Ghosh J. Cluster Ensembles-A Knowledge Reuse Framework for Combining Multiple Partitions [J]. Machine Learning Research, 2002(3): 583-617

[13] Moore A W, Zuev D, Crogan M. Discriminators for use in flow-based classification [R]. RR-05-13. London: Queen Mary University of London, 2005

[14] Yu Lei, Liu Huan. Feature selection for high-dimensional data: A fast correlation-based filter solution[C]// Proc of the 20th International Conference on Machine Learning. 2003: 1-8