

MIS 中基于部门和角色的细粒度访问控制模型

严 骏, 苏正炼, 凌海风, 朱 亮, 张蕉蕉

(解放军理工大学 工程兵工程学院, 南京 210007)

(suji1984@yahoo.cn)

摘 要:针对基于角色的访问控制模型的特点和不足,提出一种基于部门和角色的细粒度访问控制模型(D-RBAC模型),对模型中的元素进行了形式化描述,给出了其实现机制和访问控制算法。D-RBAC将角色和部门相关联,有效实现了对对象访问和数据范围的精确控制,同一角色在不同部门的权限分配以及细粒度访问控制,减少了角色管理数量,简化了开发配置过程,增加了权限管理的精确性和灵活性。最后,给出了该模型在某装备综合管理信息系统中的应用实例。

关键词:访问控制;基于角色的访问控制模型;细粒度;部门

中图分类号: TP309 **文献标志码:** A

Department-role based finely granular access control model in management information system

YAN Jun, SU Zheng-lian, LING Hai-feng, ZHU Liang, ZHANG Jiao-jiao

(Engineering Institute of Engineer Corps, PLA University of Science and Technology, Nanjing Jiangsu 210007, China)

Abstract: Concerning the characteristics and disadvantages of Role-Based Access Control (RBAC) model, the department-role based access control (D-RBAC) finely granular model was proposed in this paper. A formal description for the model elements, the implement mechanism of the model, and the algorithm of access control were given. In D-RBAC model, role was related to department, which effectively implemented the accurate control of access objects and data, and the permission assignment problem of the same role in different departments was resolved. The fine-grained permission control was realized as well. Through the model, the number of roles was decreased, the development assignments were simplified and the accuracy and flexibility of permission management were increased. Finally, an application example of this model being used in one equipment safeguard comprehensive information system was given.

Key words: access control; Role Based Access Control (RBAC) model; finely granular; department

0 引言

访问控制是计算机网络信息安全管理的主要策略,是通过某种途径显式地准许或限制用户、组或角色对信息资源的访问能力及范围的一种方法^[1]。根据访问控制对象的粗细程度,通常把只控制到主机一级的称为粗粒度的访问控制,而把控制细到不可再分解的单一功能的按钮或链接的称为细粒度访问控制^[2]。传统的访问控制方法有自主访问控制(Discretionary Access Control, DAC)和强制访问控制(Mandatory Access Control, MAC)^[3]。20世纪90年代初出现了一种基于角色的访问控制(Role Based Access Control, RBAC)^[4]技术,能有效减少授权管理的复杂性,降低管理开销,灵活地支持系统的安全策略,对用户的变化有很强的适应性,逐渐得到广泛的应用,但也存在着1.2节所述的缺点。为了能适应复杂企业的特定环境需求,基于企业环境的访问控制模型(Task-Role Based Access Control, T-RBAC)^[5]模型被提出,把任务从角色中分离出来,和角色置于同等重要的地位。在T-RBAC模型中,先将访问权限分配给任务,再将任务分配给角色,角色通过任务与权限关联,真正实现了权限的按需和

动态分配;但也存在着任务分配、角色继承和实现复杂等缺点。

为了解决以上问题,国内外学者开展了很多研究工作。陈娟娟等人^[6]提出了基于角色的差异主体访问控制模型,针对协同访问控制的特点,区分了访问主体、访问权限的单一性与复合性,在一定程度上避免了协同主体的相互串通,但模型对系统要求较高,存在较大的局限性;李细雨等人^[7]提出了基于粒逻辑的扩展RBAC访问控制模型,将权限、角色粒化,在权限粒和角色粒上加入了时间和上下文的因素,提高了授权的灵活性,但实际操作复杂,而且未验证模型的完整性和一致性;王伟然等人^[8]提出了基于组织和角色语义的访问控制模型,进一步划分了角色和受控主体,通过角色适配器进行角色授权,能够更有效地对BMP运行过程中各类参与者、管理对象和操作进行控制,但无法有效地解决管理信息系统(Management Information System, MIS)中的访问控制问题。

根据信息系统,特别是军事信息系统对访问控制的特点和要求,如何对不同层次的访问用户的数据访问范围进行精确控制,如何分配多部门下同一角色的不同权限,本文研究并改进了RBAC模型,设计了基于部门和角色的访问控制模型

收稿日期:2010-08-11。

作者简介:严骏(1962-),男,湖北武汉人,教授,博士生导师,博士,主要研究方向:工程装备管理、装备保障信息化;苏正炼(1984-),男,四川蓬溪人,博士研究生,主要研究方向:装备保障信息化;凌海风(1972-),女,浙江长兴人,副教授,博士,主要研究方向:装备管理与应用、装备保障信息化;朱亮(1983-),男,湖南慈利人,博士研究生,主要研究方向:装备管理与应用;张蕉蕉(1984-),女,浙江浦江人,助教,硕士,主要研究方向:装备保障机电一体化。

(Department-Role Based Access Control, D-RBAC), 减少了角色管理数量, 实现了访问对象和数据范围的精确控制, 并在传统的粗粒度权限管理基础上加入了“菜单—按钮”对应关系使权限得以细化, 实现了 MIS 的细粒度访问控制。

1 基于角色的访问控制

RBAC 其基本思想是用户和权限通过角色相关联, 根据安全策略划分角色, 对每个角色分配操作许可, 对用户的授权通过赋予用户相应的角色来实现。其特点是引入了角色, 使得用户和权限得到了逻辑分离, 降低了安全管理成本和管理复杂性, 使授权变得简单而灵活。

1.1 RBAC 基本概念^[9-10]

1) 用户。用户就是一个可以独立访问计算机系统中的数据或者用数据表示的其他资源的主体, 在一般情况下是指人。

2) 角色。角色是指一个组织或任务中的工作或位置, 它代表了一种资格、权利和责任。一方面它表示了用户的职责划分; 另一方面也表示了一类用户可以访问的系统的功能集合。

3) 权限。权限是对计算机系统中的数据或者用数据表示的其他资源进行访问的许可, 是“控制对象 + 操作”, 它可分为对象访问控制和数据访问控制两种。

4) 会话。会话是一个动态概念, 用户激活角色时建立会话, 它是一个用户和多个角色的映射, 一个用户可以打开多个会话。

在给角色分配权限时, 要遵循最小权限原则和职责分离原则。最小权限原则是指该角色对应的用户的权限不能超过他执行工作时所需的权限; 职责分离原则是指用户的访问权限不会超越它们对履行职责的必要性。RBAC 模型如图 1 所示。

1.2 RBAC 模型的缺点

虽然 RBAC 模型比较灵活和完善地实现了访问控制, 但也存在如下缺点^[11]: 1) 模型粗糙, 最小权限约束粒度还不够细化; 2) 灵活性差, 角色授权很难保证多个角色与权限关联构成的权限集合与该用户实际需要的操作权限集合严格相等; 3) 运行代价高, 应用系统在实现其权限管理的过程中需要多次访问角色表、权限表和功能表并依据约定的规则进行权限的许可性匹配; 4) 难以实现拥有相同角色的用户访问不同的数据范围的控制; 5) 无法解决当同一角色存在于不同部门且拥有与部门相关的功能权限时的权限分配问题。

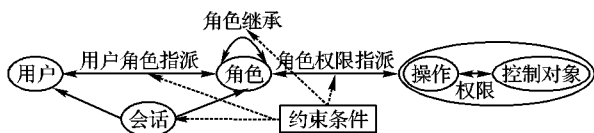


图1 RBAC 模型

2 基于部门和角色的细粒度访问控制模型

2.1 模型概念和控制机制

定义1 部门(D): 部门是系统管理对象的组织结构, 每个角色都与部门的某个组织相关联。

定义2 用户会话(US: $S \rightarrow U$): 映射每个会话到一个用户。

定义3 角色会话(SR: $S \rightarrow 2^R$): 映射每个会话到一组角色。

本模型对 RBAC 基本模型进行了扩展, 引入部门这一对象, 把角色和部门相关联, 将角色定义为部门下的角色, 通过角色、部门等方式对功能进行分组归纳; 再通过用户和角色、用户和部门、用户直接和功能的关系, 抽象出用户与功能的总关系视图^[12], 如图 2 所示。

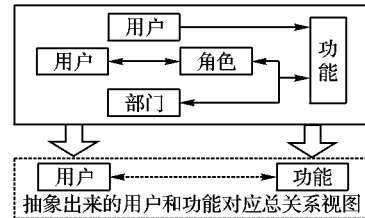


图2 权限控制机制模型

授权管理时, 系统权限的控制对象为每个模块的最低一级功能; 菜单的权限拥有者指派为某个“部门 + 角色”, 或者特殊地直接指派到某个用户; 菜单的操作根据每个菜单的具体功能可分为查看、编辑、审批等; 每个菜单的数据访问范围可限制为用户本人、用户角色所在部门或者直接指定到某个部门, 也可以不加限制, 并可主动配置。整个模型如图 3 所示。

当用户 → 角色 + 部门 → 功能授权和用户 → 功能授权两条路径发生重叠时, 系统将按照取并集的规则进行管理, 使之更有效地实现访问控制。

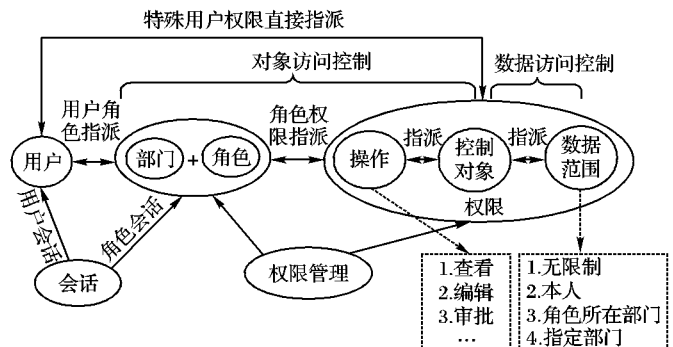


图3 基于部门和角色的访问控制(D-RBAC)模型

2.2 模型要素

D-RBAC 模型由以下几部分组成:

1) 部门集 $D = \{d_1, d_2, \dots, d_n\}$ 。

2) 用户集 $U = \{u_1, u_2, \dots, u_n\}$ 。

3) 角色集 $R = \{r_1, r_2, \dots, r_n\}$, D-RBAC 模型中, 将部门和角色相关联, 因此, 角色 r_i 是一个二元组 (o_i, d_i) , 其中 o_i 是角色标识符, 而 d_i 是 o_i 的关联部门信息。

4) 权限集 $P = \{p_1, p_2, \dots, p_n\}$; 权限 p_i 是一个三元组 (ao_i, h_i, dr_i) , 其中 ao_i 表示权限的访问控制对象, h_i 表示权限的操作集合, 而 dr_i 表示访问的数据范围。

5) 会话集 $S = \{s_1, s_2, \dots, s_n\}$ 。

模型中的主要函数关系包括:

1) 用户角色指派 $assigned_users_roles: U \times D \rightarrow 2^R$, 即给用户 $u \in U$ 分派一组与部门 $d \in D$ 关联的角色集。

2) 角色权限指派 $assigned_roles_permissions: R \times D \rightarrow 2^P$, 即给予部门 $d \in D$ 相关联的角色 $r \in R$ 分派一组权限集。

3) 用户权限指派 $assigned_users_permissions: U \rightarrow 2^P$, 即给用户 $u \in U$ 直接分派一组特殊权限集。

4) 用户角色激活 $active_roles: S \times U \rightarrow 2^R$, 即在一个会话期 $s \in S$ 内, 激活用户 $u \in U$ 可承担的一组角色。

5) 用户权限合成 $users_permissions_compose: S \times U \rightarrow 2^P$, 其中 $\{p \in P \mid P \subset assigned_roles_permissions(P) \cup assigned_users_permissions(P)\}$ 。

$users_permissions(P)$ },即会话 $s \in S$ 中用户 $u \in U$ 的权限合成是用户角色权限和用户直接权限的并集。

6) 对象访问控制 $objects_access_control: S \times U \rightarrow 2^{(ao,h)}$, 其中 $\{(ao,h) \in assigned_roles_permissions(ao,h) \cup assigned_users_permissions(ao,h)\}$, 即会话 $s \in S$ 中用户 $u \in U$ 的对象访问控制, 包括可访问对象 ao 和权限操作 h , 是其角色权限和用户直接权限中访问控制对象的并集。

7) 数据访问控制 $data_access_control: S \times U \rightarrow 2^{(ao,dr)}$, 其中 $\{(ao,dr) \in assigned_roles_permissions(ao,dr) \cup assigned_users_permissions(ao,dr)\}$, 即会话 $s \in S$ 中用户 $u \in U$ 对可访问对象 ao 的数据访问控制是其角色权限和用户直接权限中的可访问数据范围 dr 的并集。

2.3 访问控制算法

D-RBAC 模型实现访问控制的算法按以下步骤进行, 如图4所示。

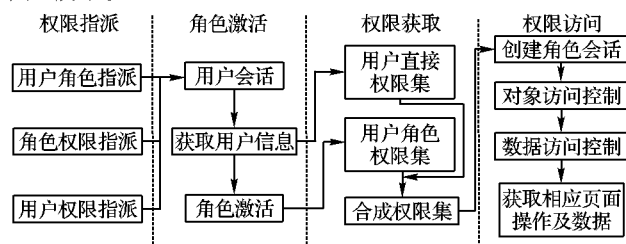


图4 D-RBAC模型访问控制流程

1) 权限指派。根据 $assigned_users_roles$ 、 $assigned_roles_permissions$ 、 $assigned_users_permissions$ 进行用户角色指派、角色权限指派和用户权限指派。

2) 角色激活。根据用户登录信息创建用户会话, 获取用户信息, 然后使用 $active_roles$ 激活用户角色。

3) 权限获取。根据用户信息和用户角色信息获取用户直接权限集和用户角色权限集, 则使用 $users_permissions_compose$ 得到用户的合成权限集。

4) 权限访问。点击系统菜单, 创建角色会话, 根据 $objects_access_control$ 和 $data_access_control$ 实现对象访问控制和数据访问控制, 获取相应页面操作及访问数据。

2.4 模型分析

与其他访问控制模型相比, D-RBAC 模型具有以下几个特点:

1) 精细粒度划分能力。模型中权限控制对象的操作和数据范围都进行了层次划分, 直接定位到菜单页面下不可再分的原子按钮或链接, 而且随着层次划分深度的加大, 模型将具备更细粒度的访问控制能力。

2) 权限分配的灵活性。模型通过授权管理不仅可以控制对象的权限分配给角色, 由角色再传递给用户, 而且还允许将权限直接分配给某些用户, 使得权限分配具有极大的灵活性和适应性。

3) 角色管理的方便性。模型把角色与部门相关联, 将角色定义为部门下的角色, 解决了相同角色在不同部门下的不同访问数据范围和权限分配问题, 而且还减少了单纯意义上的角色数量, 便于角色管理和配置。这样, 产生登录用户动态菜单树时, 首先将用户所在部门与拥有菜单权限的角色所在部门相比较, 再进行角色比较, 访问速度快。

4) 将对象访问控制与数据访问控制相分离, 便于模型的系统实现。对象访问控制和数据访问控制都可以由授权管理灵活主动配置, 方便系统管理和应用。

5) 实用性强。一般部门的组织结构稳定, 角色与部门相关联, 能最大限度保持稳定。而且一旦部门组发生增删、重组, 只需在授权管理时显式地调整与角色相关联的部门即可, 便于实际应用。

3 应用案例

随着我军装备保障信息化建设的不断发展, 基于网络的装备管理信息系统正逐渐成为部队广泛使用的现代管理手段。由解放军理工大学课题组研发的“某装备保障综合管理信息系统”采用了 D-RBAC 进行访问控制, 系统以 J2EE 平台为基础, 采用 MVC 体系结构模式, 以 SQL Server 2005 作为数据库, 在 Struts + Spring + Hibernate 整合框架下实现了访问控制和系统功能。

3.1 系统安全访问要求

本系统是一个典型的军事 MIS, 其安全访问具有如下特点和要求:

1) 操作权限因用户层次不同而不同。不同职位、不同部门的人员具有不同的使用权限, 如部队领导主要负责管理活动的决策与审批, 具体工作由机关各部门来组织和实施。

2) 系统对象因用户角色不同而不同。全局用户(如系统管理员、部队领导)可以操作所有的功能模块, 部门用户能对自己所管理的业务功能进行操作, 而某些功能只有特定角色用户才有权使用。

3) 访问数据因用户部门不同而不同。一个部门的用户不能访问操作另外一个同级别或高级别部门的数据, 但允许高级别的用户访问操作低级别部门的数据。

4) 用户权限管理必须简单、可维护。一方面, 部队人员岗位变动较为频繁, 用户权限必须是动态可调整; 另一方面, 部队系统维护人员一般未参与系统开发, 对系统各功能模块所涉及的数据表不可能有深入了解, 权限管理必须简单可操作。

3.2 基于数据库的权限控制与访问

基于 D-RBAC 模型的思想, 结合功能需求分析, 建立基于部门和角色的用户权限控制的数据库模型, 如图5所示, 图中只给出了各表的主要属性。

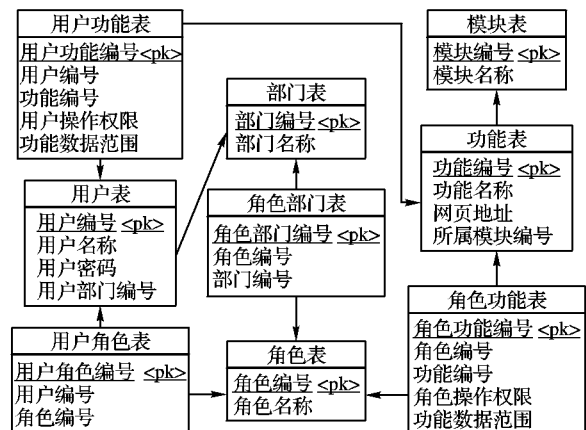


图5 访问控制数据库模型

通过以上的对应关系, 可以根据模型设计的要求找到一个用户到功能具体操作和访问数据范围的映射, 从而达到访问控制的目的。其中, 权限管理主要包括权限配置、权限访问和权限控制。

1) 权限配置。

系统为管理员提供了人员权限设置的可视化界面, 系统管理员首先创建部门、角色和用户, 并为用户分配部门和角

色;然后针对系统每个功能菜单,进行菜单权限设置,如图6所示,包括配置菜单的权限拥有者、菜单操作权限和权限拥有者可访问的数据范围。系统中所有用户的访问界面是统一的,根据具体用户所承担的角色和权限的差异,显示该用户能享有的功能服务和数据。

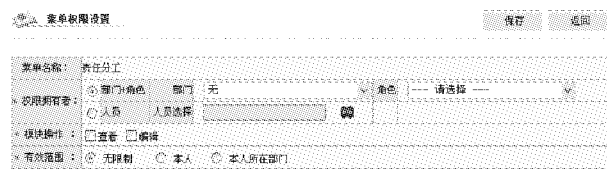


图6 菜单权限设置界面

2) 权限访问。

系统采用单点登录方式,输入用户名和密码信息后,通过自定义的代码实现验证。获取用户的基本信息、用户的角色列表、用户直接的功能列表等信息后,系统根据用户、角色和功能之间的关联关系,计算出用户的权限,在业务逻辑层采用 T-SQL 查询语句实现此服务,并返回权限关系表,保存在 Session 中。

3) 权限控制。

用户登录系统时,验证完登录信息后,系统读取 Session 中保存的用户功能权限列表,根据列表中的所有模块和功能的编号与名称动态生成用户可访问的菜单树。

系统主界面分为左右两个框架,左边是树状的结构,显示用户可以访问的模块和功能,右边是具体的功能页面。当用户点击左框架功能菜单链接或右框架中跳转页面时,在 Page_Load 事件中,根据用户权限列表中所拥有的该页面的操作权限和可访问的数据范围,显示相应的操作按钮和数据结果,实现细粒度访问控制。

3.3 应用效果

基于 D-RBAC 模型的某装备保障综合管理信息系统,把系统角色与组织机构的各部门相关联,通过顶层部门管理所有装备的全面装备保障信息,中层部门管理所辖机构的大部分装备保障信息和基层部门管理本单位的日常装备保障信息,灵活有效地实现了对单位全部装备和人员的分级精确管控和责权利精确划分,取得了很好的应用效果。

(上接第 522 页)

4 结语

本文讨论了基于提升小波和 DCT 的音频水印算法,该算法有以下特点:1) 透明性良好,嵌入图像水印时在听觉上没有影响到人耳的听觉质量;2) 图像水印对重采样、加噪声、重量化、随机剪切等常见的攻击均表现出了很强的鲁棒性;3) 水印提取时不需要原始音频信号和二值图像,是一种盲水印算法;4) 算法的信号处理时间有很明显的提高,因此更有利于硬件实现。

参考文献:

- [1] 王宏霞,范明泉. 基于质心的混合域半脆弱音频水印算法[J]. 中国科学:信息科学, 2010, 40(2): 313-326.
- [2] MOULIN P, KOETTER R. Data hiding codes [J]. Proceedings of the IEEE, 2005, 93(12): 2083-2126.
- [3] 廖琬明,张玉贤,李东晓,等. 基于小波变换的脆弱鲁棒双音音频水印[J]. 浙江大学学报:工学版, 2009, 43(4): 721-726.
- [4] KO B S, NISHIMURA R, SUZUKI Y. Time-spread echo method for

4 结语

权限管理是信息系统的重要组成部分,权限管理的技术和策略对系统的信息安全影响很大。本文通过对 RBAC 模型的分析,结合信息系统访问控制要求,提出了基于部门和角色的细粒度访问控制模型,把角色和部门相关联,权限可以直接分配到角色或用户,通过授权管理,把对象访问控制和数据访问控制灵活配置,实现了访问的精确控制。该改进方法已经经过实际项目的应用检验,可广泛应用于 MIS 的权限管理。

参考文献:

- [1] 杨亚平,李伟琴,刘怀宇. 基于角色的细粒度的访问控制系统的研究与实现[J]. 北京航空航天大学学报, 2001, 27(2): 178-181.
- [2] 吴江栋,李伟华,安喜锋. 基于 RBAC 的细粒度访问控制方法[J]. 计算机工程, 2008, 34(20): 52-54.
- [3] SNYDER L. Formal models of capability-based protection systems [J]. IEEE Transactions on Computers, 1981, 30(3): 172-181.
- [4] FERRAILOLO D, KUHN R. Role-based access control [C]// Proceedings of 15th National Computer Security Conference, Washington, DC: IEEE, 1992: 554-563.
- [5] OH S, PARK S. Task-Role-Based-Access-Control (TRBAC): An improved access control model for enterprise environment [C]// Database and Expert Systems Applications, LNCS 1873. Berlin: Springer, 2000: 264-273.
- [6] 陈娟娟,程西军,汪利虎. 基于角色的差异主体协同访问控制模型[J]. 计算机应用, 2009, 26(6): 109-110.
- [7] 李细雨,韩建民,于娟,等. 基于粒逻辑的扩展 RBAC 模型[J]. 浙江师范大学学报:自然科学版, 2009, 32(3): 304-307.
- [8] 王伟然,张淘,范玉顺. 业务过程管理中基于组织和角色语义的访问控制[J]. 信息与控制, 2009, 38(3): 276-280.
- [9] SANDHU R, FERRAILOLO D, KUHN R. The NIST model for role based access control towards a unified standard [C] // Proceedings 5th ACM Workshop on Role Based Access Control. New York: ACM, 2000: 47-63.
- [10] RAVIS, EDWARD C. Role-based access control models [J]. IEEE Computer, 1996, 29(2): 38-47.
- [11] 潘德锋,徐少平,梁庆中,等. 基于操作的 MIS 多级授权模型的实现[J]. 计算机应用, 2003, 23(21): 100-103.
- [12] 倪冬英,张晓丽. 基于 RBAC 的用户权限管理的设计与实现[J]. 济南大学学报:自然科学版, 2010, 24(2): 167-171.

digital audio watermarking [J]. IEEE Transactions on Multimedia, 2005, 7(2): 212-221.

- [5] 林樾渺. 提升格式下的小波变换在图像处理中的算法研究[D]. 西安:西安电子科技大学, 2005.
- [6] 陈金儿,王让定,王晓丽. 数字音频双重水印算法[J]. 宁波大学学报, 2006, 19(1): 54-58.
- [7] 王让定,徐达文. 基于提升小波的多重数字音频水印[J]. 电子与信息学报, 2006, 28(10): 1820-1826.
- [8] CLAYPOOLE R L, DAVIS G M, SWELDENS W, et al. Nonlinear wavelet transforms for image coding via lifting [J]. IEEE Transactions on Image Processing, 2003, 12(12): 1449-1459.
- [9] 王向阳,杨红颖. 一种新的自适应量化数字音频水印算法[J]. 声学技术, 2004, 23(2): 117-121.
- [10] 黄继武, SHI YUNQ, 程卫东. DCT 域图像水印: 嵌入对策和算法[J]. 电子学报, 2000, 28(4): 57-60.
- [11] COX I J, KILIAN J, LEIGHTON F T, et al. Secure spread spectrum watermarking for multimedia [J]. IEEE Transactions on Image Processing, 1997, 6(12): 1673-1687.