Computer Science and Application 计算机科学与应用, 2018, 8(5), 730-737
Published Online May 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.85081

Hans汉斯

Method of Universal and Real-Time Telecommand Data Protection

Jian Wang*, Shasha Zhang, Chao Lu, Bo Zhou, Mei Zhang, Wendong Li

Beijing Institute of Spacecraft System Engineering, Beijing
Email: *wangjian@cast.cn

Received: May 2nd, 2018; accepted: May 22nd, 2018; published: May 29th, 2018

Abstract

The design of a universal high real-time telecommand data protection method is introduced in this paper, which is based on a certain type of satellite. The method is based on single chip machine. The whole process is redesigned to meet the needs of task requirements in the protection state of the remote control data of the spacecraft. On the other the external interface logic of the method is separated from the algorithm, and the two parts can be independently designed and developed to make the data preserving the method versatile.

Keywords

Universal, High Real-Time, Telecommand Data Protection, Single Chip Machine

基于单片机的高实时遥控数据保护方法

王　建*，张莎莎，鲁　超，周　波，张　媚，李文东

北京空间飞行器总体设计部，北京
Email: *wangjian@cast.cn

收稿日期：2018年5月2日；录用日期：2018年5月22日；发布日期：2018年5月29日

摘　要

本文结合实际应用介绍了一种通用高实时性遥控数据保护方法。此方法以单片机为核心，在传统的数据保护方法基础上，对整个流程进行重新设计，以满足整星遥控数据在保护状态下实现遥操作任务需求，同时，整个方法设计外部接口逻辑与算法分离，两个部分可独立设计开发，使数据保护方法具有通用性。

*通讯作者。

文章引用: 王建, 张莎莎, 鲁超, 周波, 张媚, 李文东. 基于单片机的高实时遥控数据保护方法 J]. 计算机科学与应用, 2018, 8(5): 730-737. DOI: 10.12677/csa.2018.85081

关键词

通用，高实时性，遥控数据保护，单片机

1. 引言

航天器系统由不同功能的若干分系统组成[1]，数据的安全性问题始终是数据传输系统中一个十分被关注的问题[2]，对具有传输加密要求的空间飞行器，为确保该卫星测控数据的安全，需对空间飞行器遥控数据采取加密措施。

星地遥控加解密系统包括空间飞行器解密系统、地面遥控加密设备和地面配套测试设备，空间飞行器解密系统主要部分就是数据保护模块，数据保护软件就是装载在数据保护模块中的。卫星遥控数据保护软件是嵌入式软件，安装运行于航天器平台。

根据任务需求，空间飞行器提出了遥操作要求，通过地面遥操作进行空间控制动作。对数管分系统要求是在 250 ms 内需要完成以下任务：遥控单元接收上行注入的遥操作数据、完成译码、输出到星务主机；星务主机处理完遥控单元转发的遥操作数据并通过总线将其转发到航天器控制器执行相关操作。

上述遥操作要求对遥控单元中数据解密提出了高实时性要求。根据实时性要求，提出了一种基于单片机的通用高实时性遥控数据保护方法，以满足任务遥操作需求。

该方法将遥控数据保护分割为接口部分和内核部分，为这两个部分分配独立的资源，以实现在算法变化情况下最大限度的减少更改，提高通用性，并将密级要求高的算法部分限定在最小范围内，以利于工程化实施。接口部分负责与外围电路进行信号交互和功能调度控制，同时负责同步字方式字的判断以及密指令、数据解密等功能，内核部分主要实现加密算法，产生解密序列，进行安全认证，密钥更换等功能，这样逻辑业务处理与安全算法分离，即算法可以任意变换，只需提供相应接口，而接口部分可以不用任何更改，降低了耦合度，便于维护和重用，提高了可用性，维修性。通用高实时性遥控数据保护方法同时也满足了执行任务的实时性要求，实现了一种通用的高实时的设计。

遥控提供地面操控航天器的命令通道，是地面人员对航天器某个仪器进行操作的手段。遥控将地面的命令、数据等信息经过组帧副载波调制等处理，通过测控站以电磁波传输的方式通过无线信道送达卫星。遥控数据主要有以下两大类：开关指令，如电源通断、信号通断、状态设置、系统重组等切换命令；注入数据，如工作参数、工作程序、在轨维护等上行数据。

卫星遥控数据包含了重要的地面控制指令，重要的操作参数，如果这些数据被非授权方知悉，则可能对卫星运行安全以及卫星用户方利益造成损害，甚至是致命的威胁。卫星遥控数据依靠无线信道传输，无线信道是开放信道，因此非授权方可以截获遥控数据。如果不希望非授权方知悉卫星遥控数据内容，则需要对卫星遥控数据采取保护措施，进行加密处理后再上传，卫星接收到加密后的数据再进行解密处理。

目前卫星上数据保护方法通用性比较差，尤其是在同一型号中，硬件设计相同，而数据保护加密算法不同的情况下，由于目前缺乏通用性的设计，而导致数据保护方法重复设计，软件重复开发，软件模块缺乏良好的重用性，这会浪费大量的人力，时间。另外，单片机不能实现并行处理，其处理速度受限于时钟频率，最高时钟频率仅为 16 MHz [3]。一般使用单片机实现卫星遥控数据的数据保护本身就存在

延迟较大，处理时间较长的问题，本文提出一种通用高实时性遥控数据保护方法，可以在满足数据保护的基本需求的基础上，满足实时处理的要求，根据需进行合理功能划分，使其具有较高的通用性，硬件资源有限，需综合分析合理分配资源。

2. 理论简述

加密可以理解为把一组有规律、有特定意义、易于识别的码字转换成另一组具有随机性、不经解密处理无法识别的码字，解密是加密的一个逆过程。

现代密码学引入了密钥的概念。引入密钥之后，密码系统由算法、密钥以及所有可能的明文、密文组成[4]。假定密钥表示为 k，公式为

$$c = E_k(p)$$

其中 E_k 已不再是单纯的数学变换，而是引入了密钥 k 这个因子。密钥 k 是一个变化因子，明文 p 相同，算法 E 相同，只要密钥 k 不同，得到的密文 c 也不会相同。对一个好的算法 E，只要密钥 k 有一个比特不同，就可以认为是使用了不同的密钥进行加密。引入密钥之后，密码系统使用过程中可以更换密钥，只要有 1 比特不同即可认为是不同密钥，密钥空间巨大，所以密码系统安全性大为提高。

对一个优秀的密码系统，其安全性应该基于密钥的安全性而不是算法细节。密钥通常是一组随机序列。优秀的密码系统即使算法公开，在保证密钥不被非授权方获得的情况下，仍然能保证不会被非授权方所破解。使用密钥的算法可以分为对称算法和公开密钥算法。对称算法指加密和解密使用的密钥相同，加密、解密必须保证密钥同步。公开密钥算法加密、解密两端使用的密钥不同，加密密钥是公开的，解密密钥是秘密的，只要保证解密密钥的安全就保证了整个密码系统的安全[5]。

随着计算机技术的高速发展，利用高速计算设备对密码系统进行穷举攻击正变得可行。因此，密码系统的设计必须考虑密钥更换周期，密钥更换周期应综合加密任务重要性、加密算法复杂度和密钥长度来考虑，以确保运行在某个密钥下的密码系统在密钥更换周期内不会被穷举破解。部分密码系统采用了一次一密的技术，也就是密码系统使用一个密钥完成一次加密之后即更换到其他密钥。

3. 方法设计

整个遥控数据保护保分成遥控数据保护接口部分和遥控数据保护内核部分，一是主要负责逻辑处理的接口部分，二是以内核算法以及安全认证为主的内核部分，即业务逻辑与安全算法相分离，这样方便了业务的扩展，修改也提高了算法的安全性，并且便于两部分的管理。数据保护方法具有良好的通用性，能够对算法进行替换而不用修改接口部分。

数据保护接口部分侧重于对业务逻辑的处理，接收上行遥控帧，通过调用内核部分的模块对上行遥控帧进行处理。如果上行遥控帧是签名指令，则调用内核的签名指令模块，进行签名指令处理；如果上行遥控帧是密钥帧，则调用内核的密钥处理模块，进行密钥处理。

数据保护内核部分接受数据保护接口部分的调用，主要功能是实现数据保护密码算法，为星上遥控数据的解密提供解密序列，对签名进行验证，完成密钥更换等安全方面的工作。这样业务逻辑和数据保护处理部分分开，便于两部分独立开发，将涉密性很高的部分单独独立集中在内核中，降低了安全隐患，同时当外围电路或者算法需求改变时，能够对整个数据保护方法最小程度的改动，整个数据保护方法具有较高的通用性。

本方法对于同步字方式字要进行检索以及方式字的判断，在上行码速率 2 bpks 的时间内可以完成，几乎不用占用额外时间，一般同步字和方式字共 3 字节，所以对于遥操作数据解密时延不大于 24 比特数据上行传输时间，即 3 * 8/2 bpks = 12ms，满足任务对每帧注入数据的解密时延不大于 25 ms 的要求。

数据保护方法输入数据有：遥控 PCM、遥控码流同步 CP，CP 上升沿对准输入遥控 PCM 的中间位置；数据保护模块输出数据有明文数据和同步时钟，数据保护模块在接收到上行加密数据帧且解密后，将解密后的明文数据输出。在数据最后 1 bit 输出完毕后，输出数据端口保持高电平。数据与时钟的时序关系如图 1 所示。

对于 34 字节的注入数据，从发完前一帧到开始发后一帧时，要在 250 ms 内处理完毕，并完成输出。同步字以及方式字共 3 字节传输时间为 12 ms，34 字节数据的传输时间为 34 * 8/2 bpks = 136 ms，剩余的时间为 102 ms，下一帧的 12 ms 是可以利用的，也就是说总共有 114 ms 的时间完成数据处理，时钟构造，解密序列生成等功能，算法需要的时间较多，所以采取接收一字节就进行解密然后输出一比特，输出的内容是延时了 3 个字节(12 ms)的，因为首先进行同步字检索和方式字的判断，输出 1 bit 时同时构造同步输出时钟，同时，数据保护部分应该保证在进行解密处理时有足够的解密序列已经生成。数据保护接口部分对于 34 字节解密时中断时间也有要求，综合业务逻辑和安全算法两方面的因素，数据保护接口部分每比特的中断处理时间应该不超过 120 us，数据保护内核部分应该在 85 ms 内完成 48 字节解密序列的生成，数据处理时间为 120 us * 34 * 8 = 32,640 us，总共需要的时间为 32.64 ms + 80 ms = 112.64 < 114 ms，这样既满足了对每帧注入数据的解密时延不大于 25 ms 的要求，也符合对于 34 字节的注入数据，从发完前一帧到开始发后一帧时，要在 250 ms 内处理完毕，并完成输出的要求。

数据保护方法的设计中设立了解密允许、解密禁止两条指令作为解密“开关”，和以前加密数据+签名的方式不一样，此任务中的加密数据帧不带签名，一旦发送解密允许，为解密允许状态后即对数据进行解密，不用进行签名验证，节约时间，这也是为了满足任务的要求。同时，数据保护应该保证在进行解密处理时有足够的解密序列已经生成，数据保护接口部分对于 32 字节解密时中断时间也有要求，综合业务逻辑和安全算法两方面的因素，要求平均每比特的中断处理时间不超过 120 us，数据保护内核部分应该在 85 ms 内完成 48 字节解密序列的生成。综上所述，遥控数据保护方法有较高的实时性。

通用高实时数据保护方法分割方案在资源上体现在地址上的分割，内容上是业务逻辑与安全算法的分割同时要考虑资源空间相对独立，没有重叠部分，这样在软件实现处理过程中不会对成彼此造成干扰，同时在工程实现上也便于将两个编译后的 hex 合成一个完成的 hex，按约定好的地址先将地址靠后的内核软件的 hex 载入，再将接口软件载入，最后进行烧写。

4. 工程验证

单片机是单片微型计算机的简称，是指将中央处理器、存储器、定时计数器、时钟接口和多种输入/输出接口集成在一个芯片上的计算机[5]。通用高实时数据保护方法实现以单片机为核心，其任务是接收

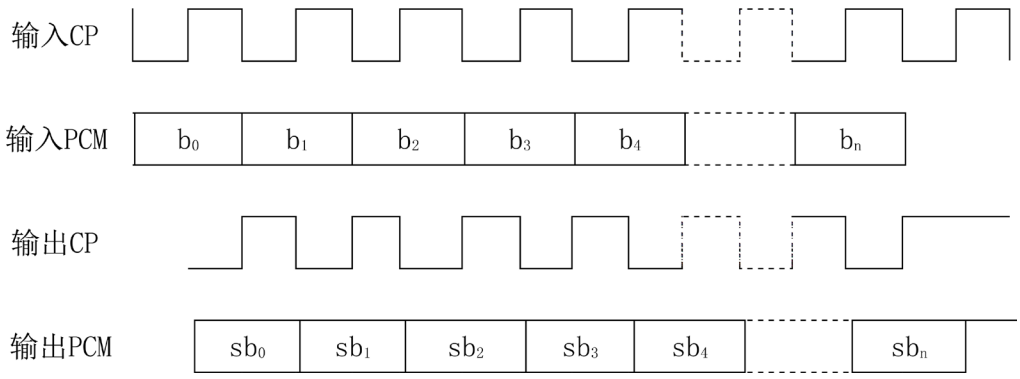

Figure 1. The time sequence relation of output and input data
图 1. 遥控数据输入输出信号的时序关系

地面的签名指令、加密数据、密钥，进行指令和数据的签名认证、数据解密和密钥更换。主要由以下部分组成：单片机、数据存储器、程序存储器、密钥存储器、看门狗电路。程序运行过程中要合理喂狗。如果程序故障，狗咬复位后，单片机从头开始执行。数据保护模块运行环境如图 2 所示。

数据保护接口部分与数据保护内核部分共同分配使用单片机系统的硬件资源，两部分相对独立所以需要考虑内部 RAM 资源以及外部 RAM 资源、程序存储器 ROM 地址资源的合理分配，同时要对接口地址进行约定。构成及接口图如图 3 所示。

使用单片机，遥控数据保护功能由外部中断触发，一个 CP 下降沿引起一次中断，一次中断完成一个遥控 PCM 比特的接收和处理。单片机具有高可靠性，只要有遥控 PCM 送来，其码同步 CP 必然引起外部中断，外部中断处理函数完成一个比特的接收、处理和输出，所以本设计方案不会导致遥控数据的增多或者丢失。

根据设计数据保护软件可相应的分成遥控数据保护接口软件和数据保护内核软件，数据保护接口软件与数据保护内核软件的关系如图 4 所示，数据保护接口软件与数据保护内核软件的信息交互关系如图 5 所示。

遥控数据保护软件可以分为两部分，一是主程序，二是中断处理函数。

主程序的功能包括：程序初始化，判断同步字方式字，中断设置，复位识别码维护，输出遥测。

遥控数据保护软件使用了 3 个中断：

1) 定时器/计数器 0：解密数据和同步时钟输出中断

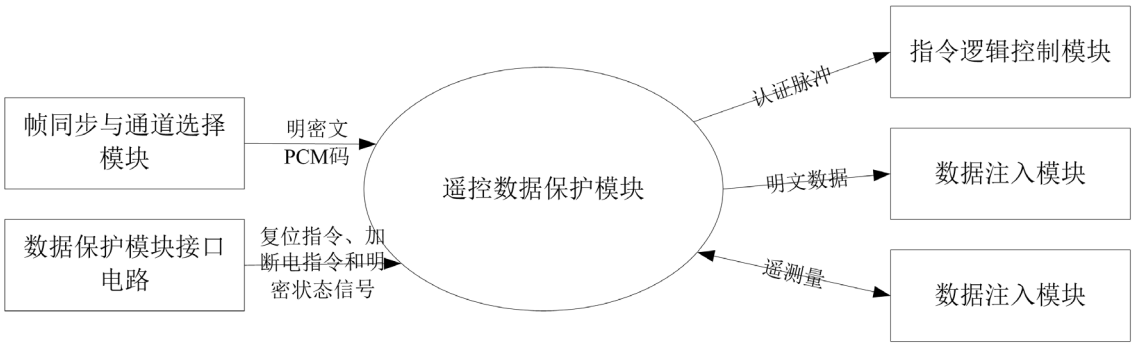

Figure 2. Data protection model environment
图 2. 遥控数据保护模块环境图

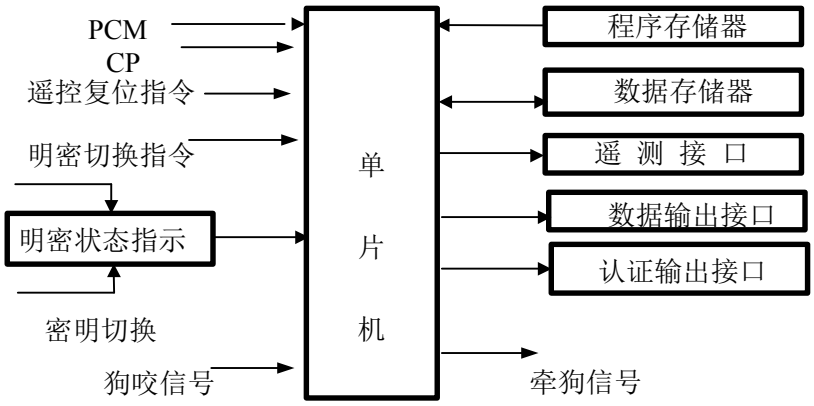

Figure 3. Input and output signal sketch map about 80C32
图 3. 单片机输入输出信号接口示意图

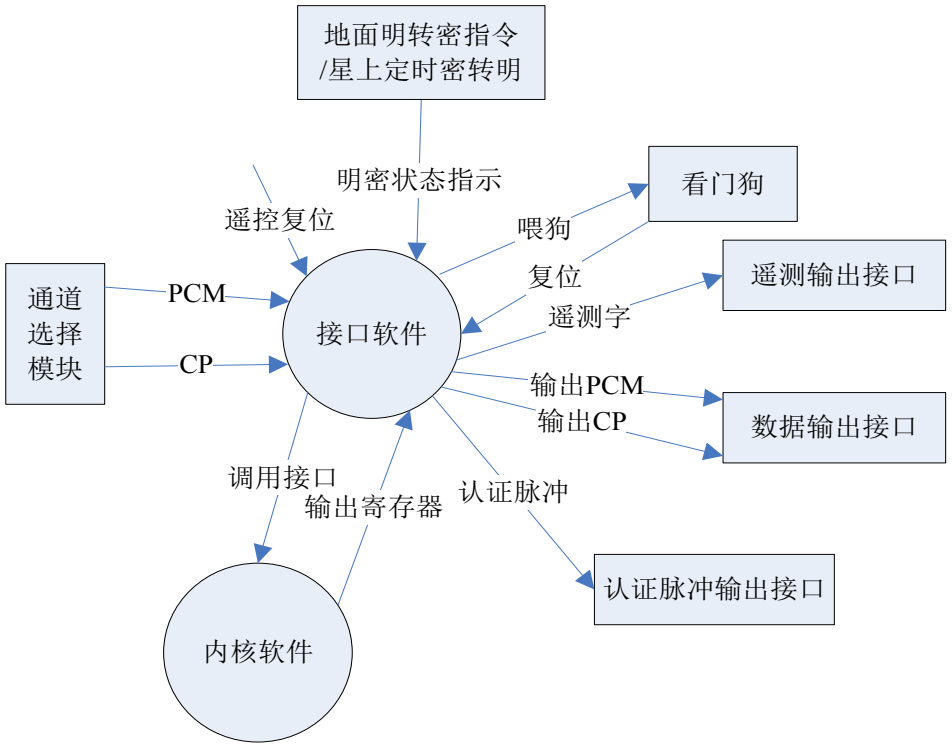

Figure 4. The relationship of interface software and inner core software
图 4. 接口软件与内核软件关系图

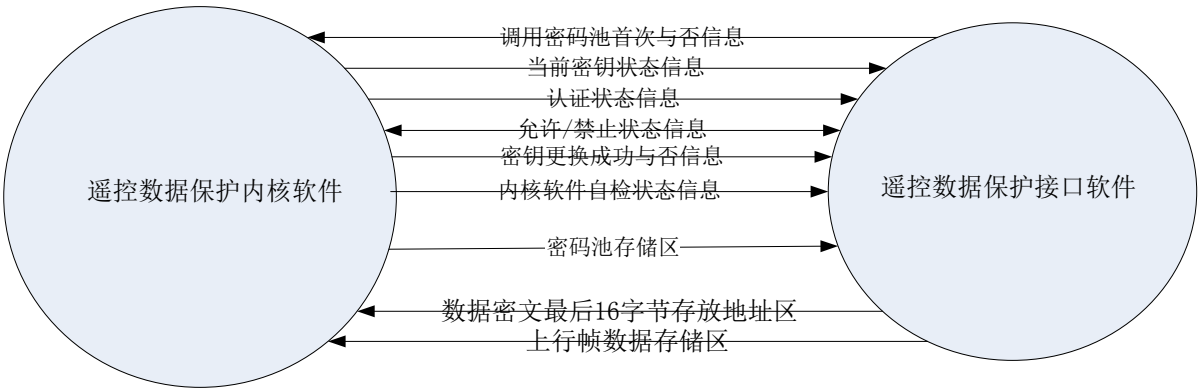

Figure 5. Information transmission between interface software and inner core software
图 5. 接口软件与内核软件信息交互关系图

2) 外部中断 1：PCM 码流输入同步时钟

3) 定时器/计数器 1：解密允许定时器

遥控数据输入输出信号的时序关系如图 1 所示，根据需求利用定时器定时器/计数器 0 以及外部中断 1 相互配合对数据进行处理同时构造同步输出时钟。定时器/计数器 0 用于 PCM 码的接收和处理，输出数据的同步时钟的构造，外部中断 1 用于构造输出同步时钟以及启动定时器/计数器 0。定时器/计数器 0 功能复杂，程序分支多，程序设计务必高效，以确保每个遥控 PCM 比特的处理都在半个 PCM 时间周期内完成。定时器/计数器 1 用来定时解密允许状态，当定时时间内未收到任何一条解密允许指令，星上转为解密禁止状态。

遥控数据保护软件主程序流程图如图 6 所示。

遥控数据保护软件定时器/计数器 0 流程图如图 7 所示。

经过软件仿真实，数据保护接口软件处理数据的中断最长的时间在在方式字的搜索上，需要时间为 119 us，其它情况下均小于 110 us，数据保护内核软件生成 48 字节的时间为 75 ms 均实时性符合要求。

5. 结束语

这种基于单片机的通用高实时的遥控数据保护方法能够在航天器软硬件资源有限的情况下满足对遥控数据保护的要求，并能完成高实时性遥操作任务，在某型号上已经应用，并通过了在轨测试，目前航天器在轨运行多年，各项功能正常，得到用户高度认可，达到卫星设计总体要求的各项功能、性能指标。业务逻辑和安全算法相分离，根据需求可以使用安全等级不一样的算法，对于接口部分可以不进行修改，

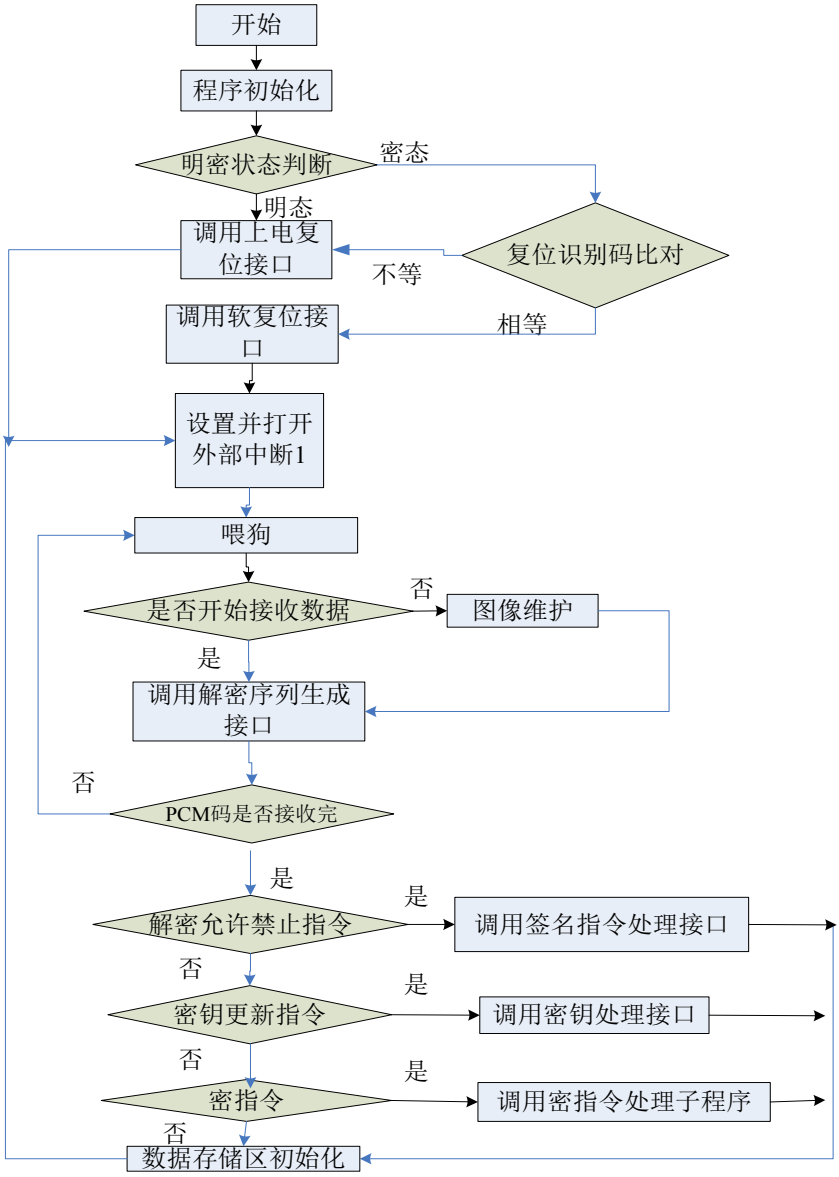

Figure 6. The main flow chart of data protection interface software
图 6. 遥控数据保护接口软件主程序流程图

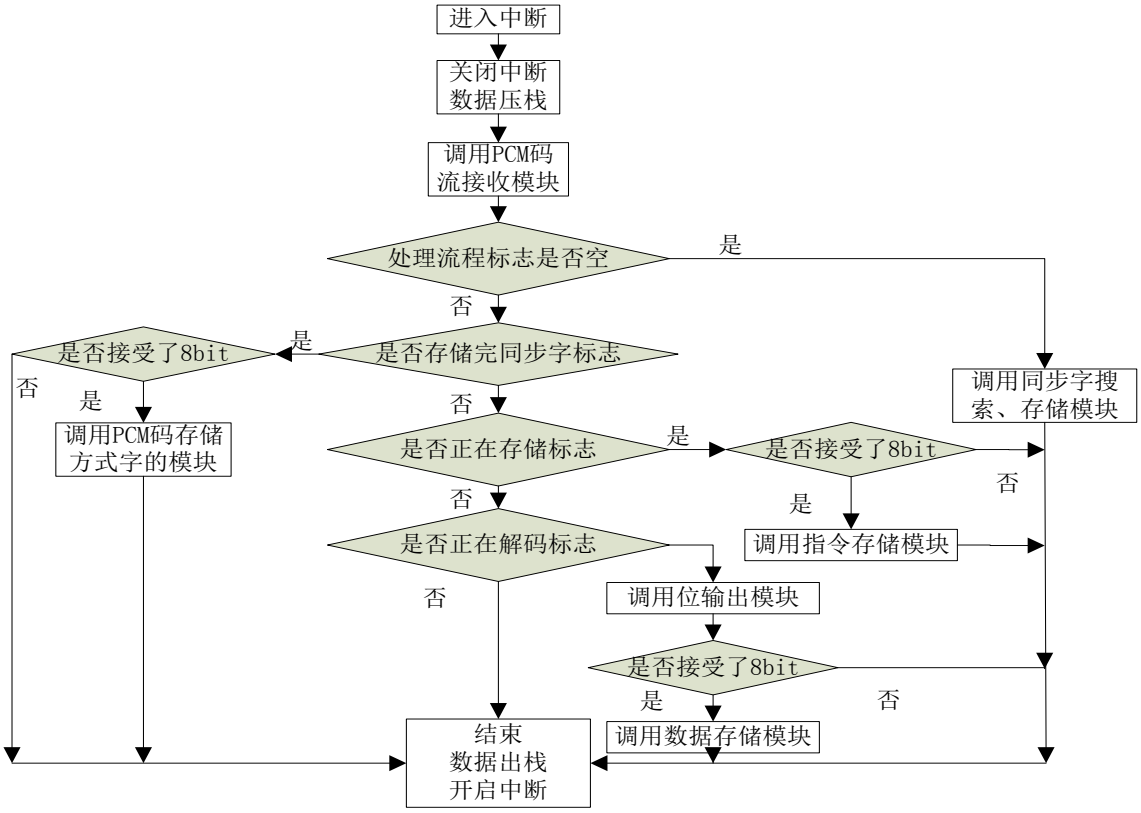

Figure 7. Data protection interface software timer interrupt 0 flow chart
图 7. 遥控数据保护接口软件定时器中断 0 流程图

当外围修改如果算法不变，也只需修改接口部分，不用对内核部分进行任何修改，是一种通用高实时的数据保护方法。

参考文献

[1] 彭成荣. 航天器总体设计[M]. 中国科学技术出版社, 2011.

[2] 谭维炽, 顾莹琦. 空间数据系统[M]. 中国科学技术出版社. 2006.

[3] 万福君, 潘松峰, 刘芳, 等. MCS-51 单片机原理、系统设计与应用[M]. 清华大学出版社. 2008.

[4] 谭维炽, 胡金刚. 航天器系统工程[M]. 中国科学技术出版社. 2009: 253.

[5] Bruce Schneier 著. 应用密码学(协议、算法与 C 源程序) [M]. 吴世忠, 祝世雄, 张文政, 等, 译. 机械工业出版社, 2004.

知网检索的两种方式：

1. 打开知网页面 http://kns.cnki.net/kns/brief/result.aspx?dbPrefix=WWJD
   下拉列表框选择：[ISSN]，输入期刊 ISSN：2161-8801，即可查询
2. 打开知网首页 http://cnki.net/
   左侧“国际文献总库”进入，输入文章标题，即可查询

投稿请点击：http://www.hanspub.org/Submission.aspx
期刊邮箱：csa@hanspub.org