CTD 海洋观测数据多重压缩加密算法设计

单海艳[1],熊学军[1,2*],郭延良[1],于 龙[1]

(1. 国家海洋局 第一海洋研究所,山东 青岛 266061;
2. 青岛海洋科学与技术国家实验室 区域海洋动力学与数值模拟功能实验室,山东 青岛 266237)

摘 要:对数据进行压缩、加密是解决海洋观测数据卫星传输通信费用高、数据安全性低等问题的有效手段。针对温盐深仪(Conductivity Temperture Depth, CTD)海洋观测数据,提出了一种新的加密算法——多重压缩加密算法。该算法结合数据特点,将数据压缩和加密技术结合在一起,不仅能对数据进行有效加密,同时还能对数据进行有效压缩。为保证数据解密时能够完全还原,算法需首先对整体数据进行误码检测,将数据分为误码区和正常数据区,然后对误码区保持原码不变,对正常数据区进行压缩加密编码。最后通过编程实现了该算法,并对算法的应用效果进行了测试。结果表明,该算法具有很好的压缩和加密效果。

关键词:CTD 海洋观测数据;数据压缩;数据加密算法

中图分类号:P717 **文献标识码**:A **文章编号**:1002-3682(2018)02-0023-07

doi:10.3969/j.issn.1002-3682. 2018.02.003

目前用于海洋数据传输的通信方式有多种,其中卫星通信因其通信距离远、覆盖面积广、系统可靠性高、数据误码率低等优点,被广泛应用在海洋监测平台数据传输中。海上观测平台、移动调查船舶、观测浮标或潜标等海洋监测平台基本都配备了卫星数据通信模块。当前多种卫星系统逐步组网完成,应用于海洋方面的主要有 Argos、海事卫星、铱星、全球星以及中国自行研制的北斗卫星。

卫星通信虽然有其自身的优点,但也存在一些突出的问题。一方面是卫星数据传输的资费以数据量计算,通信费用高。为了降低通信费用,需要最大限度地减少通信数据量,采用数据压缩技术对数据进行压缩是有效的解决办法[1]。另一方面是数据的安全性问题。我国自主产权的北斗卫星通信系统虽然能够保证通信的安全性和保密性,但其覆盖范围较小,主要覆盖我国国土和领海范围[2],所以很多情况下需要选择国外的卫星通信系统,如 Argos 和铱星系统等。但这些卫星通信系统的数据传输均要先通过国外的数据处理中心,经处理之后再分发给国内用户,数据的安全性从根本上得不到保证[3]。所以为了保证数据安全,需要采用数据加密技术对数据进行加密。

海洋观测数据的压缩和加密技术属于跨界技术,涉及多个领域,海洋观测数据若直接使用通用的压缩和

收稿日期:2018-03-16

资助项目:国家科技重大专项科研任务——南海北部内波流监测、预报、预警系统研究及应用(2016ZX 05057015);海洋工程装备科研项目——500 米水深油田生产装备 TLP 自主研发-内波流预警方案研究及内波流监测系统研制;国家自然科学基金项目——黄海暖流的多时相特征及其发生机制研究(41376038);国家自然科学基金委员会-山东省人民政府海洋科学研究中心联合资助项目——海洋环境动力学和数值模拟(U1606405);国家海洋局全球变化与海气相互作用专项子课题——黑潮结构时空变化特征对中国近海环流的影响分析(GASI-03-01-01-02),黑潮不稳定性及多核结构(GASI-IPOVAI-01-05),东印度洋南部水体综合调查夏季航次(GASI-02-IND-STSsum);国家重大科学研究计划——太平洋印度洋对全球变暖的响应及其对气候变化的调控作用—热带太平洋印度洋海洋观测 (2012CB955601);海洋公益性行业科研专项——常用海底声纳测量仪器计量检测关键技术研究与示范应用(200905024);国家自然科学基金青年基金——东海黑潮三维结构及季节变化研究(40406009);国家重大科学仪器设备开发专项——自容式声学多普勒流速剖面仪开发(2012YQ12003908);中央级公益性科研院所基本科研业务费专项资金资助项目——黄海东北部开敞性海湾余流特征及形成机制研究(2015P02)

作者简介:单海艳(1989-),女,硕士研究生,主要从事区域海洋动力学及调查技术方面研究. E-mail: shanhy@fio.org.cn

* **通讯作者**:熊学军(1976-),男,研究员,博士,博士生导师,主要从事区域海洋动力学及调查技术方面研究. E-mail: xiongxj@fio.org.cn

(陈 靖 编辑)

加密算法,不结合数据自身特点,就无法取得理想的效果。又因为海洋观测数据量大、数据类型复杂,所以目前海洋观测数据的压缩和加密技术还没有取得有效进展,海洋数据基本上是明文打包传输。CTD 是海洋调查的主流仪器,大洋长时间持续观测的 CTD 资料数据量大,直接获取困难,需要通过卫星进行传输。本文以 CTD 数据为例,充分结合其数据特点,设计了一种新的加密算法——多重压缩加密算法,该算法将数据压缩和加密技术结合在一起,不仅能对数据进行有效加密,同时还能对数据进行有效压缩。

1 数据压缩与加密技术

1.1 压缩技术

数据压缩是一种消除原始数据之间的冗余,并通过特殊的编码方式减小原始数据占用存储空间的技术[4]。根据数据解压后是否可恢复原始数据可把压缩技术分为有损压缩和无损压缩两类。

有损压缩方法利用了人类视觉、听觉对图像、声音中的某些频率成分不敏感的特性,允许压缩的过程中损失一定的信息。虽然不能完全恢复原始数据,但是所损失的部分对理解原始图像或音频的影响较小,却换来了比较大的压缩比。有损压缩广泛应用于语音、图像和视频数据的压缩。常用的算法有主成分分析法、小波变换等[5]。

无损压缩是利用数据的统计冗余进行压缩,可完全恢复原始数据而不引起任何失真,压缩和解压缩是一个可逆过程。无损压缩的压缩率受到数据统计冗余度的理论限制,压缩率比较低,广泛应用于对数据内容的完整性有较高要求的处理中,如文本数据、程序、指纹图像、医学图像等的压缩[6]。常用的无损压缩算法有 Huffman 编码、算术编码、游程编码、LZ 系列编码等。

为了保证数据的完整性,对海洋观测数据的压缩只能采用无损压缩技术。不同压缩算法对不同类型的数据有效,如果使用的算法不合适,压缩后的数据大小甚至可能大于原数据,所以针对不同类型的数据应选择或设计合适的算法。我们结合 CTD 数据自身的特点,设计了多个针对性的压缩步骤。

1.2 加密技术

一个数据加密系统至少包括算法、明文、密文和密钥四个部分[7]。数据加密过程就是把原来可被直接识别的数据(明文),按某种算法进行处理,使其与一串数字(密钥)相结合,变换成无法直接识别的、无意义的一段数据(密文)。密文只能在输入相应的密钥之后才能还原出本来内容,通过这样的途径可以达到保护数据不被非法窃取、阅读的目的。将明文转换成密文的过程称为加密,将密文还原成明文的过程称为解密[7]。一般算法是公开的,密钥是保密的,一个加密算法的强度除了依赖于算法本身以外,还往往与密钥长度有关,通常密钥越长,强度越高[8]。如果加密的数据被窃取,即使知道加密算法,若没有加密的密钥,也不能轻易获得被加密保护的信息。

数据加密的技术可以分为两类:对称加密和非对称加密[9]。对称加密是不论加密方或解密方都采用同样的密钥进行相应处理的方法,故又称为私有密钥加密。对称加密方法操作简单,使用率比较高,但要注意密钥的保密性。DES 加密算法是典型的对称加密算法。

非对称加密是在加密和解密的过程中分别采用不同的密钥进行相应的处理。相较于对称式加密技术,非对称式加密技术的加密算法和公钥是可以公开的,而私钥则需要由用户保管。需要说明的是,虽然公钥与私钥是成对使用,且公钥是公开的,但是用户是无法根据公钥信息来计算出私钥信息的。该加密技术加密性高,应用场合灵活,但加密算法复杂,加密与解密速度比较慢,被加密的数据块长度不宜太大[10]。RSA 加密算法是典型的非对称加密算法。

海洋环境观测数据的卫星传输过程是从海上观测平台至数据处理中心,加密方与解密方是同一用户,密钥不需要传输,自己保存即可。海洋观测数据通常数据量比较大,数据特点较为明显。所以综合考虑选择自主设计对称加密方法。我们根据 CTD 数据特点,设计了多个针对性加密步骤,同时结合压缩步骤,对数据

进行多重加密。

2　CTD 海洋观测数据特点

要实现对海洋观测数据的压缩和加密，首先要把握海洋观测数据的特征。CTD 是测量海水温度、盐度、深度等信息的仪器。海洋的温盐深观测是现今海洋调查的基本内容之一，CTD 能适应如走航实时观测、定点自容观测、抛弃式探头观测等多种观测方式，是目前物理海洋调查中使用最为广泛的仪器设备之一[11]。CTD 工作时，每隔一个采样间隔采集一次海水的温盐深信息，得到一条 CTD 数据。CTD 数据包括电导率、温度、压力等直接观测量和时间标记，以及一系列计算导出量。本文以美国海鸟公司生产的带有压力传感器的 SBE 37-SM MicroCAT 为例，其默认的数据格式为 tttt.tttt，ccc.ccccc，ppppp.ppp，ssss.ssss，vvvvv.vvv，dd mmm yyyy，hh:mm:ss <cr><lf>，详细信息见表 1。

表 1　CTD 观测数据格式

Table 1　CTD observation data format

内　容	说　明
tttt.tttt	温度/℃
ccc.ccccc	电导率/S·m^{-1}
ppppp.ppp	压力/分巴
ssss.ssss	盐度
vvvvv.vvv	声速/m·s^{-1}
dd mmm yyyy	日，月，年
hh:mm:ss	时，分，秒
<cr><lf>	结束标志回车换行

数据为采用 ASCII 码格式表示的十进制数据，数据高位无有效数据时用空格补充，小数点前一位和低位无有效数据用“0”表示。所有的数据之间通过逗号隔开，日期和时间前面还要多一个空格。观测要素中温度、电导率、压力为直接观测量，电导率传感器测量范围为 0～7 S/m，温度传感器测量范围为－5～35 ℃，压力传感器最大量程为 7 000 m。盐度和声速为计算导出量，是根据直接观测量计算而得的量，可根据需求设置是否输出。

总的来说，CTD 数据主要有以下几个特点：1）数据是以 ASCII 码格式表示的十进制数据；2）数据中含有大量分隔符，如逗号、空格以及回车换行符等；3）数据的时间标记（年月日和时分秒）是具有固定时间间隔的时间序列；4）盐度和声速要素可以由其他要素计算得出；5）各要素都有一定的数值变化范围。进行算法设计时应充分考虑并利用这些特点以达到更好效果。

3　多重压缩加密算法设计

3.1　总体设计

多重压缩加密算法，顾名思义是对数据进行多重压缩和加密。算法专门针对 CTD 观测数据，充分结合数据特点设计了多个步骤，将数据压缩和加密技术结合在一起，在压缩过程中加密、在加密过程中压缩。算法主要在两个层次上实现压缩目的：一是针对性压缩，省略数据中非数字字符和可以后期计算得出的内容；二是整体性压缩，通过进制转换、位拼接方法对数据进行整体性压缩。算法的加密措施主要体现在两个方面：一方面，压缩是加密的一种方式，压缩的步骤同时都可以起到一定的加密作用；另一方面，利用置换、代替等方法对数据进行各种变换操作，并且引入密钥机制，进一步增加破解难度。为保证数据解码后能够完全恢复原数据，算法每一步都是可逆的，并且加入了误码检测机制。当数据中出现误码时，对误码按行原位固定，保证解码时能将误码数据完全恢复且不影响其他数据源。

3.2　步骤设计

本文充分结合 CTD 数据自身特点进行算法步骤设计，对数据进行多重压缩和加密，并对出现误码的情况提出了解决方法。

3.2.1 压缩加密编码

为了充分结合CTD数据特点,编码时直接对原始数据进行操作,具体措施如下:

1)时间标记处理

对于数据中的时间标记,只编码记录其始、终点,然后将其略掉,可节省大量空间,注意编码记录时将月份用数字表示。

2)省略导出量

CTD输出的基本要素包括温度、电导率、压力等直接观测量及其时间标记,根据需要还可输出一些可计算导出量,如盐度、声速等数据,这些数据可以后期计算补充,所以为了节省空间,可以设置不输出这些导出量,或者将数据中的导出量略掉。

3)极值取反

CTD数据中的温度和压力要素可能会取负值,由于负号的存在会额外增加数据占用空间,所以应想办法将负数变为正数。本算法采用的方法是将各要素数据整数部分分别向极值取反,极值是指各要素取值范围的最大值。以SBE 37-SM MicroCAT为例,根据其测量范围,这里温度、电导率和压力的极值应分别取35,7和7000。取反是指用极值减去原数值。极值取反后负数变成了正数,并且改变了原数据值,起到了一定的加密作用。

4)省略小数点及分隔符

数据中的小数点和分隔符如空格、回车符、换行符等,占用了很大的存储空间,所以可以省略这些数值以外的字符。为了保证能够在解密时还原数据,在省略这些字符之前应固定各要素整数部分及小数部分的数字位数。以SBE 37-SM MicroCAT为例,根据其测量范围,这里温度、电导率、压力的整数位位数分别固定为2位、1位、4位,位数不足时在数字前补0,小数位位数分别为4位、5位、3位。

5)算法组合

将各要素整数部分和小数部分分离,然后再通过一定的算法进行重新组合。比如将温度整数部分扩大一倍,然后将各要素整数部分拼接成一个数放在前面,小数部分各自作为一个数依次放在后面。

6)偏移替换

进行这一步时需将每条数据看成一个数字串,由用户设定一串十进制数作为密钥,密钥的长度与经前面步骤处理后一条数据中数字的个数相同。然后让密钥与每一条数据进行结合,结合前首先循环移位相应的位数,如与第1条数据结合前循环左移1位,与第2条数据结合前循环左移2位,以此类推。密钥与每一条数据进行结合的方法为:根据密钥让数据的每一位数字进行偏移,密钥每一位数字与数据每一位数字一一对应,密钥的每一位数字决定数据每一位数字偏移的位数。如数据第1位为1,密钥第1位为5,则将1偏移5位后变成6,数据第2位为8,密钥第2位为2,则将8偏移2位后变成0,以此类推。

7)进制转换

CTD数据是以ASCII码格式表示的十进制数据,其中每一个数字都占一个字节,占用存储空间很大,所以我们将前面处理后的时间标记和观测数据转化为二进制格式,将大大节省空间。

8)位拼接

将各数据进行位拼接,生成新的字节,进一步减小数据量。位拼接是由每个值的实际范围来确定每个值的最小表达位数,根据表达位数,将数据在位的层面按一定顺序首尾相接,再断截成字节,这样做可以减少数据之间的位空间浪费[12-13]。海洋观测数据在通信过程中,一般每个数值按字节传输,至少占用8位或者它的整数倍,若采取位拼接算法,则可显著压缩数据。所有的数据都有有效的数值范围,根据这个范围确定位数,能够有效地减少存储数据的位的数目。

3.2.2 误码处理

因为该算法是根据数据特点设计的,所以如果出现误码将不再适用。为保证数据解密时能够完全还原,并

且不影响对其他正常数据的压缩加密，对误码采用“按行原位固定”的方法处理，即对于误码所在的整条数据保持原码不变。具体实施时需要首先对整体数据进行误码检测，将数据分为误码区和正常区，误码区为存在误码的单条或相邻的多条数据，正常区为由误码区自然分隔而成的数据正常的连续区域。然后对误码区和正常区按不同方法进行编码。对于误码区，按行原位固定，保持原码不变。对于正常区，对数据进行压缩加密编码。

误码检测包括 2 个方面：1）检查数据是否严格符合数据格式，若出现不符合数据格式或超出数据范围的情况都应视为误码，并将其所在的整条数据视为误码区，若连续几条数据中都出现了误码，则将这几条数据视为一个误码区；2）检测时间标记的连续性，即时间标记是否严格按照采样间隔递增。若出现其中 2 条数据时间间隔变大或变小，但前后数据的时间标记正常且数据正常，则应依此为分界线将前后数据划分为 2 个正常区；若个别数据中的时间标记出现异常跳变，则将其作为误码处理。

3.3　执行流程

多重压缩加密算法执行流程图如图 1 所示。首先对整体数据进行误码检测，将数据划分为多个误码区和正常区。然后对各个数据区按顺序依次进行编码。编码时首先判断数据区类型，若为误码区，按行原位固定，保持原码不变，然后在误码区前添加误码区标记符和数据长度；若为正常区，对数据进行压缩加密编码，然后在正常区前添加正常区标记符和编码后数据长度。

由于算法的各个步骤都是完全可逆的，所以整个算法流程是完全可逆的，因此解码时可以完全无失真地恢复原始数据序列。解码流程为该算法的逆过程，首先读取第一个数据区标记符和数据长度，然后判断该数据区类型，若为误码区，则根据数据长度将该区域数据原码输出；若为正常区，则根据数据长度将该区域数据取出，对数据进行压缩加密编码的逆操作，并将得到的数据输出，这样第一个数据区便解码完成。接着继续对后面的数据进行同样的操作，直至将所有数据完全解码。

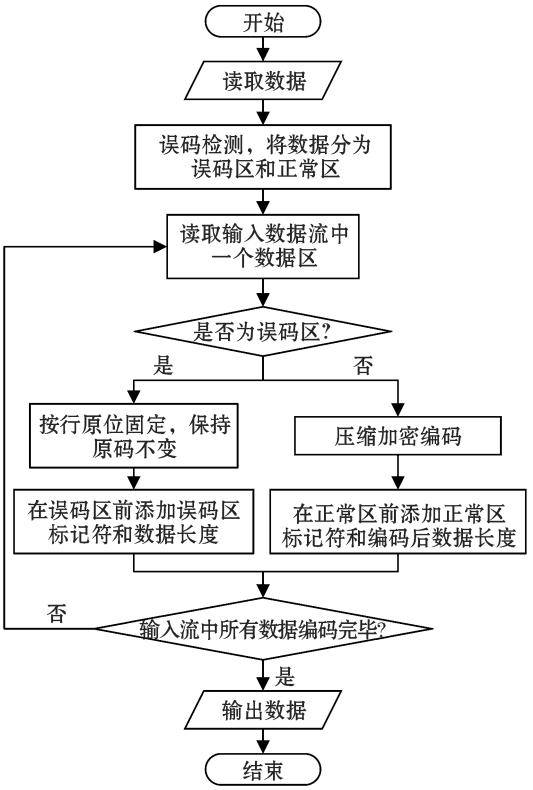

图 1　多重压缩加密算法执行流程图

Fig.1　The flow chart of multiple compression encryption algorithm implementation

4　应用效果与分析

根据上文介绍的算法，本文以 SBE 37-SM MicroCAT 为例，在 matlab 平台上编写了相应的程序。运用编写的程序对 CTD 数据进行编码和解码测试，测试结果表明，本算法是无损的，解码后可以完全恢复原数据。下面对其压缩和加密效果进行分析。

首先分析压缩效果，选取几组长度不同的 CTD 观测数据，数据中只含温度、电导率和压力三种观测要素以及时间标记。分别运用多重压缩加密算法、LZW 算法[12] 和 Huffman 算法[1] 对数据进行处理，处理后统计压缩率((原数据大小－压缩后数据大小)/原数据大小)并进行对比，结果如图 2 所示。可以看出，多重压缩加密算法的压缩率比较稳定，大约为 85％左右；Huffman 算法的压缩率略有起伏，大约为 63％左右；LZW 算法的压缩率在数据量较小的时候压缩率较小，随着数据量增加压缩率逐渐升高，最后在 73％上下起伏。通过比较可以得出，多重压缩加密算法的压缩率最高，也最为稳定，压缩效果最好。

然后分析加密效果，截取 50 条采样数据，使用多重压缩加密算法进行处理，将处理后结果转化为十进制进行输出，结果如图 3。可以看出，编码后的数据已经完全不具有原数据的特征，起到了加密的作用，符合预期的效果。

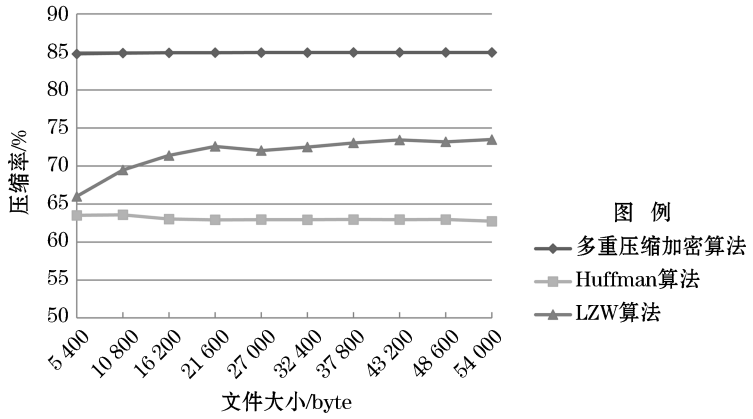

图 2 不同算法压缩率对比图

Fig.2 Comparison diagram of compressed ratios of different algorithms

141 14 205 23 214 124 17 73 62 230 8 8 192 164 154 211 231 241 42 123 107 95 103 35 76 31 139 186 160 22 52 34 107 240 231 39
29 45 155 101 13 74 102 64 153 90 200 179 25 66 149 196 208 215 169 83 188 44 53 74 118 57 7 92 206 232 6 41 32 195 19 74 156
14 194 48 225 239 196 234 109 72 228 20 173 223 90 203 57 25 47 239 237 78 109 116 155 152 169 36 188 80 67 52 60 5 244 25 73
244 5 66 221 121 190 178 92 45 244 217 9 225 225 86 251 83 186 105 87 33 201 136 88 186 134 132 11 122 70 12 98 175 235 150
112 199 34 183 251 13 26 66 74 182 200 180 175 246 204 69 208 162 10 94 207 229 106 66 213 156 38 151 78 233 81 21 58 27 161
230 74 12 211 217 161 17 89 252 22 223 8 19 219 44 107 146 133 253 135 72 71 158 205 148 33 37 55 206 75 157 226 237 227 83
207 70 58 224 114 195 29 79 247 88 161 80 162 37 0 128 19 149 115 86 111 35 153 189 140 126 163 90 206 201 108 217 208 214 57
162 219 196 194 80 241 231 251 163 225 137 32 74 128 39 129 17 234 126 11 140 228 49 56 207 78 8 156 114 218 58 201 68 187 10
145 25 195 116 26 61 92 208 51 238 27 43 34 134 132 59 22 249 208 47 27 24 82 178 197 230 93 245 51 90 131 22 213 72 93 242 79
54 170 230 244 5 30 42 167 44 209 217 8 245 144 226 48 99 5 141 200 18 27 250 187 57 199 102 89 131 105 30 244 113 9 242 108
134 242 42 141 137 45 234 20 251 64 129 46 121 215 1 151 235 110 72 122 12 133 133 18 45 0 73 156 194 1 176 122 27 202 210 101
82 241 210 114 78 97 205 134 209 153 19 221 38 30 1 138 213 110 28 13 79 129 244 1 176 152 2

图 3 多重压缩加密算法输出结果

Fig.3 Output result of multiple compression encryption algorithm

5 结 语

卫星通信技术在海洋观测数据传输中被广泛地应用，为解决海洋数据卫星传输存在的资费高、安全性低等问题，需要对数据进行压缩和加密。针对 CTD 海洋观测大数据，提出了一种新的加密算法——多重压缩加密算法，可以同时实现对数据的有效加密和有效压缩。最后通过编程实现了多重压缩加密算法，并对其压缩和加密效果进行分析。结果表明，针对 CTD 数据，该算法的压缩效果优于 LZW 算法和 Huffman 算法，加密效果也符合预期。在海洋监测平台上，将 CTD 采集得到的数据通过多重压缩加密算法进行编码处理，形成数据量较小的密文，然后通过卫星通信系统传输至岸站数据处理中心，最后使用多重压缩加密算法的逆运算进行解码，便可得到原始采集数据，编码和解码时使用同一密钥。通过多重压缩加密算法的处理，CTD 数据在通过卫星传输时不仅能节省通信费用，还能保证数据安全。

参考文献(References)：

[1] CHENG F L. Applied huffman data compression to the data communication via satellite[J]. Ocean Technology, 2005, 24(3): 18-21. 成方林. Huffman 数据压缩技术在卫星数据通信中的应用[J]. 海洋技术, 2005, 24(3): 18-21.

[2] WANG F J, XIONG X J, PU D, et al. Satellite transmission link of ocean observation data——taking the application of Iridium transmission link as the example[J]. Coastal Engineering, 2017, 36(1): 52-61. 王凤军, 熊学军, 蒲定, 等. 海洋观测数据的卫星传输链路——以 Iridium 传输链路应用分析为例[J]. 海岸工程, 2017, 36(1): 52-61.

[3] DANG C Q, ZHANG S P, QI Z H, et al. Research on data transmission of deep and remote sea GPS wave buoy based on BeiDou satellites system[J]. Transducer and Microsystem Technologies, 2015, 35(1): 46-48. 党超群, 张锁平, 齐占辉, 等. 基于北斗卫星系统的深远海 GPS 波浪浮标数据传输研究[J]. 传感器与微系统, 2015, 35(1): 46-48.

[4] CAI M, QIAO W X, JU X D, et al. A new coding method for lossless data compression[J]. Journal of Electronics & Information Technology, 2014, 36(4): 1008-1012. 蔡明，乔文孝，鞠晓东，等. 一种新的数据无损压缩编码方法[J]. 电子与信息学报，2014，36(4)：1008-1012.

[5] SUN Q Y, WANG L Z, WU F P. Data compression method introduction and analysis[J]. Journal of Yunnan University (Natural Sciences Edition), 2007, 29(Suppl.1): 115-118. 孙秋月，王丽珍，吴凤萍. 数据压缩方法介绍及分析[J].云南大学学报(自然科学版)，2007，29(增刊 1)：115-118.

[6] WU W Q. Research of lossless compression algorithms for acoustic communication data[J]. Modern Electronics Technique, 2012, 35(9): 103-105. 吴文强. 水声通信数据无损压缩方法的对比研究[J]. 现代电子技术，2012，35(9)：103-105.

[7] LI F J. The application of data encryption technology in computer network communication security[J]. Computer & Telecommunication, 2017(5): 59-61. 李方军. 数据加密技术在计算机网络通信安全中的应用[J]. 电脑与电信，2017(5)：59-61.

[8] HU M Y. Analysis and research of traditional data enciphered algorithm[J]. Network Security Technology & Application, 2006(3): 72-74. 胡美燕. 传统数据加密算法的分析与研究[J]. 网络安全技术与应用，2006(3)：72-74.

[9] LIU P. Encrypting transmission of data on the web[J]. Computer Knowledge and Technology, 2008(3): 421-424. 刘平. 浅谈网络数据的加密传输[J]. 电脑知识与技术，2008(3)：421-424.

[10] ZHOU S F. Encryption method of data network transmission[J]. Agriculture Network Information, 2010(11): 104-105. 周四方. 网络传输数据的加密方法[J]. 农业网络信息，2010(11)：104-105.

[11] REN Q, YU F, WEI C J, et al. Comparison and analysis on conductivity-temperature-depth system (CTD) data quality[J]. Studia Marina Sinica, 2016, 51: 288-295. 任强，于非，魏传杰，等. 温盐深测量仪(CTD)资料质量对比分析[J]. 海洋科学集刊，2016，51：288-295.

[12] WANG W Y, LI W Q, WANG X Y, et al. Application of data compression in the communications system of an oceandata buoy[J]. Shandong Science, 2015, 28(2): 1-5. 王文彦，李文庆，王晓燕，等. 数据压缩技术在海洋资料浮标通信系统中的应用[J]. 山东科学，2015，28(2)：1-5.

[13] LI M, SHI H Y. Research of communication mechanism based on BeiDou Satellite for large buoy[J]. Ocean Technology, 2012, 31(1): 1-5. 黎明，时海勇. 基于北斗卫星的大型海洋浮标通信机制研究[J]. 海洋技术，2012，31(1)：1-5.

Design of Multiple Compression Encryption Algorithm for CTD Ocean Observation Data

SHAN Hai-yan[1], XIONG Xue-jun[1,2], GUO Yan-liang[1], YU Long[1]

(1. *The First Institute of Oceanography, SOA*, Qingdao 266061, China;
2. *Laboratory for Regional Oceanography and Numerical Modeling, Qingdao National Laboratory for Marine Science and Technology*, Qingdao 266237, China)

Abstract: The data compression and encryption are effective means for solving the problems of high communication cost and low data security of ocean observation data when transmitted by satellite. A new encryption algorithm, multiple compression encryption algorithm, is proposed for the CTD ocean observation data. This algorithm makes full use of the data characteristics and combines the data compression with the encryption technology. Thus, the data can not only be encrypted but also compressed effectively. In order to ensure that the data can be restored totally when decoding, the algorithm should first perform error detection on the whole data, dividing the data into error area and normal data area. And then, the data in the error area are kept unchanged and those in the normal data area are compressed and encrypted. The algorithm is implemented by programming, and its application effect is tested. It has been shown that both the compression and the encryption effects of the algorithm are good.

Key words: CTD ocean observation data; data compression; data encryption algorithm

Received: March 16, 2018