扇区接缝软指纹反拷贝技术

赵星明 (山东水利专科学校)

摘要:软盘控制器写扇区数据是从数据场的同步字段开始的,因磁头定位及转速的误差,使某些字段的数据发生变化,以变形的数据作为"指纹"并嵌入被加密的应用程序中,便可以辨别是原盘还是复制盘。对于正常扇区更具有隐蔽性和对抗性。

一、引 言

近几年来,我国计算机技术发展迅速,大批优秀软件不断推出。软件开发者为了保护自己的合法权利和经济效益,对程序加密。软件加密技术可以说是五花八门,各有千秋。但软件加密技术不仅是反拷贝技术,还包括反跟踪技术和密文技术。对软件加密需投入大量的人力和财力,因此,国内对软件加密使用的反拷贝技术的种类并不多。最先使用的反拷贝技术已被很多解密者轻易地破译,如额外磁道法、额外扇区法等,以后所使用的超级扇区技术、未格式化磁道法、人为生成伪 CRC 法、磁道接缝软指纹技术等因解密较困难而被广泛采用,但这些反拷贝技术都有一个显著的共同特点,即人为地在磁盘上制作一个明显的特殊标记。不论是在正常磁道或额外磁道上,都能被解密者轻易地找到加密点,然后仿真原盘"指纹"而被复制。扇区接缝软指纹反拷贝技术并不是一种新技术,只是本文增加了新的内容。

二、扇区接缝软指纹反拷贝技术的原理

磁盘的格式化命令将每个磁道沿径向划分成若干个扇区,扇区物理长度为 512 个字节。实际上 512 个字节是指扇区中数据域的长度而不是指整个扇区的长度,扇区中除了数据域外还有其它域。每个扇区由标识域、间隙 1、数据域、间隙 2 组成,标识域包括同步字段(SYNC)、ID 地址标志(AM1)、ID 字段和循环冗余校验码(LYCRC),数据域包括同步字段(SYNC)、数据标志(AM2)、数据字段(DATA)和校验码(CRC),两个间隙用作缓冲。图 1 示出了扇区的完整构成。

	←——标识域——→					间缝 1	←——数据域——→					间缝 1
	SYNC	AM1		ID	CRC	GAP1	SYNC	AM2		DATA	CRC	GAP2
MFM	12 字节	3 字节	1 字节	4 字节	2 字节	22 字节	12 字节	3 字节	1 字节	512 字节	2 字节	可变字节
	00H	A1H	FEH	* *	* * *	4EH	00H	A1H	FBH / F8H	(DATA)	* * *	4EH

图 1

每个字段的内容是格式化时自动填入的,若格式化参数不变,两片软盘的同一道同一扇区的每个字段的内容是一样的。每个扇区的第一个 SYNC 用于读 ID 场的同步,第二个 SYNC 用于读数据场的同步。软盘控制器是从数据场的 SYNC 开始写扇区数据的,因为不同的磁盘机会有转速上的差别,同一驱动器转速也会发生波动,因此,每写一次扇区数据场的同步字节,位置就会移动。当重写一个扇区数据时,本次磁头定位点与前一次定位点之间存在偏差致使数据场 SYNC 和 GAP2 发生了变化。我们可以把刚格式化的扇区写入数据或重复写入,然后读出整个扇区,把内容变化的某些域的数据作为软"指纹",并嵌入被加密的应用程序中,便可以辨别是原盘还是复制盘。

三、扇区接缝软指纹反拷贝技术实现方法

根据扇区接缝软指纹反拷贝的原理,可以延伸出异常 ID 法和正常 ID 法。下面以 360K 软盘为例说明其实现方法。

1.异常 ID 法

①对第 41 道(或其它道)0 面(或 1 面)进行特殊格

式化，1 扇区 ID 字段的 N 值为 04，其它扇区 ID 字段的 N 值均为 02，各扇区 ID 字段表示如下：

```
DB 40, 00, 01, 04
DB 40, 00, 02, 02
DB 40, 00, 03, 02
DB 40, 00, 04, 02
DB 40, 00, 05, 02
DB 40, 00, 06, 02
DB 40, 00, 07, 02
DB 40, 00, 08, 02
DB 40, 00, 09, 02
```

格式化时采用的数据域物理长度均为 512 字节。

②读出第 41 道 0 面 1 扇区，这样就可以把第 2 扇区的全部内容读出，而不是仅仅读出数据域的内容。

```
-d200 9ff
181B:0200  F6 F6 F6 F6 F6 F6 F6 F6-F6 F6 F6 F6 F6 F6 F6 F6 ................

181B:03F0  F6 F6 F6 F6 F6 F6 F6 F6-F6 F6 F6 F6 F6 F6 F6 F6 ................
181B:0400  2B F6 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E +.NNNNNN
181B:0410  4E 4E 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNN
181B:0420  4E 4E 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNN
181B:0430  4E 4E 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNN
181B:0440  4E 4E 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNN
181B:0450  4E 4E 4E 4E 4E 4E 00 00-00 00 00 00 00 00 00 00 NNNNN.....
181B:0460  00 00 A1 A1 A1 FE 28 00-02 02 2D B1 4E 4E 4E 4E .....(..-.NNN
181B:0470  4E 4E 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNN
181B:0480  4E 4E 00 00 00 00 00 00-00 00 00 00 00 00 A1 A1 NN..............
181B:0490  A1 FB F6 F6 F6 F6 F6 F6-F6 F6 F6 F6 F6 F6 F6 F6 ................
```

这样，可以看到第 1 扇区数据字段以后内容和第 2 扇区的全部内容，但这些数据不能作为“指纹”。

③读出第 41 道 0 面 2 扇区的数据字段，然后写入，再按第 2 步骤读出来第 1 扇区内容。

```
-d200 9ff
181B:0200  F6 F6 F6 F6 F6 F6 F6 F6-F6 F6 F6 F6 F6 F6 F6 F6 ................

181B:03F0  F6 F6 F6 F6 F6 F6 F6 F6-F6 F6 F6 F6 F6 F6 F6 F6 ................
181B:0400  2B F6 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E +.NNNNNN
181B:0410  4E 4E 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNN
181B:0420  4E 4E 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNN
181B:0430  4E 4E 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNN
181B:0440  4E 4E 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNN
181B:0450  4E 4E 4E 4E 4E 4E 00 00-00 00 00 00 00 00 00 00 NNNN.....
181B:0460  00 00 A1 A1 A1 FE 28 00-02 02 2D B1 4E 4E 4E 4E .....(..-.NNN
181B:0470  4E 4E 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNN
181B:0480  4E 4E 04 00 00 00 00 00-00 00 00 00 00 00 05 0D NN..............
181B:0490  0D 0F DF F6 B7 B7 B7 B7-B7 B7 B7 B7 B7 B7 B7 B7 ................
```

发现第 2 扇区的内容发生了变化，并且重复第 3 步骤，读出的内容都不一样。这是由于磁头定位误差使第 2 扇区的数据场 SYNC 错位而影响了其他字段，这些变形的数据很难复制，可作为“指纹”来辨别原盘和复制盘。

需要说明的是，被加密的程序在识别“指纹”时，应判别第 1 扇区 CRC 错和读出内容的最后字节，以防解密者仿真。

2.正常 ID 法

异常 ID 法加密的软盘，其加密点很容易被找到。正常 ID 法是读出正常格式化的正常磁道的某一扇区的内容作为“指纹”。这有点不可思议，实际上“指纹”是不能用 13H 或 40H 中断读出来的，它必须采用软盘控制器编程读出，在此的“指纹”也是由于磁头定位误差使数据场 SYNC 和 GAP2 发生变化形成的。以 360K 软盘第 40 道 0 面 1 扇区为例，说明正常 ID 法“指纹”的形成。

①采用软盘控制器编程读出第 40 道 0 面 1 扇区至 2 扇区内容

```
-d100 4ff
0B87:0100  F6 F6 F6 F6 F6 F6 F6 F6-F6 F6 F6 F6 F6 F6 F6 F6 ................

0B87:02F0  F6 F6 F6 F6 F6 F6 F6 F6-F6 F6 F6 F6 F6 F6 F6 F6 ................
0B87:0300  2B F6 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E +.NNNNNNN
0B87:0310  4E 4E 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNN
0B87:0320  4E 4E 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNN
0B87:0330  4E 4E 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNN
0B87:0340  4E 4E 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNN
0B87:0350  4E 4E 4E 4E 4E 4E 00 00-00 00 00 00 00 00 00 00 NNNN.....
0B87:0360  00 00 A1 A1 A1 FE 28 00-02 02 2D B1 4E 4E 4E 4E .....'...-.NNN
0B87:0370  4E 4E 4E 4E 4E 4E 4E 4E-4E 4E 4E 4E 4E 4E 4E 4E NNNNNNNN
0B87:0380  4E 4E 00 00 00 00 00 00-00 00 00 00 00 00 A1 A1 NN..............
0B87:0390  A1 FB F6 F6 F6 F6 F6 F6-F6 F6 F6 F6 F6 F6 F6 F6 ................
```

②用 13H 中断读出 1 扇区内容并重新写入

③重复步骤①

```
-d100 6FF
0B87:0100  F6 F6 F6 F6 F6 F6 F6 F6-F6 F6 F6 F6 F6 F6 F6 F6 ................

0B87:02F0  F6 F6 F6 F6 F6 F6 F6 F6-F6 F6 F6 F6 F6 F6 F6 F6 ................
0B87:0300  2B F6 4E 81 C9 C9 C9 C9-C9 C9 C9 C9 C9 C9 C9 C9 +.N.........
0B87:0310  C9 C9 C9 C9 C9 C9 C9 C9-C9 C9 C9 C9 C9 C9 C9 C9 ................
0B87:0320  C9 C9 C9 C9 C9 C9 C9 C9-C9 C9 C9 C9 C9 C9 C9 C9 ................
0B87:0330  C9 C9 C9 C9 C9 C9 C9 C9-C9 C9 C9 C9 C9 C9 C9 C9 ................
0B87:0340  C9 C9 C9 C9 C9 C9 C9 C9-C9 C9 C9 C9 C9 C9 C9 C9 ................
0B87:0350  C9 C9 C9 C9 C9 C0 00 00-00 00 00 00 00 00 00 00 ................
0B87:0360  00 14 34 34 3F C4 E0 00-40 5F 2B E9 C9 C9 C9 C9 ..44?.@~+.
0B87:0370  C9 C9 C9 C9 C9 C9 C9 C9-C9 C9 C9 C9 C9 C9 C9 C9 ................
0B87:0380  C9 C0 00 00 00 00 00 00-00 00 00 00 00 14 34 34 ..........44
0B87:0390  3F 7E DE DE DE DE DE DE-DE DE DE DE DE DE DE DE ?~..........
```

与步骤①的内容比较，发现从 1 扇区 GAP2 开始，后面的内容发生了变化。另外，还会发现软盘控制器在写入数据时，自动在数据后面写入 CRC 码和一个 4EH，

并不是只写入一个 CRC 码。

正常 ID 法使每一片软盘都可以作为加密盘，具有较强的隐蔽性和对抗性。但作者至今还没有见到采用此法加密的软件。

四、结 论

由于掌握解密技术的人越来越多，迫使国内的加密技术不断发展，尤其是反拷贝技术发展较快。如 KILL、KV200 杀病毒软件采用了软盘控制器编程加密方法，并声称系统盘不再更换，这说明了反拷贝技术已达到了很高的水平。扇区接缝指纹反拷贝技术的方法和途径多种多样，对抗性强弱不一，以上介绍的方法都对抗 COPYIIPC 和 COPYWRIT 软件的拷贝。