

基于使用控制的数字版权管理系统安全性分析

王昌达^{1,2}, 宫婷婷^{1*}, 周从华^{1,2}

(1. 江苏大学 计算机科学与通信工程学院, 江苏 镇江 212013; 2. 江苏大学 工程技术研究院, 江苏 常州 213164)

(* 通信作者电子邮箱 yanjuan_82@126.com)

摘要:针对现有数字版权管理(DRM)系统屡遭破解的问题,通过调研分析其安全机制,提出一种内容与权限分离的细粒度使用控制方案。该方案首先根据秘密分割的思想将数字许可证一分为二,实现身份验证与授权管理的分离;然后通过细粒度授予临时权限文件,确保数字内容在使用中能够细致控制;最后采用多项完整性检查来提高防篡改攻击的能力。模型检测结果表明,该方案及策略能够实现设计要求并基本满足数字版权管理安全性需求。

关键词:数字版权管理;使用控制;内容权限分离;细粒度;安全性分析

中图分类号: TP309.2 **文献标志码:** A

Security analysis of digital rights management system based on usage control

WANG Chang-da^{1,2}, GONG Ting-ting^{1*}, ZHOU Cong-hua^{1,2}

(1. School of Computer Science and Telecommunication Engineering, Jiangsu University, Zhenjiang Jiangsu 212013, China;

2. Institute of Engineering Technology, Jiangsu University, Changzhou Jiangsu 213164, China)

Abstract: Through the research and analysis about the security mechanisms of the existing Digital Rights Management (DRM), a fine-grained Usage Control (UCON) plan separated rights from content was proposed in order to avoid being cracked now and then. Firstly, based on the concept of secret division, digital license has been divided into two sections to realize the separation of authentication and authorization management. Then temporary permission files were fine-grainedly granted to ensure that digital content can be dedicatedly controlled in usage. Finally integrity checks were used to improve the ability of anti-tampering attacks. The model checking results show that this plan and its policy can realize the design requirements and fairly satisfy the security requirements of DRM.

Key words: Digital Rights Management (DRM); Usage Control (UCON); separation of content and right; fine-grain; security analysis

0 引言

近年来,互联网的快速发展有力推动了数字作品和数字软件广泛融入现代人的生活。由于数字内容无损复制和易于分发的特性为非法复制和使用、传播提供有利条件,关于对数字版权的保护引起了人们的高度关注。数字版权管理(Digital Rights Management, DRM)以一套完整的技术手段确保数字内容不被非法使用,保护数字内容所有者(包括创作者、运营商、用户等)的合法权益^[1-3]。DRM的使用促进了网络、多媒体、交互数字电视、P2P、无线移动通信等多个平台提供高品质的数字内容,完善平台间的交流共享,同时也有效地保护知识产权^[4]。

在对现有 DRM 机制和相关技术的研究中,较常见的方案是基于数字许可证的版权保护方案,通过许可证完成认证与授权,这种方案限制了用户灵活使用数字内容,也存在被攻击破解的安全问题。结合现有 DRM 存在的问题,提出了一种在使用控制中内容和权限相分离的 DRM 方案。根据使用控制模型策略和 DRM 安全性需求,建立一套完整的规则。通过对模型的分析,验证本方案较传统方法具有较强的安全性以及更细的控制粒度。

1 DRM 技术

1.1 DRM 技术模型

DRM 贯穿了整个数字内容价值链,从数字内容的生产到分发、从销售到使用追踪的整个流通过程,数字内容主要包括电子书、数字电影、数字音乐、图片、软件等^[5]。DRM 强调的是一种系统化的理念而非是某一种特殊的技术,它是密码、信息隐藏、认证、通信、安全容器、数字证书、唯一标识等多种技术的组合体。DRM 系统根据具体应用综合使用各种技术,将原始数字内容进行从上到下层层封装,并在相关法律、管理、审计、教育措施支持下实现版权保护和权限控制功能。DRM 技术体系模型如图 1^[6]所示。

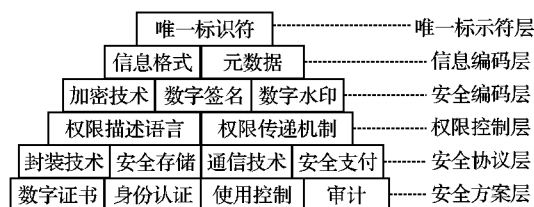


图 1 DRM 技术模型

1.2 DRM 的安全性需求

现有的 DRM 解决方案大多是通过使用数字许可证来保

收稿日期: 2012-03-03; **修回日期:** 2012-05-11。 **基金项目:** 国家自然科学基金资助项目(61003288); 江苏省自然科学基金资助项目(BK2010192); 教育部博士点基金资助项目(20093227110005); 江苏省六大高峰人才项目(1631170006); 江苏省高校自然科学基金研究计划项目(07KJB520016); 江苏大学高级人才项目(07JG053)。

作者简介: 王昌达(1971-), 男, 上海人, 副教授, 博士, 主要研究方向: 信息安全; 宫婷婷(1987-), 女, 黑龙江双鸭山人, 硕士研究生, 主要研究方向: 信息安全; 周从华(1978-), 男, 江苏大丰人, 副教授, 博士, 主要研究方向: 信息安全。

护数字内容的版权,用户得到数字内容后,必须获得相应的数字许可证才能够正常使用。目前有两种主要方法。

1) 硬件许可证方法。将数字许可证与专用的安全设备绑定,使得数字内容只能在带有该专用设备的机器上使用,用于提供高级别的防拷贝保护,如 smart-card、硬件保护锁,或者“安全 USB 狗”等。由于额外的硬件保护设备提高了使用成本,这种方法一般适用于较为昂贵的专用 DRM 系统中,如 Apple iTunes、McAMOS Technology、盛大电子书等。

2) 软件许可证方法。将数字许可证与用户相关配置信息绑定,使得数字内容只能在被绑定的机器上使用。这种方法不需要额外的硬件设备,使用成本相对较低,Microsoft WMRM^[7], IBM EMMS, RealNetworks Helix DRM, Intertrust DigiBox 和 Adobe Content Server^[8],书生公司的 SureDRM 等版权保护系统,都采用了这种基于软件许可证方法。

DRM 系统可以分成数字内容分发、身份认证、许可证分配、使用控制、审计追踪等几个部分。在对市场主流 DRM 产品进行调研并结合相关技术难题^[9],发现现有 DRM 主要有以下几个方面问题。

1) 网络引入的安全性问题。由于大多数 DRM 需要在客户端安装客户软件来支持与服务器之间的通信,这为黑客提供了一个攻击目标^[10],可能遭受账户盗用、恶意篡改^[11]、重放攻击^[12]、伪装欺骗等攻击。

2) 保障用户利益问题。现有 DRM 对出版发行商的利益给予了过度关注,用户隐私保护以及权利转移^[13]方面存在缺陷。例如许可证中存有用户硬件信息,权限往往无法转移或借出,从而限制了用户灵活使用数字内容。

3) DRM 系统自身安全问题。DRM 系统自身存在安全隐患,加上疏于管理升级,往往会被黑客破解,进而失去版权保护作用。

一个完善的 DRM 系统必须兼顾创作者、运营商和用户三方的权益,通过对 DRM 普遍存在的问题进行分析,一般认为好的 DRM 系统需满足以下安全性需求^[14]。

1) 通信和数据安全需求。DRM 应该保证运营商能够在不安全的公共信道上进行安全的数字内容传输。

2) 数据安全认证需求。在对数字内容或客户端 DRM 的完整性进行检查时,DRM 系统可以提供数字摘要或者水印信号,确定数据真实性和完整性。

3) 用户身份认证需求。DRM 系统需要对使用数字内容的使用者进行身份信息认证,确保其身份可靠。

4) 使用控制需求。DRM 在使用中应能完成以下三个方面对用户权限的管理:防止未经授权的用户通过欺骗或破解的方式使用数字内容;允许授权用户转移所拥有的权限,但不允许将数字内容以未经保护的形式保存或分发;防止用户对数字内容进行许可范围之外的操作。

5) 侵权行为发生时的取证需求。当盗版和侵权的行为发生时,DRM 系统应具备相应的取证功能。例如从盗版作品中检测到数字指纹或水印信号作为侵权的证据。

2 基于 UCON 的 DRM 保护方案

2.1 UCON 模型

使用控制模型(Usage Control, UCON_{ABC}),是由 Park 等^[15-16]提出的一种综合传统访问控制(Traditional Access Control, TAC)、信任管理(Trust Management, TM)以及 DRM 的新模型。UCON_{ABC}模型作为新一代访问控制模型,其使用决策基于授权(Authorizations)、义务(oBligations)、条件(Conditions),如图 2 中所示^[17],与 TAC 相比,能更好地满足

现代信息系统对不同决策因素的授权需求。

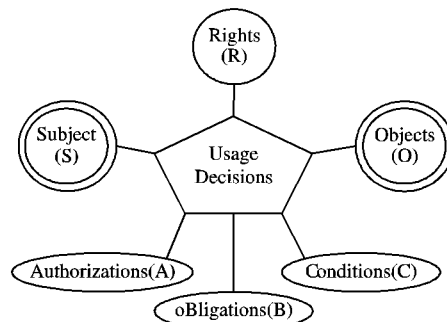


图 2 UCON_{ABC}模型组成

UCON 模型是新一代的访问控制模型,其功能涵盖了几乎所有的 TAC,如访问控制矩阵、自主访问控制、强制访问控制、基于角色的访问控制模型等。UCON 具有属性可变性和决策连续性,这些新特性是在授权的基础上,增加了义务和条件这两个决策因素,通过将过程管理细分为前(pre)、中(on)、后(post)三个阶段,并同时引入了动态管理功能而实现的。使用控制过程中各状态之间的转换是通过决策判断(包括授权谓词 P_A 、义务谓词 P_B 、条件谓词 P_C 的判断,以及使用控制行为 A_A 和义务行为 A_B 的执行)实现的,如图 3 所示^[18]。

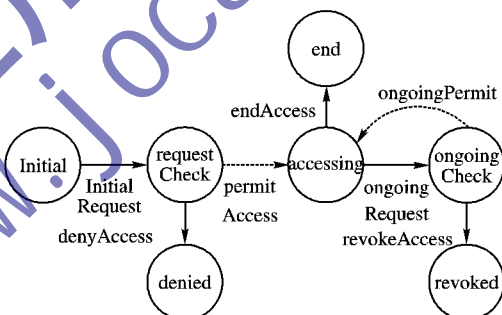


图 3 使用控制中状态转换

2.2 基于 UCON 的保护方案

现有的数字媒体版权保护大多采用基于数字许可证的 DRM 系统。这种将认证信息和权限一起放置于许可证内的方法,其优点是:在客户端便能够实现对数字内容的使用控制,方便用户离线使用;其缺点是:1) 没有结合防止对程序进行分析和篡改的技术,客户端的 DRM 和数字内容很容易被剪切和篡改;2) 数字许可证一旦与用户硬件信息绑定将难于修改,同时也会带来权限转移的不便;3) 获得许可证后,在离线状态下对数字版权内容进行使用控制,监管机构没有得到足够反馈信息,审计工作难以完成,因此无法及时发现和应对后续的侵权行为。

基于 UCON 的使用控制策略,将重点解决以下几个方面问题:权限管理、完整性保护和身份认证。对比基于数字许可证的版权保护方案,本文的使用控制方案有以下几点不同。

1) 在线许可证。随着 3G 网络和 WiFi 的建设,基于网络的许可证已经成为可能,在线许可证的使用将有利于细粒度控制使用。

2) 许可证分割。基于 Shamir^[19]和 Blakley^[20]秘密分割的思想,将许可证分割成为身份认证和权限管理两部分,实现统一认证和细粒度授权。

3) 权限文件和认证信息的存放方式。用户权限信息存放于授权服务器中,并且只进行更新不向外发送。当用户请求权限时,授权服务器将发送具有固定使用期限的临时权限文件。用户身份认证信息仅存放于权威认证机构,由权威认

证机构进行检查,以防止篡改、伪造以及相关信息泄露。

4) 认证标识和权限时效。权威认证机构进行身份认证后颁发具有较长时限的认证标识(如 24 h)。而临时权限的

使用期较短可以由授权机构设定(如 2 h),在其使用期结束前用户能够离线使用数字内容,到期时需再次联机申请。

本文提出的具体策略见图 4 中所示的使用控制过程。

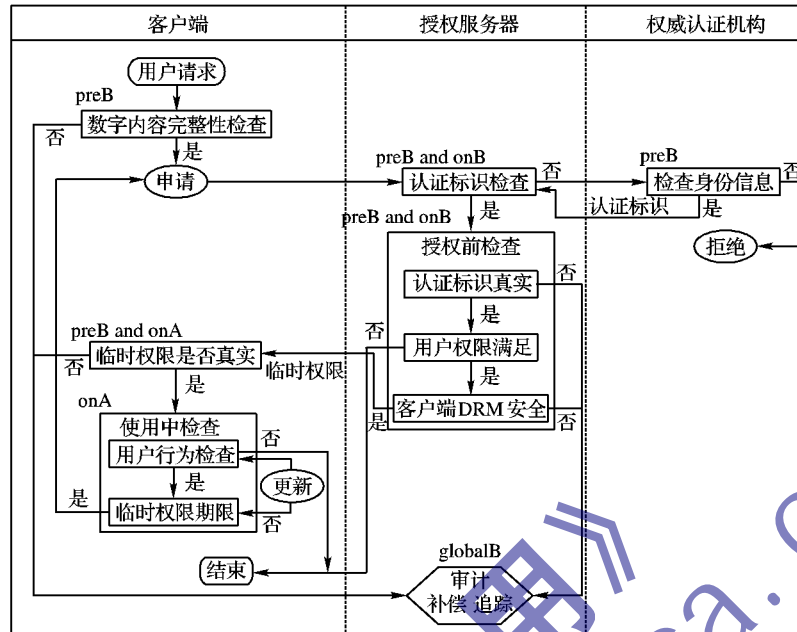


图 4 使用控制流程

从图 4 能够看出整个使用控制过程主要是由客户端 DRM、授权机构以及认证机构共同完成的,通过安全检查(包括数字内容文件安全和客户端 DRM 安全)和授权检查(包括用户权限和临时权限文件)等,管理用户规范使用数字内容。安全检查为 UCON 模型中的义务判断。客户端 DRM 检查所请求的数字内容是否完整,由于数字内容使用时是连续的,仅需一次 preB 检查即可;而使用过程中授权机构多次发送临时权限文件,需要对客户端进行多次 onB 检查以保证客户端使用环境的安全。另一类权限检查为 UCON 模型中的授权判断。授权机构发送临时权限前确认请求的权限是否在用户权限范围内,即 preA and onA 检查,而使用中检查临时权限文件是否到期即为 onA 检查。需要指出的是,这种动态访问授权管理是 UCON 所特有的,TAC 则需要等一次访问结束后才能进行权限更新。基于 UCON 的版权管理方案,客户端代替授权服务器进行频繁的权限检查,减少了授权服务器的工作量,方便在临时权限使用期用户脱机使用,且能够实现细粒度控制和有效的管理能力。即使恶意用户有违法行为,因临时权限的使用也不会造成严重损失。在权威认证机构的参与和审计补偿的实施下,保证了 DRM 系统安全运作。

3 DRM 使用控制策略的模型检测

3.1 使用控制模型形式化

数字内容使用控制流程参与主体,主要有用户、客户端 DRM、授权机构,主要使用了 $UCON_{ABC}$ 模型中的 preA onA preB onB onC 组合模型来实现使用过程的动态控制。 S, O, r, R 分别为主体集、客体集、请求权限、用户权限集。由图 3 中各状态转换关系,给出使用控制策略中主要规则。

1) 安全审核阶段。

此阶段主要是安全认证,客户端 DRM 对请求使用的内容文件进行内容完整性认证,之后带有认证机构颁发的身份认证标识,由授权机构检查客户端安全。这个阶段可以采用 $UCON_{preBpreC}$ 模型实现, $s, o, obs, obo, ob(obs, obo)$ 分别代表主体、客体、义务主体、义务客体、义务操作。

$permitaccess(s, o, r) \rightarrow \Diamond(\Theta(\text{initialrequest}(s, o, r) \wedge \text{verifyIntegrity}$

$(\text{userDRM}, o)) \wedge \text{checksecurity}(\text{authServer}, \text{userDRM}) \wedge (\text{connectState} = \text{TRUE}))$

2) 权限审核阶段。

当安全认证完成后,授权机构会核对用户权限是否满足请求权限,如果满足则发送临时权限文件,并更新用户使用时间等属性。这个阶段可以采用 $UCON_{preApreBpreC}$ 模型实现, s, att, o, att 分别代表主体属性、客体属性。

$permitaccess(s, o, r) \rightarrow \Diamond(\Diamond \text{initialrequest}(s, o, r) \wedge (\Theta((s, id, r) \in o.\text{serverACL}) \wedge \text{send}(\text{server}, \text{temporaryright}) \wedge (\text{connectState} = \text{TRUE})) \wedge \text{preupdate}(o.\text{totalTime}))$
 $\text{preupdate}(o.\text{totalTime}): o.\text{totalTime}' = o.\text{totalTime} - \text{temporaryright.lifetime}$

3) 使用控制阶段。

此阶段从客户端获得临时权限开始,首先检查临时权限文件的完整性,然后检查临时权限文件是否到期,监督管理用户使用数字内容,以保证使用行为在授权范围之内。这个阶段可以采用 $UCON_{onApreB}$ 模型实现。

$permitaccess(s, o, r) \rightarrow \Theta \text{checktruth}(\text{userDRM}, \text{temporaryright})$
 $\Box((\neg(\text{temporaryright.lifetime} > o.\text{usageTime}) \wedge (\text{state}(s, o, r) = \text{accessing})) \rightarrow \text{ongoingrequest}(s, o, r))$
 $\Box((\neg(r \in \text{range}(\text{temporaryright})) \wedge (\text{state}(s, o, r) = \text{accessing})) \rightarrow \text{endaccess}(s, o, r))$
 $\text{ongoingrequest}(s, o, r) \rightarrow \bigcirc \text{onupdate}(o.\text{usageTime})$
 $\text{onupdate}(o.\text{usageTime}): o.\text{usageTime}' = 0$
 $\text{endaccess}(s, o, r) \rightarrow \bigcirc \text{postupdate}(o.\text{usageTime})$
 $\text{postupdate}(o.\text{usageTime}): o.\text{usageTime}' = 0$

4) 再请求阶段。

临时权限的使用期较短,当使用期结束时就会再次请求。由于数字内容文件的使用过程连续,可以跳过内容完整性认证 $\text{verifyIntegrity}(\text{userDRM}, o)$ 进行客户端安全检查,即接下来直接重复 2)、3) 阶段的步骤就可以了。这个阶段在使用时发生,因此涉及到前面阶段中 preA、preB、preC 将都变为 onA、onB、onC。

3.2 实验验证

网络上流行的 DRM 系统都采用了较为完善的数字版权

保护技术,即使不断改进还是屡屡被攻破,由此可见对于数字内容保护的威胁很大程度上来自黑客和高手的破解。下面从数字内容面对破解威胁的角度,对现有 DRM 系统存在的安全性问题进行分类。

1) 客户端 DRM 被控制。客户端的权利描述、验证数字签名及监督执行模块被攻击者控制或篡改,使得使用过程中控制程序的一些功能失效,进而版权保护完全失去作用。

2) 数字内容文件的剪切。一些数字内容文件只进行加密处理,而没有添加数字水印或者重新编码,这样的文件在完成解密操作后,很容易被攻击者去除掉与版权保护相关的部分。

3) 许可证的篡改。很多许可证中的认证信息是基于运行数字内容设备的硬件信息,这些信息往往容易遭到篡改,例如硬盘的序列号等硬件信息是可以被修改的。

4) 假冒用于验证的数字签名。数字签名的验证公钥可能被伪造,攻击者用自己的私钥签名,并且用自己的公钥替换真正公钥,进行验证。当信任与安全体系被攻破的时候,攻击者伪造的签名得到通过。

针对以上所列的安全问题,使用模型检测工具 NuSMV 逐一检测验证使用控制策略,结果表明基于 UCON 的数字版权管理系统不存在以上安全性问题:

1) 用在线认证的方式,授权服务端对客户端的敏感代码进行篡改检测,发现篡改时要求客户端下载原版的 DRM 部件才能再运行,并且对可能的违法行为进行审计;

2) 使用控制开始时首先进行数字内容完整性检测,利用数字水印技术防止攻击者剪切头文件;

3) 身份认证由权威认证机构完成,并颁发带有其签名的

认证标识;

4) 采用动态的、多状态关联的签名检查,防止一般的重放攻击。

限于篇幅的关系,只附上安全性问题 1) 的测试结果:

由上文 DRM 使用控制策略知,当授权服务端发现客户端 DRM 被篡改后,任何数字内容将不允许被使用,即:

$$G((\text{systemstate} = \text{requestCheck} \mid \text{systemstate} = \text{ongoingCheck}) \ \& \ \text{errorReporting} = \text{DRM}) \rightarrow X((\text{systemstate} \neq \text{accessing}) \ \cup \ (\text{systemstate} = \text{denied} \mid \text{systemstate} = \text{revoked}))$$

假设使用过程中通信是安全的,模拟计时使用数字内容进行测试,遍历所有的状态。由检测结果(图 5)可知,应用基于 UCON 的 DRM 使用控制策略在检测到篡改用户端 DRM 的行为后,能够有效地阻止数字内容的后续使用,达到保护数字版权的目的。

```
*** This version of NuSMV is linked to the Minisat SAT solver.
*** See http://www.cs.chalmers.se/Cs/Research/FormalMethods/Minisat
*** Copyright (c) 2003-2005, Niklas Een, Niklas Sorensson

NuSMV > read_model -i ucon.smv
NuSMV > flatten_hierarchy
NuSMV > encode_variables
NuSMV > build_model
NuSMV > print_reachable_states
系统状态: 2233 (2^11.1248) out of 1.09936e+09 (2^68.7195)
NuSMV > check_properties
-- specification G(((systemstate = requestCheck | systemstate = ongoingCheck)
& errorReporting = DRM) -> X(systemstate != accessing | (systemstate = denied
| systemstate = revoked))) is true
NuSMV > 主:
```

图5 NuSMV 检测结果

4 结语

本文提出的使用控制模型与现有 DRM 产品之间主要差异如表 1。

表1 使用控制策略比较

功能	现有 DRM 产品的使用控制策略	本文提出的使用控制策略
权限管理	权限分发 用户在购买权限后,用户的权限数据会存储在相关服务器上,待分发许可证时再置于许可证中,用户就拥有购买的所有权限	用户购买权限后,用户的权限数据会一直存储在授权服务器上,分发权限时只发送临时权限,用户不能获得全部权限
	权限有效期 许可证的有效期,即用户所购买权限的有效期	临时权限的有效期由授权服务器自行设置,且远远小于用户购买权限,使用期间需要多次发送
	文件管理 支持离线使用许可证,不支持权限更新、借出、赠予,大部分也不支持权限修改	不支持离线使用,支持权限更新、修改、借出、赠予等
内容保护	义务顺序性 获取许可证需完成相应的义务,义务行为一般具有一定顺序性	临时权限的获取需满足严格的义务顺序
	权限约束 数字内容使用时 DRM 部分检查用户的操作是否在权限范围之内	用户端 DRM 除了检查用户行为,还要检查临时权限生命期以便申请新临时权限
完整性保护	元数据验证 具有防篡改机制	不仅检查用户端 DRM 完整性,还检查数字内容的完整性,防止恶意篡改、剪切;另外,对接收到的文件(证书、权限文件)检查其真实性,防止伪造、篡改
	审计补偿 采用防篡改机制和水印技术,跟踪内容使用,发现盗版行为采取法律手段	通过真实性和完整性验证保证用户端安全,发现侵权行为及时上报权威机构收集数据,并针对侵权用户采取补偿行为
身份认证	隐私保护 用户信息存放在相关服务器中,隐私保护不足	用户信息由权威机构保存,并有严格消息传递规则,用户信息安全性较高
	相关绑定 通常许可证与硬件绑定,或者与应用软件绑定,灵活性和方便性较差	通过权威认证机构将用户与权限绑定,方便用户使用,灵活性较高

本文将 UCON_{ABC} 模型应用于 DRM 系统的核心功能——数字内容的使用控制流程,克服了 TAC 和基于数字许可证的使用控制中一些不足和缺陷,实现了使用控制流程细粒度化和动态化管理,将数字版权管理中认证、授权、使用结合成统一体系,更适用于现代信息系统。

参考文献:

[1] JAMKHEDKAR P A, HEILEMAN G L. Digital rights management

architectures[J]. Computers and Electrical Engineering, 2009, 35 (2): 376 - 394.

[2] 范科峰, 莫玮, 曹山. 数字版权管理技术及应用研究进展[J]. 电子学报, 2007, 35(6): 1139 - 1147.

[3] SACHAN A, EMMANUEL S, DAS A, et al. Privacy preserving multiparty multilevel DRM architecture[C]// CCNC'09: Proceedings of the 6th IEEE Conference on Consumer Communications and Network-

- king Conference. Piscataway, NJ: IEEE Press, 2009: 1128 - 1132.
- [4] 张志勇, 牛丹梅. 数字版权管理中数字权利使用控制研究进展[J]. 计算机科学, 2011, 38(4): 48 - 54.
- [5] 林丽, 李艳, 关德军. 数字版权管理系统中安全模型的研究与设计[J]. 通化师范学院学报, 2011, 32(10): 14 - 16.
- [6] 张晓林. 数字权益管理技术[J]. 现代图书情报技术, 2001(5): 3 - 10.
- [7] ZENG WENJUN, LEI S. Efficient frequency domain selective scrambling of digital video[J]. IEEE Transactions on Multimedia, 2003, 5(1): 118 - 129.
- [8] 曾婷, 张成昱, 肖燕. 电子图书数字权限管理系统比较研究[J]. 图书馆杂志, 2004, 23(8): 55 - 60.
- [9] 徐新光. 数字版权管理的技术和难题[J]. 广播与电视技术, 2006, 33(12): 75 - 79.
- [10] CHOR B, FIAT A, NAOR M. Tracing traitors[C]// CRYPTO'94: Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer-Verlag, 1994: 257 - 270.
- [11] CHOI S, HAN J, JUN S I. Improvement on TCG attestation and its implication for DRM[C]// ICCSA'07: Proceedings of the 2007 International Conference on Computational Science and Its Applications. Berlin: Springer-Verlag, 2007: 912 - 925.
- [12] ABBADI I M, ALAWNEH M. Replay attack of dynamic rights within an authorised domain[C]// SECURWARE'09: Proceedings of the 2009 the Third International Conference on Emerging Security Information, Systems and Technologies. Washington, DC: IEEE Computer Society, 2009: 148 - 154.
- [13] BHATT S, SION R, CARBUNAR B. A personal mobile DRM manager for smartphones[J]. Computers and Security, 2009, 28(6): 327 - 340.
- [14] 张海鑫, 程丽红, 李顺东. 数字版权管理系统中的使用控制模型[J]. 计算机技术与发展, 2009, 19(12): 135 - 157.
- [15] PARK J, SANDHU R. The $UCON_{ABC}$ usage control model[J]. ACM Transactions on Information and System Security, 2004, 7(1): 128 - 147.
- [16] PARK J, SANDHU R. Towards usage control models: Beyond traditional access control[C]// Proceedings of the 7th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2002: 57 - 64.
- [17] ZHANG X W, PARISI-PRESICCE F, SANDHU R, *et al.* Formal model and policy specification of usage control [J]. ACM Transactions on Information and System Security, 2005, 8(4): 351 - 387.
- [18] KATT B, ZHANG X W, BREU R. A general obligation model and continuity-enhanced policy enforcement engine for usage control [C]// Proceedings of the 13th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2008: 123 - 132.
- [19] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612 - 613.
- [20] BLACKLEY G R. Safeguarding cryptographic keys[C]// Proceedings of the National Computer Conference. Washington, DC: IEEE Computer Society, 1979: 313 - 317.

(上接第2770页)

因为单一的混沌序列都是由确定性的方程产生,理论上攻击者可以通过相空间重构的方法对加密信息进行破译。

从图6的相图分析可得出,单一的未经设计的加密混沌系统是单一的曲线,很容易受到攻击;而本文设计的加密系统相图是无规律的,这无疑对采用相图进行攻击的攻击者来说,是很难实现的。

4 结语

基于单一混沌加密算法实现简单,但密钥空间小,安全性差。本文设计了一种基于双混沌互反馈的数据加密算法,采用 Logistic 映射和 Tent 映射两个单一混沌映射利用给定初始值 x_1 和控制参数 μ, λ , 初始迭代次数 b, b' 再进行迭代后将值进行互反馈得出子密钥序列,使密文具有不可预测性。通过以上对该算法的仿真分析可知,此算法取得了很好的加密和解密效果;再通过改变参数进行加解密可得此混沌系统对初始条件极其敏感。最后进一步对设计的混沌加密系统进行安全性分析可知此算法密钥空间大且加密强度高,能有效防止攻击者利用穷举、统计、相图进行的攻击,是比较安全可靠的,而且具有很好的应用前景。

参考文献:

- [1] 包浩明, 朱义胜. 基于多层密钥的混沌映射保密通信系统[J]. 电子学报, 2009, 37(6): 1222 - 1225.
- [2] 李永华, 王冰. 基于混沌序列的图像加密算法[J]. 计算机应用, 2009, 29(5): 100 - 102.
- [3] 晋建秀, 丘水生. 基于物理混沌的混合图像加密系统研究[J]. 物理学报, 2010, 59(2): 792 - 799.
- [4] 谢建全, 阳春华, 黄大足, 等. 基于 Logistic 映射的加密算法的安全性分析与改进[J]. 小型微型计算机系统, 2010, 31(6): 1073 - 1076.
- [5] 叶瑞松, 庄乐仪. 基于帐篷映射迭代的置乱方法[J]. 计算机应用, 2009, 29(10): 2713 - 2715.
- [6] 郭建胜, 张锋. 一种图像加密算法的等效密钥攻击方案[J]. 电子学报, 2010, 38(4): 781 - 785.
- [7] XIE JIANQUAN, YANG CHUNHUA, XIE QING, *et al.* An encryption algorithm based on transformed Logistic map[C] // International Conference on Networks Security, Wireless Communications and Trusted Computing. Washington, DC: IEEE Computer Society, 2009: 111 - 114.
- [8] 徐淑英, 王继志. 一种改进的混沌迭代加密算法[J]. 物理学报, 2008, 57(1): 37 - 41.
- [9] 赵雪章, 席运江. 一种基于混沌理论的数据加密算法设计[J]. 计算机仿真, 2011, 28(2): 120 - 123.
- [10] GUO WEN-PING, CHEN YING. Chinese character encryption algorithm based on Logistic mapping[C]// 2010 3rd IEEE International Conference on Computer Science and Information Technology. Washington, DC: IEEE Computer Society, 2010: 478 - 481.
- [11] 王静, 蒋国平. 基于密文反馈的 Logistic 映射认证加密算法[J]. 东南大学学报, 2010, 40(9): 84 - 91.
- [12] 李恩, 吴敏, 熊永华. 一种基于双混沌映射的加密算法设计与应用[J]. 计算机应用研究, 2009, 26(4): 1512 - 1514.
- [13] 董斌辉, 周健勇. 混沌随机全排列置换加密算法及应用[J]. 计算机工程与应用, 2011, 47(8): 59 - 61.
- [14] 张永, 温涛, 郭权, 等. 混沌同步密钥流生产算法评价方法[J]. 计算机工程与应用, 2010, 46(20): 68 - 70.
- [15] 刘成斌. 混沌加密算法的研究与实现[D]. 北京: 北京邮电大学, 2008.