(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104994411 A
(43)申请公布日 2015.10.21

(21)申请号 201510364658.5

(22)申请日 2015.06.29

(71)申请人 北京国泰信安科技有限公司
地址 100876 北京市海淀区西土城路10号北邮科技大厦1208室

(72)发明人 马兆丰 黄勤龙 许艳萍 邱宝林 王真

(51)Int.Cl.
H04N 21/266(2011.01)
H04N 21/2347(2011.01)
H04N 21/254(2011.01)
H04N 21/835(2011.01)
H04N 21/854(2011.01)

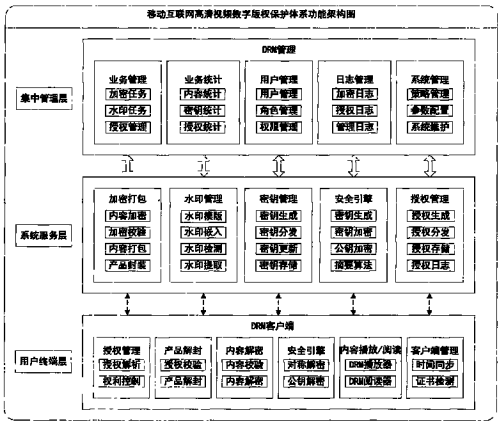
权利要求书1页 说明书6页 附图3页

(54)发明名称

一种移动互联网高清视频数字版权保护体系

(57)摘要

一种移动互联网高清视频数字版权保护体系，是高清视频在移动互联网中生产、传输、交易、使用过程中的各方权利进行明确的定义、辨别、交易、保护、监控和跟踪的全面解决方案。功能包括加密打包、密钥管理、安全引擎、授权管理、DRM管理系统和DRM移动客户端等，实现多种格式的高清视频，完成高清视频内容的加密和产品封装，生成相应的高清视频使用授权，通过移动互联网投递到移动用户终端，在移动用户终端的客户端播放器对受保护的内容经过授权认证后，通过电脑、移动终端等设备播放应用，并支持对高清视频播放的控制管理。这种保护方式保障了高清视频可控可管地传播和有效利用，促进了信息环境健康发展。



CN 104994411 A

1.移动互联网高清视频数字版权保护体系，其特征在于，包括：

(1) 支持对多种格式的高清视频内容进行加密保护，如 mkv、rmvb、avi、MP4、flv、wmv 等；

(2) 支持的国际主流加密算法，如 AES、RSA-1024/2048 公钥算法、摘要算法 SHA-1 等；

(3) 支持多种加密方式，如多线程加密、任务化加密、批量内容加密、内容加密校验等；

(4) 支持多种授权策略，如内容使用的时间限制，包括开始时间、结束时间和累计时长的限制；内容使用的次数限制；一个内容多个授权；授权与用户和设备绑定；用户域和设备域，支持限制用户域内用户的数量和设备域内设备的数量；用户查看本地授权权限信息，包括许可、约束、优先级等；一次申请，多次获取授权；支持反授权。

2.移动互联网高清视频数字版权保护移动客户端，其特征在于，包括：

(1) 支持主流的移动智能终端操作系统，如 Android，IOS 及 Windows Phone，并兼容系统的各个版本；

(2) 支持适配于移动智能终端各种屏幕尺寸，从小尺寸 4.0 到大尺寸 7.0；

(3) 支持对高清视频内容流畅的播放控制，如开始、暂停、快进、后退、跳跃、全屏、悬浮窗等。

一种移动互联网高清视频数字版权保护体系

技术领域

[0001] 本发明涉及数字出版领域，主要用于在移动互联网的环境下采用一种数字版权保护 (DRM) 体系实现对高清视频可控可管的传播和保护。

背景技术

[0002] 数字出版以其数字化制作，网络化传输、高效、低成本的优点成为出版的发展潮流。随着信息社会的快速的发展，高清视频在互联网媒体信息传播方面使用的越来越广泛，个人不但可以快速方便的从多种信息通路获得高清视频，同时也具有对其大规模非法复制、传递、销售的能力，极大的损害了版权人的利益，抑制了高清视频数字出版的快速发展。

[0003] 数字版权保护技术是对高清视频在信息网络中生产、传输、交易、使用过程中的各方权利进行明确的定义、辨别、交易、保护、监控和跟踪的全面解决方案，成为数字出版不断发展的基本保障之一。

[0004] 多种格式的高清视频，经过版权加密后，生成有效的授权证书，通过移动互联网投递到用户终端，在用户终端的客户端对受保护的内容经过授权认证后，用户通过电脑、移动终端等设备浏览应用。保障了高清视频广泛传播和有效利用，促进了信息环境健康发展。

[0005] 本发明在国内外版权保护标准和规范的基础上，研制、开发一套适合于移动互联网环境下的高清视频版权保护软件系统，包括内容加密、密钥管理、安全引擎、授权管理和版权保护管理等核心功能，实现对数字内容的版权保护，支持移动互联网环境下的内容发行和授权分发。

发明内容

[0006] 一种移动互联网高清视频数字版权保护体系的功能包括加密打包、密钥管理、安全引擎、授权管理、DRM 管理系统和 DRM 移动客户端等，完成内容加密和产品封装，同时向用户分发产品使用的授权，在移动终端用户获得合法授权，实现对产品的解封、内容的解密、内容的播放和可控使用。

[0007] 加密打包使用密钥管理系统提供的内容密钥对高清视频进行加密，然后对加密后的视频内容计算内容摘要。内容打包就是加密打包系统按照相关格式对加密后的视频内容打包。最后将受 DRM 保护的封装高清视频产品，通过移动互联网推送给用户。

[0008] 密钥管理负责管理 DRM 系统中使用的各种密钥，并维护高清视频内容与加密密钥的映射关系。

[0009] 安全引擎系统提供各种主流的加解密算法，如 DES、RSA、国密等，并进行内容加密密钥加密、数字签名、身份验证等加解密运算，安全引擎系统支持与 PKI/PMI 系统集成。

[0010] 授权管理负责向 DRM 移动终端用户提供授权的生成和下载服务，包括授权生成、授权分发、授权策略管理、授权日志管理等模块。

[0011] DRM 管理分成四部分 :业务管理，管理加密任务和授权等 ;业务统计，主要对内容、密钥和授权进行统计等 ;用户管理，主要进行用户、角色和权限管理等 ;日志管理，主要管

理日志、授权日志和加密日志等；系统管理，主要进行策略管理、参数配置和系统维护等的管理。

[0012] DRM 移动客户端运行在移动智能终端，执行与高清视频使用相关的授权和约束，通过 DRM 高清视频播放器控制用户对高清视频内容的使用。DRM 移动客户端获取合法授权后，首先验证授权的完整性和可靠性，验证通过后，使用利用高清视频加密密钥对内容进行解密，并根据授权中的权利信息控制用户对内容的使用控制。

附图说明

[0013] 图 1 移动互联网高清视频数字版权保护体系功能架构图

[0014] 图 2 移动互联网高清视频 DRM 移动客户端功能架构图

[0015] 图 3 移动互联网高清视频数字版权保护体系实现效果图

[0016] 图 4 移动互联网高清视频 DRM 移动客户端实现效果图

具体实施方式

[0017] 1. 加密打包

[0018] (1) 内容加密

[0019] 加密打包系统接收到高清视频内容加密请求及相关参数后，向密钥管理系统请求内容密钥，使用内容密钥对需要加密的内容文件进行加密，同时按照规定的格式对加密后的高清视频内容进行打包。

[0020] (2) 加密校验

[0021] DRM 系统对加密后的数据进行解密，计算解密后数据的 Hash 值，并与原始文件的 Hash 值做比较，以校验原始文件是否被正确加密。

[0022] (3) 内容打包

[0023] 加密打包系统把加密后的内容，按照规定的格式对加密后的内容进行打包。

[0024] (4) 产品封装

[0025] 加密打包系统接收到高清视频产品封装请求及相关参数后，向密钥管理系统请求产品密钥，使用产品密钥对产品里内容的内容密钥进行加密，同时按照规定的格式对加密后的内容密钥进行封装。

[0026] 2. 密钥管理

[0027] (1) 密钥生成

[0028] 在系统初始化阶段，密钥管理系统向安全引擎系统发送服务系统公私钥对生成指令，从安全引擎系统得到服务系统公钥。密钥管理系统向 PKI 系统申请建立公钥证书，获得服务系统的公钥证书。

[0029] 根据内容加密系统的请求，密钥管理系统向安全引擎系统发送内容密钥和产品密钥生成指令。密钥管理系统接收安全引擎系统返回的内容密钥和产品密钥，并发送给内容加密系统。

[0030] (2) 密钥分发

[0031] 产品密钥使用用户公钥进行加密，封装在授权中分发到用户终端，终端只有使用用户私钥才能进行解密，这样一方面确保终端用户能够在任何时间快速得到产品密钥，另

一方面禁止非法用户盗取产品密钥。

[0032] (3) 密钥更新

[0033] 密钥管理系统可以根据业务需要更新产品密钥，当产品密钥在用户终端泄漏时，也需要密钥管理系统进行密钥更新。

[0034] (4) 密钥存储

[0035] 内容密钥和产品密钥使用密钥管理系统内部的保护密钥加密后存储在密钥管理系统中。保护密钥由安全引擎系统生成，存储在安全引擎系统。密钥保护算法采用 128 位 AES。

[0036] 3. 安全引擎

[0037] 安全引擎向密钥管理系统提供各种加解密服务，并进行签名 / 验证、内容加密密钥加密等加解密运算。

[0038] 安全引擎系统支持的算法包括 :RSA 算法（含公私钥对生成算法、加解密算法、签名 / 认证算法）、对称密钥加解密算法、Hash 算法、随机数生成算法等。

[0039] (1) 密钥生成

[0040] DRM 系统到 PKI 系统注册的过程中，密钥管理系统请求安全引擎生成服务系统公私钥对，采用 RSA 算法，公钥模长 1024 位。安全引擎使用根密钥加密服务系统私钥，并保存服务系统私钥的 Hash 值，以保证密钥的机密性和完整性。

[0041] 根据密钥管理系统的请求生成内容密钥和产品密钥，并返回给密钥管理系统。

[0042] (2) 密钥加密

[0043] 安全引擎系统生成保护密钥，对内容密钥和产品密钥进行加密后将密文的内容返回给密钥管理系统，供密钥管理系统存储。

[0044] 安全引擎系统接收到密钥管理系统的获取产品密钥请求（包括加密的产品密钥、用户公钥证书及 PKI 系统的公钥）后，使用保护密钥还原出产品密钥，使用用户的公钥加密产品密钥，然后将加密后的产品密钥返回给密钥管理系统。

[0045] (3) 公钥加密

[0046] 安全引擎系统接收到密钥管理系统的获取产品密钥请求（包括加密的产品密钥、用户公钥证书及 PKI 系统的公钥）后，使用保护密钥还原出产品密钥，使用用户的公钥加密产品密钥，然后将加密后的产品密钥返回给密钥管理系统。

[0047] (4) 数字签名

[0048] 签名功能用于实现授权权利信息的签名，验证功能用于服务系统与客户端信息交互过程中用户身份的验证。对授权权利信息签名时使用服务系统的私钥，验证用户身份时使用用户的公钥。

[0049] 4. 授权管理

[0050] (1) 授权生成

[0051] 授权生成模块负责根据用户的订购信息，包括 :用户标识、设备标识、产品标识以及权限信息等。

[0052] 授权生成模块收到授权分发模块的授权提取请求，包含设备绑定信息、用户公钥证书及用户签名信息，将用户公钥证书及用户签名信息发送到安全引擎系统请求验证用户身份，验证通过后，查找到产品标识，然后将产品标识发送给密钥管理系统，获得密钥管理

系统返回的经过加密后的产品密钥后，基于授权权利描述语言生成待签名的授权，再将其发送给安全引擎系统请求签名，在得到安全引擎系统返回的签名信息后，生成最终的授权文件，并发送到授权管理和授权分发模块。

[0053] (2) 授权分发

[0054] 授权分发模块将最终的授权文件通过移动互联网链路分发到 DRM 客户端。

[0055] (3) 授权存储

[0056] 授权存储模块将授权及相关信息存储到数据库。

[0057] (4) 授权日志

[0058] 授权日志管理模块建立授权生成、授权分发、授权使用等日志，日志内容包括：授权标识、用户标识、内容标识、生成时间、分发时间等。

[0059] 5. DRM 系统管理

[0060] (1) 业务管理

[0061] 业务管理模块主要负责内容加密情况、授权分发与使用情况的统计、分析。主要包括以下功能：

[0062] ➢加密任务

[0063] 主要负责对授权信息进行查询，包括设备绑定信息、用户公钥证书及用户签名信息等。

[0064] ➢授权管理

[0065] 根据媒体内容的来源不同，对授权进行分类统计。

[0066] (2) 业务统计

[0067] ➢内容统计

[0068] 包括按内容来源的统计、按内容投放时间的统计、按内容种类的统计等。

[0069] ➢密钥统计

[0070] 包括按内容密钥的统计、按产品密钥的统计、按域密钥的统计、按照时间段生成内容密钥的统计、按照时间段生成产品密钥的统计等。

[0071] ➢授权统计

[0072] 包括按内容的授权统计、按内容来源的授权统计、按指定时间段生成授权的统计、按照时间段分发授权的统计等。

[0073] (3) 用户管理

[0074] ➢用户管理

[0075] 包括加密打包系统操作人员的管理、授权管理系统操作人员的管理等。

[0076] ➢角色管理

[0077] 包括角色的创建、角色的修改、角色的删除、角色的查询等。

[0078] ➢权限管理

[0079] 包括权限的分配、权限的删除、权限的修改等。

[0080] (4) 日志管理

[0081] ➢加密日志

[0082] 包括内容加密日志、内容密钥加密日志、产品密钥加密日志等。

[0083] ➢授权日志

[0084] 包括授权申请日志、授权生成日志、授权分发日志。

[0085] ➢管理日志

[0086] 包括业务管理日志、用户管理日志、系统管理日志等。

[0087] (5) 系统管理

[0088] DRM 系统管理主要完成与系统用户、数据、操作有关的业务系统管理，包括对用户角色的设置功能，对客户按照业务的定制情况进行分组管理；系统事件及用户事件的日志管理；系统的功能维护；系统的运行状态记录。

[0089] 主要功能如下：

[0090] ➢策略管理

[0091] 包括授权申请策略、授权生成策略、授权分发策略、内容发行策略等。

[0092] ➢参数配置

[0093] 包括 DRM 服务系统参数配置、系统参数配置等。

[0094] ➢系统维护

[0095] 包括系统维护计划的创建、系统维护计划的删除、系统维护计划的修改、自动记录系统运行状态和系统运行环境参数、系统自动报警和纠错。

[0096] 6.DRM 移动客户端

[0097] 移动互联网高清视频 DRM 移动客户端包括 DRM 播放器 / 阅读器模块、产品解封模块、内容解密模块、安全引擎模块、授权管理模块、客户端管理等六个功能模块，各个模块的功能如下：

[0098] (1) 授权管理

[0099] 实现对授权进行权利解析，另外，还对授权的有效性进行判断和控制。授权管理单元包括授权解析和控制两个功能模块。DRM 客户端调用授权管理模块判断用户是否有权限播放受 DRM 保护的文件。

[0100] (2) 产品解封

[0101] 通过 DRM 客户端调用产品解封模块恢复出产品密钥，然后使用产品密钥解密出内容密钥。

[0102] (3) 内容解密

[0103] 通过 DRM 客户端调用内容解密模块恢复出内容密钥，然后对加密后的文件进行解密，内容解密单元支持 128 位的 AES 算法。

[0104] (4) 安全引擎

[0105] 负责存储用户数字证书和公私钥对等关键信息，并调用相关加解密算法，进行数字签名、身份认证、Hash 值计算、解密内容密钥等操作。安全管理单元支持 1024 位的 RSA 算法和计算 Hash 值的 SHA-1 算法，通过软件实现。

[0106] (5) 内容播放 / 阅读

[0107] 通过位于控制层和播放层之间的 DRM 客户端实现对内容的播放 / 阅读控制，包括检测授权状态（调用授权管理模块，检测内容当前对应的授权的有效性）、控制授权使用、媒体内容解析（解析受DRM保护的文件格式，获取待解密的加密数据块）、记录授权日志、解密媒体内容（调用内容解密模块，解密待解密的加密数据块）等功能。

[0108] (6) 客户端管理

[0109] 实现日志管理（记录授权的使用日志）、时间同步（与服务器端同步时间）、计数器（记录用户播放文件的次数）等功能。

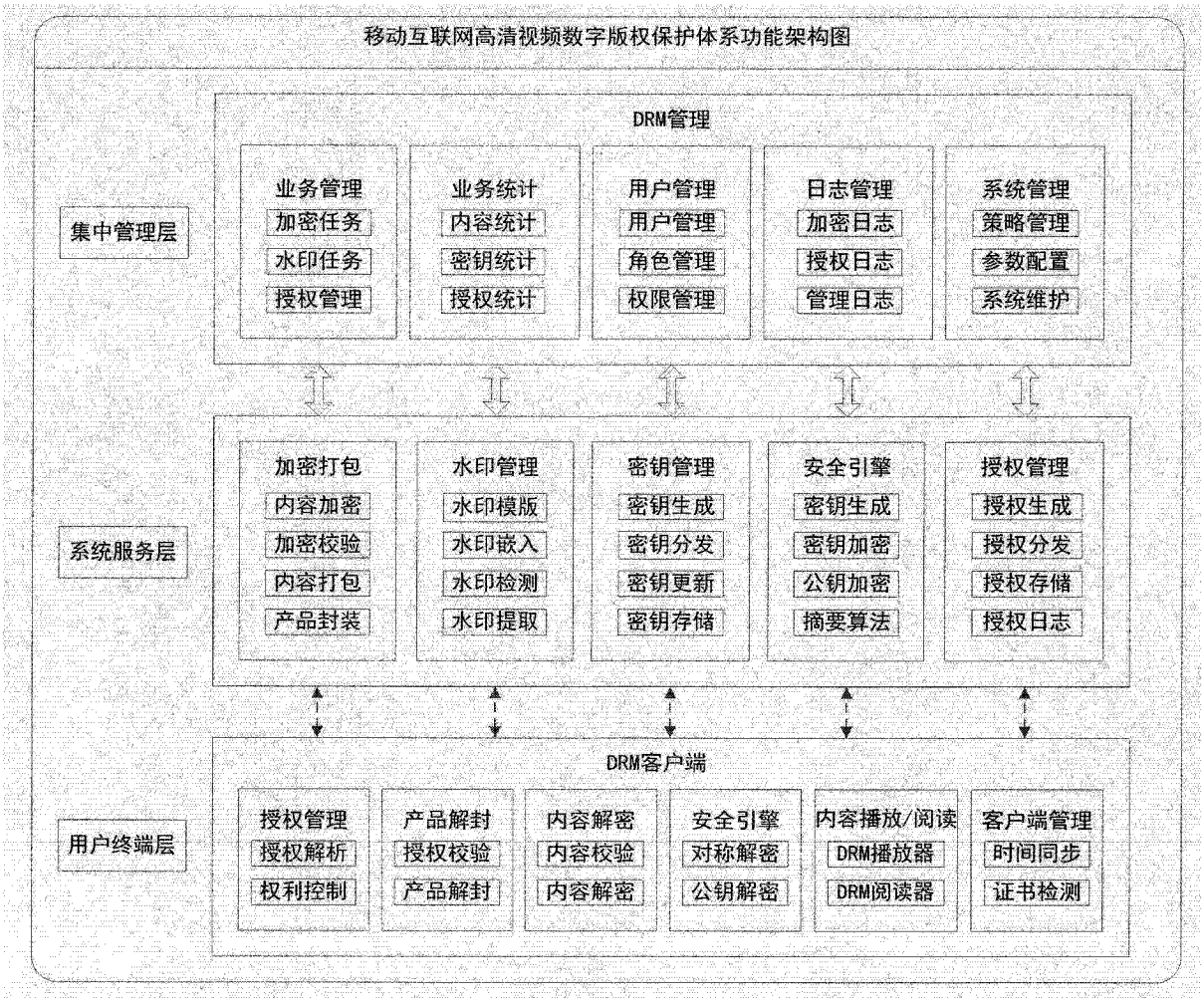

移动互联网高清视频数字版权保护体系功能架构图
DRM管理
集中管理层
业务管理
加密任务
水印任务
授权管理
业务统计
内容统计
密钥统计
授权统计
用户管理
用户管理
角色管理
权限管理
日志管理
加密日志
授权日志
管理日志
系统管理
策略管理
参数配置
系统维护
系统服务层
加密打包
内容加密
加密校验
内容打包
产品封装
水印管理
水印模版
水印嵌入
水印检测
水印提取
密钥管理
密钥生成
密钥分发
密钥更新
密钥存储
安全引擎
密钥生成
密钥加密
公钥加密
摘要算法
授权管理
授权生成
授权分发
授权存储
授权日志
DRM客户端
用户终端层
授权管理
授权解析
权利控制
产品解封
授权校验
产品解封
内容解密
内容校验
内容解密
安全引擎
对称解密
公钥解密
内容播放/阅读
DRM播放器
DRM阅读器
客户端管理
时间同步
证书检测

图 1

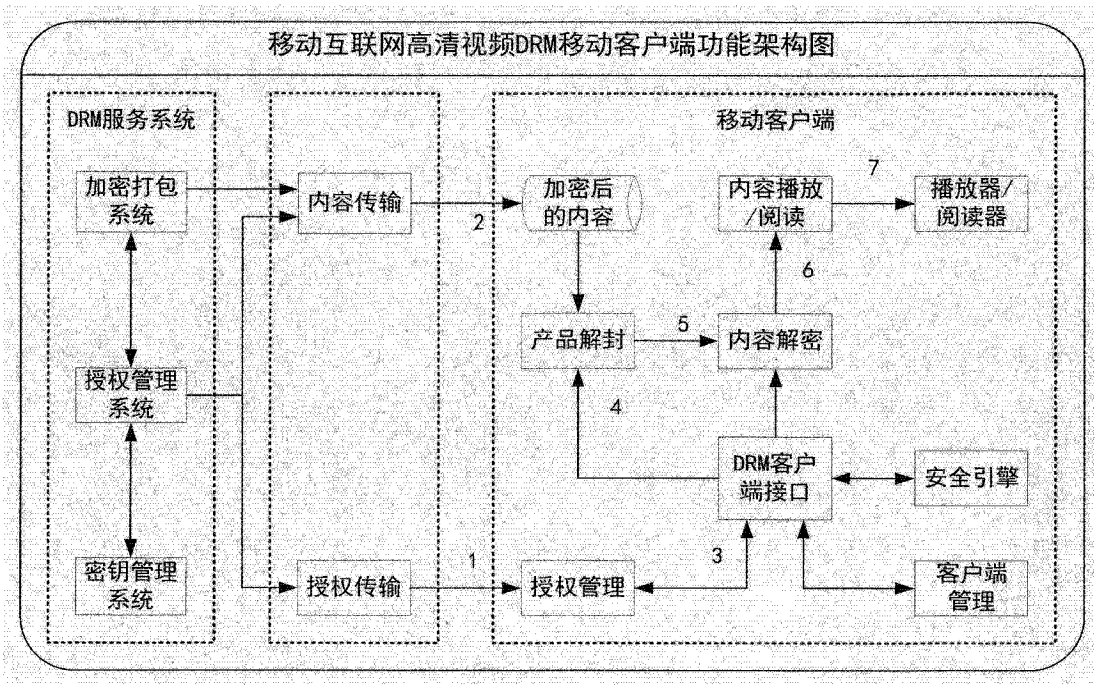

移动互联网高清视频DRM移动客户端功能架构图
DRM服务系统
加密打包系统
授权管理系统
密钥管理系统
内容传输
授权传输
移动客户端
加密后的内容
产品解封
内容播放/阅读
播放器/阅读器
内容解密
DRM客户端接口
安全引擎
授权管理
客户端管理
1
2
3
4
5
6
7

图 2

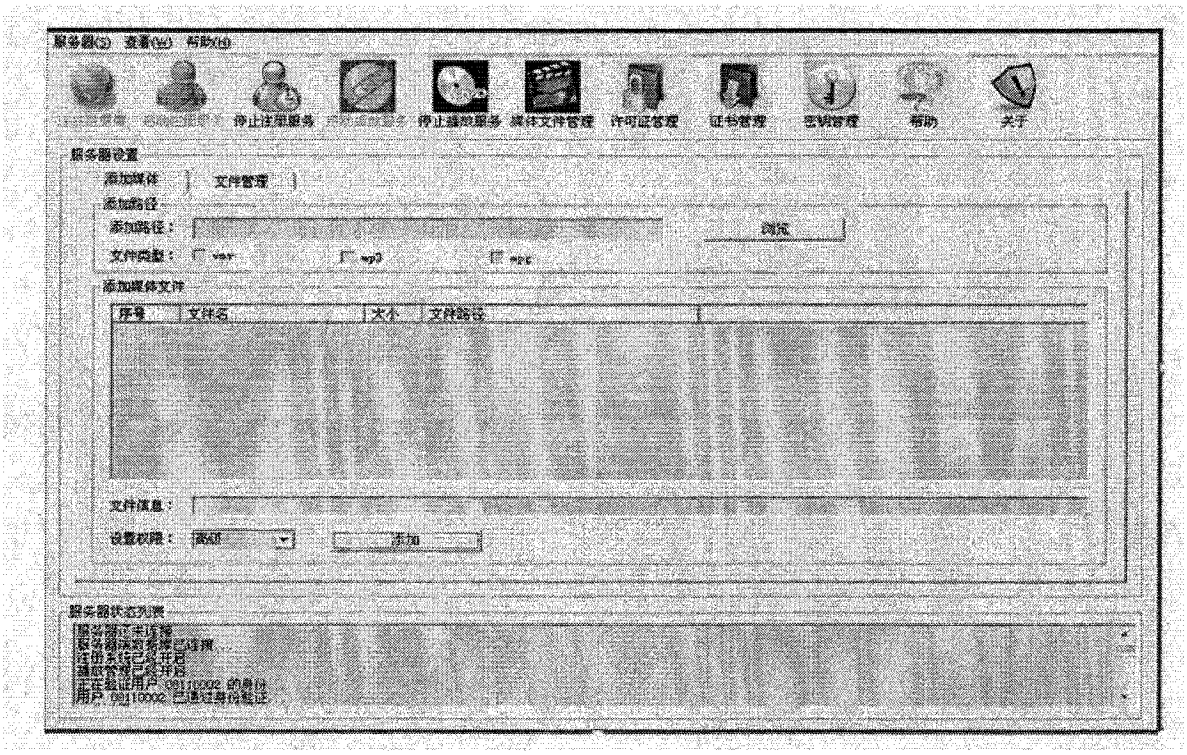


图 3

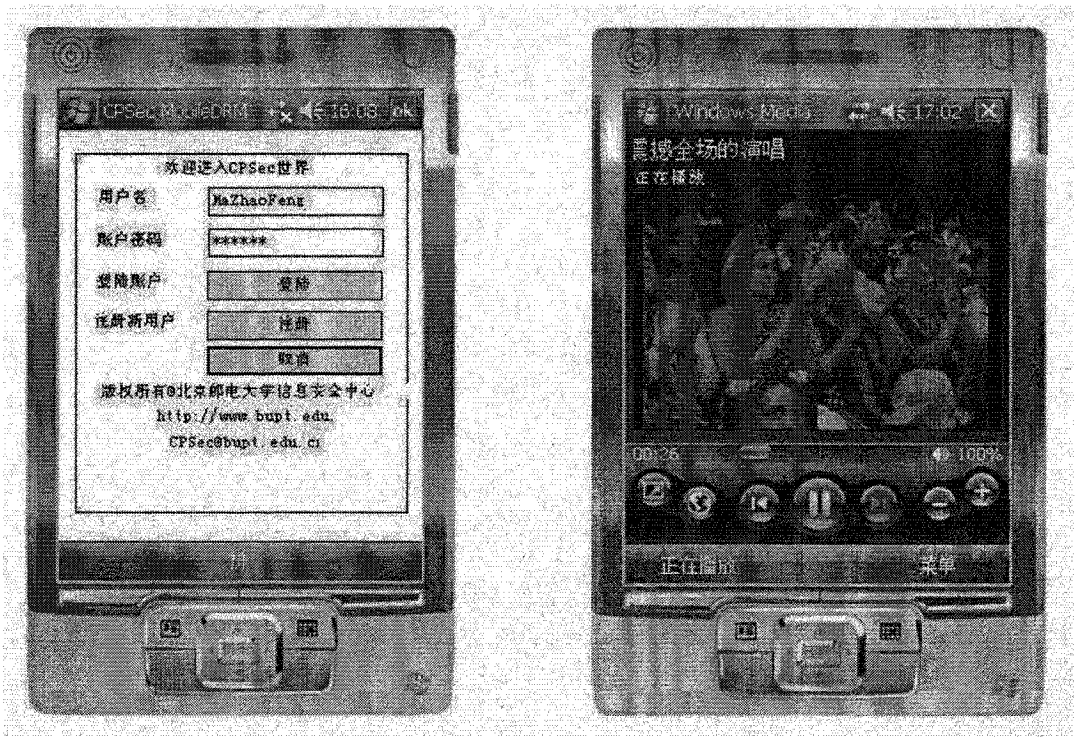

欢迎进入CPSec世界
用户名
MaZhaoFeng
账户密码
******
登陆账户
登陆
注册新用户
注册
取消
版权所有@北京邮电大学信息安全中心
http://www.bupt.edu.
CPSec@bupt.edu.cn
Windows Media
17:02
震撼全场的演唱
正在播放
00:26
100%
菜单

图 4