视频数据库多级访问控制

熊金波[1,2]，姚志强[1,2]，马建峰[1]，李琦[1]
(1. 西安电子科技大学 计算机学院，陕西 西安 710071；2. 福建师范大学 软件学院，福建 福州 350108)

摘 要：针对视频数据库中涉及敏感信息的视频数据分级保护问题，提出视频数据库多级访问控制模型。在该模型中，设计用户身份辨别及身份强度算法，其结果作为用户安全等级隶属函数的输入，该函数值为用户安全等级隶属度，并与视频数据安全等级隶属度一起作为授权规则中安全等级隶属度比较函数的输入，其函数值结合时间元素能够灵活地实现多级访问控制。与已有的访问控制模型相比，该模型最突出的特点是实现动态授权和视频数据分级保护。

关键词：多级访问控制；身份辨别；动态授权；安全等级
中图分类号：TP309 **文献标识码：**B **文章编号：**1000-436X(2012)08-0147-08

Multilevel access control for video database

XIONG Jin-bo[1,2], YAO Zhi-qiang[1,2], MA Jian-feng[1], LI Qi[1]
(1. School of Computer Science and Technology, Xidian University, Xi'an 710071, China;
2. Faculty of Software, Fujian Normal University, Fuzhou 350108, China)

Abstract: In regards to the critical issues of classification protecting sensitive information of the data stored in video database, a multilevel access control model for the video database was proposed. A series of algorithms was designed and developed in the model where a method of distinguishing user identity and an algorithm to ensure good identity strength were presented. The result of them was then used as the input to user's security level membership function. The user's security level membership degree was subsequently acquired from the result of this function, and it is then, together with the security level membership degree of video data, used as input to the comparison function of security level membership degree in authorization rule. As a result, the multilevel access control can be implemented neatly through combining the result of the comparison function with time element. Compared with the existing access control models, the most outstanding characteristics of the proposed model are realizations of dynamic authorization and video data classification protection.

Key words: multilevel access control; identity distinguish; dynamic authorization; security level

---

收稿日期：2011-08-24；**修回日期：**2012-06-25
基金项目：长江学者和创新团队发展计划基金资助项目(IRT1078)；国家自然基金委员会—广东联合基金重点基金资助项目(U1135002)；国家科技部重大专项基金资助项目(2011ZX03005-002)；中央高校基本科研业务费基金资助项目(JY10000903001)；福建省自然科学基金资助项目(2011J01339)；福建省教育厅科技基金资助项目(JK2010010)
Foundation Items: Changjiang Scholars and Innovative Research Team in University (IRT1078); The Key Program of NSFC-Guangdong Union Foundation (U1135002); Major National S&T Program(2011ZX03005-002); The Fundamental Research Funds for the Central Universities(JY10000903001); The Natural Science Foundation of Fujian Province (2011J01339); Science and Technology Foundation of Education Department of Fujian Province (JK2010010)

1 引言

近年来，网络计算技术以及面向Web服务技术的迅速发展促使视频应用变得越来越普及，覆盖众多的应用领域，如普适教育、家庭娱乐、数字社区、新闻报道和各种视频采集、编辑和后期处理等[1]。视频数据快速增长趋势不可避免地给用户带来安全方面的担忧，如肖像、身份信息、个人健康数据、公司商业秘密数据等敏感信息的泄漏可能给用户或企业带来不可估量的损失。因此，迫切需要一种安全机制，不仅需要具备能够对视频数据实施安全等级划分的视频安全分级机制，还需要具有适应大规模用户动态访问需求的动态授权方法。

访问控制是保护视频数据库中敏感信息安全的重要安全机制，主要用于防止非授权访问和确保合法用户对视频数据的受限访问和使用。近年来，有关多媒体尤其是视频数据访问控制的研究受到学术界的广泛关注，包括对视频数据库[2~4]和多媒体应用[1,5,6]的访问控制研究。

文献[2]在已有成果的基础上，给出了视频数据库层次语义簇模型和基于散列表的索引结构，提出了支持多层次访问视频元素的访问控制模型，并对模型中的过滤规则和访问控制规程进行了形式化定义和详细分析。文献[3]在此基础上进行了适当扩展，在视频数据层次模型中添加注释构成混合层次结构，通过改进文献[2]的检索算法进一步提高了视频检索和访问控制的效率。以上文献研究的视频数据都是开放的，不考虑涉密和敏感信息的安全保护。然而，对于涉及不同敏感程度信息的视频数据实施安全分级保护对于视频数据的安全传播和共享十分重要。

为了对涉及隐私数据的多媒体内容实施安全保护，文献[1,5,6]提出了一种基于安全判别规则的多层访问控制方法。该方法使用MPEG(moving picture experts group)-7标准[7]描述数据对象，并对RBAC (role-based access control) 96模型[8]的基本概念进行扩展，分别定义安全对象、安全用户和安全操作。通过评价安全用户子集的元素与嵌入到安全对象的安全判别表达式的结果，并依据判别表达式的层次可以实现多层访问控制。该模型虽有考虑敏感信息的安全保护问题，但是没有对不同敏感程度的数据内容制定安全等级的分级机制，且授权方式仍和以往模型一样，采用预定义的静态授权方式，因而难以适应大规模用户的动态访问需求。

当前研究虽然取得了一定的成果，但是针对视频数据库中敏感视频信息的安全分级保护问题，还需要解决以下2个关键问题。

1) 建立用户身份辨别机制以及用户与视频数据对象的安全等级划分原则。网络中存在大量的用户，视频数据库服务提供者并不具备这些用户的先验知识[9]，因此，在提供服务之前，首要任务是需要依据时间和环境因素[10~12]建立基于多属性的用户身份辨别机制以有效区分合法用户和非法用户，并进一步对合法用户进行安全等级的确定。同时，网络中存在大量多源异构视频信息，其中存在涉及个人或商业敏感的信息，必须对这些信息提供安全保护以免泄露而造成不必要的损失。因此，需要对视频数据根据其敏感程度划分安全等级，只有匹配安全等级要求的合法用户才能授权访问相应安全等级的视频数据。

2) 动态授权和多级访问控制。已有的视频数据库访问控制模型采用预定义访问策略的静态授权方式，不足以适应大规模分布式网络环境下对视频数据服务的动态访问需求。因此，必须设计动态授权方法。同时，访问控制方法应该充分集成视频数据的层次语义模型和交叉索引结构，结合用户安全等级和视频数据对象的安全等级以实现敏感信息保护的多级访问控制机制。

为了解决以上关键问题，本文提出视频数据库多级访问控制模型(VDMAC, multilevel access control model for video database)。VDMAC的核心思想为：首先，结合MPEG-7标准[7]描述视频数据对象，扩展文献[2]的视频层次语义数据库模型，给出语义交叉索引结构以提高检索效率；其次，提出基于多属性的用户身份辨别方法、用户身份强度算法和安全等级划分方法，并给出视频数据的安全等级隶属度计算方法和安全等级确定方法；最后，提出采用动态授权机制实现对敏感视频数据分级保护。VDMAC是对已有工作的有益补充，为大规模分布式环境下视频数据库敏感信息的安全分级保护和动态授权提供一种有益探索。

2 视频数据库层次语义树模型

为了有效地实现视频数据层次访问控制，已经提出视频数据层次语义簇模型[2]和扩展层次数据库模型[3]。在此基础上，VDMAC模型扩展文献[13]

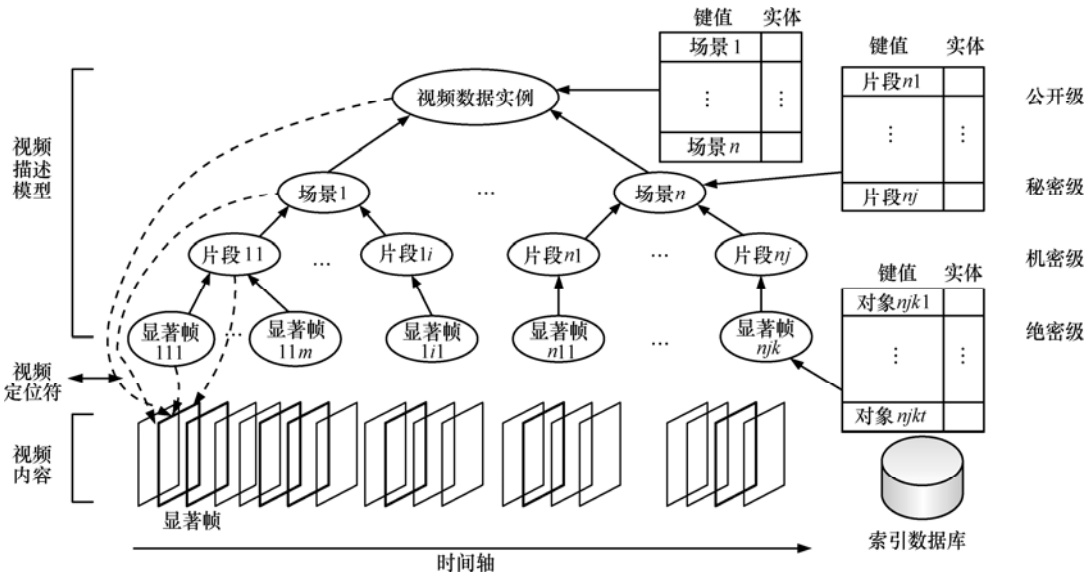


图 1　视频层次语义树模型和语义交叉索引结构

对多媒体的描述方式，采用 MPEG-7 标准[7]描述视频数据对象。

VDMAC 模型选用 MPEG-7 标准的主要原因是它具备两大特征[1,13]。首先，MPEG-7 标准具有强大的语义描述功能，能够将视频数据内容分解和组织成树型结构。该描述允许将视频内容分解成许多不同的“部分”，如图 1 所示。可以将视频内容分割成不同的场景，每个场景分割成不同的段，段又包含不同的帧等，而每个这样的“部分”都通过视频内容定位符关联相应的视频实体。其次，MPEG-7 标准的描述方案具有很好的可扩展性。因此，采用 MPEG-7 标准有利于从视频中分离出待保护的、涉及敏感信息的视频数据并组织成层次语义树模型，经过描述符和描述方案的适当扩展，可以描述更多类型的视频实体，从而可以方便地实现更细粒度的多级访问控制。

本文在文献[2,3]的基础上建立语义交叉层次索引结构。比如视频内容实例维护一个它所有场景的散列表，每个场景维护一个它所有片段的散列表，每个片段维护一个它所有数据帧影射到磁盘存储位置的散列表。在此基础上，本文从两方面对原来的索引结构进行优化：首先，在视频数据库中建立一个整体的视频数据库散列表，检索时可以快速定位到相关的所有视频内容，再根据单个视频内容的散列表准确定位到对应视频实体。另一方面，单个视频内容中维护一个场景散列表，比如医学教学视频中建立一个以手术为主的手术场景散列表，便于快速检索整个视频中相似场景信息，从而构建语义交叉索引结构。在此基础上，下面详细分析 VDMAC 模型。

3　多级访问控制模型 VDMAC

本文提出的 VDMAC 模型由 3 个主要模块组成，如图 2 所示。身份辨别模块负责网络环境下用户身份的辨别，填补以往模型[2~4]在这方面的空白。根据用户的综合属性由身份强度函数得到用户的身份强度值，从而准确区分非法用户和合法用户。授权引擎模块将用户的身份强度值作为安全等级隶属函数的输入，该函数计算的安全等级隶属度确定用户的安全等级，类似方法计算出授权对象的安全等级隶属度及安全等级。用户和授权对象的安全等级隶属度作为动态授权规则中隶属度比较函数的输入，最终由该比较函数的结果决定是否授权及授权级别。查询引擎模块主要根据授权规则的要求，检索视频数据并把查询结果返回给用户。访问控制的整个会话过程均记录在审计模块中。

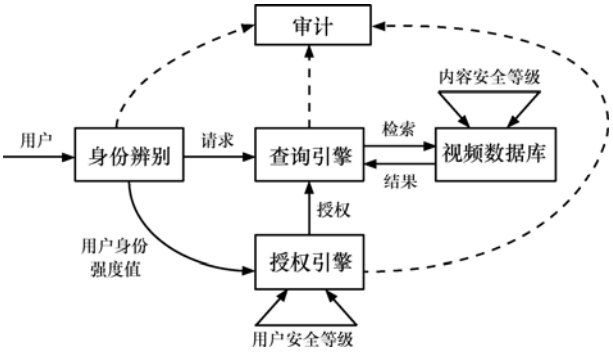


图 2　VDMAC 模型模块结构

3.1 身份辨别

身份辨别模块负责网络环境下用户身份的辨别，根据综合属性因素及身份强度函数计算出身份强度值，然后和系统安全管理员给定的身份阈值进行比较，身份强度值低于阈值则属非法用户，高于阈值则属合法用户，从而区分非法用户和合法用户，并拒绝非法用户的访问请求。

以健康医疗(eHealth)视频数据库为例，考虑如何对用户进行身份辨别，可供其他服务参考。现代医疗系统中，电子病历发挥越来越重要的作用，各医院多种类型的电子病历文件、影像文件、各类手术视频、诊断视频、教学视频等视频数据都可能需要实现共享和互操作，其中有大量的视频数据涉及病人及医院的隐私等敏感信息。因此，如何区分合法用户和非法用户的访问请求成为保护视频数据安全的基本需求，而已有的访问控制模型都不能满足该需求。

1) 身份辨别属性。该属性指能够表示用户身份的属性集合。主要包含：用户身份 *Identity* (包括用户名、密码，用 ID 表示；用户的职称或职务，如主任医师，副主任医师、护士长、主管药师，医师、护士、药师，非医护人员等，用每个人的指纹信息表示 *Fingerprint*； $Identity = ID \wedge Fingerprint$)，环境属性 *Environment* (如能体现医务人员工作环境的相关属性：医师位置信息、医用操作系统软件、计算机 MAC 地址等)，时间属性 *Time*(上班时间，如 9:00~17:00)。

2) 属性权值分配。根据医疗系统实际情况及多次实验测试，获得经验值给用户辨别属性分配权值如下：*Identity* 分配 50%，(其中 *ID* 与系统预定义相符则赋值 1，否则为 0；*Fingerprint* 的赋值如下：院长、书记赋值为 1，表示完全拥有访问数据库能力；主任医师或处级以上干部赋值为 0.8，副主任医师、护士长、主管药师及副处级干部赋值 0.6，一般医师、护士、药师等赋值 0.4，其他员工赋值 0.2，非医护人员赋值 0)，*Environment* 分配 30%(在用户自己的办公室位置、医用操作系统软件、计算机 MAC 地址这 3 个指标分别赋值 0.5、0.3、0.2)，*Time* 分配 20%(上班时间段则赋值 1，否则赋值 0)。

3) 用户身份强度(identity strength)函数：$IDS = Identity \times 50\% + Enviroment \times 30\% + Time \times 20\%$

VDMAC 模型规定身份强度阈值为 0.6。

身份辨别举例：假如一名副主任医师($Fingerprint = 0.6$)上班时间($Time = 1.0$)在他办公室使用预先注册的身份($ID = 1.0$)提出访问医疗视频数据库请求，且操作系统匹配，MAC 地址有更改($Enviroment = 0.5 + 0.3 + 0 = 0.8$)。依据 3)，可以计算出该医师的身份强度值 $IDS = (1.0 \wedge 0.6) \times 50\% + 0.8 \times 30\% + 1.0 \times 20\% = 0.74$，因 0.74>0.6，说明该医师是合法用户，其提交的访问控制请求可以被 VDMAC 系统进一步处理。

3.2 授权引擎

1) 合法用户安全等级划分

根据用户身份强度值 *IDS* 确定用户安全等级，将用户的安全等级划分成公开级(unclassified，处于该级别的主体 *s* 能够访问不涉密视频数据)、秘密级(classified，能访问秘密级视频数据)、机密级(secret)和绝密级(top secret)。借鉴文献[14,15]采用下面脆弱边界数范围作为安全等级的划分：*unclassified*=[0.6,0.7]，*classified*=(0.7,0.8]，*secret*=(0.8,0.9]，*top secret*=(0.9,1.0]。如果当一个主体 s_1 的 $IDSs_1 = 0.7$ 时为公开级，而当另一个主体 s_2 的 $IDSs_2 = 0.701$ 时为秘密级，可能觉得低估了 s_1 的安全等级而高估了 s_2 的安全等级，为了使安全等级能够平滑过渡，采用模糊逻辑中的梯度函数[15]来实现该功能：

$$trapmf(x;a,b,c,d) = \max\left(\min\left(\frac{x-a}{b-a}, 1, \frac{d-x}{d-c}\right), 0\right)$$

用户的安全等级隶属函数(membership function)规定如下，用户身份强度值为该函数的输入：

unclassified： $uc_s(x) = trapmf(x;0.6,0.6,0.65,0.73)$

classified： $c_s(x) = trapmf(x;0.65,0.73,0.77,0.83)$

secret： $s_s(x) = trapmf(x;0.77,0.83,0.87,0.95)$

top secret： $ts_s(x) = trapmf(x;0.87,0.95,1.0,1.0)$

则 $md_s = \{uc_s(x), c_s(x), s_s(x), ts_s(x)\}$ 称为用户的安全等级隶属度(membership degree, *md*)。

给定一个主体 *s* 的身份强度值 *IDSs*，则可以根据隶属函数计算出安全等级隶属度，比如，一个主体 s_1 的 $IDSs_1 = 0.7$ 时，其安全等级隶属度为 $md_{s1} = \{uc_s(0.7), c_s(0.7), s_s(0.7), ts_s(0.7)\}$，即 $md_{s1} = \{0.375, 0.625, 0, 0\}$。另一个主体 s_2 的 $IDSs_2 = 0.701$ 时，他的安全等级隶属度 $md_{s2} = \{uc_s(0.701), c_s(0.701), s_s(0.701), ts_s(0.701)\}$，即 $md_{s2} = \{0.363, 0.637, 0, 0\}$。因此，主体 s_1 和 s_2 的安全等级隶属度

比较接近。

2) 视频数据层次关系及安全等级划分

已有的研究工作均没有对视频数据进行安全等级划分，文献[15]中对文档进行安全标记考虑。在此基础上，为了实现对视频数据敏感信息的保护需求，本文对层次语义树模型定义安全等级。设计一个视频数据自动计分系统。以健康医疗视频数据库系统为例，基于下面 4 个部分计算视频数据的安全强度值，每部分都有一个上界：产生视频数据的作者(赋值 0.3)，视频数据内容(0.3)，传播视频数据的途径(0.2)和访问请求者(0.2)。每个部分都包含一些具有不同安全值的特征，这些特征的安全值都由安全专家定义。给定一个视频数据，其安全强度值由以上特征总和计算得出，规定最低值为 0.5，最高值为 1.0。

根据视频数据的安全强度值确定其安全等级，和用户安全等级类似，划分成公开级、秘密级、机密级和绝密级。类似采用下面脆弱边界数范围作为安全等级的划分：*unclassified*=[0.5,0.6]，*classified* =(0.6,0.75]，*secret*=(0.75,0.9]，*top secret*=(0.9,1.0]。为了解决安全等级平滑过渡问题，同样采用模糊逻辑中的梯度函数 $trapmf(x;a,b,c,d)$ [15]。

视频数据安全等级的隶属函数规定如下：

unclassified：$uc_v(x)=trapmf(x;0.50,0.50,0.55,0.65)$

classified：$c_v(x)=trapmf(x;0.55,0.65,0.70,0.80)$

secret：$s_v(x)=trapmf(x;0.70,0.80,0.85,0.95)$

top secret：$ts_v(x)=trapmf(x;0.85,0.95,1.0,1.0)$

则 $md_v=\{uc_v(x),c_v(x),s_v(x),ts_v(x)\}$ 称为视频数据的安全等级隶属度。

给定一个视频数据，其安全等级隶属度由隶属函数决定，比如安全强度值为 $IDSv_1=0.75$ 的视频数据 v_1，其安全等级隶属度 $md_{v1}=\{uc_v(0.75),c_v(0.75),s_v(0.75),ts_v(0.75)\}$，即 $md_{v1}=\{0,0.5,0.5,0\}$。安全强度值为 $IDSv_2=0.751$ 的视频 v_2，其安全等级隶属度 $md_{v2}=\{uc_v(0.751),c_v(0.751),s_v(0.751),ts_v(0.751)\}$ 即 $md_{v2}=\{0,0.49,0.51,0\}$。

3) 动态授权方法

授权处理一个合法用户是否能够采用什么方式访问哪部分视频数据。在 VDMAC 模型中，每个授权的对象为视频数据层次语义树模型中的节点，可以是视频数据、场景、片断、关键帧等。

采用 S 表示所有授权主体的集合，VD 表示视频数据库，V_i 表示单一的视频数据，则 $VD=\{V_i\,|\,V_i\in VD\},i\geqslant 1$。$A$ 表示所有授权的集合，授权规定如下。

动态授权。动态授权(DA, dynamic authorization)由一个 5 元组 $da=<s,v,comp,time,qr>$ 表示，其中 $s\in S,v\in VD,da\in A$，$qr\in[++|+|-]$，$time=[t_i,t_j]$，$(0:01\leqslant t_i<t_j\leqslant 24:00)$，$comp=compare(md_s,md_v)$：

$$compare(md_s,md_v)=\begin{cases}1, & md_s-md_v\geqslant 0\\ 0, & md_s-md_v\in(-0.2,0)\\ -1, & md_s-md_v\leqslant -0.2\end{cases}$$

$$qr=\begin{cases}++, & \text{if } compare(md_s,md_v)=1\\ +, & \text{if } compare(md_s,md_v)=0\\ -, & \text{if } compare(md_s,md_v)=-1\end{cases}$$

授权描述说明：s 表示授权主体，v 表示授权对象，$comp=compare(md_s,md_v)$ 是安全等级隶属度比较函数，md_s 表示授权主体的安全隶属度，md_v 表示视频对象的安全隶属度，比较函数的值由上面公式确定，当 $compare(md_s,md_v)=1$ 时，授权质量等级元素 $qr=++$ 表示可以获得高质量访问的授权，当比较值为 0 时，$qr=+$ 表示可以获得低质量访问的授权，当比较值为 -1 时 $qr=-$ 表示拒绝授权访问。高质量即为原视频数据的质量，低质量是在原质量的基础上，对某些敏感信息经过模糊化处理[3]，并不影响用户访问该视频内容；时间元素 $time=[t_i,t_j]$ 表示在 $t_i\sim t_j$ 时间范围内访问有效，该值由安全管理员为视频数据预先指定的，*time* 元素可省，省略时表示全时有效。

该授权具有动态性。是否获得授权以及授权质量等级完全由安全等级隶属度比较函数的值决定。同一个主体在不同的环境、位置和时间段时具有不同的身份，可以计算出不同的身份强度值，从而获得不同的安全等级隶属度，根据系统授权规则中隶属度比较函数的值可以自动获得不同的授权；而对象的安全等级隶属度，在必要的情况下，也可以由系统安全管理员根据需要调整隶属函数因子，即可获得不同的安全等级隶属度。综上，该授权方法可以实现自适应的动态授权。

授权举例：授权 $A_1=<Jim,Cure,compare(0.85,0.80),[8:00,17:30],[++|+|-]>$ 描述的是当一个授

权主体 *Jim* 的安全隶属度为 $md_s = 0.85$，授权对象为视频数据 *Cure* 的安全隶属度为 $md_v = 0.80$ 时，因为 $md_s - md_v = 0.85 - 0.80 \geqslant 0$，$compare(md_s, md_v) = 1$，所以主体 *Jim* 在时间 $time = [8:00,17:30]$ 范围内可以获得 $qr = ++$ 高质量访问 *Cure* 的授权。

由于一个主体 *s* 可以属于多个用户组，也可以获得多个授权。而视频数据存在层次关系，已有的访问控制模型[2~6]都可能存在授权冲突问题。而本文提出的授权方法中，授权对象可以精确到视频数据层次语义树种的叶子节点，即可以实现多级授权。通过 *comp* 函数计算比较用户和视频数据的安全等级隶属度来确定是否授权，因此，VDMAC 模型极少有授权冲突的情况。

3.3　查询引擎

查询引擎主要接收合法用户的访问控制请求，根据授权引擎的授权，从视频数据库中检索到授权的视频数据，并将结果返回给该用户。为了确保合法用户仅能访问到被授权的视频数据并提高检索效率，本文结合视频数据库层次索引结构，基于授权对象的相关性规定视频数据库映射方法[2,3]。

视频数据映射。考察一个视频数据内容中，与授权视频元素 *v* 语义相近的数据，关于 *v* 的视频数据 *V* 的映射定义为 $\bigcap_v V$，它是视频元素 v_i 的集合，满足 $v_i \in_k v, k \geqslant 0$。表示在层次语义树模型中，$\bigcap_v V$ 只包含 *v* 节点的所有子节点，$\bigcap_v V = \{o \mid o \in_k v, v \in V, k \geqslant 1\}$。

视频数据库 *VD* 包含多个视频数据 V_i，由索引结构可知，视频数据库维护了一个视频数据散列表，通过该表可以快速检索到与授权视频元素 *v* 语义相近的视频数据，从而获得关于 *v* 的关于视频数据库 *VD* 的映射 $\bigcap_v VD = \{V_i \mid v \in V_i, V_i \in VD\}, i \geqslant 1$，然后根据 V_i 中与授权 *v* 语义相近的场景散列表，即可以获取映射 $\bigcap_s V_i$，从而快速定位到相应的场景 *s*，进而检索到授权对象 *v*。该方法的主要特点是先依据授权规则对视频数据进行过滤，然后在小范围内检索授权对象，从而提高查询效率。

3.4　多级访问控制

VDMAC 模型能够很好地集成合法用户的安全等级和视频数据的安全等级及其组织层次。

系统安全管理员可以灵活地控制视频数据的安全等级隶属度。当该等级设置较低时，总能满足 $md_s - md_m \geqslant 0$，即 $compare(md_s, md_m) = 1$，即合法用户均可获得授权访问；而当遇到需要进一步保护的视频对象时，则根据安全等级隶属度函数进行隶属度计算，然后根据动态授权规则中隶属度比较函数的结果来确定哪些视频数据被授予哪个安全等级的权限以及授权的质量等级。这样只有匹配动态授权规则的合法用户才能访问受保护的视频数据，从而实现多级访问控制，达到对视频数据的分级保护。

除了可以给单个用户授权外，VDMAC 模型还可以给用户组授权。根据系统的需要，合法用户可以属于一个或多个用户组，某些特殊情况下，需要给用户组授权。当用户组的所有用户都需要获得授权时，可以由系统安全管理员设置合适的用户组安全等级隶属度，当该隶属度大于或等于授权对象时，用户组的所有用户能以组角色获得授权。

3.5　非多级访问控制

VDMAC 模型为层次语义树模型，涉及个人隐私和单位秘密的视频数据都位于层次语义树模型的低层。因此，低层视频对象的安全等级要高于其上层的安全等级，如图 1 所示。当系统安全管理员将最底层视频数据的安全等级设置成公开级时，整个视频数据内容也都为公开级。此时，通过身份辨别模块的合法用户都可以获得访问视频数据库资源的授权；或者系统安全管理员将通过身份辨别模块的合法用户的安全等级隶属度都设置成 1.0，即 $md_s - md_m \geqslant 0$ 恒满足，因此 $compare(md_s, md_m) = 1$，说明合法用户均可以获得访问视频数据库的授权，从而实现非多级访问控制。

4　定性分析与比较

从以下 3 个方面将 VDMAC 模型与相关的工作进行定性分析与比较。

1) 用户身份辨别、用户和视频数据的安全等级。文献[1,5,6]通过预定义安全判别表达式和安全子集定义安全用户和安全多媒体对象，在安全方面有具体措施，且取得了较高的效率。与此相比，VDMAC 模型提出了一种辨别用户身份合法性的新思路，并通过借鉴文献[15]的模糊逻辑推理思想，明确给出了用户和视频对象的安全等级划分方法，该方法为多级访问控制提供直接依据。

2) 环境和时间因素。文献[2]在访问控制授权中考虑时间因素，将连续时间段赋予某一请求者但粒度不够。文献[10~12]综合考虑角色、时间和环境因素定义用户访问行为，提出基于行为的访问控制

表 1　　**视频数据库访问控制模型综合分析与比较**

性质模型	用户身份辨别	安全等级	角色	时间因素	环境因素		授权类型	多级访问控制
					位置	平台		
CBMAC[1,5,6]	定义安全用户	支持	支持	不支持	支持	不支持	静态	支持
文献[3]模型	不支持	不支持	支持	不支持	不支持	不支持	静态	支持
Bertino[2]模型	不支持	不支持	支持	部分支持	不支持	不支持	静态	支持
文献[13]模型	定义安全用户	支持	支持	不支持	支持	不支持	静态	支持
文献[14]模型	模糊判断	支持	支持	不支持	不支持	不支持	静态	不支持
VDMAC 模型	支持	支持	支持	支持	支持	支持	动态	支持

模型，很好地解决移动计算、协作环境和云计算环境中的访问控制问题。VDMAC 模型借鉴并扩展了已有成果，将时间和环境因素用于用户身份辨别和动态授权中。

3) 授权类型和多级访问控制。文献[2,3]提出在视频数据库中建立基于层次语义的组织结构和与之对应的索引结构，实现了层次访问控制机制且取得了较高的效率，相比以前的访问控制模型取得了重大突破。由于授权规则必须预定义，使得这些方式不能很好地适应大规模网络环境下的服务提供。VDMAC 在以上层次语义模型和索引的基础上新增加语义交叉索引结构以提高数据检索效率，并能实现动态授权。VDMAC 能够通过用户和视频数据的安全等级隶属度函数以及授权规则中的隶属度比较函数执行动态匹配，从而获得相应授权，以满足大规模网络环境下用户自适应动态授权需求。此外，已有模型都只在多媒体数据服务提供端实现多层访问控制，而 VDMAC 模型分别在用户请求端和视频数据服务提供端通过定义用户和视频数据的安全等级以及授权匹配实现多级访问控制，形成闭环结构。

改进文献[10]的评价因素，将 VDMAC 模型与已有的几种访问控制模型进行了定性分析与比较，结果如表 1 所示。

5　结束语

本文研究了如何辨别大规模网络环境下用户身份的合法性以及用户安全等级的划分，如何组织视频数据及建立有效的语义交叉索引结构，如何确定视频数据的安全等级等问题。为了更好地保护涉及隐私和敏感信息的视频数据，提出了针对视频数据库的多级访问控制（VDMAC）模型。

VDMAC 模型主要由身份辨别、授权引擎和查询引擎 3 个模块组成，详细分析了各模块的功能及算法，并对已有的几种访问控制模型进行了比较和分析，结果表明本文所提模型更适合涉及个人隐私和敏感信息的视频数据库的安全管理。

本文的主要贡献是提出用户身份辨别机制，给出身份强度算法，为系统自动辨别合法用户和非法用户提供依据；利用模糊逻辑中的安全等级隶属函数及隶属度确定安全等级，明确用户和视频数据安全等级划分方法；制定动态授权规则，通过构造安全等级隶属度比较函数灵活地实现动态授权，实现请求者多安全等级和视频数据提供者多安全等级的多级访问控制机制。

下一步的研究工作的重点是基于 XACML[16]标准实现 VDMAC 原型系统，并将其应用于 eHealth 视频数据库系统及其他视频应用服务；基于 VDMAC 研究基于隐私保护的多级授权委托和授权撤销模型；将 social relationship[17]结合到用户身份辨别中，以使 VDMAC 授权更灵活；对该模型进行访问控制的综合性能分析包括访问控制精确度统计和动态授权策略的安全评估。

参考文献：

[1] PAN L, ZHANG C N. A criterion-based multilayer access control approach for multimedia applications and the implementation considerations[J]. ACM Transactions on Multimedia Computing, Communications and Applications, 2008, 5(2):17:1-29.

[2] BERTINO E, FAN J P, FERRARI E, *et al*. A hierarchical access control model for video database systems[J]. ACM Transactions on Information Systems, 2003, 21(2):155-191.

[3] NGUYEN A T T, TRAN K D. An extended video database model for supporting finer-grained multi-policy and multi-level access controls[J]. Journal of Polibits, 2008, 38(2): 49-63.

[4] PAN L, ZHANG C N. Using metadata to protect the audiovisual contents in MPEG-7 applications[A]. SAM '04[C]. Las Vegas, Nevada, USA, 2004.

[5] PAN L, ZHANG C N. A criterion-based role-based multilayer access control model for multimedia applications[A]. ISM '06[C]. San Diego, California, USA, 2006.

[6] PAN L, ZHANG C N. A Web-based multilayer access control model for multimedia applications in MPEG-7[J]. International Journal of Network Security, 2007, 4(2):155-165.

[7] SALEMBIER P, SMITH J. MPEG-7 multimedia description schemes[J]. IEEE Transactions on Circuits and Systems for Video technology, 2001, 11(6):748-759.

[8] SANDHU R, COYNE E, FEINSTEIN H, *et al*. Role-based access control models[J]. IEEE Computer, 1996, 29(2):38-47.

[9] ARDAGNA C A, VIMERCATI S D C. Expressive and deployable access control in open Web service applications[J]. IEEE Transactions on Services Computing, 2011, 4(2):96-109.

[10] 李风华,王巍,马建峰等. 基于行为的访问控制模型及其行为管理[J]. 电子学报, 2008,36(10):1881-1890.
LI F H, WANG W, MA J F, *et al*. Action-based access control model and administration of actions[J]. Acta Electronica Sinica, 2008, 36(10):1881-1890.

[11] 李风华,王巍,马建峰. 协作信息系统的访问控制模型及其应用[J]. 通信学报. 2008, 29(9):116-123.
LI F H, WANG W, MA J F. Access control model and its application for collaborative information systems[J]. Journal on Communications, 2008, 29(9):116-123.

[12] 林果园,贺珊,黄皓等. 基于行为的云计算访问控制安全模型[J].通信学报, 2012, 33(3):59-66.
LIN G Y, HE S, HUANG H, *et al*. Access control security model based on behavior in cloud computing environment[J]. Journal on Communications, 2012, 33(3):59-66.

[13] PAN L, ZHANG C N. A criterion-based role-based multilayer access control model for multimedia applications[A]. ISM '06[C]. Washington, DC, USA, 2006.

[14] MARTÍNEZ-GARCÍA C, NAVARRO-ARRIBAS G, BORRELL J. Fuzzy role-based access control[J]. Information Processing Letters, 2011, 111(10): 483-487.

[15] NI Q, BERTINO E, LOBO J. Risk-based access control systems built on fuzzy inferences[A]. ASIACCS '10[C]. New York, NY, USA, 2010.

[16] MOSES T. Extensible Access Control Markup Language (XACML)[R]. Technical Report, OASIS, 2003.

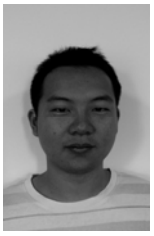
[17] FONG P W L. Relationship-based access control: protection model and policy language[A]. CODASPY '11[C]. San Antonio, Taxas, USA, 2011.

作者简介：

熊金波（1981-），男，湖南益阳人，西安电子科技大学博士生，福建师范大学讲师，主要研究方向为访问控制技术与结构化文档安全。

姚志强（1967-），男，福建莆田人，西安电子科技大学博士生，福建师范大学教授，主要研究方向为信息安全。

马建峰（1963-），男，陕西西安人，博士，西安电子科技大学计算机学院院长、教授、博士生导师，主要研究方向为密码学、计算机网络与信息安全。



李琦（1989-），男，江苏淮安人，西安电子科技大学博士生，主要研究方向为基于属性的密码学与访问控制技术。