第15卷 第1期 华侨大学学报(自然科学版) Vol.15 No.1
1994年1月 Journal of Huaqiao University (Natural Science) Jan.1994

软盘防拷贝加密方法*

陈 建 生

(华侨大学计算机科学系,泉州 362011)

摘要 分析软磁盘介质记载信息的方法、磁盘拷贝原理和国内外常见防拷贝技术,提出一种生成不可拷贝的指纹码的技术及其应用方法.

关键词 防拷贝,加密,软盘,指纹

分类号 TP 311.52

随着微电子技术的迅猛发展和微机应用的日益普及,软件的商品性日趋明显并已成为一种公开出售的计价商品.因此,存储在软盘上的软件的防拷贝问题,已成为软件开发者和销售商密切关注的问题.本文从基本原理出发,研究PC系列机拷贝与反拷贝的技术,启发人们打破框框,设计并实现高性能的防拷贝新方法.

1 磁盘介质记载信息的方法

通过下面论述可以看出,生成不可拷贝的指纹码虽有技术难度,但是可能的.

1.1 磁记录原理

写入信息时,在磁头线圈中通过不同方向的磁化电流,在磁盘介质上磁化出两种不同极性的磁化区域,表示"0"与"1".读出信息时,不同极性的磁化区域使线圈中感应出电压信号,从而获得所记载的二进制信息.

1.2 磁记录方式

磁记录的方式很多,这里只介绍与本文有关的3种记录方式.

1.2.1 NRZ-1(不归零逢1变化制记录方式)

写"1"时,改变磁化电流的方向,使磁记录层的磁化状态发生翻转;写"0"时,保持原来的磁化状态不变(图1).NRZ-1虽缺乏自同步能力,但却是一种重要的磁记录方式.它是分析、设计FM和MFM的基础,而FM和MFM则是NRZ-1的

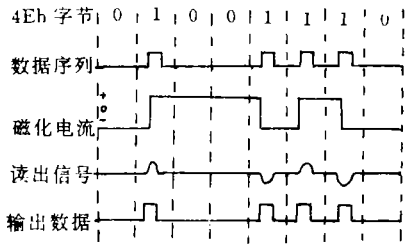

图1 NRZ-1记录方式

* 本文1993-03-31收到;福建省自然科学基金资助项目

改进型.

1.2.2 FM(调频制记录方式)与MFM(改进的调频制记录方式) FM在数据序列中插入同步信号,使原数据序列中的"1"对应记录序列中的"11","0"对应"10". 改造后的数据,再按NRZ-1方式记录(图2). 同理.MFM也按一定规则把数据序列改造为记录序列,然后按照NRZ-1方式进行记录. 它在位单元的中央写数据位,但是仅在前1个位单元和当前位单元都没有数据位写入(均为"0")时,才在位单元前写时钟位(图3).PC机常用的360 kB,1.2 MB,720 kB,1.44 MB软盘,均采用此记录方式. 由于FM和MFM的记录序列都按NRZ-1记录到磁介质上,所以可用NRZ-1读出FM/MFM的记录序列.

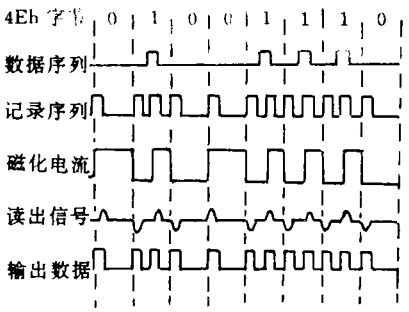

图2 FM记录方式

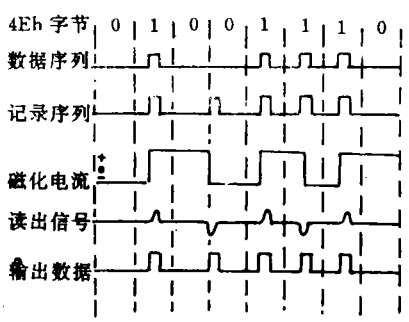

图3 MFM记录方式

1.3 磁盘上数据记录格式

磁道分成前置部、扇区部和后置部三部分,它们在磁盘上的位置如图4.

(1)前置部. 这部分位于磁道之首,由80个4 Eh字节,12个00 h字节,3个C 2h字节,1个F Ch字节和50个4 Eh字节依次相接而成.

(2)扇区部. 不同容量的磁盘,在扇区部所含有的扇区个数(记为n)不同,360 kB,1.2 MB,720 kB和1.44 MB盘的n值分别为9,15,9和18. 每个扇区具有以下结构(表1).

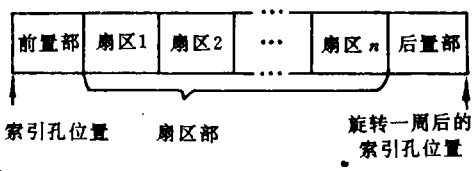

图4 磁道展开图

表1 扇区格式

内 容	00 h	A1h	FFh	C	H	R	N	CRC	4Eh	00h	A1h	FBh	用户数据	CRC	4Eh
字节数	12	3	1	1	1	1	1	2	22	12	3	1	$128*2^N$	2	X

其中,X为扇区间的间隙长度,格式化时可通过磁盘参数更改,其典型值为80(360 kB和720 kB盘)或84(1.2 MB盘)或108(1.44 MB盘);N用来确定每个扇区的数据字节数($128*2^N$),格式化时可以更改. 通常,N的取值为0~5(高密盘为0~6),DOS取$N=2$. 其它的N

值一般用在磁盘的防拷贝保护上．

(3)后置部．这部分位于磁道的最后，即在扇区部结束点到索引孔之间，并全部用 4 Eh 填满．其字节数跟数据扇区个数和格式化时磁盘驱动器的转速有关．

上面所及，是在 DOS 下的软磁盘数据记录格式；反之，要使写在盘上的程序、数据可由 DOS 读/写，又必须有以上的磁盘信息格式．

2　软盘信息防拷贝常见方法

国内外加密软件(用于大多数应用软件和电脑游戏程序)常用的制造密码的方法有：(1)无格式(空)的磁道；(2)超出常规范围的磁道；(3)每道的扇区数非 DOS 标准值；(4)用慢速驱动器格式化软盘；(5)磁道扇区 ID 序列为乱序；(6)用 FM 模式写磁盘；(7)简单利用磁道在索引孔处的接合点的信息；(8)激光盘；等等．其中，用方法(1)～(6)做成的软盘不能用 DOS 常规拷贝命令复制(见下文 3)，但可被拷贝硬件所仿制．方法(7)稳定性差，且不实用．因此，目前许多软件采用激光盘．方法(8)是利用激光束烧坏磁盘中一个或几个扇区的介质，有效地防止拷贝硬、软件的复制．但是，它会被拷贝软件模拟而获得拷贝，容易被人工破密，且不可写保护，不能避免病毒的攻击．我们提出的方案，可有效地防止拷贝硬、软件的复制，不烧坏任何扇区，用户可用 100%的磁盘空间，并允许磁盘在写保护状态下运行程序．

3　磁盘拷贝原理

3.1　DOS 格式的拷贝

在 DOS 下可运行 DOS 常规命令，或使用工具软件实现按文件拷贝和全盘拷贝．其中，以全盘拷贝最透彻，它把盘上所有 DOS 能识别的磁道上的所有扇区，完全复制到目标盘．全盘拷贝时，先读取源盘第 0 道上的首扇区，获取其中的介质描述字节，结合源盘所在驱动器的配置信息，从而了解源盘是何种容量的磁盘．然后，逐磁道地读出每面上的所有扇区，并按与源盘一样的格式先格式化目标盘，再把读出的内容写到目标盘的对应位置上．(见表 2)．

表 2　DOS 磁盘格式

格式特征	5.25″盘		3.5″盘	
	360kB	1.2MB	720kB	1.44MB
介质描述符	FDh	F9h	F9h	F0h
面　数	2	2	2	2
每面磁道数	40	80	80	80
每道扇区数	9	15	9	18
每扇区字节数	512	512	512	512

3.2　特殊磁道格式的拷贝

磁盘上数据记录格式倘非上述的标准 DOS 格式，所述全盘拷贝将失效．也就是说磁道的怪异格式可防止按 DOS 格式拷贝．但是，微机软件市场上存在很多强功能的拷贝工具如 Copy II pc，Copywrite，Locksmith 等，它们对于每个磁道均试用软盘适配卡所容许的各种磁道格式．由于磁盘最终要在软盘适配卡的控制下读出，再怪异的格式也要在硬件的支持下才能读出其中信息，所以单靠改变磁道格式的防拷贝盘一般均能被此类软件攻克(虽然拷贝速率很慢)．于是，很多防拷贝盘采用以下方法：针对流行的拷贝软件的弱点(或称拷贝死角)，使一种或多种上述强功能拷贝工具失效．然而，这些防拷贝盘最终很难抵御拷贝硬件(如专门拷贝机和一般电脑可用拷贝卡)的攻击．

当前,拷贝硬件的功能很强,比如拷贝卡就是一种特殊的软盘适配卡,能够十分精确地以NRZ-1记录方式读写磁盘上所记录的一切.它不仅可按NRZ-1读出FM/MFM所记录的信息,而且可精确地写目标盘,凡是磁盘上的一切数据位均在其拷贝范围内,几乎无所不拷.面对功能强大的拷贝硬件,为编写既可在DOS下运行又可防拷贝的程序,必须在盘上生成不可由拷贝硬件拷得的密码.这种密码必须具有不可拷贝性、不可预知性和信息的稳定性,不能取自正常读写区的信息.生成这种密码是可能的,下面说明本文所用的方法.

4 新防拷贝加密法

4.1 原理

经过反复实验,我们发现软盘磁道信息位序列的内在规律及其特殊性,经开发而形成一种防拷贝的基本手段.现以360 kB为例说明.

所谓"磁道的信息位序列"指读1磁道时,从检测到索引孔开始到再次检测到索引孔结束所读出的信息位串,它是在该软盘被格式化时形成的,并与格式化该盘的软盘驱动器的瞬时转速有关,也与磁盘自身的特性参数有关.如果按DS DD(360 kB)软盘驱动器的理想转速300 r/min计算,磁盘上每一磁道所记载的数据为50 000个信息位(合6 250字节,此为磁道的总记载能力),在格式化软盘时驱动器转速上的微小误差和软盘片的不同,都可造成每一磁道几十个到上百个信息位的信息位序列长度差.这种信息位序列的不同是必然的,因为不同软盘驱动器的转速是不会完全相同的,即使同一台驱动器的转速也不可能匀速〔一般旋转周期为(200±6)ms〕.假如驱动器转速变慢,转1周时间变成201 ms,则1磁道所含的信息多了250个信息位.另外,不同软盘的特性参数不可能完全一样,也必然导致不同的软盘对于所有磁道的信息位序列具有特殊性.

利用被保护程序将要存入的软盘片上40 * 2(面)个磁道上的信息位序列位数,以实现原版软盘的识别,此值称为密码.对于不同软盘此值基本上不会相同,这与人的指纹有些类似,故又称为指纹码.本指纹码可由FDC读,但不能写入磁盘,因为它不在磁盘数据信息域中,即使用特殊的拷贝卡或拷贝机也无法制造出每道的信息位序列位数与原版盘完全相同的软盘.所以,用这种方法加密的程序,是不能用拷贝硬、软件复制的.

4.2 应用方法

根据上述原理,我们编写了1个PC系列机防拷贝加密程序.它被用来把软件(任何可执行程序.EXE或.COM,记为S_0,T_0,U_0,……)变换、加工成防拷贝的新版本(记为S_{CP},T_{CP},U_{CP},……),并存于具有防拷贝指纹码的软盘(记为D_{CP})上.软件出售后,合法购买者可以使用D_{CP}上的S_{CP}等,而该软盘的复制品D′上的可执行程序S′等,则不能正常执行.防拷贝程序功能分为两大部分:生成含有指纹码的软磁盘D_{CP}的程序MKDCP;把无密程序S_0变换成具有防拷贝能力的S_{CP}的程序MKSCP.

用MKDCP生成防拷盘,在对其格式化时作了特殊处理,使每面上的每一磁道均含有整数个信息位.以360 kB盘在360 kB驱动器上格式化为例:磁道旋转1周的额定时间为(200±6) ms,而每个信息位占有这段时间中的4 μs,格式化磁盘时若不经特殊处理,磁道结束点就不会恰在信息位边界上.经过处理过的磁盘D_{CP}在所有磁道上含有的信息位数所构成的数

组，即是该盘的指纹码．因为使用拷贝软件或拷贝硬件把 D_{CP} 拷贝到 D′ 时旋转周期为(200±6)ms 将导致磁道信息位数为 50 000±1500，说明磁道位数变化范围很大，2 个磁道含有信息位数相同的概率则很小，因而拷贝成 D′ 的磁道要恰在信息位边界上的可能性就更小了．考察整个磁盘可以看出，所有道上的信息位数要完全对应相等几乎不可能．因此，D_{CP} 含有不可拷贝的指纹码．

MKSCP 读取无密程序 $S_0(T_0,U_0,\cdots\cdots$，一张磁盘 D_{CP} 可以存放多个防拷贝程序)，经加工处理变成 S_0'，添加上外壳程序 E_{CP}，得到防拷版 $S_{CP}(T_{CP},U_{CP},\cdots\cdots)$．防拷版由 DOS 装入内存运行时先执行 E_{CP}，它读取 D_{CP} 的指纹码若正确，就作为密钥把 S_{CP} 中的 S_0 反变换成 S_0 并转入运行，便进入原软件正常的执行流程．反之，拷贝版的指纹码不同，不能把 S_0' 反变换成正确代码，因此程序死锁．

5　结束语

本文的防拷贝加密程序经专家技术鉴定认为：用普通微机软盘驱动器，实现含整数个信息位磁道、程序防跟踪、防分析技术，为国内首创；其防拷贝能力领先于同类防拷贝加密程序．它在保护软件的开发者和销售商的合法权益，有效地阻止软件的无偿扩散以及防止软件失窃等方面，都具有实用价值和推广意义．

参　考　文　献

1　Foster C. Cryptanalysis for microcomputers. New York: Hayden, 1982. 101～123

2　何重阳. PC 软件破解技术彻底研究. 台北：儒林图书有限公司，1990. 129～138

3　朱传乃．80286 微型计算机系统原理分析与维修．北京：科学出版社，1992. 48～73

Encryption of Diskette by Copy Protection

Chen Jiansheng

(Dept. of Computer Science, Huaqiao Univ., Quanzhou, 362011)

Abstract　For the purpose of copy protection, the author analyses the method of recording information on a diskette and the principle of copying information from a diskette; and also the techniques of copy protection commonly used at home and abroad. Based on these analyses, a new method of creating an uncopyable 'fingerprint' code is proposed. Its application are exemplified.

Keywords　copy protection, encryption, diskette, fingerprint