Windows Mobile 智能手机中 Flash 数据读取功能的设计与开发①

姜 明 严项琦 (杭州电子科技大学 软件与智能技术研究所 浙江 杭州 310018)

摘 要: 阐述了如何在 windows mobile 5.0 的环境下越过文件系统直接读取 OneNand Flash。首先介绍了 OneNand Flash 的特点，然后简要地介绍了 windows mobile5.0 系统，最后介绍了如何按块读取 OneNand Flash 中的数据并将读取的数据传输给 PC。结合 Windows Mobile 上开发 GHOST 软件的实例，详细介绍了数据读取以及数据传输的全过程，并给出了部分关键代码。

关键词: Windows Mobile；OneNand Flash；数据读取

Flash Data Reading Function Based on Windows Mobile Smartphone

JIANG Ming, YAN Xu-Qi(Institute of Software and Intelligent Technology, Hangzhou Dianzi University, Hangzhou 310018, China)

Abstract: This paper explains how to read data from OneNand Flash bypass the file system in Windows Mobile 5.0 smartphone. Firstly, the characteristics of OneNand Flash and Windows Mobile 5.0 operation system are briefly introduced. Then, the paper elaborates the method of reading data from OneNand Flash with blocks and transmiting the data to PC. At last, with the instance of developing a GHOST sorftwore on Windows Mobile system, this paper explains the method in detail and shows part of the key source code.

Keywords: Windows mobile; oneNand flash; data reading

1 引言

如今，智能手机的使用日益广泛，基于智能手机的操作系统也是层出不穷，例如 Windows Mobile、嵌入式 Linux、Symbian 等。智能手机从硬件架构到软件系统与桌面电脑非常相似，主要由 CPU、内存、非易失性存储器以及其他 IO 设备构成。在非易失性存储器方面，有 NOR Flash，NAND Flash 以及结合两者优点的 OneNand Flash。

与桌面电脑类似，安装了操作系统的智能手机具有使用方便、功能强大等特点。然而，智能手机同时也具备了桌面电脑上的诸多困扰，例如病毒破坏或用户误操作而导致系统崩溃等问题。举例而言，互联网上流传的“食人鱼”病毒，该病毒能使被感染的手机耗电极快，除此之外，还有不少手机病毒能够损坏数据等。重新安装操作系统不仅费时费力，而且无法恢复用户先前已安装的各种软件配置和用户数据，针对此特点，开发一款针对 Windows Mobile 智能手机的 GHOST 的软件对快速恢复系统有着极大的意义。然而，利用 Windows Mobile 文件系统提供的接口无法读取操作系统部分，即无法完整地备份整个系统。所以，GHOST 软件必须越过文件系统直接按块读取 OneNand Flash 数据。

2 OneNand介绍

OneNand Flash是三星公司推出的一款Flash存储设备，不少移动设备都采用的三星的 OneNand Flash 作为存储器，比如多普达的智能手机。

OneNand Flash 内部采用 NAND 的 Flash 阵列存储数据，而接口则采用 NOR Flash 的接口。OneNand 的结构图如图 1 所示[1]：

① 收稿时间:2009-06-27;收到修改稿时间:2010-03-21

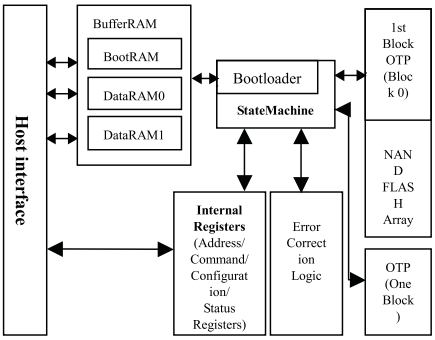

图 1　OneNand Flash 结构图

NAND Flash 价格便宜，存储容量大，但是不支持芯片内执行(XIP)，且接口复杂，管理困难。NOR Flash 支持片内执行，接口简单，可靠性高，但是其容量小，成本高昂。而 OneNand Flash 则是集成上述两者的优点，接口简单，寿命长，容量大，读取写入速度快，成本低廉等。

以 1Gb 的 OneNand Flash 为例，它具有 5KB 的片上(on-chip)缓存以及 128M 的 NAND 存储阵列，5KB 的缓存又分为 1KB 的 BootRAM，和 4KB 的 DataRAM，BootRAM 存放启动代码以供设备读取。4KB 的 DataRAM 又分为独立的两个缓存，DataRAM0 和 DataRAM1，该部分缓存存放 NAND 存储阵列中的数据。NAND 存储阵列又可分为主存储区(main area)和备用区(spare area)[2]，主存储区分为 1024 块(Block)，每块 128KB，一块分为 64 页(Page)，每页 2KB，一页又可分为 4 扇区，每个扇区 512 个字节。而备用区每块 4KB，每页 64 个字节，每个扇区 16 个字节，主存储区主要存放用户数据，而备用区存放 ECC 校验数据。

除此之外，OneNand Flash 还分布了 4KB 的寄存器用于 Flash 的读、写、擦除及编程等控制。

3　Windows Mobile 5.0介绍

Windows Mobile 5.0 是微软推出的一款开放的，可剪裁的，32 位的用于移动设备的操作系统，它继承了桌面 Windows 系统的许多功能，又突出了嵌入式系统的特点。该系统分为 Windows Mobile 5.0 for pocket pc 和 Windows Mobile 5.0 for smartphone。它基于 windows ce 5.0 的内核，并提供了强有力的个人商务管理功能，比如提供了 Office 套件，具有联系人、短消息管理、电子邮件管理以及多媒体管理等诸多功能，不但如此，Windows Mobile 5.0 允许开发人员或用户量身定制特定功能。

Windows Mobile 5.0 采用了 FAT 文件系统，内存空间划分为两部分，即内核地址空间和用户地址空间。在 Windows Mobile 5.0 中，所有进程共享一个 4G 的虚拟地址空间，从地址 0x80000000 到 0xFFFFFFF 这段空间是内核空间，而从 0x00000000 到 0x7FFFFFFF 这段空间是用户空间，其中 0x00000000 到 0x41FFFFFF 这段空间用于存放进程的虚拟地址空间，而 0x42000000 到 0x7FFFFFFF 这段地址空间是所有进程共享的，如果某已经成需要额外的地址空间，则在上述区域内申请[3]。与桌面 Windows 一样，Windows Mobile 也向开发人员提供许多功能与桌面 Windows 功能一致的 API，以此帮助用户来设计应用软件。

4　数据读取

4.1 地址映射

在 Windows Mobile 5.0 系统上，工作在用户地址空间的应用程序是无法访问内核地址空间的，同样也不能直接读取物理内存，但这不意味着应用程序无法操作物理地址，事实上，Windows Mobile 提供了一系列 API，这些 API 能将物理地址映射到应用程序能访问到的地址空间，如此一来，应用程序就能访问物理地址了[4]。

本文所描述的程序中，用到了 MmMapIoSpace 函数，该函数需要一个起始的物理地址以及需要映射的大小。映射 BootRAM 区域的示例代码如下[2]：

```
LARGE_INTEGERla={ONF_BOOT_ADDR,
ONF_BOOT_ADDR};
la.QuadPart = ONF_BOOT_ADDR;
m_pONFBP = (volatile USHORT *) MmMapIoSpace (la,
BOOTMAPSIZE, false);
```

同理，映射 DataRAM 与寄存器的代码也类似。

m_pONFDATARAM0，m_pONFDATARAM1，m_pONFREG 分别表示 DataRAM0、DataRAM1 和寄存器区域的起始地址。除此之外，本文还涉及了下述寄存器：

m_pONFBLOCKADDR:表示 NAND 存储阵列中的块地址。

m_pONFPAGESECTORADDR :表示 NAND 存储阵列中页地址和扇区地址。

m_pONFBUFRAMSTART ：表示加载到 BufferRAM 的扇区数量。

m_pONFISR :表示 OneNand Flash 的中断状态。

m_pONFCMD：命令寄存器，用于读取、写入等操作。

4.2 数据读取

在 Windows Mobile 5.0 下按块读取数据的操作流程如图 2 所示：

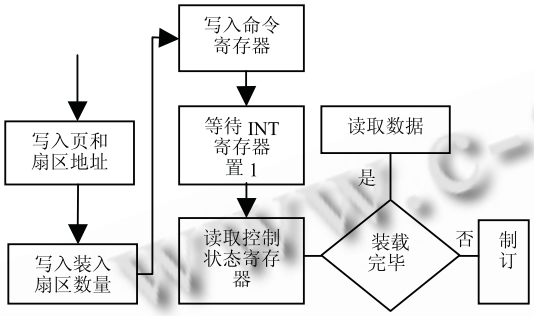

图 2 数据读取流程图

本文利用定义 GetFlashData 函数读取 OneNand Flash 数据，关键代码如下[5]：

```
WRITE_REG_USHORT(m_pONFBLOCKADDR,
dwBlockAddr);
WRITE_REG_USHORT(m_pONFPAGESECTORADDR,
usPageSectorAddr);
WRITE_REG_USHORT(m_pONFBUFRAMSTART, usSBR);
WRITE_REG_USHORT(m_pONFCMD,
CMD_LOADMAIN);
Delay();
memcpy((PCHAR)pBuf,
(LPCVOID)(m_pONFDATARAM0), DATAMAPSIZE);
memcpy((PCHAR)pBuf+DATAMAPSIZE,(LPCVOID)(m_
pONFDATARAM1),
DATAMAPSIZE);
```

dwBlockAddr 指示块地址，usPageSectorAddr 指示页地址和扇区地址，usSBR 只是装载扇区数目，本文中 usSBR 值为 4。CMD_LOADMAIN 只是装载数据的命令，如果装载主存储区值为 0x0000，装载备用区则为 0x0013。

Delay()函数获取控制寄存器中的值，测试数据装载是否完毕，实现如下：

```
USHORT usStatusMask = 0x2000;
usStatusMask                                    &=
READ_REG_USHORT(m_pONFCTRLSTATUS);
while (true)
{
    if (usStatusMask == 0) // ready
     return;
}
```

文中 memcpy(…)函数拷贝已经装载到缓存中的数据。

5 数据传输

5.1 数据传输基本思想

本文中所涉及的软件需要将读取的数据备份到桌面电脑中，因此需要移动设备和桌面进行同步数据传输。数据传输的基本思想如下：

(1) 移动设备读取数据并将数据数据写入到文件(本文中该文件文件名为 mobiledata.txt)；

(2) 桌面电脑与移动设备相连接，并获取移动设备上的 mobiledata.txt 文件内容，如果文件不为空，则复制 mobiledata.txt 文件内容至桌面电脑文件(本文中该文件文件名 desktopdata.txt) 并清空 mobiledata.txt；

(3) 移动设备定时测试 mobiledata.txt 是否为空，如空，则表明数据已被桌面电脑读取，重复步骤 1 直至所有数据读取完毕；

(4) 桌面电脑定时测试 mobiledata.txt，如果文件内容不为空，则重复步骤(2)；

5.2 数据传输程序

在移动设备端，只需要调用 API 创建文件并写入数据即可，就不多做介绍。

在桌面电脑端，需要用到 RAPI(Remote API)，RAPI 提供了一系列函数，能使桌面电脑应用程序操作移动设备。

```
hFile=CeFindFirstFile(MOBILEFILENAME,
(LPCE_FIND_DATA)&wfd);
if (wfd.nFileSizeLow != 0)
{
hFile = CeCreateFile(MOBILEFILENAME, GENERIC_
READ | GENERIC_WRITE, FILE_SHARE_READ | FILE_
```

```
SHARE_WRITE, NULL,OPEN_EXISTING, FILE_ ATTRI-
BUTE_NORMAL, NULL);
}
CeReadFile(hFile, pBuf, DATASIZE, &dwReadSize,
NULL);
CeCloseHandle(hFile);
hFile = CeCreateFile(MOBILEFILENAME, GENERIC_
READ | GENERIC_WRITE, FILE_SHARE_READ | FILE_
SHARE_WRITE, NULL, TRUNCATE_EXISTING, FILE_
ATTRIBUTE_NORMAL, NULL);
CeCloseHandle(hFile);
```

程序首先调用 CeFindFirstFile 查询 mobiledata.txt 是否存在，如果存在则调用 CeReadFile 读取 mobiledata.txt 文件，最后清空该文件。CeCreateFile 函数第五个参数若指明 TRUNCATE_EXISTING 则为清空该文件。

在本程序中，还利用了 SetTimer 函数设置了定时器，定时查看文件是否可以读写。

6 结语

本文基于 windows mobile 智能手机系统，利用 OneNand Flash 提供的物理特性读取数据，与普通的数据读取不同的是该程序没有利用 Windows Mobile 的文件系统，从而能按物理块的方式顺序地、完整地读取 OneNand Flash 中的所有数据，为进行系统级数据备份提供了有效的技术手段。

参考文献

1 Samsung Electronics Co., LTD. KFG1G16Q2B-DEBx. [2007-12-27].http://www.samsung.com/global/business/semiconductor/products/fusionmemory/Products_OneNAND.html

2 陈晓风.OneNand Flash 的操作性能与应用研究.海峡科学, 2008,12;48－52.

3 姜波. Windows CE.Net 程序设计.北京:机械工业出版社, 2007.

4 [2009-03-16] http://msdn.microsoft.com,

5 何宗键.Windows CE 嵌入式系统.北京:北京航空航天大学出版社, 20