计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2017,26(11):36−44 [doi: 10.15888/j.cnki.csa.006092]
©中国科学院软件研究所版权所有.
E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

面向存储介质的数据安全删除①

吴莎莎[1], 王敏燊[1], 吴艺萍[1], 熊金波[1,2]

[1](福建师范大学 软件学院, 福州 350117)
[2](福建省公共服务大数据挖掘与应用工程技术研究中心, 福州 350117)
通讯作者: 熊金波, E-mail: jinbo810@163.com

摘　要: 随着信息通信技术的快速发展, 存储介质中的信息量显著增加, 这些信息的长期存储容易导致隐私泄露, 仅仅删除存储介质文件索引表无法达到彻底删除的目的, 具有一定的安全隐患, 如何保护存储介质中的信息隐私安全备受关注. 针对上述问题, 首先介绍安全删除相关的基础知识, 包括存储介质的基本结构、存储原理和删除原理; 然后分析主流的数据安全删除标准, 并研究这些标准的特性; 最后, 设计与实现一种能够达到数据不可恢复的安全删除原型系统, 并对现有数据删除软件进行测试与分析. 结果表明所开发原型系统能够实现存储介质中的数据安全删除, 有效保护数据安全与隐私.

关键词: 存储介质; 安全删除; 隐私保护; 数据安全; 覆写

引用格式: 吴莎莎,王敏燊,吴艺萍,熊金波.面向存储介质的数据安全删除.计算机系统应用,2017,26(11):36–44. http://www.c-s-a.org.cn/1003-3254/6092.html

Storage Medium-Oriented Data Secure Deletion

WU Sha-Sha[1], WANG Min-Shen[1], WU Yi-Ping[1], XIONG Jin-Bo[1,2]

[1](Faculty of Software, Fujian Normal University, Fuzhou 350117, China)
[2](Fujian Engineering Research Center of Public Service Big Data Mining and Application, Fuzhou 350117, China)

Abstract: With the rapid development of information and communication technology, the amount of information in storage medium is significantly increasing. Just deleting the index file on table cannot really delete the information. Long-term storage of those information may easily lead to data leakage. Therefore, secure deletion of the storage medium is one of the most attractive research areas. In order to address this problem, the basic knowledge about storage medium is introduced in this paper, including the basic structure, the principle of storage and the principle of deletion of the storage medium. Then, some commonly standards of data deletion are analyzed, the characteristics of these standards are studied. Finally, we design and implement a secure deletion prototype system, and the existing data deletion software is tested and analyzed. The result demonstrates that the secure deletion prototype system can safely delete the data in the storage medium and effectively protect users' privacy.

Key words: storage medium; secure deletion; privacy protection; data security; overwrite

1　引言

信息技术和新型存储技术的飞速发展, 催生出各类新兴的、大容量的存储介质. 这类存储介质具有容量大、体积小、携带方便、操作简单等优良特征, 超越了传统的纸质存储介质, 使得人们更倾向于使用这类存储介质, 这也促使存储介质中的数据量急剧增多[1]. 这些数据往往包含个人隐私信息, 一旦泄露将会给用户带来严重影响.

① 基金项目: 国家自然科学基金 (61402109, 61370078); 福建省自然科学基金 (2015J05120); 福建省高校杰出青年科研人才培育计划 (2015)
收稿时间: 2017-02-20; 修改时间: 2017-03-23; 采用时间: 2017-04-05

© 中国科学院软件研究所 http://www.c-s-a.org.cn

这类存储介质给人们带来极大的便捷, 同时也带来隐私安全隐患. 当存储介质中的数据不再被用户需要时, 用户可以删除该数据. 但这种方法只是对文件分配表进行重新设置, 不会使数据从存储介质的物理数据区中消失, 删除的数据仍然存在于存储介质中, 数据被恢复的可能性很高, 这对存储介质中数据的安全造成极大的威胁[2]. 因此, 如何对存储介质中的数据进行安全删除成为人们关注的内容.

现有的存储介质数据删除方式主要有三种, 分别为物理摧毁、消磁和数据覆写[3-5]. 其中, 物理摧毁和消磁属于硬销毁技术. 通常硬销毁技术一旦使用, 存储介质将无法再次使用, 因此, 一般不常采用此类方法进行数据删除. 数据覆写属于软销毁技术, 和硬销毁技术不同的是, 软销毁技术对数据进行销毁后, 存储介质能够继续使用. 存储介质中的数据区如果仅以全“0”的方式覆写, 仍可通过深度数据恢复技术对数据进行恢复, 其原理是基于磁盘的剩磁效应, 磁盘被覆写后, 仍可以在深度显微镜下观察到之前数据的痕迹. 因此, 以全“0”对数据进行覆写后仍可被恢复. 增加覆写的次数和覆写数据的随机性, 能够降低数据被恢复的可能性[3]. 目前的数据删除标准有 DOD 5220.22-M 简单擦除、DOD 5220.22-M 标准擦除[6,7]、Guttman 标准[8]、RCMP TSSIT OPS-Ⅱ标准[9]等. 这些数据删除标准提高了存储介质中数据的安全性, 但仍存在一些局限性. 比如, DOD 5220.22-M 标准没有从理论方面论证 7 次或 3 次覆写的原因, 也没有评估它的安全性, 不符合用户的数据价值度; Guttman 标准虽然论证了安全性, 但是 35 次的覆写非常耗时, 并且覆写数据又存在大量冗余[10].

针对上述存储介质数据安全删除中存在的问题, 本文首先对安全删除相关的基础知识, 包括存储介质的基本结构、存储原理和删除原理进行介绍; 然后分析主流的数据安全删除标准, 并深入研究这些标准的特性以及存在的局限性, 最后在此基础上, 设计并实现一种能够根据用户对不同数据的安全需求, 灵活自定义安全删除的原型系统, 解决现有的问题.

文章接下来的组织结构如下: 第 2 部分介绍存储介质的结构和存储原理; 第 3 部分概述存储介质的删除原理; 第 4 部分对删除标准进行介绍和分析; 在第 5 部分介绍本文提出的原型系统; 最后在第 6 部分总结全文.

2 存储介质的结构与存储原理

目前常用的存储介质有硬盘、光盘、Flash 存储器和固态硬盘, 下面分别对其结构和存储原理进行分析.

2.1 硬盘

硬盘是常用的存储介质之一, 是现代计算机主要的存储媒介, 由一个或多个铝制或玻璃制的碟片组成, 碟片外覆盖有铁磁性材料. 硬盘有许多不同类型, 本文所描述的硬盘指机械硬盘.

2.1.1 硬盘的基本结构

硬盘的内部由磁头组件、磁头驱动组件、盘片等[11]组成, 各部分功能如下所述.

(1) 磁头组件. 硬盘是根据磁场变化读写数据. 磁头通过感应盘片的磁场变化读取盘片中的数据, 通过改变盘片上的磁场写入数据. 为了保护硬盘, 磁头在工作时, 悬浮于盘片上空, 不与盘片接触. 关闭电源后, 磁头返回盘片的着陆区.

(2) 磁头驱动组件. 硬盘中, 磁头是靠磁头驱动组件来工作的, 硬盘的寻道时间与磁头驱动组件息息相关. 高精度的轻型磁头驱动机构能够正确的驱动和定位, 保证数据读写的可靠性.

(3) 盘片. 盘片是硬盘磁性存储材料、保护材料等的载体, 多由铝合金或玻璃基底组成. 其中磁性介质的物理性能和磁层结构影响着数据存储的密度和稳定性.

新买的硬盘不能直接使用, 必须对其进行分区并格式化后才能储存数据. 经过格式化分区后, 逻辑上每个盘片的每一面都会被分为磁道、扇区、柱面这几个虚拟的概念[12].

2.1.2 硬盘的存储原理

硬盘是利用磁粒子的极性记录数据. 磁头在读取数据时, 将磁粒子的不同极性转换成不同的电脉冲信号, 再利用数据转换器将原始信号转换成电脑可以识别的二进制流数据; 写操作与此相反.

当接口电路接收到微机系统传来的指令信号时, 通过前置控制电路, 驱动音圈电机发出磁信号, 磁头感应阻值变化对盘片数据信息进行正确定位, 并将接收后的数据信息解码, 通过放大控制电路传输到接口电路, 反馈给主机系统完成指令操作[12].

2.2 光盘

光盘多作为电子出版物的存储介质, 可以存储文字、声音、图形、图像等多媒体数字信息. 以下对光盘的基本结构和数据存储原理进行介绍.

© 中国科学院软件研究所 http://www.c-s-a.org.cn

2.2.1 光盘的基本结构

光盘的物理结构主要分为五层, 分别为基板、记录层、反射层、保护层、印刷层. 本节重点讲述基板与记录层.

(1) 基板. 基板是光盘各功能的载体, 也是光盘的物理外壳. 不同类型光盘的基板并无任何区别.

(2) 记录层. 记录层是光盘录入信号的地方, 其在基板上涂上有机染料, 来供激光记录信息. 烧录后的反射率不同, 读取的信号长度也不同. 反射率的变化形成“0”与“1”信号, 借以读取信息.

2.2.2 光盘的存储原理

光盘的数据存储原理因光盘的类型不同而不同. 本节对不可重复擦写的光盘和可重复擦写的光盘进行介绍.

(1) 不可重复擦写. 不可重复擦写光盘是一种仅可一次录入的光盘. 烧录时形成“坑”, 有“坑”和无“坑”的状态形成“0”和“1”的信号. “坑”与“坑”之间的凹凸交界均代表二进制“1”, 两个边缘之间代表二进制“0”. 这些“坑”是不能恢复的, 将永久性地保持现状, 这也就导致了光盘不可重复擦写.

(2) 可重复擦写. 可重复擦写[13]光盘的记录层涂抹的是某种碳性物质. 当激光在烧录时, 改变碳性物质的极性, 来形成特定的“0”、“1”代码序列. 这种碳性物质的极性可以重复改变, 因此, 此类光盘可以重复擦写.

2.3 Flash 存储器

Flash 存储器具有非易失、抗震动、体积小等特性, 并且不需要电来维持存储的信息. 并且 Flash 存储器容量大、价格较低, 因此 Flash 存储器的使用越来越广泛.

2.3.1 Flash 存储器的基本结构

Flash 存储器主要可以分成 NOR Flash 和 NAND Flash 两大类[6], 两者的共同点是都将存储单元组织为块阵列. 块是擦除操作的最小单位, 页是读操作和写操作的基本单位. 两种类型的 Flash 存储器也存在一定的差异. NOR Flash 存储器以并行的方式连接存储单元, 有独立的数据线和地址线, 传输效率高, 但容量小、价格高. 因此, NOR Flash 存储器多用于手机及嵌入式系统的代码存储. NAND Flash 存储器以串行的方式连接存储单元, 读取速度较慢, 但写操作和擦除操作相对于 NOR Flash 存储器较快, 且容量大、价格低. 因此, NAND Flash 存储器多用于数码相机、MP3 等进行数据储存[14]. 本文主要介绍 NAND Flash 存储器, 因其更适合存储系统. NAND Flash 存储器的页通常为 512 B、2 KB、4 KB, 一个块通常包括 32、64 或 128 个页. 每个页包含数据区和带外区, 数据区用于存储用户数据, 带外区用于存储纠错码等用于 Flash 存储管理的信息.

2.3.2 Flash 存储器的存储原理

Flash 存储器具备电子可擦除可编程的性能, 并且不会因为断电丢失数据同时可以快速读取数据. Flash 存储器的基本结构是每单元一个晶体管, 电流通过时它的状态从“1”变成“0”. 读取数据时是一次读取一块, 通常是一次读取 512 个字节. 在对页进行写操作之前需要判断该页中所有的位是否为“1”. 如果全部为“1”, 则可以进行写操作; 否则, 需要先进行擦除操作. 在数据更新时, Flash 存储器无法做到就地更新, 而是雇佣一个新的地址来写入新数据, 保留原始数据并将其标记为无效[16].

2.4 固态硬盘

固态硬盘 (Solid State Drive, SSD) 是基于半导体存储芯片阵列的硬盘. 与传统的机械式硬盘不同, SSD 没有采用任何机械结构, 是完全电子化的. SSD 具有容量大、抗震性好、低功耗、无噪音等优点. 由于 SSD 的诸多优良特性, 使其得到广泛使用.

2.4.1 固态硬盘的基本结构

固态硬盘是用固态电子存储芯片阵列制成的硬盘, 由控制单元和存储单元组成. SSD 的内部主体是一块 PCB 板, 其基本配件分为控制芯片、缓存芯片和闪存芯片三部分. 控制芯片的作用是合理调配数据在各个芯片上的负荷, 连接闪存芯片和 SATA 接口; 缓存芯片的作用是辅助控制芯片进行数据处理; SSD 的闪存芯片多用 NAND Flash 存储器, 主要分为单层单元 (Single Level Cells, SLC) 和多层单元 (Multi-Level Cells, MLC) 的 NAND 闪存[17].

2.4.2 固态硬盘的存储原理

SLC 每单元存储一个比特或两种状态“1”或者“0”, 而 MLC 每单元存储两个比特或四种状态, 即“00”、“01”、“10”、“11”四种状态. SSD 有一个平均故障间隔 (MTBF, mean time between failure), 一般是每单元 10000-100000 次写操作, 所有可用的 NAND Flash 存储器被均匀的使用. 反复在某个指定部分进行写操作会降低其使用寿命. 因此, SSD 使用耗损均衡, 在单页被再次使用或者删除前将数据写入可用的页中.

损耗均衡是 SSD 控制器运行的一个算法, 使数据

© 中国科学院软件研究所 http://www.c-s-a.org.cn

均匀的分布在整个 NAND Flash 存储器的所有页. 它的目的是增加驱动器的整体续航能力使其超过单个 NAND 单元的续航能力. SSD 控制器保留驱动器中所有可用空间的轨道, 不会真的删除任何数据直到可用的页被利用, 即使这些文件在文件系统中已经被删除[18].

SSD 不仅拥有 Flash 存储器的优势, 而且还有丰富的内部并行特性[19], SSD 进行读/写操作时不需要寻道, 所以读/写的速度比硬盘要快. 并且工作温度范围大[17], 大多数 SSD 可以在-10-70 摄氏度的环境下工作, 而一般的硬盘工作温度是 5-55 摄氏度. 但也存在一些局限性, 比如成本高、价格贵等. 本节介绍了常见的四种存储介质的基本结构和数据存储原理, 并在表 1 进行对比.

表 1 存储介质的综合比较

存储介质类型	存储结构	存储原理	优势	局限性	应用场景
硬盘	由磁头组件、磁头驱动组件、盘片等[11]组成	利用磁粒子的极性记录数据	容量大、响应速度快、传输速率高、存储非线性、价格低	机械寻道导致读、写速度较慢; 有噪音	笔记本电脑等
光盘	分为五个部分: 基板、记录层、反射层、保护层、印刷层	通过改变一个存储单元的某种光学性质, 使其性质变化反映被存储的二进制“0”、“1”信息	记录介质磨损小, 受环境污染的影响小; 光盘的光道记录比磁盘的磁道记录密	存储容量比其它存储介质小	电子出版物的存储介质、激光视盘DVD等
Flash存储器	存储单元组织为块阵列, 块由页组成, 每个页分为数据区和带外区两个部分	页是读操作和写操作的基本单位; 对页进行写操作之前需要判断该页中所有的位是否为“1”	非易失性、固态性、体积小、重量轻、抗震动、高性能、低能耗等	NOR Flash:容量小、价格高; NAND Flash: 读取速度较慢	NOR Flash: 手机、BIOS芯片以及嵌入式系统中进行代码存储; NAND Flash: 数码相机、笔记本电脑中进行数据存储
固态硬盘	采用固态电子存储芯片阵列制成的存储介质, 由控制单元和存储单元两部分组成	文件存储在页中, 页组成块	读写速度快、防震抗摔、低功耗、无噪音、工作温度范围大、轻便	成本较高、价格贵	移动硬盘、笔记本电脑、服务器等

3 存储介质的删除原理

本节分别对硬盘、光盘、Flash 存储器和 SSD 的删除原理进行简要介绍.

3.1 硬盘删除原理

硬盘的删除方法主要有: 覆写、消磁和物理摧毁. 具体的删除原理如下所述:

(1) 覆写. 该方式是通过软件或设备自行产生新数据将旧数据的存储地址处覆写[12]. 大多数使用的新数据是全“0”或全“1”的代码数据以及随机产生的代码数据. 部分机构要求, 首先使用全“0”的代码数据, 再使用其反码, 最后使用随机的代码数据, 进行多次的覆写达到更好的删除效果. 全“0”和全“1”覆写时, 原来的“0”和“1”的数据不变, 恢复时能够得到原来的碎片信息. 随机覆写可能每一位都改变, 恢复数据的概率与前一种相比较低.

(2) 消磁. 该方式是通过电子控制驱动生成一个强磁场, 使表面的磁性颗粒极性方向全部相同, 达到安全删除数据的目的. 并且在消磁的过程中磁盘的伺服信息被清空, 硬盘将无法使用[3]. 消磁这种方式非常彻底, 无法恢复.

(3) 物理摧毁. 物理摧毁是指通过外力对其彻底毁坏, 达到安全删除数据的目的. 主要手段有: 回炉、粉碎、焚烧、解体; 甚至融解等简单、粗暴的物理摧毁方式等; 化学腐融, 使用化学物品溶解磁盘表面的氧化铁颗粒. 这些方法费时、费力、效果差, 因此未被广泛使用.

3.2 光盘删除原理

光盘的数据删除方法主要有激光刻录和物理摧毁两种, 下面对其删除原理进行简要概述.

(1) 激光刻录. 激光刻录适用于光盘类存储介质. 光盘是使用激光改变粒子极性进行存储, 重新激光刻录光盘用新数据将旧数据覆写, 达到无法恢复的目的.

(2) 物理摧毁. 这个方式是最简单、最粗暴、最为彻底的摧毁方式, 常常用盘片划损、外力破损甚至融解等物理摧毁方式. 使用此方法后, 光盘将无法继续使用.

3.3 Flash 存储器删除原理

Flash 存储器的数据删除方法主要有两种: 第一种

© 中国科学院软件研究所 http://www.c-s-a.org.cn

是对文件的所有数据进行覆写; 第二种是对文件数据进行加密, 然后再采用第一种方法删除密钥.

文献[20]提出一种“0”覆写和块擦除混合的删除方案. “0”覆写是用“0x00”覆写页上的内容来保证现有数据安全删除的方法; 块擦除是通过擦除操作来删除块上所有数据, 如果此时有效页在块上, 那么这些页将会被存储到其它块中, 这就造成额外的读操作和写操作. 文献[20]中所提方案的步骤如下: (1) 搜索需要被删除的页; (2) 检查采用覆写方式删除页的花费是否比块擦除更低, 如果是, 就采用“0”覆写方式删除; (3) 否则, 采用块擦除方式删除.

文献[21]提出一种基于数据加密的安全删除方法. 随机产生密钥对文件进行加密, 密钥存储在一个块中. 因此, 进行擦除操作的时候只需删除文件对应的密钥, 虽然文件仍然存在, 但是密钥已被删除, 无法对文件进行解密, 所以视为文件已被安全删除. 文献[21]所提方案的步骤如下: (1) 搜索存储需要删除的文件对应的密钥所在页; (2) 检查该块中除需要删除的密钥外是否存在有效密钥, 如果存在, 则将有效密钥存储到其它块中; (3) 删除该块.

3.4 固态硬盘删除原理

SSD 控制器只有在用完不包含任何数据的空余空间或页并且没有被主操作系统引用或者删除的时候才开始删除数据. SSD 中文件是存储在页中, 页组成块. 当数据被写入页后, 只能在块中被删除. 一个块可以存储多个文件, 但块是最小的删除单位. 新数据写入 SSD 时, 磁盘控制器需要创造空闲空间或页. 当需要创造空闲空间时, SSD 使用缓存, 缓存位置通常是 SSD 中的一个芯片. 新数据被写入空闲页. 块中的最无效页的数据被删除, 并且标记为“1”. 然后在缓存中, 这些页被从块中移除, 仅留下有效页. 最后数据块从缓存中移动到有效块. 新的重置块被添加到控制器的空闲空间中[18].

近年来, 针对硬盘的数据安全删除方法已经很成熟, 但由于 SSD 和硬盘存在许多的不同, 所以现有的硬盘安全删除方法并不全都适合运用于 SSD 中. 因此, 文献[22]提出一种适合 SSD 的安全删除方法, 能够更好的保护用户的隐私信息, 但也存在局限性, 比如文件删除速度慢.

本节对四种存储介质的删除原理进行概述, 并且在表 2 进行归纳总结.

表 2 存储介质删除方式对比

存储介质类型	删除方式	是否做到安全删除	局限性
硬盘	覆写	具体和选择的覆写方式与覆写次数有关	覆写次数较少的情况下, 有可能恢复部分数据
	消磁	是	硬盘将无法使用, 成本高
	物理摧毁	存在被恢复的可能性	硬盘不能继续存储, 成本高
光盘	激光刻录	是	仅限于光盘类
	物理摧毁	是	光盘不能继续存储
Flash存储器	覆写和块擦除结合[20]	不满足NSA/CSS安全删除要求	不满足NSA/CSS安全删除要求; 多层单元的Flash存储器中运用块删除时会破坏数据完整性
	基于数据加密[21]	不满足NSA/CSS安全删除要求	没有进行覆写操作不能很好的保护数据的安全删除
SSD	基于口令的单文件加密和安全删除方法[22]	是	文件删除速度慢

4 安全删除标准

目前数据安全删除的标准很多, 例如, DOD 5220.22-M 简单擦除、DOD 5220.22-M 标准擦除、Guttman 标准、RCMP TSSIT OPS-Ⅱ标准等. 本节对 DOD 5220.22-M 简单擦除、DOD 5220.22-M 标准擦除和 Guttman 标准进行介绍.

4.1 DOD 5220.22-M 简单擦除

DOD 5220.22-M 简单擦除标准中根据不同的存储介质类型有不同的删除方法, 这里以移动硬盘产品为例, 推荐的擦除方式是, 首先用相同字符对所有可能的区域进行一次覆写, 然后用其反码再覆写一次, 最后再用随机数据进行覆写, 可以有效地覆写原有的数据信

© 中国科学院软件研究所 http://www.c-s-a.org.cn

息. 该推荐擦除方式的一种可能覆写序列如下:

(1) 写入全“1” “11111111”

(2) 写入全“0” “00000000”

(3) 写入随机数据 “sdhignwd”

4.2 DOD 5220.22-M 标准擦除

不同的数据, 其敏感性是不同的. DOD 5220.22-M 简单擦除可以对原有的数据进行有效的覆写, 但仍存在被恢复的可能性, 对于需要更高安全级别的数据不能满足其对安全性的要求. 在这种情况下, 可以考虑使用 DOD 5220.22-M 标准擦除对数据进行覆写. DOD 5220.22-M 标准擦除使用 7 次覆写, 该方法进行三次随机数覆写、两次相同字符覆写、两次覆写数据的反码. 相比于 5220.22-M 简单擦除, 更为复杂. 并且多使用随机数据, 更具有随机性, 删除安全性得到一定程度的提高.

一种可能的覆写序列如下:

(1) 写入全“0” “00000000”

(2) 写入全“1” “11111111”

(3) 写入随机数据 “deigngi3”

(4) 再写入全“1” “11111111”

(5) 再写入全“0” “00000000”

(6) 再写入随机数据 “dhii3iea”

(7) 再写入随机数据 “deog83ha”

4.3 Guttman 标准

Guttman 标准[8]运用实现 35 次覆写, 耗时较长, 适合用于极为机密、有价值的数据. 标准规定其前 4 遍以及后 4 遍采用 0 到 255 随机数进行覆写, 剩余次数根据相应的数据流和编码方式进行覆写. 表 3 对本节提到的安全删除标准进行比较.

表 3 安全删除标准比较

安全删除标准	覆写次数	覆写方式	耗时	安全性
DOD 5220.22-M简单擦除	覆写3次	一次相同字符覆写, 一次其反码覆写, 一次随机数据覆写	短	低
DOD 5220.22-M标准擦除	覆写7次	两次相同字符覆写, 两次其反码覆写, 三次随机数据覆写	较短	中
Guttman标准	覆写35次	前4次和后4次为0到255的随机数, 剩余的根据特定的数据流和编码方式进行覆写	较长	高

5 安全删除原型系统设计与分析

5.1 原型系统开发环境

原型系统运行环境为 Windows7 操作系统, Microsoft Visual Studio2010 以上版本, CPU 环境为 AMD Athlon(tm) II X2 250 Processor 3.00 GHZ, RAM 为 4.00 GB, 硬盘为 500 GB.

5.2 原型系统概述

本文在 PC 平台上开发了一种面向存储介质的安全删除原型系统, 采用随机数据覆写的方式, 根据用户所需的安全性自行选择擦除次数, 同时兼容 DOD 5220.22-M 简单擦除标准和 DOD 5220.22-M 标准擦除标准. 原型系统能够提供第一遍以相同字符覆写, 第二遍用其反码覆写, 第三遍以随机数据覆写的 DOD 5220.22-M 简单擦除删除方式, 以及 0 到 255 随机数据和反转数据组成的 7 次覆写的 DOD 5220.22-M 标准擦除删除方式. 并且开发了快速删除功能、DOD 5220.22-M 删除功能、自选擦除次数删除功能, 以及复制功能、查询功能、USB 监听功能等.

5.3 原型系统模块结构设计

本系统使用制作界面优异的 Microsoft Visual Studio 2016 开发软件. 开发重点在于计算机与存储介质的交互关系.

系统主要分为查看文件模块、复制模块和删除模块. 安全删除原型系统的体系结构如图 1 所示.

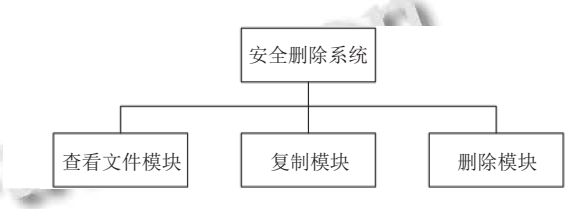

图 1 系统体系结构

(1) 查看文件模块: 包括 USB 监听、文件信息全部显示和条件检索三部分, 如图 2 所示.

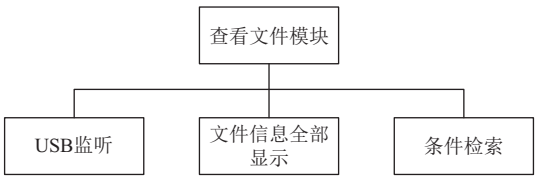

图 2 查看文件模块结构图

(2) 复制模块: 包括复制的目的地址选择和文件复制备份两部分, 如图 3 所示.

(3) 删除模块: 包括快速删除、DOD5220.22-M 标准、自定义删除等, 如图 4 所示.

© 中国科学院软件研究所 http://www.c-s-a.org.cn

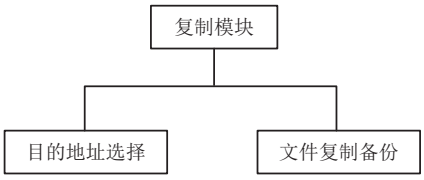

图 3 复制模块结构图

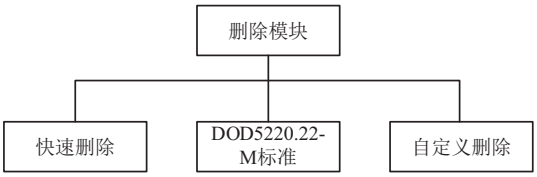

图 4 删除模块结构图

由于每个用户的需求不同, 所要求的擦除次数也不同. 并且, 采用随机数更具随机性, 对数据的覆写更为彻底. 因此, 本文开发的安全删除原型系统需要自定义删除功能.

安全删除原型系统由一个判断和四个动作组成: 首先, 对参数的正确性进行判断, 如果正确, 则获取用户的擦除次数和存储空间大小, 对该空间进行分组, 每组根据擦除次数使用随机数覆写. 如图 5 所示.

5.4 原型系统测试与评价

为排除外界因素的影响, 本节采用各种不同的删除软件对普通文件进行删除操作, 普通文件由各种格式的文档、视频数据、音频文件、图片、软件等组成, 固定为 4.33 GB.

系统测试用到的删除软件概述如下: Active CD/DVD RW Eraser, 可积极擦除 DVD-RW、DVD+RW 或 CD-RW 媒体从磁盘上清除旧数据; 光盘刻录大师, 具有光盘备份与复制、刻录数据光盘、制作光盘映像、刻录光盘映像文件、擦除盘片等强大功能; Ashampoo Buring Studio, 已支持的 CD 和 DVD 刻录机超过 1500 种, 操作方便, 是一款用户体验不错的刻录工具; Free Disc Burner, 可将任何文件、文件夹或数据刻录到任何光盘, 可以将文件写到已经使用过的光盘, 并擦除光盘里的资料, 支持蓝光; ISO Burner, 是易使用和强有力的 ISO 刻录工具; Ones 刻录软件, 是一款小巧简洁的刻录软件, 无需安装, 绿色环保; Astroburn Pro, 是一款可以快速进行光盘刻录与制作的软件, 提供了几乎所有的储存格式类型刻录、复制和删除功能.

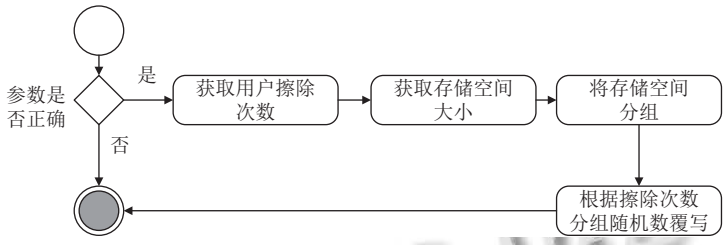

图 5 安全删除原型系统流程图

本节对所开发原型系统安全删除 4.33 GB 文件的删除时间进行测试并与现有删除软件进行对比, 实验结果如图 6 所示. 从图 6 中可以看出, 大部分可恢复软件的删除时间较短, 但这些软件无法实现数据的安全、不可恢复删除. 本文原型系统的删除时间比不可恢复删除软件 Ones 略高, 但在可接受的范围. 本文考虑到不同用户对数据安全的需求不同, 设计了自定义删除功能, 用户可以根据实际数据的安全需求选择删除次数和覆写方式.

图 7 根据删除文件后的效果对删除软件进行分类, 其中, 光盘刻录大师等删除软件能够在短时间内实现文件的快速删除, 但被恢复的可能性很高; Quick DVD/CD Burner 等软件的删除时间相对较长, 删除后的文件不可读取, 能够达到较好的删除效果; AVS Disc Creator 删除时间较短, Ones 和本文原型系统的删除时间相对较长, 但均可实现对文件的安全删除.

6 结论

随着新型存储技术的出现, 计算机和存储介质的体积大幅度减小, 内存容量变大, 其存储的个人信息量显著增加. 当人们删除存储介质中的数据时, 仅仅删除的是存储介质中的文件索引表, 存储空间中的二进制流数据仍然存在, 无法达到彻底删除数据的目的, 如何对存储介质中数据实施有效的安全删除十分必要. 本文介绍了常见存储介质的物理结构和逻辑结构, 并总结这些存储介质的删除原理, 对部分现有的安全删除

© 中国科学院软件研究所 http://www.c-s-a.org.cn

标准进行归纳和介绍. 最后, 针对存储介质中数据的安全删除问题, 本文设计并实现一种自定义覆写次数的数据安全删除方法与原型系统, 实现数据安全、不可恢复的删除, 从而达到保护隐私信息的目的.

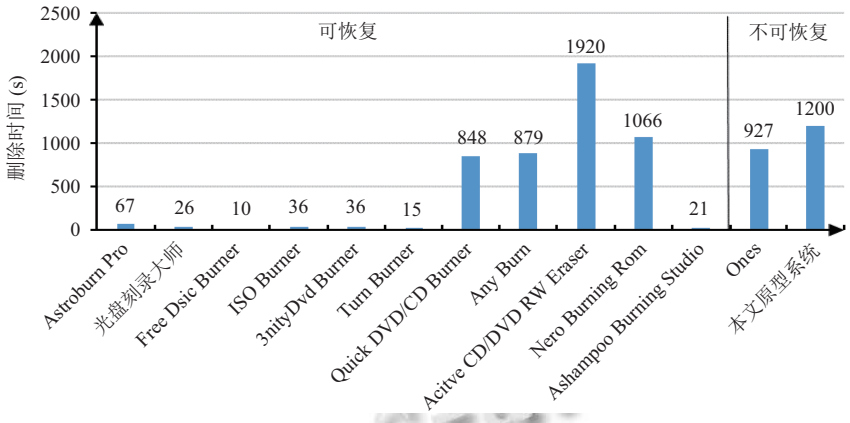

图 6 删除软件测试时间比较

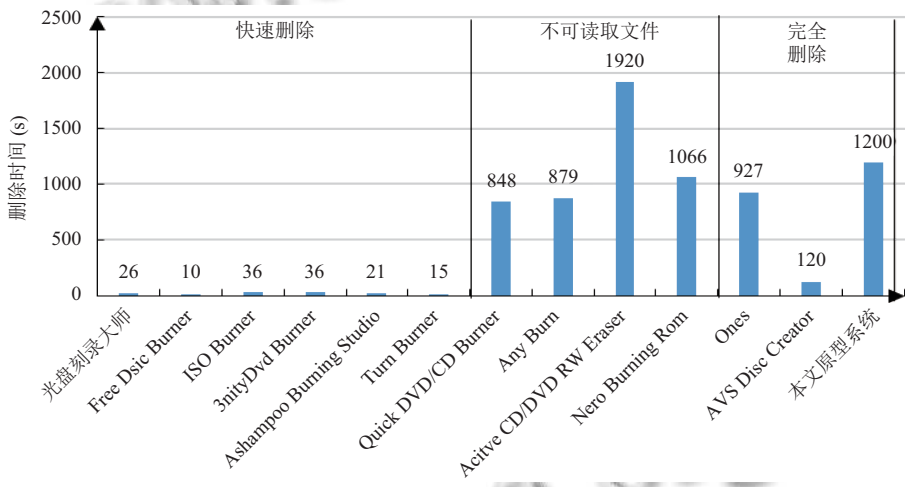

图 7 显示分类测试时间比较

参考文献

1 张冬. 大话存储-存储系统底层架构原理极限剖析. 北京: 清华大学出版社, 2015: 19–58.

2 唐迪, 魏英. 存储介质数据销毁技术研究. 信息安全与技术, 2012, 3(1): 8–9, 15.

3 侯丽波. 硬盘客体重用的安全等级保护覆写机制研究. 信息网络安全, 2012, (4): 64–66.

4 高志鹏, 徐志强, 吴世雄, 等. 硬盘自擦除技术的研究. 信息网络安全, 2012, (12): 60–64.

5 Zhang P, Zhang W, Niu SZ, *et al*. User level secure deletion for USB flash disks. Proc. of the 2014 2nd International Conference on Systems and Informatics (ICSAI). Shanghai, China. 2014. 1072–1077.

6 Lee B, Son K, Won D, *et al*. Secure data deletion for USB flash memory. Journal of Information Science and Engineering, 2011, 27(3): 933–952.

7 Frields J. National industrial security program. operating manual supplement. Washington, DC: Department of Defense, 1995.

8 Guttman P. Secure deletion of data from magnetic and solid-state memory. Proc. of the 6th Conference on USENIX Security Symposium, Focusing on Applications of Cryptography. San Jose, CA, USA. 1996, 8.

9 Police RCM. Hard drive secure information removal and destruction guidelines. Retrieved September, 2003, (25): 2007.

10 程玉. 磁介质数据销毁技术的研究[硕士学位论文]. 成都: 电子科技大学, 2010: 1–89.

© 中国科学院软件研究所 http://www.c-s-a.org.cn

11 裘正定. 计算机硬件技术基础. 北京: 高等教育出版社, 2007: 186–211.
12 管乐乐, 袁建国, 张曦. 基于特定扇区定位的磁盘阵列结构分析. 微型电脑应用, 2015, 31(5): 30–32.
13 胡乾顺, 胡大友. 光盘存储原理与文件结构探析. 计算机应用研究, 1998, 15(5): 35–37.
14 郑文静, 李明强, 舒继武. Flash 存储技术. 计算机研究与发展, 2010, 47(4): 716–726.
15 Chang LP, Kuo TW. Efficient management for large-scale flash-memory storage systems with resource conservation. ACM Trans. on Storage (TOS), 2005, 1(4): 381–418. [doi: 10.1145/1111609]
16 Shin I. Implementing secure file deletion in NANDbased block devices with internal buffers. IEEE Trans. on Consumer Electronics, 2012, 58(4): 1219–1224. [doi: 10.1109/TCE.2012.6414988]
17 王刚. 计算机网络存储技术. 计算机系统应用, 2015, 24(1): 14–20.
18 Freeman M, Woodward A. Secure state deletion: Testing the efficacy and integrity of secure deletion tools on solid state drives. Proc. of the 7th Australian Digital Forensics Conference. Perth Western Australia. 2009. 32–40.
19 范玉雷, 赖文豫, 孟小峰. 基于固态硬盘内部并行的数据库表扫描与聚集. 计算机学报, 2012, 35(11): 2327–2336.
20 Sun K, Choi J, Lee D, *et al*. Models and design of an adaptive hybrid scheme for secure deletion of data in consumer electronics. IEEE Trans. on Consumer Electronics, 2008, 54(1): 100–104. [doi: 10.1109/TCE.2008.4470030]
21 Lee J, Heo J, Cho Y, *et al*. Secure deletion for NAND flash file system. Proc. of the 2008 ACM Symposium on Applied Computing. Fortaleza, Ceara, Brazil. 2008. 1710–1714.
22 Choi Y, Lee D, Jeon W, *et al*. Password-based single-file encryption and secure data deletion for solid-state drive. Proc. of the 8th International Conference on Ubiquitous Information Management and Communication. Siem Reap, Cambodia. 2014, 5.

www.c-s-a.org.cn

© 中国科学院软件研究所 http://www.c-s-a.org.cn