文章编号:1671-4598(2024)03-0169-07 DOI:10.16526/j.cnki.11-4762/tp.2024.03.025 中图分类号:V19 文献标识码:A

基于区块链的实景三维地理信息数据加密控制系统设计

范 巍,黄 蕾,赵 晶
(湖北省测绘成果档案馆,武汉 430000)

摘要:为解决由公钥文本、私钥文本不匹配造成的信息数据错误加密问题,实现对实景三维地理信息数据的按需加密处理,设计了基于区块链的实景三维地理信息数据加密控制系统;设置CPU主机端调度模块、地理信息数据处理模块和混合加密模块作为主要元件,联合数字签名结构,完善矢量化计算单元的连接形式,完成对数据加密控制系统硬件的设计;按照区块链编码原则,确定关键区块角色的组成情况与公钥密码体制定义条件,并以此为基础,计算数据多项式结果;再根据Curl加密节点部署形式,求解隐藏加密向量的具体数值,实现对实景三维地理信息数据的加密处理;结合相关硬件应用结构,完成基于区块链的实景三维地理信息数据加密控制系统的设计;实验结果表明,设计系统的公钥文本、私钥文本之间的长度差不超过0.25 kB,能够较好解决由密钥文本不匹配造成的信息数据错误加密问题,符合按需加密处理实景三维地理信息数据的实际应用需求。

关键词:区块链技术;实景三维;地理信息数据;加密控制系统;数字签名;数据多项式;Curl加密节点;公钥文本;私钥文本

Design of Blockchain-Based Real-time 3D Geographic Information Data Encryption Control System

FAN Wei, HUANG Lei, ZHAO Jing
(Hubei Archives of Surveying and Mapping Production, Wuhan 430000, China)

Abstract: To solve the incorrect encryption of information data caused by mismatch between public key text and private key text, and to achieve the on-demand encryption processing of real 3D geographic information data, a realistic 3D geographic information data encryption control system based on blockchain was designed. Set the CPU host scheduling module, geographic information data processing module, and hybrid encryption module as the main components, combine digital signature structure, improve the connection form of vectorizing the calculation unit, and complete the hardware design of the data encryption control system. According to the principles of blockchain encoding, determine the composition of key block roles and the definition conditions of public key cryptography, and based on this, calculate the data polynomial results. Based on the deployment form of Curl encryption nodes, the specific values of hidden encryption vectors are solved to achieve the encryption processing of realistic 3D geographic information data. Combining the relevant hardware application structure, complete the design of blockchain-based realistic 3D geographic information data encryption control system. The experimental results show that the length difference between the public key text and private key text of the designed system does not exceed 0.25KB, which can effectively solve the incorrect encryption of information data caused by the key text mismatch, and meets the practical application requirements of on-demand encryption processing of realistic 3D geographic information data.

Keywords: blockchain technology; rRealistic 3D; geographic information data; encryption control system; digital signature; data polynomial; curl encryption node; public key text; private key text

0 引言

实景三维地理信息是描述地物景观特征的物理参量,可以从时间、空间等多个角度反映出地表对象在区域性环境中的表现形式,对于环境信息、GIS等应用系统而言,该类型数据样本参量能够表现出地貌、地形、地质等地表对象的真实存在状态[1-2]。在实际应用过程中,随着主机元件检测所得实景三维地理信息数据总量的增大,公钥文本、私钥文本之间的匹配程度会不断下降,而这则会直接导致信息数据错误加密的问题。因此,对实景三维地理信息数据进行加密控制具有重要意义。

目前相关领域学者针对数据加密系统进行了研究,文献[3]设计了PSK量子型随机加密系统,根据海森堡不确定性原理,定义多进制型的密文信号传输机制,再借助ADC芯片结构,对密文信息进行采样处理。文献[4]设计

收稿日期:2023-04-26; **修回日期**:2023-06-05。
作者简介:范 巍(1980-)男,硕士研究生,高级工程师。
引用格式:范 巍,黄 蕾,赵 晶.基于区块链的实景三维地理信息数据加密控制系统设计[J].计算机测量与控制,2024,32(3):169-175.

了多中继物理层网络编码系统，根据主机元件内信息数据的实时吞吐率水平，确定码源参量的实际取值范围，再根据传播译码系数的实际计算结果，调节中继器设备，从而实现对信息数据加密行为的有效控制。然而上述两种系统对于实景三维地理信息数据的按需处理能力有限，并不能有效解决信息数据的错误加密问题。

从狭义层面上来看，区块链是按照时间顺序排列的链式数据结构，能够准确描述出区块组织之间的连接与包含关系，从而在定义唯一密码文本的同时，建立完善的信息数据编码机制[5]。而从广义层面上来看，区块链体系的应用需要在验证数据结构块链式存储关系的基础上，重新安排分布式节点所处位置，一方面可以利用密码学原则约束数据样本的传输与访问行为，另一方面也能够实现对自动化脚本代码的完全执行，从而实现对信息数据传输格式的重新定义。由于区块链条之间的连接关系始终保持稳定状态，且每一区块主机都具备独立保存信息参量的能力，所以随着链条体系复杂化程度的不断增大，服务器主机中的数据样本累积量虽然会不断增大，但核心处理器元件的运行速率却并不会明显下降。相较于其他类型的数据传输机制，区块链技术能够最大化保障信息数据参量的传输安全性，且终端节点可以为信息样本的传输提供动力支持，因此下级客户端对象很难改写已被主机元件存储的数据文件，这也是区块链体系安全性等级相对较高的主要原因。基于此，设计了基于区块链的实景三维地理信息数据加密控制系统。

1 数据加密控制系统硬件设计方案

为有效实现实景三维地理信息数据加密控制，设计实景三维地理信息数据加密控制系统硬件执行方案，采用主要应用模块（CPU 主机端调度模块、地理信息数据处理模块、混合加密模块）、数字签名结构（SHA256 模块、SSL 模块、Kernel 签名机制）和矢量化计算单元等多个主要元件，本章节将针对其具体设计方案展开研究。

1.1 主要应用模块

1.1.1 CPU 主机端调度模块

在实景三维地理信息数据加密控制系统中，CPU 主机端调度模块负责执行数据样本查询、信息上下文机制定义、明文数据加载、加密队列设置等多项指令程序，以 CPU 运行设备作为核心执行元件，可以按照实景三维地理信息数据的互传需求，读取关键文本参量，从而在保证加密码源完整性的同时，实现对信息数据传输速率的有效控制[6]。Open CL 查询设备具有较强的信息识别能力，可以直接读取区块链组织中传输的实景三维地理信息明文数据，并可以按照信息参量的实时排列形式，定义地理信息传输所遵循的上下文机制。通常情况下，符合上下文机制的实景三维地理信息数据会经由通道组织，由 Open CL 查询设备传输至数据样本加载内核中，由于该传输过程的实现需要信息加密队列组织的配合，所以当内核组织中数据样本实时累积量达到一定数值标准之后，调度元件、CPU 运行设备与主机端核心设备之间才会建立信息数据互传关系。CPU 主机端调度模块连接结构如图 1 所示。

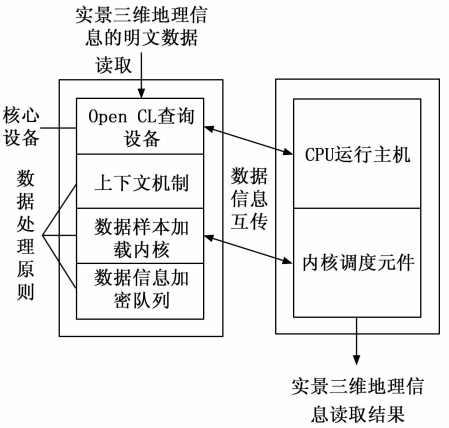

图 1 CPU 主机端调度模块结构图

对于实景三维地理信息数据加密控制系统而言，CPU 运行主机、内核调度元件的运行等级相同，特别是在处理数据参量时，二者同时建立与核心设备的信息互传关系，但只有内核调度元件具有输出信息读取结果的能力，所以为避免 CPU 主机端调度模块中出现信息参量过量累积的情况，Open CL 查询设备在单位时间内提取的明文数据样本总量不宜过大。

1.1.2 地理信息数据处理模块

地理信息数据处理模块是负责对实景三维地理信息全景图进行分区处理的结构元件，可以在最大化保障数据样本统一性的同时，划分成多个不同的小型像素单元，从而节省主机元件在加密数据样本时所需的等待时长，使得矢量化计算单元能够对信息参量公钥文本、私钥文本进行准确定义[7]。通常情况下，全景图中待加密的实景三维地理信息数据参量保持连续性的分布状态，且像素节点之间完全没有间隙，对于矢量化计算单元而言，如果直接处理这种类型的地理信息数据，在加密处理过程中，极易使主机元件所定义公钥文本、私钥文本长度与真实值出现偏差，而这将直接导致信息数据的错误加密问题。未经处理的实景三维地理信息全景如图 2 所示。

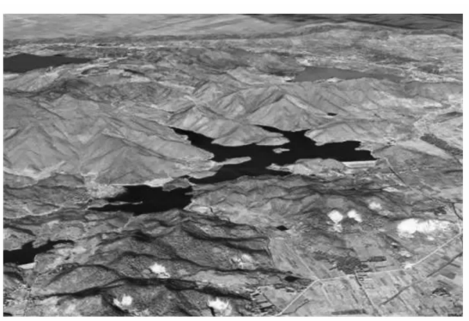

图 2 实景三维地理信息全景图

而在地理信息数据处理模块的作用下，全景图被切割

成多个独立的小像素单元，在加密控制系统中，每一个小像素单元都对应一个实景三维地理信息数据参量。相较于完整的地理图像，控制主机在加密较短信息参量时，能够更加精准地定义公钥文本与私钥文本长度，从而避免信息数据错误加密问题的出现[8]。经过处理后的实景三维地理信息图像如图 3 所示。

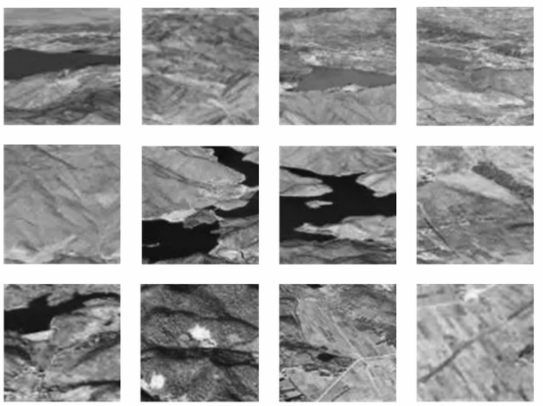

图 3　处理后的实景三维地理信息

与 CPU 主机端调度模块不同，地理信息数据处理模块对于实景三维地理信息的作用表现在图像完整度方面，因此其对于待加密信息数据参量实时传输能力的要求相对较低。

1.1.3　混合加密模块

混合加密模块是实景三维地理信息数据加密控制系统的核心应用部件，可以同时录入与加密原则相关的明文与密文参量，并借助内核元件，对信息数据样本进行混合处理。由于系统控制主机对于明文参量、密文参量的识别能力不同，因此完成编码的加密结果并不保持混合输出状态。AES-CTR 加密芯片只具有模糊识别能力，所以在提取实景三维地理信息数据的过程中，混合了明文参量和密文参量，但加密控制主机对于信息数据的编码遵循准确性原则，因此 AES-CTR 加密芯片提取到的数据样本并不能被系统主机直接利用[9]。数据样本混合单元的设置是为了在混合明文、密文参量的同时，建立两个完全独立的信道组织，从而使得码源输出结果能够保持非相关状态，以供系统主机对待加密实景三维地理信息数据参量进行自主选择。混合加密模块的设计原理如图 4 所示。

在混合加密模块中，FPGA 单元由 AES-ECB、AES-CBC、DES、RSA 四类应用设备组成，其中前两类设备负责识别明文参量，后两类设备负责识别密文参量[10]。此外，混合加密模块作为数字签名结构的上级负载元件，能够将实景三维地理信息数据加密结果直接反馈回系统控制主机，并以此达到对区块链码源信息进行矢量化计算的目的，从而在根本上解决信息数据错误加密的问题。

1.2　数字签名结构

数字签名结构由 SHA256 模块、SSL 模块、Kernel 签名机制三部分共同组成。

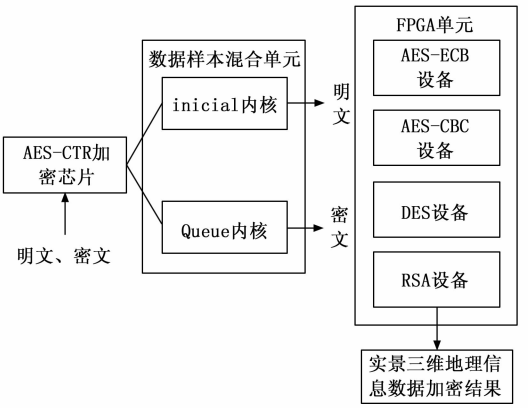

图 4　混合加密模块设计原理

1.2.1　SHA256 模块

SHA256 模块负责定义与实景三维地理信息数据相关的共享对象，可以在 CPU 主机端调度模块、混合加密模块保持完全开放状态的情况下，直接调取经过处理后的实景三维地理图像小像素参量[11]。在加密控制系统中，数字签名需要得到主机元件的直接认证，所以 SHA256 模块在提取小像素参量时，还应按照一致性原则，对所涉及明文信息与密文信息进行整合处理。

1.2.2　SSL 模块

SSL 模块可以基于摘要文件，对实景三维地理信息数据进行识别，在加密信息参量的过程中，SHA256 模块与 SHA256 模块保持稳定连接关系，所以 SSL 模块所选择摘要定义标准，将直接影响与系统主机匹配的数字签名表达形式[12]。相较于 SHA256 模块，SSL 模块在完善加密体系时，更注重保障数字签名结果的完整性，如果混合加密模块输出结果只包含一类码源参量，或明文、密文参量间差异性不明显，那么 SSL 模块则不能对实景三维地理信息数据进行加密处理。

1.2.3　Kernel 签名机制

Kernel 签名机制可以用来描述数字签名文件的完整性。由于系统控制主机对于实景三维地理信息数据的加密处理完全参考数字签名文件，所以在定义 Kernel 签名机制时，还要参考 SHA256 模块与 SSL 模块之间的实时连接关系。此外，系统数字签名结构的设计还要求明文参量、密文参量在区块链体系中应同时保持稳定且自由地传输状态。

1.3　矢量化计算单元

实景三维地理信息数据加密控制系统的执行目标就是将一个明文项参量加载到一个密文项参量上，再将整个数据包单元输入区块链体系，从而控制系统主机内加密指令的执行速率。然而在系统运行过程中，实景三维地理信息数据的加密行为并不会一直按照控制主机的预设情况进行，所以公钥文本、私钥文本极易出现不匹配关系，这就表示单纯加密并不能实现对信息数据参量的有效控制，还需在执行核心指令之前，按照既定原则对所涉及数据样本进行优先化处理，也就是满足区块链运行需求的矢量化计算[13]。

整个处理流程完全在矢量化计算单元中进行，前置对象 ST 计算单元与矢量化记忆文件之间的数据样本传输行为具有双向性特征，这就保证了系统主机在执行加密处理的过程中，明文参量、密文参量始终保持同频传输状态。后置对象 LD 计算单元由 8 个 SIMD 设备和 8 个 Unit 设备共同组成，前者接收待加密的矢量化记忆文件，后者则可以对完成处理的数据样本进行直接存储。矢量化计算单元结构模型如图 5 所示。

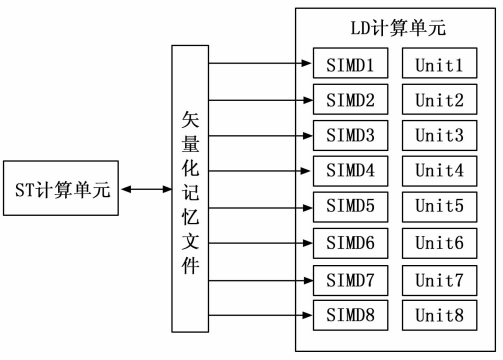

图 5 矢量化计算单元结构模型

为避免实景三维地理信息数据在加密过程中出现混乱传输状态，ST 计算单元、LD 计算单元之间信息参量的传输不满足双向性特征，由于后者配置独立的数据样本存储单位，所以其对于码源信息的存储能力比前者更强[14]。

2 实景三维地理信息数据的加密处理

在各级硬件结构的支持下，为完成对实景三维地理信息数据加密控制系统的设计，还需按照区块链编码原则，求解数据多项式计算结果，从而在满足 Curl 加密节点部署需求的同时，确定隐藏加密向量的实际取值范围。

2.1 区块链编码原则

2.1.1 区块角色组成

对于实景三维地理信息数据加密控制系统而言，其区块链编码原则的实现需要移动终端用户、边缘服务器、身份管理中心三类角色对象的共同配合。

1）移动终端用户：

为实现对地理信息数据加密行为的准确控制，区块链体系的移动终端用户需要在 OBT 单元的配合下，才能实现对实景三维信息的定义，且在区块链网络模型中，已被定义的信息参量必须借助通道组织，才能由终端节点传输至其他服务器元件中[15]。但由于数据样本加密模板的定义必须满足一致性原则，所以移动终端用户在提取信息参量时，整个区块链体系必须保持完全连通状态。

2）边缘服务器：

边缘服务器可以将实景三维地理信息数据由区块链主机下沉至身份管理中心，由于移动终端用户负责调度所有密码文本，所以在服务器处于持续连接状态的情况下，系统控制主机每提取到一个数据参量，边缘服务器机构中都会生成一套全新的加密模板，而这些密码模板在得到身份管理中心的识别与认证之前，都直接存储于系统数据库单元中。

3）身份管理中心：

身份管理中心是一个完全可靠的加密处理机构，负责管理边缘服务器输出的源码模板。在区块链体系中，如果有新的边缘节点加入服务器，那么控制主机所遵循的编码原则极易出现混乱，而在身份管理中心的作用下，密码文本可以长期存储于系统数据库主机中，因此当新节点加入服务器组织时，数据库主机会自动向外推送源码模板，当前情况下，加密控制系统的运行速率虽然会出现一定程度的下降，但实景三维地理信息数据与码源参量之间的对应关系却并不会发生改变[16]。

2.1.2 公钥密码体制

公钥密码体制是具有高度对称特征的数据加密模板。受到区块链体系编码角色组成形式的影响，加密码源、解密码源并不会出现在同一套密码文本中，但由于控制系统的运行必须得到唯一的加密结果，所以公钥密码体制在规范加密码源、解密码源时，必须对实景信息数据加密行为与解密行为进行分别处理。

区块链组织规定：加密码源作用下，实景三维地理信息数据会在矢量化计算单元中转化为密文状态，且这种编码行为具有不可逆性；解密码源作用下，处于密文状态的信息参量会在地理信息数据处理模块中再次转化为实景三维信息[17]。而所谓公钥密码体制就是完全包含加密与解密行为的区块链加密执行周期，出于精确性考虑，只有在加密码源、解密码源同时保持完整状态的情况下，区块链组织才具有执行加密指令的能力[18]。

对于区块链公钥密码体制的定义满足如下表达式：

$$E=(\chi-1)^2\cdot\frac{\alpha\bar{w}+\delta\bar{e}}{\beta\mid\Delta Q\mid} \tag{1}$$

其中：χ 表示对称加密特征，$\bar{w}$ 表示实景三维地理信息数据的加密码源，$\bar{e}$ 表示解密码源，α 表示区块链体系中的密码查询参数，δ 表示明文查询参数，ΔQ 表示实景三维地理信息数据在区块链体系中的单位累积量，β 表示实时转码参量。由于加密控制系统的公钥密码体制只存在于区块链体系中，所以加密指令的执行，要求系统数字签名结构、矢量化计算单元等硬件应用结构必须保持稳定的连接状态。

2.2 数据多项式计算

数据多项式是指符合多级编码条件的实景三维地理信息数据，在区块链编码原则的作用下，系统控制主机所选取的编码对象必须符合数据多项式定义标准，一方面可使移动终端用户、边缘服务器、身份管理中心三类区块角色之间进行自由转换，另一方面也能够为矢量化计算单元提供足量的可提取数据样本。区块链体系在定义多项式对象时，要求实景三维地理信息数据加密码源、解密码源的传输方向必须保持一致，且整个加密过程中，数据库主机中的信息参量存储行为不可以发生间断[19]。设定 ε_1、ε_2 表示

两个随机选取的信息参量分类项式定义条件，为满足多项式定义原则，要求 $\varepsilon_1 \neq \varepsilon_2$ 的不等式取值条件恒成立，q' 表示与 ε_1 匹配的区块链编码参量，q'' 表示与 ε_2、ε_1 匹配的区块链编码参量，$\widetilde{R}$ 表示实景三维地理信息数据的身份管理特征，联立上述物理量，可将数据多项式定义结果表示为：

$$I_\gamma = \widetilde{R} \times \left| \frac{q'^{\varepsilon_1}}{q''^{\varepsilon_2}} \right|^2 \tag{2}$$

联立公式（1）、公式（2），可将数据多项式计算表达式定义为：

$$O = \sum_{\gamma=1}^{+\infty} I_\gamma \times \sqrt{(\Delta T \cdot E)^{\frac{1}{+}}} \Big|_{u \neq 0} \tag{3}$$

式中，γ 表示实景三维地理信息数据的公钥密码参量，ΔT 表示区块链体系中的数据样本加密周期，u 表示区块角色转换系数[20]。区块链体系的存在是为了配合实景三维地理信息数据加密控制系统的运行，而数据多项式则是区块链体系定义数据样本参量所遵循的必要条件，因此在定义过程中，控制主机要求公钥密码体制必须与区块角色保持一一对应关系。

2.3　Curl 加密节点部署

Curl 节点是负责加密处理实景三维地理信息数据的区块链端点对象，对于信息参量具有较强的承载能力，可以在保障数据多项式计算特征的同时，提取区块链体系中的待编码对象，从而使得矢量化计算单元能够直接提取系统数据库主机中的信息实景三维信息参量[21]。区块链体系编码数据多项式对象时，要求加密码源、解密码源必须保持高度同源性的传输特征，且为使区块链体系的完整性得到保证，Curl 节点在单位加密周期内，只能提取同一类型的数据样本参量。设 u_1、u_2、…、u_n 表示区块链体系中 n 个随机选取的实景三维地理信息数据样本，且 $u_1 > 0$、$u_2 > 0$、…、$u_n > 0$ 的不等式取值条件同时成立，φ_1、φ_2、…、φ_n 分别表示与不同数据样本参量对应的加密指标，联立上述物理量，可将 Curl 节点 p_1、p_2、…、p_n 的定义结果表示为：

$$\begin{cases} p_1 = \varphi_1 \cdot u_1 \\ p_2 = \varphi_2 \cdot u_2 \\ \vdots \\ p_n = \varphi_n \cdot u_n \end{cases} \tag{4}$$

在公式（4）的基础上，设 $\overline{S}$ 表示区块链体系中的密钥文本传输均值，a 表示 Curl 节点在区块链体系中的部署参数，f 表示实景三维地理信息数据的同源性传输特征，φ 表示同源条件下的数据对象加密参量，联立公式（3），推导 Curl 加密节点部署条件如公式（5）所示。

$$P = \overline{S} \times \left(\frac{|O^{a-1}|}{f \cdot \varphi} \right)^2 (p_1 \cdot p_2 \cdot \cdots \cdot p_n) \tag{5}$$

部署 Curl 加密节点时，区块链体系与系统控制主机对于实景三维地理信息数据的处理能力相同，且由于数据库机制始终对待加密信息保持连续录入状态[22]，所以实景三维数据在相邻 Curl 节点之间的传输速率较快，加密码源、解密码源也必须在区块链边缘服务器中进行频繁转换。

2.4　隐藏加密向量

隐藏加密向量决定了加密控制系统主机对于实景三维地理信息数据的承载能力，在 Curl 加密节点部署形式保持不变的情况下，该项物理量的取值越大，就表示系统主机对于实景三维地理信息数据的承载能力越强[23]。所谓隐藏加密就是指针对非直接传输数据所定义的加密原则，对于区块链体系而言，由于移动终端用户、边缘服务器之间的直接连接关系会使很多信道组织处于空闲状态，所以系统主机在加密实景三维地理信息数据时，很难实现对密码参量的完全查询，而在隐藏加密行为的作用下，系统主机可以根据密码参量之间的数值差，来判断未查询信息数据所处位置，从而最大化保障主机元件对实景三维地理信息数据加密行为的控制能力[24]。设 d 表示针对移动终端用户的信息样本隐藏编码参数，g 表示针对边缘服务器的信息样本隐藏编码参数，关于二者取值，公式（6）所示的不等式条件恒成立。

$$d \neq g \tag{6}$$

规定 h_1、h_2 表示两个不相等的实景三维地理信息数据加密指标，其取值满足公式（7）所示表达式。

$$h_1, h_2 \in [1, +\infty) \tag{7}$$

联立公式（5）、公式（6）、公式（7），可将隐藏加密向量计算结果表示为：

$$K = (\kappa \vec{j} P)^2 - \left(h_1 \frac{dg}{l_1} + h_2 \frac{dg}{l_2} \right) \tag{8}$$

其中：κ 表示区块链体系中的数据样本加密服务参量，$\vec{j}$ 表示系统主机中的数据样本实时加密向量，l_1 表示基于 h_1 指征的码源参数，l_2 表示基于 h_2 指征的码源参数。至此，实现对相关参数指标的计算与处理，联合相关硬件应用结构，完成基于区块链的实景三维地理信息数据加密控制系统的设计。

3　实验分析

为了验证设计的基于区块链的实景三维地理信息数据加密控制系统的有效性，实验根据公钥文本、私钥文本之间的匹配关系，分析信息数据错误加密问题出现的概率，选择设计的基于区块链的实景三维地理信息数据加密控制系统、文献［3］PSK 量子型随机加密系统和文献［4］多中继物理层网络编码系统作为三组不同的实验系统。

3.1　原理描述

对于实景三维地理图像而言，主机元件在对其中所包含信息数据进行加密处理时，所定义公钥文本与私钥文本之间的匹配关系，可以用来描述信息数据错误加密问题的出现概率。在不考虑其他干扰条件的情况下，公钥文本定义长度、私钥文本定义长度之间的物理差值越小，就表示两类文本的匹配性越强，信息数据错误加密问题的出现概率相对较小，主机元件可以实现对实景三维地理信息数据的按需加密处理。

选择实景三维地理图像作为实验对象，如图 6 所示。

其中，X 轴对应水平方向、Y 轴对应竖直方向，Z 轴对应三维空间方向。

本次实验的具体实施流程如下：

1）调节图 6 所示实景三维地理图像的亮度水平，并利

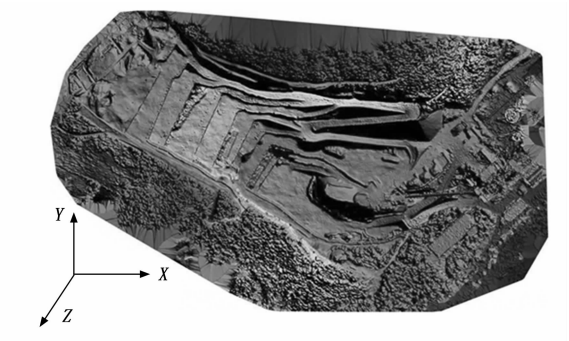

图 6 实景三维地理图像

用 Windows 主机提取其中的信息数据对象。

2）应用设计的基于区块链的实景三维地理信息数据加密控制系统对所得信息数据进行编码处理，并在处理过程中，记录公钥文本、私钥文本的定义长度，所得数据为实验组变量。

3）应用文献［3］PSK 量子型随机加密系统对所得信息数据进行编码处理，并在处理过程中，记录公钥文本、私钥文本的定义长度，所得数据为对照（1）组变量。

4）应用文献［4］多中继物理层网络编码系统对所得信息数据进行编码处理，并重复上述实验步骤，所得数据为对照（2）组变量。

5）分别统计实验组、对照（1）组、对照（2）组公钥文本与私钥文本之间的定义长度差值，并以此为基础，研究主机元件对实景三维地理信息数据的按需加密处理能力。

3.2 数据处理

实验组、对照组公钥文本与私钥文本定义长度的具体实验数值如图 7 和图 8 所示。

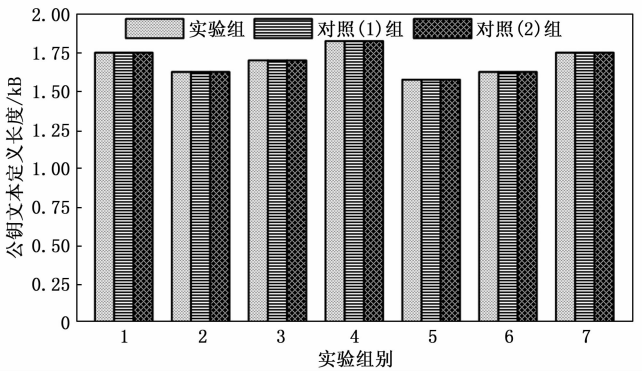

图 7 公钥文本定义长度

根据图 7、图 8 中的实验结果，统计实验组、对照组公钥文本与私钥文本之间的定义长度差，具体实验结果如表 1 所示。

分析表 1 可知，第 2 实验组别处，实验组公钥文本、私钥文本的定义长度差取得最大值为 0.25 kB，整个实验过程中，实验组长度差均值为 0.13 kB。第 6 实验组别处，对照（1）组公钥文本、私钥文本的定义长度差取得最大值为 0.75 kB，与实验组最大值相比，增大了 0.50 kB，整个实

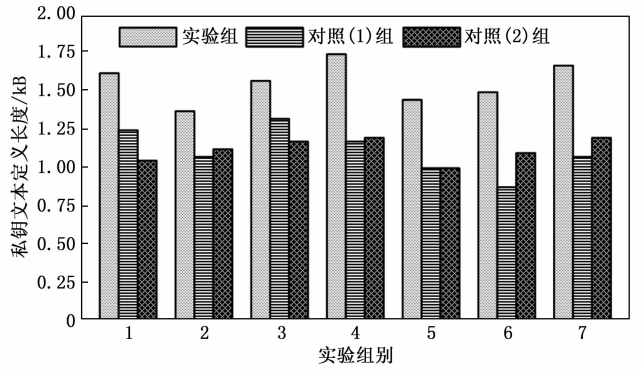

图 8 私钥文本定义长度

验过程中，对照（1）组长度差均值为 0.58 kB，与实验组均值相比，增大了 0.45 kB。第 1 实验组别处，对照（2）组公钥文本、私钥文本的定义长度差取得最大值为 0.69 kB，与实验组最大值相比，增大了 0.44 kB，整个实验过程中，对照（2）组长度差均值为 0.57 kB，与实验组均值相比，增大了 0.44 kB。

表 1 公钥文本、私钥文本的定义长度差

实验组别	定义长度差值/kB		
	实验组	对照(1)组	对照(2)组
1	0.12	0.50	0.69
2	0.25	0.52	0.50
3	0.11	0.37	0.54
4	0.09	0.65	0.63
5	0.14	0.61	0.61
6	0.13	0.75	0.51
7	0.09	0.64	0.54

3.3 实验结论

综上可知本次实验结论为：

1）文献［3］PSK 量子型随机加密系统在控制公钥文本、私钥文本定义长度差方面的应用能力相对有限，因此该系统的应用，不足以解决由公钥文本、私钥文本不匹配造成的信息数据错误加密问题。

2）文献［4］多中继物理层网络编码系统对于公钥文本、私钥文本定义长度差值的控制能力也无法满足实际应用需求，因此该方法的应用，也不足以解决由公钥文本、私钥文本不匹配造成的信息数据错误加密问题。

3）设计的基于区块链的实景三维地理信息数据加密控制系统的应用，可以有效控制公钥文本、私钥文本之间的定义长度差值，从而解决由公钥文本、私钥文本不匹配造成的信息数据错误加密问题，符合按需加密处理实景三维地理信息数据的实际应用需求。

4 结束语

设计的实景三维地理信息数据加密控制系统，以区块链技术为基础，联合 CPU 主机端调度模块、数字签名结构等多个硬件应用结构，在计算数据多项式表达条件的同时，

对 Curl 加密节点进行按需部署。随着这种新型控制系统的应用，由公钥文本、私钥文本不匹配造成的信息数据错误加密问题得到了较好解决，可以实现对实景三维地理信息数据的按需加密处理。

参考文献：

[1] 黄林周，姜紫薇，黄　印. 实景三维地理信息系统在智慧林业中的应用 [J]. 地理空间信息，2023，21 (3)：49 - 51.

[2] 张晓恒，吕希奎，聂良涛. 基于倾斜摄影的城市轨道交通三维实景环境建模方法 [J]. 城市轨道交通研究，2019，22 (11)：79 - 82.

[3] 谭业腾，蒲　涛，郑吉林，等. PSK 量子噪声随机加密系统的实现方法研究 [J]. 量子电子学报，2022，39 (3)：423 - 430.

[4] 唐　猛，李海华，谢灵运，等. 多中继物理层网络编码系统加密设计及安全性能研究 [J]. 云南大学学报 (自然科学版)，2021，43 (4)：652 - 662.

[5] 龚琴，孙学军. 基于区块链的物联网可撤销属性基加密算法 [J]. 计算机仿真，2022，39 (2)：371 - 374.

[6] 汤小春，赵　全，符　莹，等. 面向 Dataflow 的异构集群混合式资源调度框架研究 [J]. 软件学报，2022，33 (12)：4704 - 4726.

[7] 吴　涛，汪　璐，秦建新，等. 基于众源地理数据的个性化路线服务框架及应用实验 [J]. 地理与地理信息科学，2022，38 (1)：51 - 56.

[8] 李　忠，任东宇，周　启，等. 一种面向海量基础地理信息数据更新的多人协同作业方法 [J]. 测绘通报，2022，546 (9)：145 - 151.

[9] 田洪亮，王佳玥，李晨曦. 基于混合算法区块链和节点身份认证的数据存储方案 [J]. 计算机应用，2022，42 (8)：2481 - 2486.

[10] 韩益亮，郭凯阳，吴日铭，等. 格上基于 OBDD 访问结构的抗密钥滥用属性加密方案 [J]. 通信学报，2023，44 (1)：75 - 88.

[11] 朱　辉，黄煜坤，王枫为，等. 一种基于图形处理器的高吞吐量 SM2 数字签名计算方案 [J]. 电子与信息学报，2022，44 (12)：4274 - 4283.

[12] 孟　博，王潇潇，郑绪睿，等. 一种安全的 PKI 与 IBC 之间的双向异构数字签名方案 [J]. 中南民族大学学报 (自然科学版)，2021，40 (2)：184 - 192.

[13] 周　游，李　杰，贺光辉. 面向高精度随机计算单元的加法运算电路与 MAX 运算电路设计 [J]. 微电子学与计算机，2021，38 (7)：1 - 6.

[14] 尹震宇，徐光远，张飞青，等. 面向 Zynq 平台的卷积神经网络单元设计与实现 [J]. 小型微型计算机系统，2022，43 (2)：231 - 235.

[15] 戴　波，赖旬阳，胡　凯，等. 基于多角色节点的区块链可扩展方案研究与设计 [J]. 浙江工业大学学报，2021，49 (5)：487 - 493.

[16] 段　婷，王维平，朱一凡，等. 基于区块链智能合约的 UAV 集群访问控制机制 [J]. 系统仿真学报，2021，33 (11)：2656 - 2662.

[17] 黄文俊，李　旭，杨明强，等. 无线自组网分布式编码域非正交多址机制性能分析 [J]. 兵工学报，2022，43 (12)：3082 - 3092.

[18] 王　练，朱朝辉，吴海莲，等. 不完美反馈下基于立即可解网络编码的多播重传机制 [J]. 系统工程与电子技术，2021，43 (12)：3703 - 3708.

[19] 韦修喜，黄华娟. 一种基于 Newton-Armijo 优化的多项式光滑孪生支持向量机 [J]. 陕西师范大学学报 (自然科学版)，2021，49 (1)：44 - 51.

[20] 楼旭阳，张智豪. 饱和输入下一类多项式系统的数据驱动控制 [J]. 大连理工大学学报，2023，63 (1)：102 - 110.

[21] 仝　军，田洪生，吴翠红. 考虑节点能量特征的无线传感数据加密传输方法 [J]. 传感技术学报，2022，35 (9)：1277 - 1281.

[22] 段晓聪. 基于无线传感网络分簇策略的分布式数据库加密存储研究 [J]. 传感技术学报，2022，35 (12)：1728 - 1732.

[23] 周洪波，尹文双，刘静漪，等. 基于变参超混沌与可逆向量积的图像加密算法 [J]. 重庆师范大学学报 (自然科学版)，2021，38 (5)：90 - 97.

[24] 谭　云，张春虎，秦姣华，等. 基于指数复合型混沌系统的图像加密算法 [J]. 华中科技大学学报 (自然科学版)，2021，49 (2)：121 - 126.

(上接第 78 页)

[21] 高　倩，潘　杨，朱　磊，等. 基于 SIOU 函数的改进 YOLOv5 遥感目标检测方法 [J]. 长江信息通信，2022，35 (11)：5 - 8.

[22] DU S，ZHANG B，ZHANG P，et al. An improved bounding box regression loss function based on CIOU loss for multi-scale object detection [C] //2021 IEEE 2nd International Conference on Pattern Recognition and Machine Learning (PRML). IEEE，2021：92 - 98.

[23] GEVORGYAN Z. SIoU loss：More powerful learning for bounding box regression [J]. arXiv preprint arXiv：2205.12740，2022：326 - 330.

[24] QUARANTA L，CALEFATO F，LANUBILE F. KGTorrent：A dataset of python Jupyter notebooks from kaggle [C] //2021 IEEE/ACM 18th International Conference on Mining Software Repositories (MSR). IEEE，2021：550 - 554.

[25] FANG H S，SUN J，WANG R，et al. Instaboost：Boosting instance segmentation via probability map guided copy-pasting [C] //Proceedings of the IEEE/CVF International Conference on Computer Vision. 2019：682 - 691.

[26] 郑楚伟，林　辉. 基于 Swin Transformer 的 YOLOv5 安全帽佩戴检测方法 [J]. 计算机测量与控制，2023，31 (3)：15 - 21.

[27] 祁泽政，徐银霞. 改进 YOLOv5s 算法的安全帽佩戴检测研究 [J/OL]. 计算机工程与应用：1 - 10 [2023-05-20]. http：//kns.cnki.net/kcms/detail/11.2127.TP.20230424.1513.022.html.