一种适用于 IPTV 的数字权限管理系统

李新国[1,2]，葛建华[1]，冯利民[1]，郭 辉[1]

(1. 西安电子科技大学 综合业务网理论与关键技术国家重点实验室，陕西 西安 710071；
2. 中国人民解放军洛阳外国语学院 数学教研室，河南 洛阳 471003)

摘要：为了解决阻碍 IPTV 系统发展的数字内容盗版问题，设计了一种适用于 IPTV 的数字权限管理系统. 给出了系统中视频文件加解密、用户端许可证获取和使用等关键模块的实现方案. 通过在内容加密服务器端和用户端同时采用许可证机制，使系统实现起来更为简捷；用户端的私钥和使用记录等机密数据在智能卡内部存储和操作使系统具有更高的安全性.

关键词：数字权限管理；网络电视；许可证机制

中图分类号：TP309 **文献标识码**：A **文章编号**：1001-2400(2006)06-0943-06

A digital rights management system suitable for IPTV

LI Xin-guo[1,2], *GE Jian-hua*[1], *FENG Li-min*[1], *GUO Hui*[1]

(1. State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China; 2. Dept. of Mathematics, PLA Foreign Language Institute, Luoyang 471003, China)

Abstract: A digital rights management system is presented to prevent the pirates from pirating the digital content of IPTV. The schemes for realizing the key modules of the system such as video files encryption/decryption at the servers terminal and licenses acquiring/operating at the clients terminal are also proposed. The system is designed to be very concise by employing the license mechanism both in the content encryption server and in the clients. The secret data of the clients like private keys and operation logs are stored and operated in the inner of the smartcard, by which our system gets its characteristic of higher security.

Key Words: digital rights management; IPTV; license

计算机网络技术的发展使得音频、视频等数字产品通过网络销售成为可能. 对生产数字产品的商家来说，产品通过网上交易可以带来较大的成本缩减；在线消费的便捷性也给消费者带来极大的便利. 实现数字产品网上交易这种商业模式的最大障碍就是盗版行为，这是由数字产品的数字化特性决定的. 如果不采取任何有效的措施，盗版者可以将数字产品精确复制并大面积传播，版权所有者将遭受巨大的经济损失. 数字权限管理(Digital Rights Management，DRM)正是为了有效实现这种商业模式而设计的系统.

文献[1]对 DRM 做如下定义："DRM 是在一系列条款和条件下，在数字产品的整个存在周期内对其进行持续管理."数字产品的"存在周期"大致包括制作、传输和消费 3 个阶段. 从技术角度上看，DRM 的"持续管理"主要体现在后两个阶段. 身份认证、数据加密和防篡改软硬件技术是 DRM 系统实现"持续管理"的核心技术. DRM 系统使得消费者只能在满足许可证规定的条件下，按照许可证许可的权限对数字产品进行消费，从而最大限度地保护数字产品制作者的商业利益.

图 1 是简化的 DRM 系统模型. 一般地，DRM 系统由 6 部分组成：源端、目的端、计费中心、数字内容、许可证和信任体系. 源端通常是为目的端提供数据的计算机系统，目的端是使用数据的消费电子产品，如数字电视、移动电话等. 源端为目的端提供的数据有数字内容和许可证两类，数字内容是商家和消费者之间交易的数字产品，如音视频文件、电子图书等；许可证详细定义了目的端可以在什么条件下对数字内容进行什么

收稿日期：2005-12-18

基金项目：国家自然科学基金重点项目(60332030，60496316)资助

作者简介：李新国(1976-)，男，西安电子科技大学博士研究生.

类型的操作;数字内容通常是加密的,解密密钥使用目的端的公钥加密后放在许可证中;目的端通过购买许可证来获取解密密钥,购买许可证的费用由计费中心管理. DRM 系统中不同设备和组件之间的通信需要一个信任体系来支撑. 一个合适的信任体系可以保证源端的确有权发放许可证;保证许可证的确是可靠的;保证目的端用户在购买内容使用权限时正常交费;也可以保证目的端在使用内容时的确遵循许可证所规定的权限和条件.

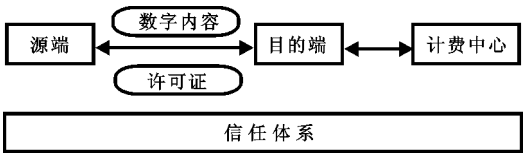

图 1 简化的 DRM 系统模型

笔者重点研究了 IPTV 系统中 H.264 视频内容[2]点播和下载业务的数字权限管理技术. 从 IPTV 实际运营的角度出发,设计了一种适用于 IPTV 的数字权限管理系统,给出了系统中 H.264 视频文件加解密、用户端许可证获取和使用等关键模块的实现方案.

1 具有 DRM 功能的 IPTV 系统结构

在 IPTV 系统中实现 DRM 功能需要系统前端增加 DRM 服务器和内容加密服务器,并且需要机顶盒软硬件的支持. 下面通过阐述 DRM 系统各组件与 IPTV 系统相关组件的关系来描述所设计的 DRM 系统.

1.1 系统结构

如图 2 所示,具有 DRM 功能的 IPTV 系统前端主要包括用户管理服务器、DRM 服务器、内容加密服务器、流媒体服务器和内容下载服务器. IPTV 系统的用户端是具有联网功能的机顶盒,机顶盒的身份由智能卡惟一标识. 其中,DRM 服务器和内容加密服务器是两个相对独立的 DRM 系统模块,DRM 的功能实现更多地体现在机顶盒设备中. 系统中各模块的功能和相互关系如下:

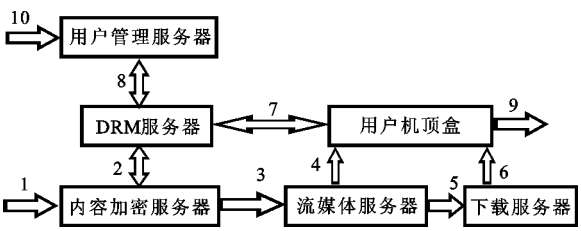

图 2 具有 DRM 功能的 IPTV 系统结构

● 内容加密服务器的功能是将获得的原始内容文件(标号 1)加密并上传到流媒体服务器(标号 3),内容加密服务器加密文件所使用的内容密钥从 DRM 服务器获得(标号 2).

● 流媒体服务器的功能是将加密后的内容文件封装成合适的文件格式,并通过实时传输协议 RTP 将数据以流的形式传给用户端机顶盒(标号 4),或者上传到下载服务器(标号 5)供用户端下载.

● 下载服务器提供用户对加密内容的完整下载服务(标号 6).

● 机顶盒设备的功能是接收流媒体服务器的 SDP 和 RTP 数据[3]、下载数字内容、从 DRM 服务器购买合法的许可证(标号 7)、解密并播放内容(标号 9).

● DRM 服务器是 DRM 系统的核心,其主要功能是管理系统中数字内容的加密密钥、通过公钥密码的方式验证内容加密服务器和用户机顶盒的合法性、发放内容许可证. 在认证机顶盒合法性时,DRM 服务器需要询问用户管理服务器该用户账户的合法性;在许可证发出以后,DRM 服务器需要给用户管理服务器一个通知(标号 8).

● 用户管理服务器的功能主要是管理用户的账户数据. 包括用户账户注册、交费、计费等. 注册和交费功能可以通过常规的办法实现(标号 10),计费功能由 DRM 服务器协助完成.

1.2 信任体系

首先,假设 IPTV 前端系统中的用户管理服务器、DRM 服务器和内容加密服务器对数字内容供应商来说是可信的. 内容供应商和 IPTV 运营商之间的商业操作可以建立这一层次的信任关系. 在信任的基础上,内容供应商就可以将原始数字内容交给 IPTV 运营商出售.

为了建立 IPTV 前端系统和终端机顶盒之间的信任关系,需要在 DRM 系统之外建立公钥基础设施(PKI 如图 3). PKI 中的根 CA 是 DRM 系统信任体系的中心,根 CA 向若干个二级 CA 颁发公钥证书,二级 CA 又为系统中的 DRM 服务器、内容加密服务器和机顶盒颁发公钥证书. 这样内容加密服务器和 DRM 服务器之间、用户机顶盒和 DRM 服务器之间就可以通过交换公钥证书执行认证协议,从而建立信任关系.

机顶盒的公钥证书和相应的私钥存放在智能卡中,智能卡是 DRM 系统的用户端安全硬件,存储在智能卡中的密钥等少量机密数据对用户是不可见的. 对智能卡的安全性假设已经广泛应用于数字电视的条件接入系统中[4, 5]. 用户端安全硬件是 DRM 系统的重要环节,DRM 系统借助此硬件在用户端判断该用户的使用权限并执行许可证中的使用规则.

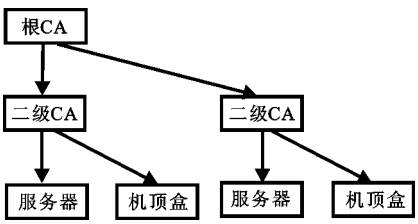

图 3　DRM 系统中的 PKI 模型

1.3　系统工作原理

原理上,具有 DRM 功能的 IPTV 系统的运行包括如下 4 个阶段.

(1)信任关系建立阶段——DRM 服务器和内容加密服务器在本地存储各自的公钥证书、相应的私钥、根 CA 公钥证书以及二级 CA 公钥证书;机顶盒智能卡制造商在每张智能卡中预埋智能卡公钥证书、相应私钥、根 CA 公钥证书以及二级 CA 公钥证书.

(2)用户注册交费阶段——机顶盒用户以用户名口令的方式向用户管理服务器注册一个账户,并向账户中预存一定金额的费用.

(3)数字内容准备阶段——内容加密服务器将 H. 264 内容按预定的格式加密,加密后的文件上传到流媒体服务器和下载服务器供用户点播和下载.

(4)内容消费阶段——当机顶盒播放器程序播放加密的点播内容或者加密的下载内容时,播放器自动链接到 DRM 服务器去获取有效的许可证,用户管理服务器通过 DRM 服务器认证具体用户的账户并计费.

2　系统主要模块实现方案

DRM 系统的主要功能模块包括内容加密服务器上的内容加密模块、DRM 服务器上的许可证发放模块、用户端的许可证申请和处理模块.

2.1　H. 264 内容的文件格式和加密算法

在内容加密服务器上运行的是内容加密模块,该模块的操作对象是经 H. 264 信源编码软件编码并按照字节流格式[2]封装出来的文件 ContentID. 264,其中 ContentID 用来标识数字内容的名字. 字节流格式文件由若干个(起始码,NALU)对子顺序排列而成[2]. 其中,起始码是 3 个固定字节"0X000001",用于将各个 NALU(Network Abstraction Layer Unit)分隔开来,并可用于计算某个 NALU 的长度;每个 NALU 由一字节的头信息和不定字节长度的净载荷组成.

运行加密模块将为原始字节流格式文件添加若干字节的文件头数据,用来表示"加密标识"、"内容名称"和"DRM 服务器地址". 加密模块的运行将按如下方法[6]在每个 NALU 头信息之后加入 4 字节的初始化向量 IV:文件中第一个 NAL 单元的初始化向量置为 0,之后的 NALU 中所添加的 IV 的数值是该单元前面所有单元净载荷的字节数之和.

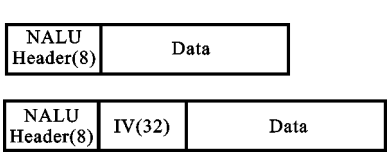

图 4　加密前后的 NAL 单元格式

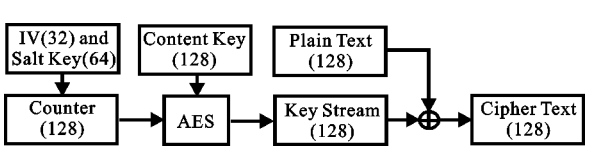

图 5　NALU 单元加密算法

加密模块的核心算法使用高级加密标准 AES,以计数器模式工作[7],密钥长度是 128 比特. 加密模块在为某个 NALU 添加了初始化向量 IV 之后,对原始 NALU 的净载荷加密,密文长度和明文长度是相等的. 图 4 是加密前后 NALU 的格式. 加密算法如图 5 所示. AES 算法使用密钥 Content Key 对 128 比特的 Counter 加密,结果是 128 比特的密钥流;NALU 中净载荷的一个 128 比特分组与密钥流逐比特异或得到 128 比特的密文. Counter 的后 32 比特是对要加密的明文分组的计数,每加密一个明文分组,Counter 加 1;Counter 的前 64 比特是一个固定的随机化种子. Counter 值的计算可以用下面的公式表示:$\text{Counter} = \text{Salt Key} * 2^{64} \oplus (\text{IV} + X)/16$,其中的"$X$"表示该分组的第一个字节与该分组所在 NALU 净载荷的第一个字节之间的

字节偏移量.

媒体播放器播放加密内容时,首先从该内容相应的许可证中解密出密钥 Content Key 和随机化种子 Salt Key,然后利用所接收到的 NALU 中的 IV 构造出要解密的数据分组的 Counter 值;使用 AES 对 Counter 加密得到密钥流 Key Stream,密钥流和加密数据分组进行逐比特异或运算就得到明文分组;进而得到原始的 NALU. 注意到内容加密服务器的操作对象是 H.264 文件,而媒体播放器中的解密模块的操作对象是加密后的 NAL 单元. 算法设计使得接收到的任何一个 NAL 单元都可以单独解密.

2.2 许可证申请和发放流程

2.2.1 内容加密服务器许可证申请和发放

在信任体系模型中虽然假设了内容加密服务器和 DRM 服务器是可信的,但是当这两台服务器通过开放网络通信的时候,两者之间的通信仍需要安全保护(通常的办法是使用 SSL 或者 TLS 协议[8]). 在 DRM 系统中,使用许可证机制来实现服务器之间的安全通信是一种更好的选择. 因为对用户端的控制必须通过许可证机制实现,这种选择将大大降低 DRM 服务器的设计和实现复杂度. 内容加密服务器申请和使用许可证的流程如下.

首先,由内容加密服务器发起和 DRM 服务器之间的双向认证协议建立信任关系. 认证成功之后,内容加密服务器将需要加密的数字内容的名称发给 DRM 服务器. DRM 服务器根据内容名称和随机信息生成该内容的加密密钥,内容加密密钥由 Content Key 和随机化种子 Salt Key 组成. DRM 服务器在本地数据库中增加一个新的"内容编号,内容名称,加密密钥和随机化种子"条目. 其中,"内容编号"是对该服务器所管理的所有数字内容的排序,也是对"内容名称"字节长度的大幅度压缩. DRM 服务器接下来为内容加密服务器生成许可证. 许可证主要包括以下数据类型:内容名称、内容编号、内容加密密钥以及 DRM 服务器对以上数据的数字签名,其中内容加密密钥使用内容加密服务器的公钥加密. 内容加密服务器得到许可证并验证其有效性之后,可以从中解密出内容加密密钥用于加密数字内容.

2.2.2 用户端许可证申请、发放和本地处理

用户端有关许可证的处理涉及身份认证、账户认证以及对智能卡中内容使用记录的操作. 以下按流程分 8 步描述用户端许可证的申请、发放和本地处理过程.

第 1 步,获取"加密标识"、"内容名称"和"DRM 服务器地址". 当机顶盒播放本地下载的内容文件时,以上数据从文件头读取;当机顶盒用户选择点播某项内容时,机顶盒向流媒体服务器发出 RTSP 请求,流媒体服务器返回 RTSP 响应和 SDP 消息,SDP 消息中包含以上数据. 播放器首先根据"加密标识"判断内容是否加密. 如果内容没有加密,则跳到第 8 步直接播放;如果内容是加密的,则执行下一步.

第 2 步,根据"内容名称"在本地查找该内容的许可证. 如果找到(用户可能之前已经购买过该内容的许可证,则该内容的许可证应该存放在本地,除非外在原因导致许可证丢失),则跳到第 5 步根据许可证中的内容编号检查该内容当前的使用记录;否则进行下一步.

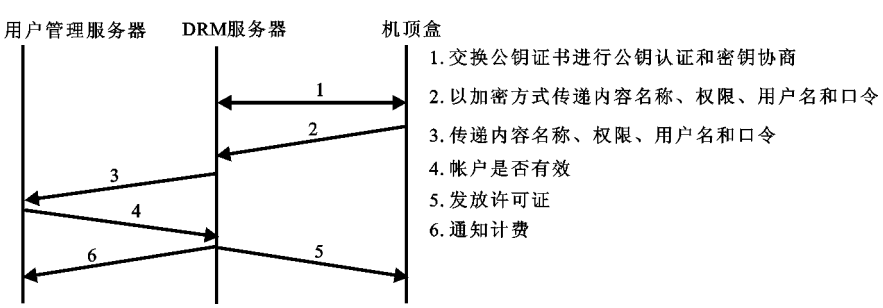

图 6 机顶盒获取许可证协议流程

第 3 步,根据"DRM 服务器地址"链接到 DRM 服务器申请许可证,如图 6 所示. 机顶盒和 DRM 服务器之间互相交换公钥证书进行双向认证和密钥协商. 认证成功之后,双方共享一个会话密钥. 此时,媒体播放器提示用户输入账户名和口令并选择将要购买的权限(例如,播放次数、播放天数等[9]);媒体播放器将"内容名

称”和用户输入的数据用会话密钥加密发给 DRM 服务器;DRM 服务器用会话密钥解密出以上数据,并将数据转给用户管理服务器;用户管理服务器根据用户选定的“内容名称”和使用权限以及账户状态和计费策略判断用户是否可以进行本次消费,并将判断结果返回给 DRM 服务器. 对于有效的返回值,DRM 服务器将为该用户签发一个相应的许可证并通知用户管理服务器计费. 许可证包括以下数据类型:内容名称、内容编号、使用权限、内容加密密钥以及 DRM 服务器对以上数据的数字签名.

第 4 步,验证许可证. 为了保证许可证是可靠的和完整的,智能卡使用 DRM 服务器的公钥验证许可证中的数字签名. 验证不通过,说明该许可证是不合法的;否则执行下一步.

第 5 步,生成使用记录. 在许可证存储在机顶盒本地之后,播放器程序将许可证中的“内容编号”和“使用权限”提取出来并在智能卡存储区中生成一条使用记录. 使用这种方式生成的一条使用记录通常只有几个字节的长度,可以大幅度降低对智能卡存储容量的要求.

第 6 步,检查使用记录. 播放器检查使用记录中的“使用权限”是否允许本次播放操作. 如果不允许,说明许可证已经失效,需要重新申请;否则执行下一步.

第 7 步,解密内容加密密钥和内容. 当用户本地存在合法的许可证并且拥有播放权限时,智能卡使用自己的私钥解密出许可证中的内容加密密钥,并更新使用记录. 此时,播放器可以使用内容解密密钥逐个解密接收的 NAL 单元.

第 8 步,播放器将原始 NAL 单元进行信源解码和播放.

需要说明的是,文中的 DRM 系统对用户权限的管理主要针对机顶盒信源解码. 实际上,权限管理范围可以进一步扩展到对解码码流的输出控制. 工业界目前已经制定了对许多数字接口的内容保护标准[10,11],如果 DRM 系统在许可证中的“使用权限”部分指定了对输出接口的要求,播放器在输出码流之前必须检查输出接口的类型,从而利用接口内容保护技术对数字内容进行持续的保护.

3　结 束 语

对网络运营商来说,IPTV 是现阶段一项非常有发展前景的增值业务. 为了解决数字内容的盗版问题,文中从 IPTV 实际运营的角度出发,给出了一种适用于 IPTV 点播和下载业务的数字权限管理系统,并设计了文件加解密、许可证获取和使用等系统关键模块的实现方案. 通过在内容加密服务器端和用户端同时采用许可证机制,使之实现起来更为简捷;用户端的私钥、使用记录等机密数据在智能卡内部存储和操作,使系统具有较高的安全性. 系统所使用的密码算法都是安全的公开算法,系统安全完全基于密钥的安全,符合 Kerckhoffs 假设. 系统中,密钥安全更具体地表现为密钥的物理安全,也就是智能卡的安全. 而在 PC 机等开放系统中实现较高安全级别 DRM 客户端功能也需要安全模块的支持[12],从这个意义上说,文中的面向机顶盒的 DRM 系统也可以扩展到开放系统中.

参考文献:

[1] Berlecon Whitepaper. DRM, DRM Patents and Mobile DRM [EB/OL]. http://www.contentguard.com/whitepapers/CGWP－FinalEng.pdf, 2005-01-12.

[2] ITU-T. Draft ITU-T Recommendation and Final Draft International Standard of Joint Video Specification [S]. ITU-T Rec. H.264|ISO/IEC 14496-10. 2003.

[3] Wenger S, Hannuksela M M, Stockhammer T, et al. RTP Payload Format for H.264 Video. RFC 3984 [EB/OL]. http://www.ietf.org/rfc/rfc3984.txt, 2005-02-15.

[4] Mooij W. Advances in Conditional Access Technology[A]. International Broadcasting Convention (IBC'97) [C]. Amsterdam: IEE, 1997. 461-464.

[5] Qu Jin, Ge Jianhua, Jiang Ming. Key Distribution for Broadcast Encryption[J]. Journal of Xidian University, 2002, 29(3): 310-313.

[6] ISMA. Encryption and Authentication Specification v1.0 [EB/OL]. http://www.isma.org, 2004-12-18.

[7] Lipmaa H, Rogaway P, Wagner D. CTR-Mode Encryption [EB/OL]. http://csrc.nist.gov/CryptoToolkit/modes/

workshop1/papers/lipmaa-ctr.pdf, 2003-01-16.

[8] Rescorla E. HTTP Over TLS [EB/OL]. http://www.ietf.org/rfc/rfc2818.txt, 2000-05-10.

[9] Guard C. Extensible Rights Markup Language (XrML) 2.0 Specification [EB/OL]. http://www.xrml.org/, 2001-11-12.

[10] Hitachi, Ltd., Intel Corporation and Matsushita Electronic Industrial Co., Ltd., Sony Corporation and Toshiba Corporation. Digital Transmission Content Protection System, Volume 1, Revision 1.3 [S]. http://www.dtcp.com, 2004-10-18.

[11] Intel Corporation, High-Bandwidth Digital Content Protection System, Edition 1.1 [S]. http://www.digital-CP.com, 2003-06-19.

[12] Kuhlmann D, Gehring R A. Trusted Platforms, DRM, and Beyond [A]. Digital Rights Management [C]. Berlin Heidelberg: Springer-Verlag, 2003. 178-205.

(编辑:李维东)

(上接第 921 页)

该算法针对性地制定了噪声抑制策略,保持了图像的重要细节,重建图像视觉效果清晰平滑,PSNR 值较高,算法时空复杂度较低.下一步将研究 ED 核形状及尺度的判定方法,从而达到自适应调整滤波器大小的目的.

参考文献:

[1] Ulichney R A. Digital Halftoning[M]. Cambridge: MIT Press, 1987. 233-331.

[2] Kite T D, Evans B L, Bovik A C. Modeling and Quality Assessment of Halftoning by Error Diffusion[J]. IEEE Trans on Image Processing, 2000, 9(5): 909-922.

[3] Hein S, Zakhor A. Halftoning to Continuous-tone Conversion of Error- diffusion Coded Images[J]. IEEE Trans on Image Processing, 1995, 4(2): 208-216.

[4] Wong P W. Inverse Halftoning and Kernel Estimation for Error Diffusion[J]. IEEE Trans on Image Processing, 1995, 4(4): 486-498.

[5] Stevenson R L. Inverse Halftoning Via MAP Estimation[J]. IEEE Trans on Image Processing, 1997, 6(4): 574-583.

[6] Kong Yueping, Zeng Ping. Inverse Halftoning for Error Diffusion Based on Pattern Recognition and Look-up Table[J]. Chinese Journal of Scientific Instrument, 2004, 25(4): 177-181.

[7] Venkata D, Kite T D, Venkataraman M, et al. Fast Blind Inverse Halftoning[A]. Proceedings 1998 International Conference IEEE Image Processing[C]. Chicago: Proceedings of IEEE Image Processing, 1998. 64-68.

[8] Shen Meiyin, Jay Kuo C C. A Robust Nonlinear Filtering Approach to Inverse Halftoning[J]. Journal of Visual Communication and Image Representation, 2001, (12): 84-95.

[9] Xiong Z, Orchard M T, Ramchandran K. Inverse Halftoning Using Wavelet[A]. Proc IEEE International Conference Image Processing[C]. New York: IEEE, 1996. 569-572.

[10] Burt P, Adelson E. The Laplacian Pyramid As a Compact Image Code[J]. IEEE Trans on Communications, 1983, 31(4): 532-540.

[11] Donoho D L, Yu T P Y. Robust Nonlinear Wavelet Transform Based on Median-interpolation[A]. Signals, System & Computers, 1997. Conference Record of the Thirty-First Asilomar[C]. Washington: IEEE, 1997. 75-79.

[12] 黄文涛, 毕笃彦, 毛柏鑫, 等. 基于中值变换和金字塔分解的图像去噪方法[J]. 电子与信息学报, 2004, 26(11): 1686-1692.

[13] Ren Huorong, Wang Jiali, Zhang Ping. Image Segmentation Algorithm Based on the Morhological Pyramid[J]. Journal of Xidian University, 2004, 31(2): 248-251.

[14] Zhao Ruizhen, Qu Hanzhang, Song Guoxiang. A Threshold Filtering Algorithm Based on the Region Relativity of the Wavelet Coefficients[J]. Journal of Xidian University, 2001, 28(3): 324-327.

(编辑:郭 华)