第 33 卷 第 2 期 计 算 机 工 程 2007 年 1 月
Vol.33 No.2 Computer Engineering January 2007
·安全技术· 文章编号：1000—3428(2007)02—0133—03 文献标识码：A 中图分类号：TP309

关系数据库零水印注册方案的研究

蒙应杰，吴 超，张 文，张秀娟
(兰州大学信息科学与工程学院，兰州 730000)

摘 要：对关系数据库的零水印方案的注册过程进行了研究，构造了关系数据库零水印的注册模型；依据注册模型提出了一套零水印注册机制，并描述了注册算法；最后分析了本方案的特点。

关键词：关系数据库；零水印；注册

Research on Zero-watermark Registration Schema for Relation Database

MENG Yingjie, WU Chao, ZHANG Wen, ZHANG Xiujuan
(School of Information Science & Engineering, Lanzhou Universty, Lanzhou 730000)

【Abstract】 This paper researches the registration process zero-watermark for relation database. it constructs the model of the zero-watermark registration and designs a mechanism of zero-watermark registration, then describes the algorithm in detail, at last it analyzes the character of the scheme.

【Key words】 Relation databases; Zero-watermark; Registration

数据库的数字水印技术是实现数据库的版权保护的重要方式之一，已有的几种数据库数字水印方案[3,4,8~10]都要在一定程度上修改数据库宿主信息，影响了数据库的使用价值；并且这些方案只适合于对精度要求不高、允许一定误差的数据库，算法的应用面较窄。为了解决以上问题，我们对文献[1]中关系数据库的零水印技术进行了研究，在国内首次提出了一种通过构造零水印，注册零水印的方式来实现数据库版权保护的方案。其本质是将数字水印技术中的图像零水印[11~16]思想移植到关系数据库中，但传统图像零水印技术存在以下几个缺陷：(1)缺少一个权威的零水印管理和认证机构，方案的可行性不高；(2)传统的检测方法[2]先要远程下载宿主信息，存储之后才能实行检测，这给网络和检测端提出了很高的要求，不适合于直接在数据库上实施；(3)一个普遍的缺陷是零水印信息都是由无意义的宿主信息构成，无法与用户的名称、商标相联系，同时单纯的零水印信息也无法保证其唯一性。

本文借鉴数字签名与认证技术中的权威机构CA(Certification Authority)的工作原理，引入一个权威的零水印管理机构(Zero-watermarking Manage Center, ZWMC)来克服传统图像零水印的缺陷。

1 相关定义

定义 1 ZWMC公钥，私钥。ZWMC的私钥为key_1，公钥为key_2。ZWMC主要利用key_1对零水印证书进行数字签名，key_2主要用来验证ZWMC在零水印证书上的签名。

定义 2 用户登录名和密钥。用户在注册零水印之前首先向ZWMC申请一个登录名name，登录密钥key_3。用户私钥key_4，公钥key_5。其中key_4主要用于注册时用户进行不可抵赖签名，key_5用于ZWMC核对用户的签名。申请过程用函数apply(name, key)表示，申请成功用户便可正式登录，否则申请失败。

定义 3 用户登录。用户登录ZWMC，填写用户名和口令，ZWMC核对登录信息。此过程用函数login(name, key_3)表示，登录成功，用户便可提交注册信息,否则登录失败。

定义 4 零水印的注册。当用户注册零水印时需要提交注册信息 P，P 是一种记录式结构：

$$P=(a, A, F, N, B, W, T_1, E)$$

其中，a是用户名称，A是用户地址，F是用户在工商行政部门登记注册的惟一编号，N是用户(公司)法人代表的姓名，B是N的身份证号，W是用户注册的零水印信息，T_1是注册时间，E是附加信息。为了表示方便，用P.a表示P中a。P.A，P.F，P.N，P.B，P.W，P.T_1，P.E也类似。提交水印的过程用函数refer(P)表示，提交成功返回零水印证书，否则提交失败。

定义 5 零水印证书。ZWMC 根据用户提交的注册信息 P，颁发零水印证书 C。C 是一种记录式的结构：

$$C=[P(a, A, F, N, W, T, E), T_2, S_2]$$

其中，$P(a, A, F, N, W, T_1, E)$是用户提交的注册信息，T_2是证书发放时间，S_2是ZWMC关于P与T_2的签名。用户颁发零水印证书的过程用函数award(c)表示，发放成功用户获得零水印证书，否则返回发放失败。

定义 6 证书验证。用户获得ZWMC颁发的零水印证书后，用ZWMC的公钥key_2对签名进行验证，从而确定注册是否成功。验证成功则用户注册成功，否则验证不通过。

2 零水印注册模型的构造

在零水印注册过程中，用户和 ZWMC 是注册的主体。从

基金项目：科技部基金资助项目(2001DBI10060)
作者简介：蒙应杰(1964－)，男，副教授，主研方向：数据库，信息安全；吴 超、张 文、张秀娟，硕士生
收稿日期：2006-03-28 **E-mail：**wuchao04@st.lzu.edu.cn

用户的角度来看注册过程是透明的，用户只需在客户端通过 Web 页面进行一些简单的操作，具体注册过程主要由 ZWMC 来完成。具体注册模型有 3 个层次 :用户层，客户端层，ZWMC 层。从用户通过客户端与 ZWMC 交互的过程来看可以将注册过程分为 3 大步骤：(1)用户在 ZWMC 中登录，然后 ZWMC 进行登录信息处理；(2)用户向 ZWMC 提交注册信息，接着 ZWMC 对注册信息进行处理；(3)ZWMC 发放零水印证书并且用户对其进行验证。用户的整个注册过程需要 ZWMC 提供一个应用服务器来完成，同时 ZWMC 需要使用一个数据库对所有处理的信息进行管理。基于以上分析本方案构造零水印注册模型如图 1 所示。

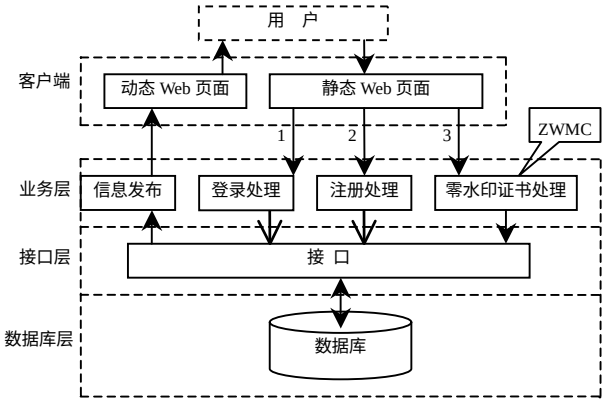

图 1 注册模型

在注册模型中，客户端的静态页面是用户与 ZWMC 的接口，动态页面用于用户与 ZWMC 进行信息交互。业务层主要有 4 大功能模块：用户登录处理模块，注册处理模块，零水印证书处理模块和信息发布模块。而所有处理信息都由底层的数据库来管理，业务层通过相关接口来访问底层数据库。

3 零水印注册设计

根据零水印注册的要求和注册模型，本方案基于 B/S 模式进行开发，设计注册系统的结构如图 2 所示。

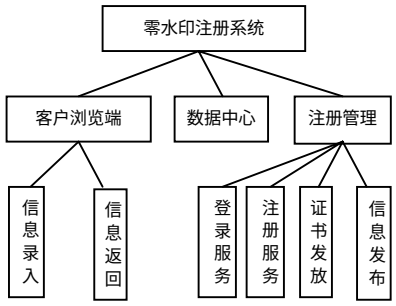

图 2 注册系统功能结构

注册管理模块是整个注册系统的核心，其功能主要有 4 个:登录服务，注册服务，证书发放和信息发布。

3.1 登录服务

登录服务主要负责用户登录名和用户密钥的申请。登录服务算法描述如下：

login{name,key_3}
输入：用户信息
输出：用户登录名和相关密钥
{apply(name,key) //用户申请登录名和相关密钥
if 申请失败 then
{用户重新申请或放弃}
else
{ 用户获得登录名name、登录口令key_3、用户公钥key_4和私钥key_5}
endif}

3.2 注册服务

注册服务主要处理用户提交的注册信息，本方案利用公钥加密和数字签名的原理相结合来实现，用户提交注册信息过程如图 3 所示。

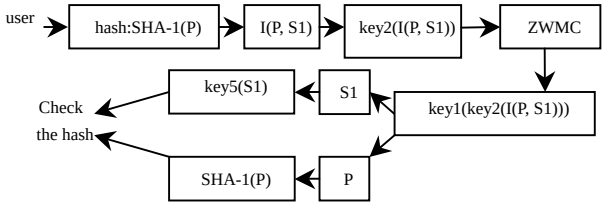

图 3 提交注册信息

根据图 3 用户提交注册服务的算法描述如下：

refer(P)//用户提交注册信息，ZWMC 核对用户签名
输入：用户注册信息
输出:：注册确认信息
{ S_1=key4(SHA-1(P))// 用户形成hash签名
$key_2(I(P, S_1))$//用户加密注册消息
$key_2(I(P, S_1))$→ZWMC//用户向zwmc提交注册信息
ZWMC 核对签名
If 签名不正确 then
{提交失败，用户再次提交或放弃}
else{
提交完成，等待 ZWMC 发放零水印证书}
Endif
}

3.3 零水印证书的发放

零水印证书发放的同时 user 要对零水印证书进行验证。零水印证书发放的关键问题是防止零水印证书被篡改和冒充。零水印证书的发放流程如图 4 所示。

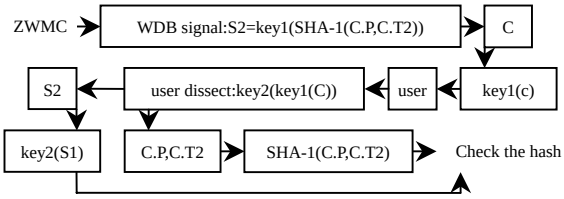

图 4 发放零水印证书

根据图 4 发放零水印证书算法过程如下：

award(C)
输入：用户加密的信息
输出：零水印证书
{ S_2=key_1(SHA-1(C.P,C.T_2))// ZWMC形成hash签名
C=[P(a，A，F，N，W，T_1，E)，T_2，S_2]
// ZWMC 形成零水印证书
key_1(c) →user//ZWMC向用户发放零水印证书
$key_2(key_1(c))$//用户解密信息
用户验证签名
if 验证通过 then
{用户获得零水印证书}
else{再次请求发放}
endif
}

3.4 信息发布

信息发布主要负责将 Web 应用服务服务器处理的结果向

用户进行反馈。

3.5 完整的注册流程描述

通过前面几个算法，一个水印的完整的注册过程可以描述如下：

```
Register(name,key3)
输入：用户登录名name和登录口令key3
输出：有效零水印证书 C
begin
{login(name,key3) //用户登录，ZWMC验证登录信息
 If 登录失败 then
  {用户重新登录或放弃}
else{
  refer(P) //用户提交注册信息，ZWMC 核对用户签名
  If 提交信息失败 then
   {用户再次提交注册信息或放弃注册}
  else{ award(c)
  If 发放失败 then
  {请求 ZWMC 再次发放零水印证书或放弃}
  else
  {注册成功，用户获得有效零水印证书}
  endif
  }endif
}endif
end
```

4 零水印注册方案分析

4.1 可行性

目前大多数数字水印不能具有法定的权威性，无法得到大规模的商业推广应用。数字水印技术的应用急需一套权威的检测机制，基于这样的出发点引入一个可信赖的，权威机构 ZWMC 来实现水印的管理。ZWMC 的引入，不仅能解决上述问题，更重要的是它颁发的零水印证书为零水印的检测提供了可信的依据，使零水印的应用推广成为可能。

4.2 可检测性

本方案中的零水印信息以零水印证书的形式存在，为零水印的检测提供了规范的依据。传统的数据库的数字水印方案如文献[1,2,7,8]在实施检测时需要远程下载原含水印的数据库信息，这对网络和本地检测提出了很高的要求，实施困难，而且没有统一的规范，可信性不高。采用本方案后，检测时只需获取有效零水印证书便可知道原数据库的零水印信息，实现了盲测[17]，能够解决传统数据库检测的难题。

4.3 安全性

零水印注册的安全性体现在两个方面：(1)用户提交注册信息中的安全性；(2)ZWMC向用户颁发零水印证书的安全性。用户在提交信息的过程中采用用户的私钥key_4对用户信息签名。因为用户user与其私钥key_4存在一一对应关系，所以用户的签名是不可抵赖签名。用户签名的主要目的是防止注册信息在传输过程中被篡改。另外用户还要用ZWMC的公钥key_2对注册信息$I(P,S_1)$进行加密，加密后的信息$key_2(I(P,S_1))$只有ZWMC用它的私钥key_1才能解密。在ZWMC向用户发放零水印证书的过程中ZWMC首先用它的私钥key_1对用户注册信息形成签名，然后采用用户公钥key_5加密零水印证书。用户只有用其私钥key_4才能解密ZWMC加密的零水印证书信息，同时ZWMC的签名很好地保证了零水印证书的完整性。

4.4 相关性

本方案中零水印相关性体现在两个方面：(1)由定义 4 可知零水印信息$P.W_1$与用户信息(P.a，P.A，P.F，P.N，P.T)相绑定，采用不可抵赖签名进行注册，解决了传统单纯零水印方案如文献[10~13]无实际意义的缺陷；(2)用户信息(P.a，P.A，P.F，P.N，P.T)的唯一性也决定了定义 5 中零水印证书C=[P(a，A，F，N，W，T，E)，S]的唯一性，很好地保证了注册零水印信息的相互独立性。

4.5 本方案的特点

基于上述分析，本方案与以往零水印方案相比主要具有以下几个特点：

(1)零水印可信度高。引入了一个水印管理机构 ZWMC，使零水印能够得到权威的认证。

(2)注册的零水印具有实际意义和唯一性。注册的零水印信息含有用户信息，克服传统图像零水印无实际意义的缺陷；用户信息的唯一性也决定了零水印的唯一性。

(3)可验证性强。零水印证书为零水印信息的确认提供了可认证的依据；也为水印的管理和维护提供了方便，更重要的是使检测脱离原载体，可实现盲测。

(4)安全性高。在零水印信息的提交和零水印证书的发放过程中将密码学与数字签名的原理相结合来保证注册过程的安全性。

5 结束语

本文对关系数据库零水印注册方案作了进一步的研究，将用户信息与构造的零水印信息绑定后在 ZWMC 中注册，同时零水印信息以零水印证书的形式存在，既保证了零水印的唯一性，又解决了传统零水印无意义的缺陷问题。另外检测时只需获取有效零水印证书即可，使检测过程与原数据库相脱离，解决了传统数据库数字水印检测的难题。另外本方案不仅适合于数据库零水印方案，也为在其他载体(图像、文本、音频等)上进行的构造式和注册型的数字水印技术的注册过程提供了借鉴。

参考文献

1 蒙应杰, 吴　超, 苏仕平, 等. 一种关系数据库零水印方案的探讨[C]. 国家科技部西南信息中心. 第 22 届中国数据库学术会议论文集. 2005: 381-383.

2 燕　晓, 蒙应杰, 王　阳, 等. 一种强干扰背景下的盲加性水印[J]. 软件学报, 2005, 16(9): 1678-1684.

3 Agraw R, Kieman J. Watermarking Relation Database[C]. Proceedings of the 28th Conference on VLDB, Hong Kong, China, 2002: 155-166.

4 Sion R. Watermarking Relation Databases[R]. ERIAS Technical Report, 2002.

5 Fabien K S, Petitolas A P. Information Hiding Techniques for Steganographyand Digital Watermarking[M]. Boston, London: Artech House, 1999.

6 Cox J, Thomson K J. Secure Spread Spectrum Watermarking for Multimedia[J]. IEEE Transaction on Image Processing, 1997, 6(12): 1673-1687.

7 Adelsbach A, Beisser S K. Watermark Detection with Zero-knowledge Disclosure[J]. Multimedia System, 2003, 9(3): 266-278.

8 张　勇, 赵东宁, 李德毅. 关系数据库的数字水印技术[J]. 计算机工程与应用, 2003, 39(25): 193-195.

9 赵　勇, 赵东宁, 李德毅. 水印关系数据库[J]. 解放军理工大学学报, 2003, 4(5): 1-4.

10 牛夏牧, 赵　亮, 黄文军, 等. 利用数字水印技术实现数据库的版权保护[J]. 电子学报, 2003, 12(A): 2050-2053.

11 杨树国, 李春霞, 孙　尧, 等. 基于小波变换的零水印方案[J]. 计算机工程与应用, 2003, 39(29): 128-130.

(下转第 138 页)