

软盘的反拷贝处理:指纹(特征)制作与识别

马晓艳¹⁾ 黄德进²⁾ 杨道沅¹⁾

(1) 北京化工大学计算机系, 北京 100029; 2) 澳门濠江中学, 澳门)

摘 要: 指纹技术是计算机加密技术的一个重要组成部分, 文中详细论述了激光孔指纹、弱位法指纹及短扇区指纹的原理、制作与识别的方法。

关键词: 指纹; 软盘; 反拷贝

中图分类号: TP 309.7

1 激光孔指纹

1.1 原理

激光加密盘是使用激光在软磁盘上烧一个很小的洞状斑痕(即激光孔), 使有激光孔的扇区出现读写异常而当作指纹使用。又由于任何拷贝工具都无法把这一激光孔拷贝到另一张软盘上去, 从而达到了无法拷贝的目的。

有激光孔的扇区的特征如下: 写此扇区时一切正常; 读此扇区时, 循环校验码(CRC)错误, 进位位为CY, 寄存器AH=10H; 读出的激光孔处的数据和写入的数据不一样; 激光孔的前缘和扇区头部的距离是固定的, 激光孔后缘和扇区尾部的距离也是固定的, 激光孔的大小也是固定的(见图1)。

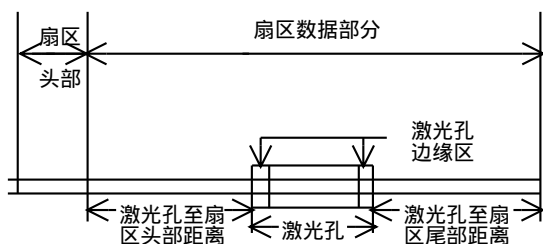


图1 扇区上的激光孔示意图

Fig. 1 The sketch map of the laser hole in a sector

1.2 制作

一般用户很难拥有用激光烧软盘的手段, 简易办法有: 格式化一张软盘; 用细针轻挑一下软盘(应在高磁道的位置); 编写一个程序, 对软盘进行

逐个扇区的读/写, 以找出孔的磁道号、磁头号、扇区号、孔大小和距离等参数, 记录到加密程序中作为原始数据, 用于和将来的测量数据相比较。注意孔的大小、深度必须适当, 以免损坏软驱磁头。

1.3 识别

用11H作为数据, 写满激光孔扇区, 再读出此扇区, 所得结果如下。

CS:0000 8C 42 11 11 11 11 11 - 11 11 11 11 11 11 11

.....

CS:00B0 11 11 11 11 11 11 11 - 11 11 11 04 40 08 04 0C

CS:00C0 0C 8E 42 F6 F7 66 F6 02 - 22 2C C0 D0 60 58 D1 81

CS:00D0 69 02 22 22 22 22 22 - 22 22 22 22 22 22 22

CS:00F0 22 22 22 22 22 22 22 - 22 22 22 22 22 22 22

.....

CS:0130 22 22 22 22 22 22 22 - 22 22 22 22 22 22 22

CS:0140 22 22 22 22 22 22 22 - 22 22 22 22 21 01 6F

CS:0150 44 42 94 13 70 4B 82 E5 - A5 C0 02 12 8E D1 11 70

CS:0160 44 0D 83 07 0E 80 2D 99 - 99 99 99 99 99 99 99

CS:0170 99 99 99 99 99 99 99 - 99 99 99 99 99 99 99

.....

CS:01F0 99 99 99 99 99 99 99 - 99 99 99 99 99 99 99

由上可见, 读出的扇区数据被分成几个区域: 激光孔前的数据区, 由写入的数据11H组成, 11H字节的个数就是激光孔到扇区头部的距离; 激光孔前部边缘区, 由无规律的随机数据组成; 激光孔区, 由相同的数据字节组成, 其数据字节的个数就是激光孔的直径; 激光孔后部边缘区, 由无规律随机数据组成; 激光孔后的数据区, 由相同的字节数据组成, 其数据字节的个数就是激光孔到扇区尾部的距离。

利用上述激光孔扇区特征, 就可以编写激光孔指纹识别程序(见图2)。

收稿日期: 1999-06-28

基金项目: 公安部资助项目

第一作者: 女, 1974年生, 硕士生

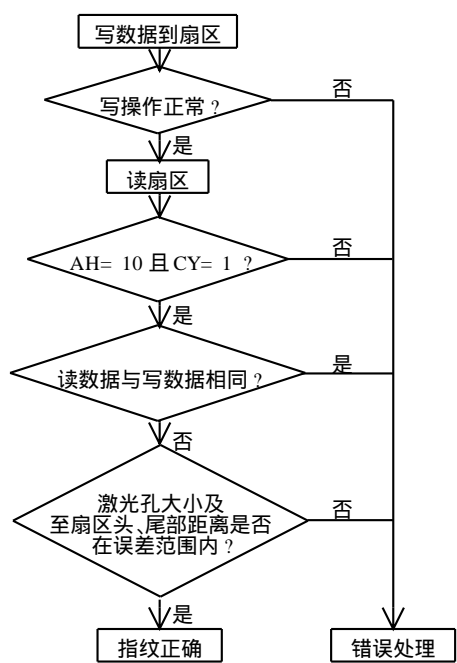


图 2 激光孔识别流程图

Fig. 2 The flowchart to find the laser hole

2 弱位法指纹

2.1 原理

磁盘中所有的信息，都是以 0 和 1 的方式记录的，当读出的记录电位高于某一阈值时，被当作 1，当读出的记录电位低于某一阈值时，被当作 0，但当读出的记录电位正好处在高阈值和低阈值的中间位置，则无法确定其值，这种电位被称为弱位。当驱动器读到弱位时，可能认为它是 1，被当作 1 拷贝出去，也可能认为它是 0，被当作 0 拷贝出去，且对同一弱位的多次读盘的结果也不同，具有很大的随机性，弱位指纹一旦被任何拷贝工具拷贝出去，便不再具有上述的弱位性质，因此是一种有效的防拷贝手段。

若扇区中含有弱位区，则有如下特性：多次读扇区，所得到的弱位区数据的结果不同，而扇区中弱位区前的正常数据区的数据固定不变；用 INT 13H 读弱位区时，AH=10H 且 CY=1；弱位区有一定的大小，弱位区距扇区头、尾部有一定的距离。

在一个磁道扇区上存在弱位区的示意图大致同图 1，其中，激光区至扇区头部距离应为弱位区至扇区头部距离，激光区应为弱位区，激光区至扇区尾部距离应为弱位区至扇区尾部距离。

弱位扇区被分为两个正常数据区和一个弱位区，如下所示(缓冲区开始地址 5A2H)。

```
26CB:05A0    22 22 22 22 22 22 22 - 22 22 22 22 22 22 22
.....
26CB:0600 22 22 22 22 22 22 22 22 - 22 22 22 22 20 22 22
26CB:0610 22 CD A8 A8 88 DE 4E 63 - 47 99 71 C1 A8 C7 3B 32
26CB:0750 AD 95 D1 D1 94 B8 00 88 - 88 88 88 88 88 88 88
.....
26CB:07A0 88 88
```

由上可见，读出的扇区数据被分成几个区域：弱位区前的数据区，由写入的数据 22H 组成，22H 字节的个数就是弱位区到扇区头部的距离；弱位区，本区数据每次读出的结果都不同，多次比较可得弱位区宽度；弱位区后的数据区，由相同的字节数据组成，其数据字节的个数就是弱位区到扇区尾部的距离。

2.2 制作

一个 INT 13H 写命令，可以分解为几个步骤(见图 3)。要想制造弱位数据区，则可在进入预定的弱位区位置时，频繁的打开和关闭控制软驱驱动器的马达来制造弱位。

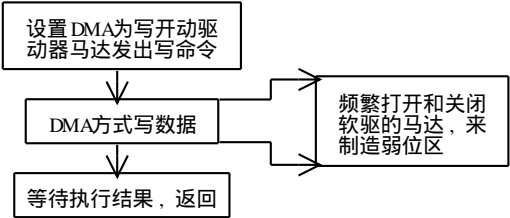


图 3 弱位区制造流程图

Fig. 3 The flowchart to make the weak region

2.3 识别

利用上述弱位扇区特征，可以编写弱位指纹识别程序(见图 4)。

3 短扇区指纹

3.1 原理

短扇区指纹是指在写扇区数据时，不写满扇区，只写一部分。用 INT 13H 读短扇区时，有 AH=10H，CY=1。正常的扇区中，对扇区中的数据要作校验码 CRC，系统自动写入(见图 5)。最有威慑力的短扇区是写满整个扇区数据，而当系统要自动写入 CRC 时，突然停止。据多次试验，各种拷贝程序都无法拷贝出此种扇区中最后几个字节数据，可当作指纹用。

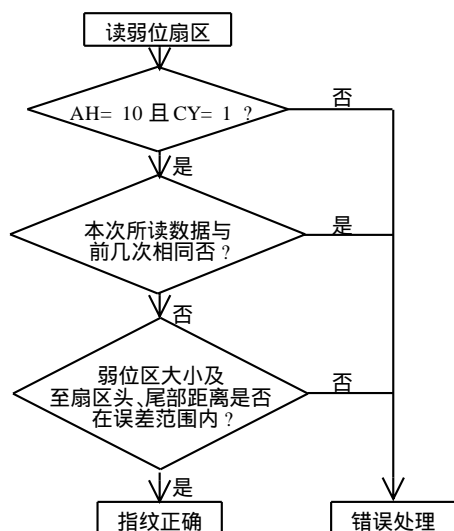


图4 弱位区识别流程图

Fig. 4 The flowchart to find the weak region

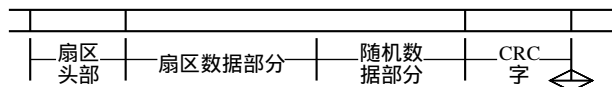


图5 短扇区示意图

Fig. 5 The sketch map of the short sector

3.2 制作

一个 INT 13H 写命令, 可以分解为图 6 左边所示的几个步骤。此图右边为短扇区制造方法。

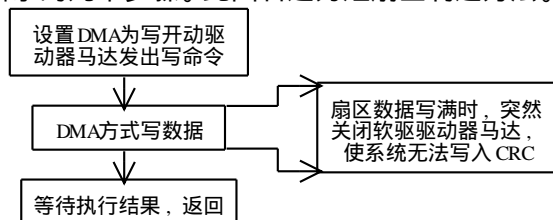


图6 短扇区制造流程图

Fig. 6 The flowchart to make the short sector

3.3 识别

以下给出短扇区识别的程序。

```

.model large
.code
start:
mov ax, @data
mov ds, ax
mov es, ax
mov bx, offset buffer2 ;指向缓冲区
xor dx, dx             ;A 驱, 0 头.
mov cx, 1001h          ;指向有短扇区磁道, 10H 道 1 扇区
mov ax, 201h           ;读
int 13h
cmp ah, 10h            ;另一特征, 读时有 CRC 错, AH = 10H
jz l12
jmp error
l12:
mov si, bx
add si, 200h - 20h ;加偏移量, 使 SI 指向扇区最后的数据
mov cx, 10h
xor bx, bx
l11:
lodsw                  ;求和
add bx, ax
loop l11
mov disk-key, bx       ;送出求和结果, 当指纹用
error:
mov ax, 4c00h
int 21h
.stack 80h
.data
buffer2 db 2000h dup (0)
end start

```

参 考 文 献

- [1] 林宣雄. 磁盘加密解密实用技术. 西安: 西安电子科技大学出版社, 1992
- [2] 毛明. 计算机软件加密实用技术. 北京: 电子工业出版社, 1993
- [3] 杨迈. 软件加密解密及反跟踪实用技术. 西安: 西安电子科技大学出版社, 1995

Method of making and discriminating fingerprint

MA Xiao-yan¹⁾ HUANG De-jin²⁾ YANG Dao-yuan¹⁾

(1) Department of Computer, Beijing University of Chemical Technology, Beijing 100029, China; 2) Haojiang middle of school, Macao, China)

Abstract: Fingerprint technology is an important part of computer software encipher, this paper presents the principles and methods to make and discriminate the laser hole fingerprint, the weak region fingerprint and the short sector fingerprint.

Key words: fingerprint; disk; anti-copy