一键恢复技术研究

Research on Instant Recovery Technology

徐 梵 （许昌学院 许昌 461000）

摘要：介绍了微机上使用的一键恢复技术的背景、方式和原理，重点讨论了目前最成熟的两类一键恢复方法，并对两类方法进行比较，深入研究了一键恢复的原理，有助于相关产品的研发。

关键词：一键恢复 一键还原 系统备份 主引导扇区 BIOS

一键恢复又常称为一键还原、即时恢复等。一键恢复技术主要用于微机数据备份，在系统受损无法使用或受到病毒严重侵害时可以只需按下一个按键就能将系统恢复到初始状态。这种技术可以方便快速地备份和恢复数据，尤其对于一般非电脑专业人士该功能非常实用。

1 一键恢复技术的背景

系统数据备份技术由来已久，包括现在常用的GHOST软件都是经典的的备份工具。但是这类软件的使用对于一般用户是不够方便的。使用它们需要具备一定水平，要对dos比较熟悉。

不少厂商推出了拥有一键恢复功能的产品，比如IBM的系统恢复、联想的一键恢复、捷波恢复精灵、技嘉Xpress Recovery、一键GHOST、一键还原精灵、一键恢复精灵，等等。它们都可以对硬盘数据进行有效的备份，需要恢复时只需要按下一个键或组合键，不需要进行过多的操作即可快速恢复至HH以前的状态。此类产品不少，优缺点并存，它们的调用原理基本上可以分为两大类：第一，基于BIOS；第二，基于引导记录。比如以上列举的，捷波恢复精灵（第一代）、技嘉Xpress Recovery的系统恢复就是基于BIOS的。一键GHOST、一键还原精灵（个人版）、一键恢复精灵等是基于引导记录的。

2 基于BIOS的一键恢复技术

BIOS中的程序是微机开机后最先运行的，在操作装载入内存之前就已经运行了。因此这时候进入一键恢复状态是不会受操作系统影响的。

一些主板BIOS中的就有这样的模块。比如捷波、技嘉的某些主板。在主板BIOS中内建一键恢复程序就可以在微机启动时进行系统备份或恢复操作了。

以Award的BIOS为例分析，表1是Award BIOS的内部模块列表

表1 Award BIOS内部模块

模块名称	用途
SYSTEM BIOS	系统中最基本的部分，所有的BIOS都有这一部分
GROUP CODE	扩展BIOS程序，是各个厂商自己定制的不同于标准AwardBIOS的功能，实际上几乎所有的厂商都会增加这一部分内容
CPU micro code	CPU微代码，用来兼容各型号CPU
ACPI table	支持ACPI的ACPI列表。只有支持ACPI的BIOS才能真正实现ACPI功能
EPA LOGO	能源之星图形文件
LOGO BitMap	BMP格式的全屏开机画面文件
VGA ROM	集成显卡的BIOS

其中GROUP CODE模块是主板厂商可以往BIOS中增加程序的模块。一键恢复程序就可以加入其中。当开机时出现“Press F9 to recovery”等字样时按下指定的键就可以进入一键恢复程序了。

还有一些主板BIOS提供的一键恢复功能不是在启动时按下某键而是要进入BIOS调置中选择进入到该功能。但它的原理也是将一键恢复程序嵌入到BIOS中。

然而并非所有主板上的 BIOS 都内置有一键恢复程序，对于一般的主板可以尝试使用捷波的 BIOS，将其 BIOS 中相关模块抽取出来并嵌入到目标 BIOS 中，即可实现。需要注意的是源 BIOS 与目标 BIOS 所支持的主板芯片组类型要一致否则目标 BIOS 很可能无法正常工作。

内建于 BIOS 的一键恢复程序可以在系统启动初期方便地调用出来使用，但是由于 BIOS ROM 的存储容量限制，所以内置程序不可以太大，这也就造成了功能单一。虽然 BIOS 中的数据是经过压缩的，但是 BIOS ROM 的存储空间仍是相当紧张，所以一些基于 BIOS 的一键恢复程序只是实现了一部分工作，完成在系统启动初期引导用户进入一键恢复界面，然后调用存储在磁盘上隐藏空间里的真正起备份恢复作用的程序来工作。备份的数据所存放的空间一般也是存在硬盘上的，这个空间是一个隐藏空间，用户不会接触到。

3 基于引导记录的一键恢复技术

此种工作方式又可再分为两类：

(1) 基于主引导记录 MBR

(2) 基于操作系统引导记录 OBR 和系统配置文件

3.1 基于主引导记录 MBR

在 BIOS 代码自检计算机后开始按照 CMOS 记录中的配置信息从引导介质上引导。对于硬盘，BIOS 引导程序将硬盘的 0 磁头 0 磁道 1 扇区的数据加载至内存 0000:7C00 处，然后检查 0000:7DFE 处是否等于 0xAA55，若不等于则转去尝试其他启动介质，如果没有其他启动介质则提示出错。如果等于 0xAA55 则执行 0000:7C00 处的程序。MBR 程序在主引导扇区中寻找标记为活动的主分区，然后进入活动分区 OBR 引导。

以上可以看出 MBR 的程序也是在操作系统加载前运行的。因此有部份程序改动了常规的 MBR 程序，修改成带有一键恢复功能的 MBR。比如一键还原精灵(装机版)就是修了 MBR 的。

这类程序修了常规的 MBR 记录，通常它们是利用了 IBM 的工具 Xpoint Boot Manager，此工具可以从 IBM 网站取得。

d2dfdzip.exe 下载解压，其中 BMGR.EXE 是主程序，Boot.BIN 是 Boot Manager 记载的跳转指令和隐藏分区卷标的信息。

BOOT.BIN 的大小为 1536 字节，正好占用三个扇区。MBR 扇区无法存放多出的 1024 字节，于是占用 2、3 扇区。BOOT.BIN 文件偏移 1BEh – 1FDh 处为 0，此空白 64 字节用来存放分区表。

当运行 MBR 程序时，被改过的 MBR 就运行了，在屏幕上显示信息，比如“Press [F11] to Start recovery system”。按下后就进入到一键恢复界面。

进入后就可以按照提示进行操作。如果不按键，MBR 引导代码则正常启动。

此类方法需要在磁上划分出一块隐藏的分区用以存放备份数据。一般是使用 PQMagic 来划分隐藏分区的，划分为隐藏分区的意义是可以防止备份数据被病毒等破坏，比如“熊猫烧香”病毒就会删除 gho 备份文件。通过使用 PQMagic，分区表中多占用了一个表项，即增加了一个主分区，非活动的主分区。这样正常启动后用户除了感到硬盘空间少了一些外不会感到还有一个分区的存在。将这个隐藏分区的 OBR 扇区做成可引导的，可以用 sys 命令实现。在这个隐藏分区中存放 ghost.exe，PQMagic 等工具。一般为方便用户，通常是做一个自启动批处理文件 autoexec.bat，文件内容为一些批处理脚本，可以自动调用 ghost 进行备份或还原。

3.2 基于操作系统引导记录 OBR 和系统配置文件

当系统交给 OBR 时，OBR 就会在磁盘上寻找系统文件进行最后的引导。OBR 将操作系统文件载入后将控制权让出，系统文件开始工作。一般要对一个启动菜单进行处理以便进行不同的引导方式。这个好处是可以处理多操作系统并存，选择其中一个操作系统并启动。按照这个原理，一键盘恢复系统也可以通过这个菜单让用户选择来进入。对于 Windows XP，在系统分区根目录有一个 ntldr 文件，它是操作系统装载器，用来装载操作系统。boot.ini 文件指定 Windows XP 的安装路径，对于多引导系统 boot.ini 包含了在启动菜单上的操作系统选择菜单。如果安装了多个操作系统，boot.ini 中将增加相应的菜单项以便在系统启动后显示操作系统菜单供用户选择。

一键恢复程序也可以加入到这个启动菜单中。首先要制作一个磁盘镜像，其中包括可引导的 OBR。并

在 boot. ini 中增加相应的菜单信息，加入镜像文件的路径就可以了。镜像文件的制作可以用 WinImage 等。当在 boot. ini 中加入了一键恢复系统的相关菜单项后，当启动出现启动菜单时按下相应按键就可以进入到一键恢复系统了。接着的情况就和基于主引导记录的一键恢复系统一样了，一般是有个 autoexec. bat 批处理文件，使用参数自动调用 ghost 进行备份或还原。

基于 OBR 的一键恢复系统的备份文件一般不是存放在隐藏分区中的。因为这之前经过了 MBR 的引导，已经建立了磁盘盘符链，隐藏分区没有被分配盘符，无法方便地访问隐藏分区。由于不是放在隐藏分区中的，所以备份文件容易被用户误删除或被病毒等破坏。因此应该妥善保存备份文件。

一般的方法是将备份文件存放在一个“畸形目录”中。“畸形目录”使得用户不能访问，同时也能避免绝大多数据病毒的访问。

“畸形目录”的实现根据主要是利用了磁盘文件系统的命名规则及不同操作系统对文件系统不同冗余度解读所造成的差异。实现“畸形目录”有很多种方法，详细情况可通过互联网查找了解。以下着重介绍一键还原精灵（家庭版）所建的“畸形目录”。

使用 Windows XP 操作系统，进入命令提示符状态，在根目录下输入：md test. . \，则建立了一个目录。使用 dir 命令查看，目录名为“test. ”。输入命令：cd test. ，回车后系统提示找不到指定路径。在资源管理器中双击此文件夹名也无法打开提示出错。如果要访问此目录，则在开始菜单中运行“x: \test. . \”（x 为目录所在盘符）便可打开。

造成此“畸形目录”的原因是文件目录的短文件名和长文件名不一致。短文件名是“TEST ~1”，但长文件名是“TEST. ”，Windows XP 显示的是长文件名，但是如果对磁盘操作时所用的是短文件名。短文件目录项中包括文件或目录的重要信息比如起始簇号，大小等等。当我们打开一个长文件名目录时，操作系统会找它的短文件名目录项。长文件名目录项找对应的短文件名目录项是通过长文件名目录项的偏移 0DH 处的值来匹配短文件名目录项。

短文件名由 11 个字符组成字符串 shortname[ ]，校验和用 chknum 表示 ，运算过程如下：int i, j, chknum =0; for (i =11; i >0; i - -)　chksum = ((chksum &1) ? 0x80 : 0) + (chksum > > 1) + shortname[j + +];

如果运算结果 chksum 与长文件名中的 0xD 偏移处数据不相等，则操作系统不会认为此短文件名目录项对应该长文件名目录项。所以当长文件名目录项中 ODH 处的值无法匹配到短文件名目录项时则无法打开目录。畸形目录的长文件名目录项中的 ODH 是不正确的。如果通过短文件名则可以正常打开，但是 Windows XP 显示的是长文件名，通过长文件名是无论如何也无法进入目录的。在 Windows 98 的命令提示符模式下使用 dir 命令可以看到“畸形目录”的短文件名因此可以用短文件名进入目录。

至于为什么使用“md test. . \”生成了长文件件名为 test. ，短文件名为 TEST ~1 的目录，是由于命令行模式下的命令解释器未对非法字符正确处理，再加上操作对文件系统目录项的解读没有足够的纠错能力。

通过使用“畸形目录”，备份的数据得到了较好的保护。

4　两类一键恢复技术的比较

目前最成熟的两类一键恢复技术对比如表 2 所示。

表 2　一键恢复技术比较

方案 \ 指标	安全性	易用性	可靠性	通用性
基于 BIOS	高	中等	高	高
基于引导记录	较高	高	较高	中等

5　结束语

现在有不少一键恢复产品，它们使用的核心技术如本文件所述，只是作为成品会更加完善，比如并不单单调用 ghost，而是会有一个系统界面，用户进入后可以有更多的选项。

本文详细地分析研究了当前一键恢复技术，这些原理和实现方法有助于开发相关产品。

（下转第 55 页）

(上接第 52 页)

参考文献

1 陈文钦,BIOS 研发技术剖析,北京:清华大学出版社,2001.

2 BIOS Boot Specification(Version 1.01). USA:Compaq Computer orporation ,Phoenix Technologies Ltd. ,Intel Corporation,1996.

3 FAT 文件系统原理. http://www.sjhf.net/pdf/fat.pdf.

4 DARMAWAN MAPPATUTU SALIHUN. Award BIOScode injection. The CodeBreakers – Journal,2005,2(1).

5 BIOS 内部模块详解. http://www.bios.net.cn/Article/wzpd/BIOSJS/BIOSJC/20060227650.html.

6 Microsoft Extensible Firmware Initiative FAT32 File System Specification(Version 1.03). USA: Microsoft Corporation,2000.