基于光盘映像文件的 CD-ROM 数据加密与解密方法

肖 飞 王运琼 李映松 李必谨

(云南师范大学计算机科学与信息技术学院 昆明 650092)

摘 要 分析了在 ISO 9660 和 Joliet 两个文件系统下 CD-ROM 光盘上数据的逻辑格式,通过修改光盘映像文件中卷描述符中的卷容量、文件和目录记录中的文件标志的方法,制作加密和解密光盘。提出了通过互换卷描述符和文件域地址的个性化加密方法。实验结果表明加密后的数据光盘具有更好的加密性能,既不能正常运行,也不能进行正常的拷贝,在一定程度上起到了知识产权保护的作用。

关键词 光盘文件系统,光盘映像文件,数据加密,数据解密

中图分类号 TP309.7 **文献标识码** A

CD-ROM Data Encryption and Decryption Method Based on CD Image File

XIAO Fei WANG Yun-qiong LI Ying-song LI Bi-jin

(College of Computer Science & Information Technology, Yunnan Normal University, Kunming 650092, China)

Abstract The logic format of CD-ROM data is expounded under ISO 9660 and Joliet file system. An encryption and decryption CD was made by modifying the volume descriptor and the directory and file record of CD image file. A special encryption method was proposed by exchanging volume descriptor and modifying the address of file. The experimental results have shown this encryption CD can not be run normally, and can not be copied too. The author's intellectual property can be protected in some extent by this way.

Keywords CD file system, CD image file, Data encryption, Data decryption

1 引言

自从 20 世纪 80 年代光盘推出以来,由于光盘存储器具有稳定、可靠、容量大、成本低的特点,适用范围越来越广,逐渐成为多媒体数据的主要存储器。也由于其低成本的制作,使得光盘盗版的现象也越来越严重^[1],严重侵害了软件知识产权,因此研究光盘数据的加密方法,成为迫切需要解决的问题,目前已经有不少研究者在进行光盘加密方面的研究^[2-4]。

光盘加密可分为软加密和硬加密,软加密方法不增加特别的硬件,具有加密成本低、加密方式灵活、携带和使用方便的特点,主要的软加密技术有密码表加密、序列号加密、许可证加密等,本文用结构性加密的方法,通过修改光盘映像文件,改变光盘属性和文件的属性,而文件的数据内容和存储位置仍然保持不变的方法实现光盘数据的加密。

光盘映像文件是光盘的完整映像,与光盘文件系统具有完全相同的存储格式,能够真实反映光盘上数据内容、逻辑结构、文件格式等特征。将未加密的光盘数据制作成光盘映像文件,然后对光盘映像文件进行适当修改后再进行刻录,可制作成具有一定保护功能的加密光盘。

2 光盘使用的文件系统

在 CD-ROM 上存储的是各种类型的文件,需要文件系统

来进行管理,以便能将 CD-ROM 当成一个文件集来处理,目前常用的支持 Windows 操作系统的光盘文件系统主要有 ISO 9660 和 Joliet。

2.1 ISO 9660 标准^[5]

ISO 9660 是第一个也是唯一的通用光盘文件系统,所有的操作系统都支持这个标准,所有的刻录软件也都支持这种格式。ISO 9660 规定每个文件由 1 个文件域组成,支持的单文件容量为 2G 字节以下,目录层次不超过 8 层,使用 ASCII 字符集,目前有 Level 1 和 Level 2 两个标准。Level 1 与 DOS 兼容,文件名采用 8.3 格式,目录标识符不超过 8 个字符,字符集由大写英文字母 A-Z、数字 0-9 及下划线组成,共 37 个字符,文件域中没有扩展属性记录。Level 2 在 Level 1 的基础上加以改进,允许使用长文件名和长目录名,但文件名与扩展名的总长度不超过 30 个字符,目录标识符的长度不超过 31 个字符,不支持 DOS。

2.2 Joliet 文件系统^[6]

Joliet 文件系统是 ISO 9660 文件系统的扩展,由 Microsoft 公司提出并实现,只支持 Windows 操作系统。该文件系统的文件名和目录标识符使用 UCS-2 字符集,用 2 个字节表示 1 个字符,字节顺序采用 Big Endian 的形式,文件名和目录标识符长度最长可达 64 个 UCS 字符(128 字节),允许目录名中带扩展名,目录层次可超过 8 层。

收稿日期:2008-11-07 本文受云南省科技厅基金(2007F2021X),云南师范大学综合性设计性实验项目资助。

肖 飞(1972-),男,讲师,主要研究方向为数据加密技术,E-mail:kmx00001@163.com;王运琼(1967-),女,博士,副教授,主要研究方向为数据加密技术、模式识别;李映松(1981-),男,讲师,主要研究方向为数据加密;李必谨(1956-),男,副教授,主要研究方向为多媒体技术。

3 光盘映像文件数据结构

1 张 CD-ROM 称为 1 卷,多张 CD-ROM 构成卷集。每卷由卷描述符、路径表记录、文件和目录描述符、数据区组成。扇区是最小的地址单元,每个逻辑扇区定义为 2^{11+n} 字节 ($n \geq 0$)。卷空间分为系统区和用户区,其中第 0—15 扇区为系统区,由系统使用,从第 16 扇区开始为用户区。

3.1 卷描述符

卷描述符说明整个 CD-ROM 盘的结构,是由固定的 2048 字节组成的记录,分为引导记录、主卷描述符、辅助卷描述符、卷分割描述符和卷描述符集终止符 5 种。每卷至少有 1 个主卷描述符和 1 个卷描述符集终止符,其它 3 种描述符根据需要可以没有或有一个。Joliet 文件系统使用辅助卷描述符来定义光盘的结构。卷描述符具有表 1 所列的形式。

表 1 卷描述符的格式

字节位置(BP)	域的名称	域值
1	卷描述符类型	0 或 1 或 2 或 3 或 255
2-6	标准的标识符	CD001
7	卷标识符的版本号	
8-2048	(取决于卷标识符类型)	(取决于卷标识符类型)

主卷描述符是最先出现的卷描述符,类型值为 1,位于第 16 扇区,记录了卷空间大小、版本信息、路径表、根目录记录的位置等;引导记录的类型值为 0,占用第 17 扇区,记录了引导系统类型和引导文件的位置;卷描述符集终止符的类型值为 255,标志着卷描述符区域的终止;辅助卷描述符的类型值为 2,本文的加密方法需要对主卷描述符和辅助卷描述符的相关域进行修改,它们的主要内容如表 2 所列。

表 2 主卷和辅助卷描述符的格式

字节位置(BP)	主卷描述符的记录域名称 (值)	辅助卷描述符记录域名称 (值)
1	卷描述符类型(1)	卷描述符类型(2)
2-6	标准的标识符(CD001)	标准的标识符(CD001)
8	未使用(0)	卷标志(0 或 1)
9-40	系统标识符	系统标识符
81-88	卷空间大小	卷空间大小
89-120	未使用(0)	换码顺序
129-132	逻辑块大小	逻辑块大小
133-140	路径表大小	路径表大小
141-144	L 型路径表位置	L 型路径表位置
149-152	M 型路径表位置	M 型路径表位置
157-190	根目录的目录记录	根目录的目录记录
191-318	卷集标识符	卷集标识符
...	...	...

从表 2 可以看出,主卷描述符和辅助卷描述符的格式完全相同,内容也很接近,只是使用的字符集不相同,导致系统标识符、路径表大小,根目录记录、卷集标识符等与标识符有关的项的记录长度会发生改变。主卷描述符使用 ASCII 字符集,每个字符 1 个字节,辅助卷描述符使用 UCS-2 字符集,由换码顺序项 BP89-120 确定具体使用的字符子集。

3.2 路径表记录

为了快速地定位光盘上的文件,光盘文件系统中增加了路径表记录,用于直接访问光盘上的任意一个子目录。路径表中各目录项按目录层次升序排列,相同层次的目录项按父目录名升序排列,同一目录下的子目录按标识符升序排列,目录项可跨扇区存储。一般情况下,路径表紧随卷描述符集终止符。路径表记录格式如表 3 所列。

表 3 路径表记录格式

字节位置(BP)	记录域名称
1	目录标识符长度(LEN_DD)
2	扩展属性记录的长度
3-6	存放目录的地址
7-8	父目录号
9-(8+LEN_DD)	目录标识符
(9+LEN_DD)	填充域

路径表由一系列可变长度的记录构成,记录每个子目录的相关信息,可跨扇区存储。扩展属性记录中记录文件的附加信息,存储在文件的前面;父目录号的确定原则是:如果当前目录号为 m ,则其父目录号为 $m-1$,根目录号为 1;填充域保证每个子目录记录的长度为偶数字节。

3.3 文件和目录描述符

CD-ROM 的每个子目录的文件和目录描述符根据需要占用一个或多个扇区,每个记录域记录了文件和目录的属性,包括文件域地址、数据长度、文件标志等,文件和目录描述符的格式如表 4 所列。

表 4 文件和目录描述符格式

字节位置(BP)	记录域名称
1	目录记录长度(LEN_DR)
2	扩展属性记录长度
3-10	文件域的地址
11-18	数据长度
19-25	日期和时间
26	文件标志
27	文件单元大小
28	交叉间隔大小
29-32	卷顺序号
33	文件标识符长度(LEN_FI)
34-(33+LEN_FI)	文件标识符
(34+LEN_FI)	填充域

每个文件和目录记录不可跨扇区存储,填充域保证每个记录长度为偶数字节,通过修改文件标志和数据长度可实现变超大文件、文件和目录的隐藏等加密方法,通过修改文件域的地址可使复制的数据无效。

4 光盘数据加密和解密的实现

根据以上对光盘数据存储结构的描述,可通过修改光盘映像文件的卷描述符相关内容或某个文件和目录记录中的域值,实现对整个光盘和某些文件数据的结构性数据加密和解密。首先用 Nero,WinISO 等刻录软件将需要进行保护的数据制作成标准的光盘映像文件,然后用 WinHex,UltraEdit 等 16 进制编辑软件修改映像文件,再用刻录软件将修改后的映像文件刻录成光盘,即可成为加密光盘。

4.1 盘数据的加密

ISO 9660 和 Joliet 文件系统都规定光盘上单个文件的最大容量是 2GB,如果将某个文件的长度修改为大于 2GB,则这个文件就不能被复制,同样如果将某个文件的属性修改为隐藏,也不能进行正常的复制,通过这些方法,可以有效防止对被保护文件的非法传播。另外,当光盘的容量大于标准容量时,整张光盘的复制也无法进行。表 5 给出了通过修改卷描述符相关内容或某个文件和目录记录中的域值能够实现的加密方式和每种加密方法需要修改的内容。

表5 加密方式表

加密方法	修改项目	修改内容
修改光盘容量	卷描述符 BP81-84 字节	目标容量
文件变目录	目录记录 BP26 的 Bit 1	1
目录变文件	目录记录 BP26 的 Bit 1	0
隐藏目录或文件	目录记录 BP26 的 Bit 0	1
变超大文件	目录记录 BP11-14 字节	目标文件大小

以变超大文件为例说明加密步骤。

步骤1 确定是否有辅助卷描述符,以判断使用的文件系统是 ISO 9660 还是 Joliet。通过搜索 16 进制代码“02 67 68 48 48 49”来确定,如果是 Joliet 文件系统,转步骤 2;否则转步骤 3;

步骤2 根据辅助卷描述符的 BP89-120 确定换码顺序,并使用对应的 UCS-2 字符集对目录名和文件名进行转换,根据 BP141-144 确定路径表的扇区号;转步骤 4;

步骤3 根据主卷描述符的 BP141-144 确定路径表的扇区号;

步骤4 到路径表扇区号,按照路径表记录格式,如表 3 所列,根据子目录名找到文件对应的子目录的地址;

步骤5 到子目录地址,按照文件和目录记录格式,如表 4 所列,根据文件名找到该文件记录的 BP11-14,这 4 个字节对应真实的文件大小,将它们修改为指定大小。

对以上加密方法进行了具体的实验验证,实验结果表明,通过以上方法加密的光盘,可以正常运行,但不能进行复制,起到了对光盘数据的保护作用。

4.2 对加密光盘数据的解密

对加密光盘进行解密时,需要先将加密光盘上的数据制作成光盘映像文件,再对映像文件进行修改。

卷描述符中的光盘容量、目录记录中的数据长度用 4 字节来表示,采用 Both Endian 的方式,占用 8 字节,它们的内容以字节为单位是对称的,即第 1 字节与第 8 字节,第 2 字节与第 7 字节、第 3 字节与第 6 字节,第 4 字节与第 5 字节的内容相同。确定该域的值时,只需要前 4 字节的内容即可。这种存储方式为数据的解密提供了方便,因为在加密时就只需要修改前 4 字节的内容,保留后 4 字节的内容为正常的值,因此只需要根据后 4 字节的内容恢复前 4 字节的内容,就可以实现解密。用类似于加密的方法,可实现对表 5 所列加密方法产生的加密光盘数据的解密,解密方法及需要修改的内容如表 6 所列。

表6 解密方式表

解密方法	修改项目	修改内容
恢复光盘容量	卷描述符 BP81-84	根据 BP85-88 恢复 BP81-84
恢复变为目录的文件	目录记录 BP26 的 Bit 1	0
恢复变为文件的目录	目录记录 BP26 的 Bit 1	1
恢复隐藏的目录或文件	目录记录 BP26 的 Bit 0	0
将超大文件变为正常大小	目录记录 BP11-14	根据 BP15-18 恢复 BP11-14

使用 ISO 9660 文件系统产生的光盘映像文件,通常没有辅助卷描述符,只需要修改主卷描述符的相关内容,Joliet 文

件系统使用 ISO 9660 的辅助卷描述符来指定 UCS-2 字符集的一系列记录特性,因此如果使用 Joliet 文件系统,需要修改辅助卷描述符的相关内容。

4.3 光盘数据的个性化加密和解密方法

以上讨论的方法,通过现有的加密与解密软件如光盘加密大师等^[7]也可实现相同的功能。为了制作出具有个性化的加密光盘,需要对光盘映像文件进行特殊的修改。以下是对几种修改方式的说明:

(1) 互换卷描述符标识符: Joliet 文件系统使用辅助卷描述符定义相关属性,将其与主卷描述符的类型值互换,由于原来的主卷描述符没有定义换码顺序,无法进行 UCS 字符集的正确转换,结果标识符显示全成为乱码,由于文件名和扩展名格式不正确,显示的文件名、文件大小和文件类型都将不正确。

(2) 修改文件域的首地址,这样复制得到的数据是不完全的、错位的,由于不能读取到正确的文件头信息,使得复制到的数据没有使用价值。

本文涉及到的各种加密方法可以联合使用,通过恢复修改项可实现解密。

用光盘加密大师、ClonyXXL 等解密软件对上述加密方法进行了测试,实验表明对第(1)种加密方法无法解密,而第(2)种方法加密的光盘则根本检测不出有加密的内容。

用上述的方法对光盘映像文件进行修改后,光盘将不能正常浏览和运行,需要自带解密程序才能使用该光盘上的数据。

结束语 本文通过对光盘映像文件的结构的分析,阐述了通过修改光盘映像文件的卷描述符和对应文件的目录记录的相应内容,实现光盘数据的结构性加密方法。最后提出了通过互换卷标识符和文件域首地址的个性化加密方法,达到使文件属性显示不正常,复制内容无效的目的。该方法具有灵活多样的特点,具有更好的加密性能,可在一定程度上达到保护合法的软件知识产权的目的。

参考文献

- [1] 王九丁. 浅谈光盘防拷贝技术[J]. 记录媒体技术, 2003, 2(2): 6-8
- [2] 孙龙霞, 刘军. 光盘加密技术的研究[J]. 军事通信技术, 2005, 26(2): 35-40
- [3] 乔志江, 赵明. 光盘加密刻录的方法与实现[J]. 沈阳电力高等专科学校学报, 2003, 5(1): 31-34
- [4] 覃祝君. 光盘加密技术的回顾与展望[J]. 记录媒体技术, 2006, 5(7): 42-46
- [5] ISO 9660-1988. Information processing -Volume and File structure of CD-ROM for Information Interchange[S]. International Organization for Standardization, April 15, 1988
- [6] Joliet Specification - CD-ROM Recording Spec ISO 9660: 1988 Extensions for Unicode[S]. Microsoft Corporation, May 22, 1995
- [7] 张亮, 程志艳, 张弘. DVD/MP3/VCD/CD-RW 光盘刻录手册[M]. 北京: 希望电子出版社, 2006

(上接第 256 页)

- [9] Donoho DL. Wavelab850[CP/OL]. http://www-stat.stanford.edu/~wavelab/Wavelab_850
- [10] Do M N. Contourlet Toolbox[CP/OL]. <http://www.ifp.uiuc.edu/minhdo/software/>
- [11] Portilla J, Strela V, Wainwright M J, et al. Image denoising u-

sing scale mixtures of Gaussians in the wavelet domain[J].

- IEEE Trans. Image Processing, 2003, 12(11): 1338-1351
- [12] Foi A, Katkovnik V, Egiazarian K. Pointwise Shape - Adaptive DCT for High-Quality Denoising and Deblocking of Grayscale and Color Images[J]. IEEE Trans. Image Processing, 2007, 16(5): 1395-1411