DOI:10.13203/j.whugis1994.04.015

第19卷第4期 武汉测绘科技大学学报 Vol. 19 No. 4
1994年12月 Journal of Wuhan Technical University of Surveying and Mapping Dec. 1994

软盘额外磁道接缝加密系统

邓 祥 龚金岭

(武汉测绘科技大学,计算机科学与工程系,武汉市珞喻路39号,430070)

摘 要 采用新颖实用的额外磁道接缝技术及一系列反动态、反静态跟踪技术,编制并实现了软磁盘加密程序Newlock,使得软磁盘加密变得更加可靠、方便。

关键词 软磁盘加密解密;额外磁道接缝;磁盘指纹;反跟踪

分类号 TP309

1 构 造

本加密系统包括反拷贝、反跟踪和密文化3部分。

1.1 反拷贝技术

我们知道,磁盘由同心的磁道组成,每个磁道又分若干扇区。对于5.25 in双面低密度软盘,每面可以容纳48条磁道,其中内圈的8个磁道因互换性较差而一般不用。但是,不用并不是不能用。实践证明,至少可以安全地使用到第44磁道,从而为格式化出第41磁道提供了可能。类似地,5.25 in双面高密度盘可以格式化出第81磁道。磁道接缝技术就是在这条额外磁道上实施的。

圆形磁道总有首尾相接之处。由于磁头定位偏差,这里不可能连接得毫无缝隙,而出现一些噪音。不同磁盘、不同磁道的接缝数据不可能完全相同。一方面,格式化的长度有限,磁道首尾间的接触是格式化不到的。因此,它存在特有的磁道接缝信号。这种信号在被当作有效数据读出时,便出现了不同的杂乱信息。另一方面,不同的驱动器其转速不可能丝毫不差,即使同一驱动器其转速也会发生波动。由于这种磁道接缝信息具有指纹一样的不可复制性与唯一性,所以利用此技术制造出来的原盘几乎片片都不相同。

具体实现如下:

```
                数据段                                  代码段
PARA  DB  28H,0,1,2,  28H,0,2,2        MOV  AX,0501H
      DB  28H,0,3,2,  28H,0,4,2        LEA  BX,PARA
      DB  28H,0,5,2,  28H,0,6,2        MOV  CX,280IH
      DB  28H,0,7,2,  28H,0,8,2        MOV  DX,0000H
      DB  28H,0,9,3                    INT  13H
```

这样格式化出的第41磁道每个扇区为512byt。尽管第9扇区$N=3$,但在格式化时由于参数不作检查,而INT 1EH中的N值仍为2,所以格式化时第9扇区仍为512byt。读的时候修改INT 1EH中的参数,使$N=3$,从而在读第9扇区时读出来的字节数是128×2^3(1K),即把接缝数据也读出来了。在此基础上,就可以对接缝数据进行直接处理了。

1.2 反跟踪技术

收稿日期:1994—03—07.邓祥,男,40岁,讲师,现从事网络和图像处理研究。

采用了可靠的指纹制作技术后，加密盘不能顺利地拷贝。但是，如果没有完善的反跟踪措施，加密系统依然起不到软件保护的作用。要达到上述目的，采用的反动态跟踪技术必须达到以下要求：

1)加密程序不能静态观看，程序以密文形式存于磁盘上(全部密文化或部分密文化)。

2)加密程序不能动态跟踪执行，如果强行跟踪，程序就无法执行并导致死机。

3)加密程序只能按顺序执行，即不能跳跃执行。

本系统主要针对以下几个方面采取了相应措施：

1)破坏动态跟踪

对 DEBUG、CODEVIEW 和 SYMDEBUG 等优秀跟踪软件，把 INT 1 和 INT 3 的中断向量地址单元作为关键数据的存取地址，从而破坏如 DEBUG 中的 T、P 以及 G 命令。另外，这些调试软件需要从键盘上输入命令以及在显示器上显示一些必要信息。针对这一要求，可以采取封锁键盘从而关闭显示器的方法，达到破坏动态跟踪的目的。

禁止键盘中断和封锁显示器显示，可以分别采取如下措施：

```
IN    AL,21H      及    MOV    AH,0BH
OR    AL,02H           XOR    BX,BX
OUT   21H,AL           INT    10H
```

在需要输入或显示的时候，则可打开键盘中断，允许显示器显示：

```
IN    AL,21H      或    MOV    AH,02
OR    AL,0FDH          MOV    BX,0001H
OUT   21H,AL           INT    10H
```

2)破坏静态跟踪

本系统采用加密程序模块化技术，采用 60 个反穷举模块，每个模块 85 或 87byt 不等，在不同模块中都有反跟踪措施。只有启动模块是以明文形式存在的，其它则以密文形式存在，其密钥通过执行上一模块产生，从而形成了一条密钥链。执行过程中，本模块产生密钥在对下一模块解密的同时，也将自己密文化。所以，在文件执行过程中，整个文件只有一块正在执行的明文模块，反汇编时也只有一块明文。另外，由于对原文件也采取了全部密文化或部分密文化措施，可以防止通过反汇编进行的静态跟踪。

3)反破译

本系统采用了由 60 个模块组成的反穷举模块组，要突破这个模块组，唯一的方法就是穷举法。这样，可以从精力和时间上拖垮破译者。另外，在设计本系统前，曾分析了 SYSGUARD.COM 软件的反动态跟踪措施。此软件也采用了反穷举模块组，但因为在每个模块中采取的反跟踪措施都是破坏 INT 1 和 INT 3 的中断向量，所以可以通过修改 DEBUG 中的 G 命令，用别的中断代替 INT 3。这样，软件中破坏 INT 3 向量对修改后的 G 命令无影响，破译者就可以长驱直入了。即使偶尔在中间死机，只要记住其中一断点，下次跟踪时直接在断点处设置，就可毫不费力地跳过去。为了克服这个问题，本系统在模块中设置了若干反跟踪措施。破译者一旦死机，就必须从头开始跟踪。

1.3 密文化技术

1)密码算法的选择

加密算法的选择至少要考虑两个问题：①密码算法的开销；②密码的抗攻击强度。我们知道，软盘中的文件加密与计算机通讯中的加密有很大差别。前者采用密文技术主要是为了反跟

踪和抗分析,密码本身不要求太复杂,所以首先要考虑的是密码的时间开销和空间开销。本系统采用了简单的对称型密码中的逐字节逻辑异或法。采用这种方法,在时间开销和空间开销方面取得了较好的效果。考虑到速度问题,可以将部分原文件密文化。

2)密钥的选择

前面已经谈到,本系统采取的指纹是额外磁道的接缝数据。一般而言,要识别此指纹,在制作过程中主程序 Newlock 就必须和附加程序 lock. ovl 进行通讯,把指纹存到 lock. ovl 中去,再在 lock 中读出接缝数据与保存的指纹逐个比较,从而达到识别指纹、判别是原盘还是复制盘的目的。但这种方法留下的痕迹太多,这些存于 lock. ovl 中的指纹很可能成为破译者破译的重要线索。本系统所采用的方法是利用指纹的累加和作为加密文件的密钥。一方面,指纹不需要保存在附加程序中,对指纹的识别隐含在对原文件的解密中。如果对原文件解密不对,则说明密钥不对。另一方面,解决了密钥的生成问题,提高了系统的抗分析强度。

2　实　施

本系统有工作主程序 Newlock. EXE 以及附加程序 lock. ovl。Newlock 主要是把 lock 挂到待加密文件中去,同时对待加密文件密文化。由于被加密的可执行文件有 COM 文件和 EXE 文件 2 类,它们的文件结构有比较大的区别。

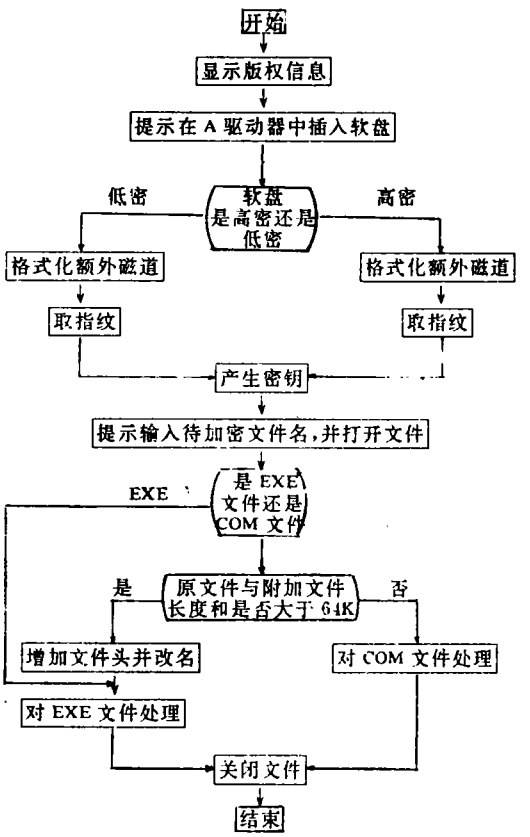

图 1　Newlock 文件主框图

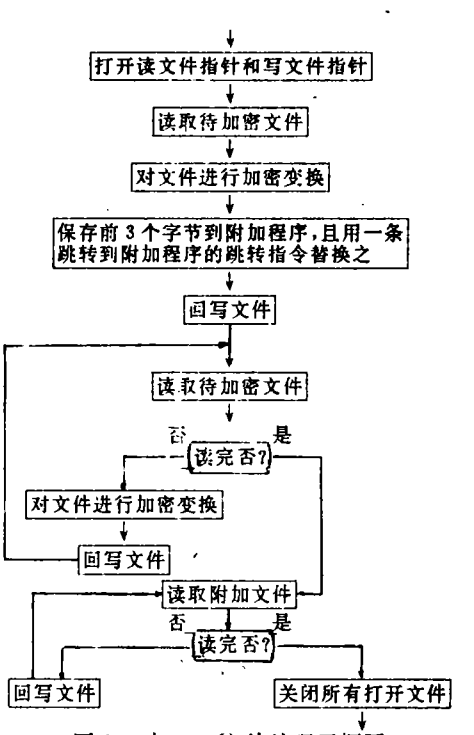

图 2　对 COM 文件处理子框图

对 COM 文件的处理,首先判断其大小,对于文件长度加上 lock. ovl 文件长度大于 64K 的则要转换成 EXE 文件。小于 64K 的文件处理比较简单,只要把附加程序挂到文件尾,同时保存

原文件前 3 个字节，且用一条跳转到附加程序的跳转指令替换之即可。

EXE 文件的处理比较繁琐。首先，要把附加文件挂到原文件尾部。为了使原文件执行时一开始就进入附加程序，必须修改文件头，使 CS：IP 指向附加程序。为了能进入原文件的原始入口，还必须保存原文件头中若干关键字节(主要是文件头中 06～1CH)。

3 评 价

1)反拷贝能力

对于一个加密系统，反拷贝能力是最基本的。本系统采用额外磁道法与磁道接缝技术，可以对抗已知的高级拷贝软件，如 COPY-WRITE 及 COPY I PC 等。

2)抗分析强度

抗分析措施可分抗静态分析和抗动态分析。本系统着眼于上述两个方面。对抗动态分析更是采取了一系列措施，如反穷举模块组以及封锁键盘和显示器等。

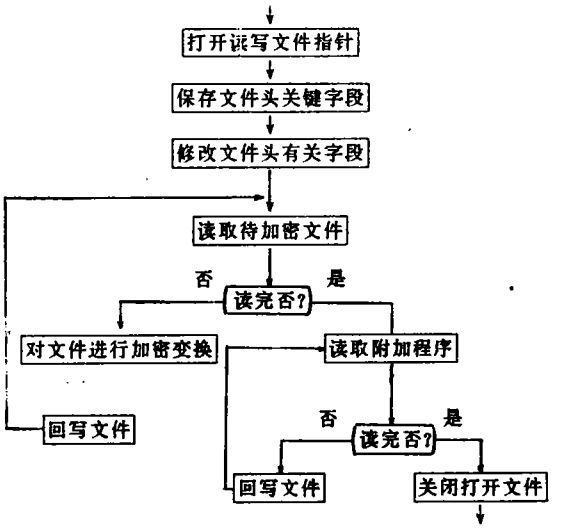

图 3 对 EXE 文件处理子框图

3)加密效率

本系统加密后的文件大约增大了 10K 左右。运行时，加载时间对用户程序的影响不明显。

4)加密成功率

为提高加密成功率，本系统主要采取了失败重复法。实践中尚未发现不成功的例子。

5)适用范围

本系统适用于 IBM-PC 系列微机及其兼容机，可以对 5.25 in 的高密和低密软盘进行加密。

参 考 文 献

1 杨 迈，李 卫，郑自修. IBM-PC 微型计算机软件加密/解密及反跟踪实用技术. 西安：西安电子科技大学出版社，1991.

2 龚金岭. 计算机加密与解密技术初探：[学位论文]. 武汉，武汉测绘科技大学计算机科学与工程系，1993

An Encrypt System by Extra Magnetic Track Gap

Deng Xiang *Gong Jinling*

(Dept. of Computer Science and Engineering, WTUSM, Luoyu Road 39, Wuhan, China, 430070)

Abstract By using extra track gap, anti-dynamic and anti-static tracing techniques, a floppy encrypt program Newlock was implemented, which makes the encryption more reliable and convenient.

Key words floppy encrypt; extra track gap; floppy fingerprint; anti-trace