doi:10.3969/j.issn.1671-637X.2013.06.021

运用密钥分存技术的数据库水印算法

白香芳[1,2]， 赵冬玲[1]， 谢昭莉[2]， 张小娜[1]
（1.济源职业技术学院信息工程系，河南 济源 459000； 2.重庆大学自动化学院，重庆 400030）

摘 要：针对数据库联合拥有者对数据库拥有权限的管理和数据库修改后的安全问题，提出一个基于密钥分存技术的数据库水印算法。该算法描述了关系数据库利用密钥分存技术将水印嵌入到数据库中，利用Lagrange插值公式，对数据库水印进行n次插值，实现数据库水印的嵌入与恢复，数据库拥有者共同负责数据库的安全性。数据的模拟仿真实验表明，该算法减少了数据库的冗余，增强了数据库水印的保密安全性，特别对数据库中部分数据受到删除攻击后水印的检测具有一定的强壮性。

关键词：密钥；数据库；数字水印；分存技术
中图分类号：V271.4；TN918 **文献标志码**：A **文章编号**：1671-637X(2013)06-0093-03

A Database Watermarking Algorithm Using Secret Sharing Technology

BAI Xiangfang[1,2], ZHAO Dongling[1], XIE Zhaoli[2], ZHANG Xiaona[1]
(1. Department of Information Engineering, Jiyuan College of Vocational Technology, Jiyuan 459000, China;
2. School of Automation, Chongqing University, Chongqing 400030, China)

Abstract: Considering the security issues in database joint owners' authority management and in modification of database, we put forward a database watermarking algorithm based on secret sharing technology. In the algorithm, the relational databases used secret sharing technology to embed the watermark in the database, and n times of interpolation were implemented to the database watermarking using Lagrange interpolation formula, thus to realize database watermark embedding and recovery, and the database owner could be jointly responsible for the security of the database and robustness. Simulation experiments showed that the proposed algorithm can reduce the redundancy of database, enhance security safety of database watermark, and has certain robustness to watermark detection when some of the data in the database are deleted.

Key words: secret key; database; digital water marking; sharing technology

0 引言

随着计算机网络技术的高速发展，安全问题显得越来越重要，关于安全问题的加密算法也有了广泛的研究，文献[1]利用混沌的特性，加强语音传输盗版追踪的安全性；文献[2]运用小波变换技术混沌加密数字图像，实现了图像变换版权认证的安全性；文献[3]将异结构时滞不确定混沌系统的控制应用于通信保密中。

目前，国防中经常使用大型信息系统数据库，许多系统要求运用大型数据库联合作业，合作化程度较高。为保证国防数据库中数据的安全性，应该在数据库中嵌入密钥算法。文献[4]提出基于二维空间元素匹配的关系数据库水印算法，解决了单机版数据库水印信息隐蔽性差的问题。对于现代化国防，如何解决联合数据库中数据的安全问题和联合版权问题具有一定的实际意义。本文通过密钥分存技术设置数据库水印算法，能很好地解决数据库联合版权问题，增强数据库的保密安全性。

收稿日期：2013-03-13 **修回日期**：2013-04-06
基金项目：2012年河南省科技厅科技攻关项目(122102210471)
作者简介：白香芳(1974—)，女，河南宜阳人，硕士生，讲师，研究方向为计算机应用、计算机自动控制等。

1 基于密钥分存技术的数据库水印设计方案

1.1 问题描述

运用密钥分存技术控制数据库联合版权方案采用Shamir密钥分存的新型数据库水印算法[5]。假设数据

库拥有者每人分配不同的私有密钥,如果要打开数据库,就必须凑齐所有人的私有密钥(或算法规定的部分密钥),证明对该数据库的管理权,通过对比密钥的正确性保证数据库的安全性。

在数据库水印方案体系中,最容易出现的问题就是由于元组删除数据攻击导致数据库水印丢失,解决水印丢失问题最常用的方法是多次嵌入水印,但这种方法容易导致嵌入信息容量的增加。这就要求数据库水印设计方案权衡元组删除攻击强壮性和嵌入信息容量之间的关系。通过多次数据分析,利用分存技术存放数字水印,然后使用 Lagrange 插入公式恢复水印能够合适地处理这两者的关系。该方案就是在关系数据库中运用密钥分存技术的数据库水印设计思想。

1.2 设计方案

基于密钥分存技术的数据库水印算法是基于Langrange插值公式提出的,将数据库水印的密钥分成 n 份,分别将 n 份子水印存放到数据库的不同位置。在提取水印时,只要检测任意 $t(t<n)$ 份水印,就可以恢复原始水印。如果这 t 份子水印可靠性最高,t 足够大,则原始水印就恢复完整。水印在取出时,利用通信中纠错编码技术对原水印信息位进行纠错编码,每一位编码后的水印信息嵌入到一个元组集合中(在集合中重复嵌入)。

利用 Langrange 插值公式中的 n 次插值,在二维空间中给出 k 个点 $(x_1,y_1),\cdots,(x_k,y_k)$,这里点 x_k 互不相同。对于所有的 k 有且仅有一个 $k-1$ 次多项式 $p(x)$ 使得 $p(x_k)=y_k$。

Langrange 插值公式是经过 n 个点的 $n-1$ 次多项式,$y_1=f(x_1),y_2=f(x_2),\cdots,y_n=f(x_n)$,即

$$P(x)=\sum_{i=1}^{n}p_i(x) \tag{1}$$

式中:

$$P_i(x)=y_i\prod_{k=1}^{n}\frac{x-x_k}{x_j-x_k}。 \tag{2}$$

1.3 Shamir 密钥分存机制

基于 Langrange 插值公式的密钥分存思想是由 Shamir 提出的。该思想是把数字水印当作密钥,分存为 n 份。在提取水印时,只要获得其中 $t(t<n)$ 份就可以恢复出水印信息,这种方法被称为 (t,n) 门限算法[6],通过这种方法提取的水印有一定程度的失真。

为了减少门限算法的失真,可以在算法中添加动态门限。假设 s 是一个自然数,从有限域 $G(s)$ 中任意取出 n 个不等的非零元素 x_i(其中,$1\leqslant i\leqslant n$),为了具有普遍性,设阈值为 t,密钥 $K^*\in G(s)$,然后将这 n 个元素分发 n 个数据库联合拥有者,从 $G(s)$ 中选择 $t-1$ 个元素 $a_1,\cdots,a_{t-1}$ 构造一个多项式

$$f(x)=K^*+a_1x+a_2x+\cdots+a_{t-1}x^{t-1} \tag{3}$$

式中,K^* 为一个私有密钥。

选取 $x_i\in G(q),i=1,2,\cdots,n$,计算 $K_i=f(x^i)(i=1,2,\cdots,n)$,称 (x_i,k_i) 为子密钥,将 (x_i,k_i) 分别分发给联合拥有者 A_i。

设有 t 个拥有者,每个所有者分别提供出自己的序号和子密钥,利用 Langrange 插值公式

$$S^*(x)=\sum_{j=i=1}^{t}k_j\prod_{i\neq j}\frac{x-x^i}{x^j-x^i} \tag{4}$$

得到一个 $t-1$ 次多项式

$$S^*(x_j)=K_j,\quad j=1,2,\cdots,t \tag{5}$$

显然有

$$S^*(x)=f(x) \tag{6}$$

则私有密钥 K^* 为

$$K^*=f(0)=S^*(0) \tag{7}$$

如果少于 t 份子密钥,则根本无法得出私有密钥 K^*。

提取密钥 K^* 后用偶校验编码对 X_i 进行对应的二进制编码,嵌入数次。恢复原始水印时,只需要提取部分水印就可以达到目的,不需要将所有嵌入的水印提取出来,减少了数据的冗余度[7]。

2 数据库水印的嵌入与提取算法

2.1 水印嵌入算法

首先预处理水印信息 W,定义恢复原始水印的最小份数的阈值为 t,为了嵌入水印信息 W,计算 $t-1$ 次多项式 $F(x)=W+d_1x+d_2x^2+\cdots+d_{t-1}x^{t-1}$,式中 $d_1,d_2,\cdots,d_{t-1}$ 为相应的系数。由于多项式 $F(x)$ 可由 t 个不同的数唯一确定,因此,选择 n 个不同的值 $x_1,x_2,\cdots,x_n$ 计算出相应的 $F(x_1),\cdots,F(x_n)$。将 $F(x_1),\cdots,F(x_n)$ 记成 $W_1,\cdots,W_n$。通过 t 及 $(x_t,F(x_t))$ 得出 $F(x)$;再使用公有密钥 $P_1,\cdots,P_n$ 分别对 $F(x_1),\cdots,F(x_n)$ 进行编码得出 $C_1,\cdots,C_n$;然后将一个关系数据库分解成相应的 n 块 $R_1,\cdots,R_n$,并将 $W_1,\cdots,W_n$ 分别嵌入到子数据库 $R_1,\cdots,R_n$ 中,就可以得到相应的含子水印的数据库 $R_1^w,\cdots,R_n^w$。

原始水印信息 W 是由 $R_1^w,\cdots,R_n^w$ 合在一起恢复出来的。将 $(X_1,R_1^w),\cdots,(X_n,R_n^w)$ 分别分发给数据库的联合拥有者 $P_1,\cdots,P_n$,从含有子水印的数据库中挑选出 t 份子水印,用来恢复出原始水印 W,即使部分数据库数据被删除,同样也可以恢复出原始水印来,证明了该方案的抗删除攻击的强壮性[8]。

2.2 水印提取算法

水印提取算法就是将数据库联合拥有者 $(P_1,\cdots,$

P_n)各自拥有的子密钥合并起来,恢复出原始水印信息。因为需要至少 t 份(门限值)子水印才能够让原始水印信息完整地恢复出来,所以如果 $s \geq t$,则算法进入下一步,否则水印提取算法立刻停止,验证者首先确定对应的水印数据库是否受到恶意攻击,从而验证拥有者的密钥真实性[5]。如果子密钥匹配,每一个拥有者用一位水印提取算法和多数判决技术分别恢复出子水印 $W_{i_j}(i_j = i_1, \cdots, i_p)$;然后再用各自的私有子密钥凑在一起恢复出 $F(X_{i_j})$[9];运用 Lagrange 插值公式从 $F(X_{i_j})(1 \leqslant j \leqslant p)$ 的 t 个值中提取出水印信息 W,将 x 值置为 0,计算 $F(0)$,得出水印信息 W,如果子密钥不匹配,则停止水印提取算法。

3　仿真实验

3.1　数据参数设置

在嵌入水印信息以前,先进行数据预处理。利用 $t-1$ 次多项式将水印信息转换为 $W = 2^a + b(a, b \in \mathbf{R}^+)$ 形式,通过改变参数 a 和 b,实现 $t-1$ 次多项式 $F(x)$ 输入值的确定。在仿真实验中,令 $b = 0$,则水印信息就转变成 $W = 2^a$ 的格式。例如 2^{50},当 $a = 50, b = 0$,其他参数分别取不同的值,所得到的水印信息多项式的参数见表 1。

表 1　多项式的参数结果

Table 1　The parameters of polynomial result

参数	值	参数	值
d_1	1	x_1	2
d_2	3	x_2	5
k	3	x_3	7
n	5	x_4	9
a	50	x_5	11
b	不使用		

扩大水印的嵌入容量是将水印信息进行多次嵌入(本次实验中嵌入了 5 次),即对水印信息进行预处理是通过花费更多的时间为代价来增强数字水印的强壮性,因为多次嵌入信息可以最大程度地避免删除元组造成数字水印丢失的现象。通过设置合理的 $t-1$ 次多项式参数,减少重复嵌入数字水印信息而花费的时间,恢复出水印信息 W,并且增加数字水印的强壮性。

3.2　密钥分存设置

表 1 中的参数是随机选取的,根据多项式得出 $F(x) = D + d_1 + d_2 x, d_1 = 1, d_2 = 3$,则针对这个参数得到的多项式为 $F(x) = D + 1 + 3x$。由于需要将密钥分割成 5 份,因此需要计算 5 次 $F(x)$ 才能将其值分别传给数据库,这些值分别来自于 x_1, x_2, x_3, x_4, x_5 的值,均由用户自己来决定,和 $F(x_1), \cdots, F(x_5)$ 一起通过算法嵌入到数据库中。在确定多项式的输出结果后,将多项式的 (t, n) 门限值设为 $(3, 5)$,将数字水印信息的密钥分存为 5 份,由 $t-1$ 次多项式可以知道,如果想得到完整的水印信息 W,至少需要 3 份子水印。

3.3　实验结果分析

实验中将数据库分成了 $n = 5$ 个子数据,恢复原始数字水印的门限值为 3。根据实验结果绘制元组删除攻击后水印检测结果分析图表,如图 1 所示。

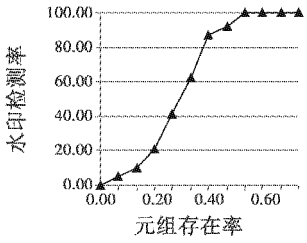

图 1　元组删除后水印检测的结果分析

Fig. 1　Watermark detecting result after deleting some tuples

通过分析图 1 可以得出以下结论:

1) 即使删除数据库中 40% 的元组,仍然可以恢复出来完整的数字水印;

2) 如果想增强抵抗元组删除攻击的强壮性,则应增大 n 值,相应减少 t 值,即删除元组的最大值的门限是由 n 和 t 的取值决定的。

4　结语

本文采用 Shamir 密钥分存技术设计关系数据库的数字水印,通过设置恰当的动态门限,很好地权衡元组删除攻击强壮性和嵌入信息容量之间的关系。分析表明,运用密钥分存技术控制数据库水印算法方案能够有效提高存放与提取水印的安全性,进一步增强了数据库水印的抗攻击能力。

参 考 文 献

[1] 肖琳君,谷爱昱,张小红. 混沌在语音保密中的应用[J]. 电光与控制,2007,14(5):110-112.

[2] 冯明库. 基于小波变换的数字图像混沌加密算法[J]. 电光与控制,2010,17(12):13-16.

[3] 梅蓉,吴庆宪,姜长生. 异结构时滞不确定混沌系统的同步/反同步控制及其应用[J]. 电光与控制,2011,18(5):37-41.

[4] 马瑞敏,陈继红. 基于二维空间元素匹配的数据库水印算法[J]. 计算机应用,2012,34(8):36-39.

[5] COX I J, KILIAN J, LEIGHTON F T, et al. Secure spread spectrum watermarking for multimedia [J]. IEEE Transactions on Image Processing, 2007, 6(12): 1673-1687.

(下转第 104 页)

[8] LIAO C M, TSENG S T. Optimal design for step-stress accelerated degradation tests[J]. IEEE Transactions on Reliability, 2006, 55(1):59-66.

[9] LI Xiaoyang, JIANG Tongmin. Optimal design for step-stress accelerated degradation with competing failure modes[C]// Annual Reliability and Maintainability Symposium, 2009: 64-68.

[10] 汪亚顺,莫永强,张春华,等. 双应力步进加速退化试验统计分析研究——模型与方法[J]. 兵工学报, 2009,30(4):451-456.

(上接第92页)

结合,才能设计出满足实用要求的高压电源。

参 考 文 献

[1] 李作民. 电视机原理与接收机[M]. 西安:西安电子科技大学出版社,1997:6-7.

[2] 戈特利布 I M. 稳压电源[M]. 北京:科学出版社,1993:52-53.

[3] BROWN M. 开关电源设计指南[M]. 徐德鸿,等译. 北京:机械工业出版社,2004:23-27.

[4] 王英剑,常敏慧,何希才. 新型开关电源实用技术[M]. 北京:电子工业出版社,1999:86-89.

[5] 徐德高,金刚. 脉宽调制变换器型稳压电源[M]. 北京:科学出版社,1983:24-31.

[6] 李定宣. 开关稳定电源设计与应用[M]. 北京:中国电力出版社,2006:104-105.

[7] 麦克·威廉亨姆. VMOS 应用电路精选[J]. 应用电子文摘,1986(3):12.

(上接第95页)

[6] 李素云,石润华. 一种动态的密钥分存方案[J]. 安徽大学学报:自然科学版,2010,34(3):38-42.

[7] 傅瑜. 关系数据库的数字水印模型[D]. 武汉:华中师范大学,2011.

[8] LOU Oujun, WANG Zhengxuan. A contourlet—domain watermarking algorithm against geometric attacks based on feature template[J]. Chinese Journal of Computers, 2009, 32(2):308-317.

[9] 张健,于晓洋,任洪娥. 一种改进的 ArnoldCat 变换图像置乱算法[J]. 计算机工程与应用,2009,45(35):14-17.

下 期 要 目

AFDX 实时流量的时间确定性中间件接入模型研究
微波着陆系统横向自动进近控制律设计
基于角点检测的双目视觉测距新方法
基于辅助粒子滤波的机动弱目标 TBD 算法
基于弦线法的去导迭代扩展卡尔曼滤波器
基于命中概率的制导炸弹可达域定量缩减方法
舰载反潜双机协同定位及其误差估计问题研究
一种基于共形阵的自适应单脉冲测角方法
一类离散时间系统的间接自适应模糊滑模控制
轮廓波和方向小波变换方法的性能比较
基于点迹态势图像处理的数据关联新方法
基于 Renyi 熵的非线性系统中传感器管理算法
基于 FPGA 和 TSC695F 的空间相机控制器设计
指数趋近律单向辅助面滑模控制
基于扩展卡尔曼滤波的动中通低成本姿态估计
高超声速滑翔式飞行器摆动突防设计