文章编号:1671-4598(2021)03-0171-05 DOI:10.16526/j.cnki.11—4762/tp.2021.03.034 中图分类号:TN929.5 文献标识码:A

基于区块链的星间通信网络安全加密控制系统设计

马 煜
(陕西中医药大学 信息化建设管理处,陕西 咸阳 712046)

摘要:目前设计的星间通信网络安全加密系统加密深度低,导致通信误码率高,无法保证星间通信网络安全;引入区块链技术设计一种新的星间通信网络安全加密系统;选择性能最优的LEO类型的卫星放置在中层的卫星网络通信轨道中,其他类型的LEO卫星则各个成为单独的卫星网络分体系,处理主体系中的杂乱通信信号;构建地面用户之间的链路关系及卫星网络链路,实现高阶层卫星通过无线电链路或光纤链路对下一阶层的卫星覆盖,完成系统硬件设计;引用区块链分布式数字化身份加密技术,通过用户使用密钥对公钥的加密保护结构图定位通信网络的状态以及通信网络的加密状态,在区块链公开性的基础上增添了用户的密钥,通过用户的独有密钥使用户使用公共的星间通信网络进行通信,实现星间通信网络安全加密;实验结果表明,基于区块链技术的星间通信网络安全加密系统能够有效提高网络安全加密系统加密深度,降低误码率。

关键词:区块链技术;星间通信网络;安全加密;加密系统;通信数据;数据加密;通信加密;安全网络

Design of Inter Satellite Communication Network Security Encryption Control System Based on Blockchain

Ma Yu
(Information Construction Management Service, Shanxi University of Chinese Medicine, Xianyang 712046, China)

Abstract: At present, the designed inter satellite communication network security encryption system has low encryption depth, which leads to high communication error rate and can not guarantee the security of inter satellite communication network. This paper introduces the blockchain technology to design a new inter satellite communication network security encryption system. In the LEO satellite network, the satellite communication network is divided into two layers: one is the satellite network, the other is the satellite network Cover, complete the system hardware design. Based on the block chain distributed digital identity encryption technology, the status of the communication network and the encryption state of the communication network are located through the encryption protection structure diagram of the public key with the block chain. The user's key is added on the basis of the openness of the blockchain. The user can communicate with the public inter satellite communication network through the user's unique key, so as to realize the security of the inter satellite communication network encryption. The experimental results show that the inter satellite communication network security encryption system based on blockchain technology can effectively improve the encryption depth of the network security encryption system and reduce the bit error rate.

Keywords: blockchain technology; inter-satellite communication network; security encryption; encryption system; communication data; data encryption; communication encryption; secure network

0 引言

卫星通信网是星间通信的无线电通信方式,以卫星作为通信中转站,在通信测控中心的管理与协调下完成长距离的通信。这种通信方式不受距离的影响,促进了军事和科学研究领域的发展,与此同时,对星间通信网络安全加密系统的研究显得尤为重要[1-3]。

TRW公司曾针对宽带卫星网络的安全通信状态应用地面分布式操作系统作为星间通信网络安全的加密系统,此系统主要是通过应用地面的卫星操控中心对广域网进行互联控制,在地面的每一个操控中心都设有一个卫星管理中心,主要负责与卫星载荷和中心终端相关联,对整个卫星的网络安全进行监察,可以随时调控星间通信网络中的信息发布、控制与状态监控,此系统虽然能够较全面地监察网络安全,但是此系统的安全加密深度不够;美国还开发了ATM-Sat项目,该项目最初应用于互联网网络管理与对星座网络系统的安全管理,使用500颗低轨卫星构造安全通信网络,对不同的卫星管理安全信息库并扩展,实现了星间通信网络网络安全加密系统的建设,此系统能够与地面的公共网络连接,再通过相应的适配器对通信两端的用户信息、位置信息、资源信息进行管理,由于适配器条

收稿日期:2020-08-20; **修回日期**:2020-09-14。
作者简介:马 煜(1989-),男,河北保定人,硕士,工程师,主要从事计算机网络安全、算法方向的研究。
引用格式:马 煜.基于区块链的星间通信网络安全加密控制系统设计[J].计算机测量与控制,2021,29(3):171-175.

件的要求过高、地面公共网络的环境复杂等因素的干扰，导致此系统存在信道的误码率过高的缺陷[4-7]。

为了解决传统系统中存在的问题，本文将基于区块链技术对星间通信网络安全加密系统进行设计，硬件模块设计了地面用户之间的链路关系及卫星网络链路，实现高阶层卫星通过无线电链路或光纤链路对下一阶层的卫星覆盖。软件部分引入区块链分布式数字化身份加密技术，通过非对称密钥实现星间通信网络安全加密，并通过实验验证了系统的有效性。

1 星间通信网络安全加密系统硬件设计

研究采用低轨卫星作为区块链技术的载体，采用 LEO 卫星作为星间通信的主体卫星，此卫星的全球覆盖性飞行时间大约为 20 分钟，建立 15 个 LEO 卫星结构网络对地面的实时信息进行采集，LEO 卫星网络的信息接收发送延迟可以达到 15～18 ms，地面的手机用户可以选择性地连接 LEO 卫星结构网络中的任意卫星作为通信载体。LEO 单体卫星可以切换信号发射波束，考虑到多普勒效应，LEO 单体卫星的波束切换频率一般控制在 2～4 分钟一次[8]。

如表 1～2 所示为 LEO 卫星结构网络的构成部分。

表 1 LEOone～three 卫星结构网络的构成部分

名称	LEO One	LEO Two	LEO Three
轨道高度	1036	980	1005
颗数	6	4	5
轨道角度	25°	68°	50°
运行范围	50N－68S	全球覆盖	全球覆盖
周期	105	163	105

表 2 LEO Four ～ Six 卫星结构网络的构成部分

名称	LEO Four	LEO Five	LEO Six
轨道高度	1005	1230	968
颗数	8	17	15
轨道角度	65°	48°	18°
运行范围	全球覆盖	全球覆盖	全球覆盖
周期	184	165	135

由于 LEO 卫星需要大量的网络结构才可以实现对全球的通信网络全覆盖，为此本文在 LEO 卫星的网络结构体系中加入 MDO 型号卫星，可以全面覆盖全球的通信网络，在空间站中的运行探测角度可以达到 90°，卫星的波束切换频率相对于 LEO 卫星更加频繁[9-10]。

本文还对卫星星座进行了设计，本文设计的卫星星座体系是按照圆形规则而设计的全覆盖式卫星集合，相对于卫星单体对星间通信网络安全的加密更加全面，如图 1 所示为本文设计的卫星星座轨道图。

星座轨道的倾角角度最高可以接近 90°，在轨道两侧的卫星所运行的卫星数量相同。卫星星座的通信信息传达主要通过卫星网络来进行信号的接收与传送，卫星网络的设计结构比较简单，功能大多具有单一性，在进行长距离的

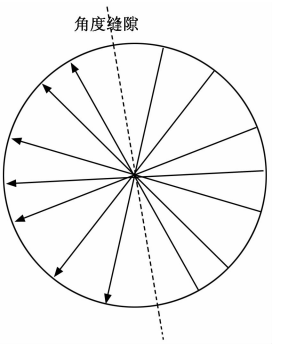

图 1 本文设计的卫星星座轨道图

信号星间通信内容传达的过程中所消耗的链路较大，因此本文在卫星网络的基础上引入了区块链技术，在区块链的基础上实现了对卫星网络的编程，指出区块链在卫星脚本中开发更多的应用服务系统，与用户之间构建功能修复性优化功能；区块链技术还实现了卫星网络的通信路径可追溯性，改变卫星网络中的链式区块结构内的储存内容，在数据层次上增加了卫星网络的时间维度，进而减少了星间通信的链路损耗。

卫星的网络通信在卫星网络中受到卫星型号、发射时间、运行轨道等多重因素的影响，为了能够更优质地发挥不同型号卫星的网络机制与性能，本文设计的卫星网络的结构布置如图 2 所示。

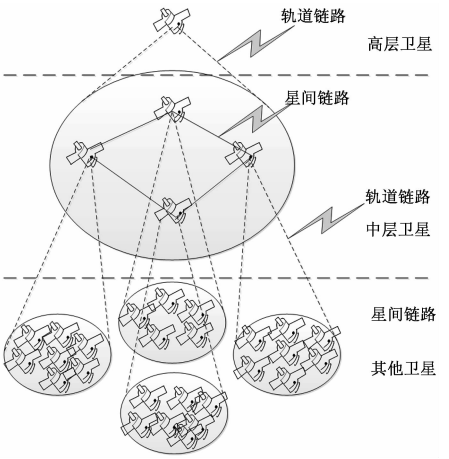

图 2 卫星网络的结构布置图

对于星间链路的设计本文系统主要采用卫星间的无线电或光纤链路，每一个层次的卫星都需要一套链路负责通信信息的接收与传递，在任何时间内链路与链路之间都能够保持关联，同时也能够关联两个卫星网络结构层次[11-13]。

轨道之间的链路同样是采用卫星间的无线电或光纤作为信息传播介质，每一个低轨道的卫星与高轨道的卫星进行通信的过程中，高阶层的卫星会通过无线电链路或光纤链路对下一阶层的卫星覆盖。地面上的用户与用户之间同样存在链路关系，用户与用户之间主要传达数据信息，因此用户之间的链路关系主要为上行链路与下行链路，用户的下行链路主要负责关联地球的发送信号和卫星的发送信号，而上行线路

主要负责关联卫星的接收信号与地球的接收信号，在同一个用户名下可以同时存在与多个链路发生关联的状态。如图 3 所示为本文系统中的卫星网络链路设计图。

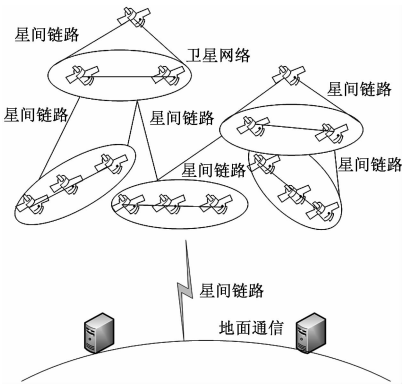

图 3　本文系统中的卫星网络链路设计图

为了能够更加精准地实现区块链在星间通信网络安全加密系统中的作用，本文分别对通信内容分析、雷达分析、通信覆盖程度分析、精准定位分析等，通过分析数据的计算结果判断星间通信网络安全的加密状态。

2　基于区块链技术的星间通信网络安全加密系统软件设计

区块链作为新兴的信息安全的核心技术之一，对于星间通信网络安全加密的身份认证鉴别是非常重要的系统组成部分，依据目前的科学手段，对星间通信网络安全加密的用户行进身份认证可以根据用户的生物特征以及身份证明来完成，此类认证方式为数字类区块链认证方式，传统的地面分布式操作系统对用户的通信信息集中式分布在网络环境中，面临着巨大的可信度问题，黑客可以通过攻击整个安全系统的用户可信度便可以获取用户的通信信息，为用户的身份认证带来巨大的安全隐患，黑客甚至可以伪造虚假的身份信息完成对用户通信网络环境的实时监控[14-15]。本文应用区块链分布式数字化身份加密技术，用户可以随时通过加密证书查询加密过程以及内容，区块链的数据查询模式主要发布在公钥掌握的数据库中，通过非对称加密算法，能够实现加密证书的注册、更新、加密状态等一系列的操作信息，保证区块链中的数据具有不可更改性。非对称加密算法能够对历史数据的储存空间进行全封闭管理，用户的加密过程不需要对全区块链内容下载即可完成加密查询与校验。区块链中的数据查询记录是对所有的用户都公开的，所以区块链技术的数据查询不能够较好地应用在公共互联网中。如图 4 所示为用户使用密钥对公钥的加密保护结构图。

区块链在卫星之间的体现主要在轨道链路中，卫星的轨道高度不同与覆盖区域不同等因素都会对区块链的安全加密技术产生干扰，由于星间通信网络的链路并非持续畅通的，当卫星的覆盖范围主要位于偏远极地区域，轨道间的区块链连接线路将会选择性关闭，为此本文将以区块链

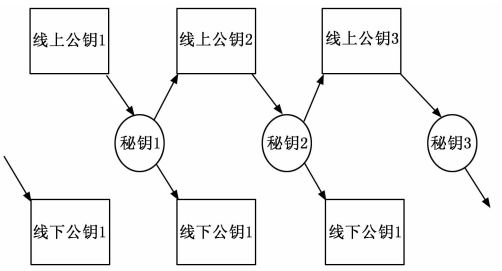

图 4　用户使用密钥对公钥的加密保护结构图

作为星间通信网络结构的链路主体，建立卫星网络的拓扑结构图如图 5 所示。

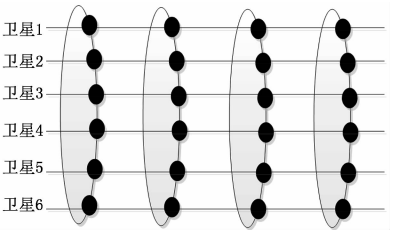

图 5　卫星网络的拓扑结构图

设定卫星的通信节点坐标为 $(\bar{x_c}, \bar{y_d})$，坐标中的 x、y 分别代表卫星在网络结构中的轨道高度与平面距离，考虑到卫星链路的反方向通信问题，还对卫星网络结构中的任意节点进行定义坐标，分别为 (x_1, y_1)、(x_2, y_2)，卫星节点与通信链路在同一平面内时定义卫星节点的 $\bar{y_d}$ 为：

$$\bar{y_d} = \begin{cases} \bar{y_b} \pm 1, & \bar{y_b} \pm 1 \in [0, M) \\ \bar{y_b} \pm 1 \mp M, & \bar{y_b} \pm 1 \notin [0, M) \end{cases} \tag{1}$$

若卫星节点与通信线路的平面位置在相邻状态，$\bar{x_c}$ 可以定义为：

$$\bar{x_c} = \begin{cases} \bar{x_a} \pm 1, & \bar{x_a} \pm 1 \in [0, N) \\ \bar{x_a} \pm 1 \mp N, & \bar{x_a} \pm 1 \notin [0, N) \end{cases} \tag{2}$$

卫星节点内的身份验证安全协议的初始化工作主要是最初的给定参数作为安全数值，区块链内的安全数据与卫星节点的安全数据分别定义为 G_1、G_2，数据之间的链路呈现双线性映射关系，映射公式定义为：

$$G_1 \times G_1 \rightarrow G_2 \tag{3}$$

卫星节点的安全参数初始化完成后，所有的网络公钥均可以重新输入程序改变成私钥，分别对应不同客户的星间通信网络安全加密任务。

完成星间通信网络安全加密系统的最后步骤为发送路由请求，经过卫星间的路由向通信节点发送安全协议，减少区块链在路由中的数据资源浪费，按照相关协议对卫星网络节点中的链路进行安全识别，使区块链中的数据相互约束，更深层次地完成加密系统，实现基于区块链的星间通信网络安全加密控制系统设计。

3　实验研究

3.1　实验环境与方法

为了验证本文系统的有效性，引用传统的地面分布式

操作系统及 ATM－Sat 项目作为实验对比方法，制定了 3 种系统的对比实验。传统的地面分布式操作系统主要对地面用户的通信网络进行连接加密工作，通过互联网模式完成对通信网络安全的加密工作，虽然具有覆盖面积广的优点，但是此系统的星间通信网络安全加密技术实现的安全性能深度不够；ATM－Sat 项目为了实现星间通信网络安全加密技术，对互联网中的通信网络安全管理数据库进行扩充，过度地依赖设备，面对星间通信链路的关联，存在着信道误码率高的问题。

如图 6 所示为本实验的环境图。

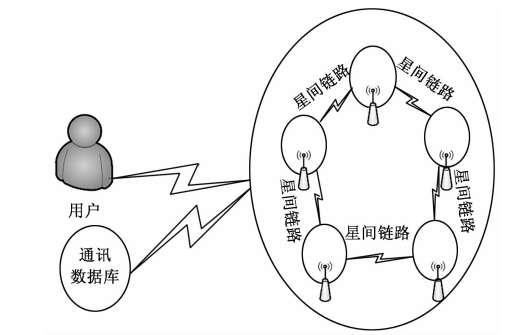

图 6 本实验的环境图

3.2 实验结果与讨论

实验主要是通过拓扑卫星间的网络监管中心与卫星链路的关联实现的。卫星首先向卫星监管中心发送安全报文，通信链路根据报文中的相关安全内容进行密钥拓扑，链路中的数据周期性地向用户的连接网络发送最新拓扑信息，方便用户对自身的星间网络安全加密操作数据查询，根据网络空间站的特点，通信链路中的众多因素会干扰通信链路的数据通断与传送，引用区块链对链路实现数据的公共管理，不断拓扑新型结构的密钥。在卫星节点处，由于链路的复杂性导致通信通道的误码率较高，甚至丢失安全通信包，因此对 3 种方法的加密深度程度进行对比，对比结果如图 7 所示。

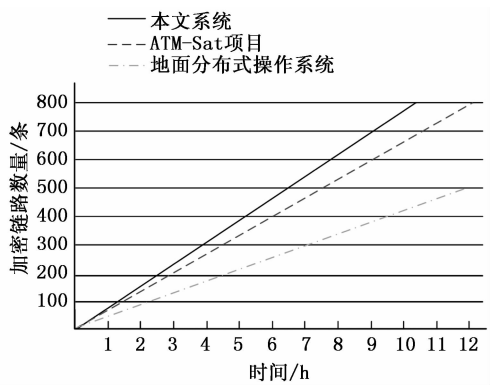

图 7 3 种方法的加密深度对比结果

根据图中的结果可知，本文所研究的系统对星间通信网络安全加密技术有着更深层次的加密技术。利用区块链技术对通信网络中的链路通道数据完成全方位覆盖，能够基于区块链技术利用路由对通信安全数据发送相关协议，区块链技术与通信链路之间呈映射关系，能够与链路中的数据结构互相结合，避免因误码率因素导致的加密误差；而地面分布式操作系统与 ATM－Sat 项目只单项地对地面的通信网络实现了安全加密，导致加密程度较弱。本实验还对 3 种系统的信道误码率进行对比，结果如图 8 所示。

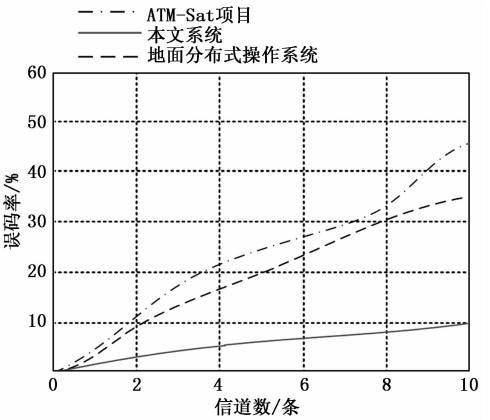

图 8 3 种系统的信道误码率对比结果

由图可知本文系统的信道误码率较小，这是由于本文采用区块链技术与通信链路之间形成映射关系，在卫星节点的安全参数内容上做出了程序性的可更改操作，为信道的环境做出了改善，本文系统还利用路由实现了安全数据与区块链数据的相互约束，满足了安全加密的数据协调性；而地面分布式操作系统与 ATM－Sat 项目的信道误码率基本采用硬件设备的自主去除，效果不明显且容易造成数据包的丢失。

4 结束语

通信技术的进一步发展与人们对通信的依赖程度提升有很大关系，在互联网的大背景下人们的通信安全性能得到了重视，通信之间的信息泄露、通信信息的被监听都成为了威胁通信安全的手段，为了改善人们的通信安全环境，本文研究基于区块链技术的星间通信网络安全加密系统，引用区块链技术加强通信网络环境的安全性，改善了传统方法中星间通信网络安全加密系统加密深度低的问题，实验结果表明，所设计系统的信道误码率低，加密深度较强，为通信网络安全环境奠定了发展基础。

参考文献：

[1] 徐 健，陈志德，龚 平，等. 基于区块链网络的医疗记录安全储存访问方案 [J]. 计算机应用，2019，39 (5)：1500－1506.

[2] 朱凤霞. 基于区块链技术的交易数据库加密技术 [J]. 电子设计工程，2020，28 (3)：93－97.

[3] 杨惠杰，周天祺，桂梓原. 区块链技术在物联网中的身份认证研究 [J]. 中兴通讯技术，2018，24 (6)：39－44.

[4] 陈 齐，王正国，李文锋，等. 区块链技术在新型网络购物平台设计中的应用 [J]. 武汉理工大学学报：信息与管理工程

版，2018，40（2）：69－73.
[5] 陶　启，崔晓晖，赵思明，等. 基于区块链技术的食品质量安全管理系统及在大米溯源中的应用研究［J］. 中国粮油学报，2018，33（12）：110－118.
[6] 李静元，范祥辉，王　颖. 基于区块链的共享经济隐私保护机制的设计［J］. 计算机应用与软件，2019，36（1）：302－307.
[7] 翟社平，李兆兆，段宏宇，等. 区块链关键技术中的数据一致性研究［J］. 计算机技术与发展，2018，28（9）：94－100.
[8] 杨信廷，王明亭，徐大明，等. 基于区块链的农产品追溯系统信息存储模型与查询方法［J］. 农业工程学报，2019，35（22）：323－330.
[9] 张旭凤，宛如星，郑忠义. 基于区块链技术的农产品物流信息系统模式［J］. 江苏农业科学，2019，47（15）：263－268.
[10] 段琼琼，项定华，史红周. 基于区块链的智能物件认证技术方案设计［J］. 信息网络安全，2018，213（9）：101－107.
[11] 范贤丽，范春晓，吴岳辛. 基于区块链和 IPFS 技术实现粮食供应链隐私信息保护［J］. 应用科学学报，2019，37（2）：33－44.
[12] 张　利，童　舟. 基于区块链技术的农产品溯源体系研究［J］. 江苏农业科学，2019，47（13）：245－249.
[13] 祁　兵，夏　琰，李　彬，等. 基于区块链激励机制的光伏交易机制设计［J］. 电力系统自动化，2019，43（9）：170－180.
[14] 宁　卓，李牧阳. 基于联盟区块链的物流信息平台 LIP－Chain［J］. 计算机技术与发展，2019，29（8）：190－194.
[15] 赵灵奇，宋宇波，张克落，等. 基于区块链和分层加密的物流隐私保护机制［J］. 应用科学学报，2019，37（2）：224－234.

（上接第 164 页）

计和 NRP－Z21 功率传感器使用 NRP2 功率计作为读数装置，N1921A 功率传感器使用 N1911A 功率计作为读数装置，YM8171 功率传感器使用的 YM2422 功率计作为读数装置。软件安装计算机操作系统为 Windows8.1 专业版 64 位操作系统，CPU 为 Corei3－4020Y，主频 1.5 GHz，计算机内存 4 GB。

校准 NRP－Z21 功率传感器时设置校准频率为 10 MHz～18 GHz，频率步进值为 1，校准频率点 36 个，平均次数 3，校准功率值 5 mW，使用传递标准法校准，自动校准软件实际测量和计算的 144 个频率点的数据，自动校准的实际运行时间为 2 min 51 s。

校准 N1921A 功率传感器时设置校准频率为 50 MHz～18 GHz，频率步进值为 1，校准频率点 32 个，平均次数 3，校准功率值 1 mW，使用交替比较法校准，自动校准软件实际测量和计算的 256 个频率点的数据，不计更换功分器连接端口的操作时间，自动校准的实际运行时间为 4 min 19 s。

校准 YM2422 功率传感器时设置校准频率为 10 MHz～18 GHz，频率步进值为 1，校准频率点 36 个，平均次数 3，校准功率值 1 mW，使用传递标准法校准，自动校准软件实际测量和计算的 144 个频率点的数据，使用图像识别方式进行读数，自动校准的实际运行时间为 5 min 37 s，所有数字图像均正确识别。

软件测试时，通过 VS 开发平台的诊断工具观察，不使用图像识别方式读数时，软件运行时内存使用为 20 MB～40 MB，CPU 使用率不超过 25%，使用图像识别方式读数时，内存使用为 40 MB～260 MB，CPU 使用率不超过 35%，一般配置的计算机均可满足软件运行要求，使用图像识别方式读数要求计算机操作系统为 64 bit，且安装有 DirectX9.0C 或以上版本。

4　结束语

自动校准控制软件的应用极大提高校准功率传感器的工作效率，软件的设计具有很强的通用性，支持主流厂商的信号源、功率计等仪器，可根据现有的仪器，配置软件的运行参数，完成自动校准。软件使用 C＋＋语言编写，具有很高的执行效率，采用面对对象的开发方法，方便对软件进行升级，实现对更多仪器的支持和扩展功能。

参考文献：

[1] 李铁虎. 射频功率传感器自动校准技术研究［D］. 广州：华南理工大学，2011.
[2] 刘　颖，龚晓峰. 一种微波功率计自动校准系统设计与实现［J］. 现代电子技术，2012，35（11）：161－163.
[3] 丁　双，任国营，张福民，等. 改进的穿线法的卡尺图像识别［J］. 计量学报，2019，40（5）：765－769.
[4] GJB 3598－1999，小功率座检定规程［S］.
[5] 李进源，谢　鸣. 18～26.5 GHz 功率密度标准装置［J］. 计量学报，2015，36（2）：171－175.
[6] 崔孝海，杨　日. 基于“层次计量架构”的通用计量软件研究［J］. 计量学报，2007（3）：284－287.
[7] Robert Sedgewick，Kevin Wayne 著，谢路云译. 算法（第 4 版）［M］. 北京：人民邮电出版社，2012.
[8] 孙　鑫. VC＋＋深入详解（第 3 版）（基于 Visual Studio 2017）［M］. 北京：电子工业出版社，2019.
[9] 安德里安·凯勒，加里·布拉德斯著，刘昌祥译. 学习 OpenCV 3（中文版）［M］. 北京：清华大学出版社，2018.
[10] 赵春江. 机器学习经典算法剖析基于 OpenCV［M］. 北京：人民邮电出版社，2018.
[11] 曾　科，高　潮，扶　新，等. 多参数数显仪表的自动识别方法研究［J］. 中国测试，2018，44（12）：122－128.
[12] 余　磊，聂　纯，马　晖，等. 基于 C＃和 SQL Server 的信号接收机自动校准系统软件设计与实现［J］. 计算机测量与控制，2020，28（3）：178－182.
[13] 苏姗姗，宋　哲. 基于 MET/CAL 的数字示波器自动校准系统［J］. 计算机测量与控制，2020，28（1）：251－254.
[14] 张　睿，周　峰，郭隆庆. 无线通信仪表与测试应用［M］. 北京：人民邮电出版社，2018.