引文格式：祁琼,段志强,吕婧.等. 一种基于混沌系统的国土调查数据加密算法[J]. 地理空间信息, 2025, 23(10):15-19. doi:10. 3969/j.issn. 1672-4623.2025.10.004

一种基于混沌系统的国土调查数据加密算法

祁　琼[1]，段志强[1]，吕　婧[1]，张　斌[2*]
（1. 湖北省空间规划研究院，湖北 武汉 430071；2. 武汉大学资源与环境科学学院，湖北 武汉 430079）

摘　要：国土调查数据具有重要价值，其安全保障至关重要。然而，现有地理信息数据安全技术往往普适性强，未能充分结合国土调查数据的独有特征，导致直接应用时存在安全防护不足和效率低下的问题。为此，深入研究国土调查数据的加密实现技术，并提出一种新的国土调查数据加密算法。针对国土调查数据的属性特征，设计了字段粒度的变密钥加密算法，有效避免数据统计特征的泄露。针对国土调查数据的空间特征，设计了基于混沌系统的区域置乱加密算法，在保证地理空间稳定性的前提下，可与访问控制模型良好集成，实现对国土调查数据的有效加密。实验分析表明，提出的加密算法具有良好的安全性和效率，尤其适用于移动端应用环境。

关键词：国土调查数据；空间数据处理；数据加密
中图分类号：P208　　**文献标志码：**B　　**文章编号：**1672-4623（2025）10-0015-05

Data Encryption Algorithm for Territory Survey Data Based on the Chaotic System

QI Qiong[1], DUAN Zhiqiang[1], LYU Jing[1], ZHANG Bin[2]
(1. Hubei Spatial Planning Institute, Wuhan 430071, China;
2. School of Resource and Environmental Sciences, Wuhan University, Wuhan 430079, China)

Abstract: Territory survey data holds significant value, and ensuring its security is crucial. However, the existing geographical information data security techniques are often general-purpose and do not fully account for the unique characteristics of territory survey data, leading to inadequate security protection and low efficiency when directly applied. To address this problem, we delved into the encryption implementation technology for territory survey data and proposed a new encryption algorithm. For the attribute features of territory survey data, we designed a variable-key encryption algorithm with field-level granularity, effectively preventing the leakage of statistical data features. For the spatial features, we designed a region scrambling encryption algorithm based on chaotic system, which could be well integrated with the access control model under the premise of ensuring geospatial stability, to achieve effective encryption of territory survey data. Experimental analysis shows that the proposed encryption algorithm offers good security and efficiency, and is particularly suitable for mobile application environment.

Key words: territory survey data, spatial data processing, data encryption

国土调查数据是制定社会发展规划的重要依据，是推进国家治理体系和治理能力现代化的数据基础，其安全性直接关系到国家数据主权与信息安全。面对当前数据传输与应用中的安全挑战，尤其是矢量地理空间数据具有的坐标特征显著、局部访问需求频繁等特点，传统加密算法在安全性与可用性平衡方面仍存在不足。近年来，混沌系统因能够生成具有初值敏感、非周期、类随机及宽频带等优良特性的伪随机序列，已成为地理空间数据加密研究的重要方向[1-3]。该类系统通过混沌映射产生的密钥流具备高复杂度和难以预测的特性，可有效应用于空间数据的置乱加密，在保持数据组织结构的同时破坏空间相关性，显著增强数据保密性[4-7]。本文聚焦于混沌系统在国土调查数据加密中的深化应用，通过构建抗退化的混沌信号生成机制，提升加密密钥的随机性与稳定性，为实现安全、可控、高效的国土数据安全管理提供理论支持与技术路径。

1　国土调查数据结构特征

国土调查的成果包括：数据成果、图件成果、文字成果和数据库成果[8-9]。数据成果包括土地分类、土地权属、耕地坡度分级、耕地细化调查、耕地质量等要素图层数据。图件数据基于数据成果生产，包括土地利用现状，地权权属，国土调查图集等地图数据。

第一作者简介：祁琼（1983—），硕士研究生，高级工程师，主要从事自然资源调查监测、地理信息系统及遥感应用工作，E-mail：123167296@qq.com。
通信作者：张斌（1997—），硕士研究生，主要从事地图制图和GIS方面的工作，E-mail：1204588387@qq.com。

文字成果是各种调查、技术、分析报告。数据库成果是以上几种成果的集成，包括国家、省、市、县4级土地利用和专项调查数据库。

在国土调查的成果中，数据库成果中包含了数据成果、图件成果和文字成果，是其他内容的集成。国土调查构建的数据库是四级数据库，分别是国家级、省级、地市级、县级，其中县级行政辖区是进行国土调查的基本单位，也是进行国土调查数据库构建的基本单位。土地利用数据库标准（以下简称标准）明确了国土调查中数据的规范，规定了土地利用数据库的内容、要素分类代码、空间要素分层、要素属性结构、数据交换格式和元数据等[10-11]。

数据库中的空间要素根据要素类型进行分层组织，每一个空间要素图层代表一种空间要素类型。要素图层包含明确的属性结构，表1以地类图斑图层为例，记录了空间要素的属性结构描述表，在对相应的要素图层建立属性表时，需要以属性结构描述表中的字段为标准。

表1 空间要素属性结构描述表
（以地类图斑属性结构描述表为例）

序号	字段名称	字段代码	字段类型	字段长度	约束条件	备注
1	标识码	BSM	Int	10	M	
2	要素代码	YSDM	Char	10	M	
3	图斑预编号	TBYBH	Char	8	O	
4	图斑编号	TBBH	Char	8	M	
5	地类编码	DLBM	Char	4	M	
6	土地分类编码	TDFLBM	Char	4	C	
7	地类名称	DLMC	Char	60	M	
8	权属性质	QSXZ	Char	3	M	
9	权属单位代码	QSDWDM	Char	19	M	
10	权属单位名称	QSDWMC	Char	60	M	
11	坐落单位代码	ZLDWDM	Char	19	M	
12	图斑面积	TBMJ	Float	12	M	单位:m^2
13	扣除地类编码	KCDLBM	Char	13	M	
14	扣除地类系数	KCXS	Float	14	O	
15	扣除地类面积	KCMJ	Float	15	O	单位:m^2
16	图斑地类面积	TBDLMJ	Float	16	O	单位:m^2
17	耕地类型	GDLX	Char	17	M	
18	耕地坡度级别	GDPDJB	Char	18	C	
19	线性图斑宽度	XXTBKD	Float	19	C	
20	图斑细化代码	TBXHDM	Char	20	C	
21	图斑细化名称	TBXHMC	Char	21	C	
22	耕地种植属性代码	GDZZSXDM	Char	22	C	
23	耕地种植属性名称	GDZZSXMC	Char	23	C	
24	耕地等别	GDDB	Int	2	C	
25	飞入地标识	FRDBS	Char	1	C	
26	城镇村属性码	CZCSXM	Char	4	C	
27	数据年份	SJNF	Int	4	M	

属性结构描述表中的字段需要规范字段值，表2以地类图斑属性描述表中的“耕地种植属性代码”字段为例，列出了该字段的属性值代码表。对具体字段的取值范围和代码表示进行统一的规范，在进行内外业调查时，字段取值必须在属性值代码表中选择，增强了数据的规范性。

表2 属性值代码表（以耕地种植属性表为例）

代码	耕地实际种植情况
GZ	耕种
WG	未耕种
XG	休耕
YM	园木
LM	林木
LH	绿化草地
MC	牧草
KT	坑塘

国土调查数据是国土调查成果的重要体现，是后续数据共享与分析平台建立的基础[12]。分析国土调查数据的特征能够为国土调查数据加密算法和访问控制的设计提供思路。国土调查数据包含以下特征：

1）数据量大：国土调查需要政府各部门广泛参与，工作任务多且对于调查时所使用的技术要求高，需要各有关部门在国家的统一领导、各方分工协作，耗时几年才能完成。所以国土调查产生的成果的数据量很大，一方面体现在总体的数据量大，包含数据、图件、文字、数据库等多方面的成果；另一方面体现在单个要素图层所承载的数据量也很大。针对如此大的数据量，在进行加密设计时，既要考虑到加密算法的安全性，又要考虑到效率的问题。

2）数据规范：为了规范国土调查过程中数据采集的工作，土地利用数据库中对空间要素分层、要素属性结构、属性值代码有明确的定义。相关的工作人员在外业或者内业中进行图斑调查时，必须按照标准中的规定输入图斑要素的性质，这是保证调查数据统计以及汇交的基础。这种规范性使得调查结果更加科学，对数据的使用也能更加高效。但是这种规范性也使得对要素属性信息进行加密时，如果对相同的属性值使用相同的密钥加密，密文也会是一样的。如果破译者破译了其中一个字段的密文，即可以立即破译其他相同的密文。即使不知道密钥，不对密文进行解密，也能通过分析密文的概率分布而求得原文。所以针对这一特征，在设计加密算法时要避免使用常密钥加密。

3）使用场景复杂：国土调查需要对全国范围内的每一块土地的各类性质等进行详尽的调查。一方面

需要克服地形地势复杂区域调查难度大的问题，另一方面需要克服野外环境网络条件差和移动端设备性能差的问题，在对国土调查数据采集、传输、使用等全过程中，都面临着以上提出的问题。所以在设计国土调查数据在移动端设备上的访问平台时，需要考虑复杂的外在条件。设计保护方法要保证在网络条件差、设备性能弱的情况下的安全访问。

2　混沌系统算法原理

混沌现象是在非线性动力系统中出现的确定性的、类似随机的过程，这种过程既非周期又不收敛，并且对初始值非常敏感。任何微小的初始值偏差都会随着迭代产生指数级别放大，所以混沌系统具有自然的伪随机特征。由于混沌系统的特征，产生的混沌序列可以作为加密的密钥流。混沌系统的非线性、伪随机性等特征大大提高了密钥序列的复杂性，使得加密密钥被破解的可能性很大程度降低[13]。

混沌序列可以通过差分方程的迭代运算产生，但是由于实际计算中存在有效精度效应，双精度实数的有效数字的位数是有限的，迭代方程产生的混沌序列在经过有限次迭代后会进入周期态，而实际生成的序列的密码特性和周期也难以度量。在字节长为N的计算机中，迭代方程最多经过2^N的迭代后，混沌序列必将进入周期态。用这样的混沌序列作为密钥流加密数据量大的矢量数据会有很严重的安全隐患[5]。

根据混沌系统维度的不同，可以分为一维混沌系统和高维混沌系统，虽然高维混沌系统具有更高的稳定性，但是考虑移动设备性能的限制，一维混沌系统能够输出稳定随机序列的同时，具有更快的速度和更高的效率。Logistic映射是一类简单却应用广泛的非线性离散混沌动力系统，定义为：

$$X_{k+1}=\mu X_k(1-X_k) \tag{1}$$

式中，μ为Logistic参数，$\mu\in[0,4]$，$X_k\in(0,1)$。当3.569 945…$<\mu\leqslant 4$时，可认为Logistic映射处于混沌态。即初始值X_0在Logistic映射的作用下产生的序列$\{X_0,X_1,X_2\ldots X_k\ldots\}$在理论上是非周期，不收敛的。同样由于有限精度效应，上式定义的迭代方程无法一直产生密钥流序列，因为其一定会退化为周期序列。当前计算机系统上双精度实数运算中的数值取值范围是10^{-308}~10^{308}。国土调查数据单个数据文件会大于百兆，在迭代过程中必须使Logistic参数μ随步长（根据待加密国土调查数据的大小计算）改变，在μ改变之后，混沌序列又从X_0开始迭代取值，通过这种方式才能保证混沌序列不会退化为周期序列[6]。由于Logistic映射等单一基于混沌系统的加密算法产生的序列周期比较短，较容易被穷举攻击所破坏，所以一般会对国土调查数据中，这种较大的矢量数据采取复合混沌系统加密。

利用MD5算法的特性，Logistic迭代初值的要求是$X_0\in(0,1)$，将不同形式的密钥散列成128位值，对该值进行运算生成16个值，作为有16位有效数字双精度实数的每一位，并将其作为Logistic映射的迭代初值。通过这种方式，在选取值和迭代初值之间增加了散列函数，增大了密钥强度，使选取的密钥可长可短，不局限于(0,1)区间，甚至可以是文件。

3　国土调查数据置乱加密算法

本文采用基于Logistic混沌系统的加密算法，对空间数据进行置乱加密，其算法思想为：每个空间要素由不同数量的坐标点组成，所以需要将一定范围内要素的所有点都进行矩阵化，同时使用混沌序列生成与坐标点集规模相同的矩阵，使用混沌序列生成的矩阵来加密要素点集矩阵。具体算法逻辑如下：

1）坐标点集的矩阵化。按照国土调查数据的组织规范，并结合访问控制中的设计，以乡镇行政区划为生成点集矩阵的基本单元，同一乡镇的要素图斑在一个矩阵中进行置乱。在进行要素点集矩阵建设之前，先使用行政区要素图层与需要加密的图层进行叠加分析，得到一个行政区域的所有要素。遍历所有的要素，将要素的坐标点信息存放到数组$P[i]$中，并记录每个要素坐标点的数量，将要素信息和坐标点的信息存入到数据表中，解密时需要使用。所有要素坐标点的总数量记为p，创建大小为$m\times n$的矩阵。

$$m=\lfloor\sqrt{p}\rfloor,\quad n=\lfloor p/m\rfloor \tag{2}$$

式中，$\lfloor\ \rfloor$为向下取整，将p个要素点存放到大小为$m\times n$的矩阵$\boldsymbol{N}$中。

2）混沌系统初值生成。Logistic混沌系统的迭代初值要求是$X_0\in(0,1)$，且至少要有6位有效数字，所以输入一个Logistic混沌映射的初值并不简单。使用SHA-1散列算法，可以将字符串、各种类型数值甚至是文件作为输入，而不必局限在（0，1）区间。增加散列函数的方式，既增大了密钥的强度，又使输入变得容易。SHA-1散列函数的公式为：

$$N=\mathrm{SHA}-1(S) \tag{3}$$

式中，$S=$'key' or file or number；$N=x_1,x_2,\ldots,x_{159}(0\leqslant x_i\leqslant 9,0\leqslant i\leqslant 159)$，$N$由160个数字组成，每个数字的

取值范围是0~9；S 为字符串、数字或者文件等类型数据。对生成的160个数字使用SHA-1算法得到14个数字，每个数字的取值范围为0~9。初始值 X_0 为 $0.n_1n_2n_3\ldots n_{14}$。

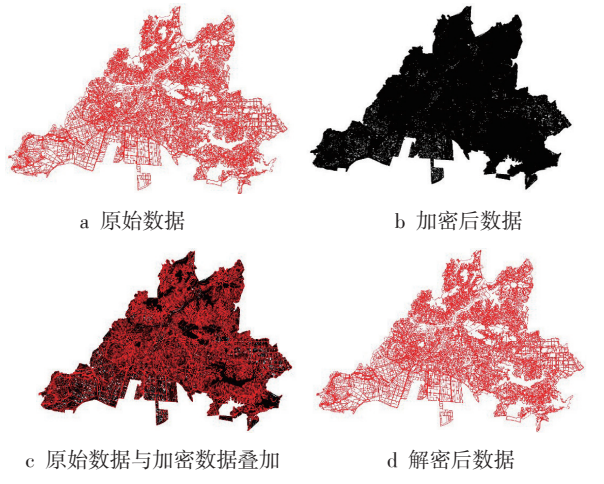
3）混沌序列的生成。2个Logistic混沌映射公式分别是 $X_{m+1}=\mu_1 X_m(1-X_m)$ 和 $Y_{n+1}=\mu_2 Y_n(1-Y_n)$，映射的初值取上文生成的 N，2个映射函数会生成2个 N。为了增加迭代输出的随机性，如果i mod2=0则通过混沌系统输出2个序列用于加密，这种方式同时增强了混沌系统的雪崩效应。在下一次迭代时交换2个映射函数的值。将 x_m 和 y_n 的取值记录到序列中，截取 x_m 的前 m 个值组成序列 $a=\{x_i|i=0,1,\ldots m-1\}$，截取 y_n 的前 n 个值组成序列 $b=\{y_j|j=0,1,\ldots n-1\}$。对混沌系统产生的序列 a 和 b 分别进行升序排列，得到序列 A 和序列 B 以及序列的索引序列 IA 和 IB，其中序列 IA 是序列 A 中元素在对应序列 x 中的索引形成的索引序列，序列 IB 与序列 B 的关系相同。

4）空间数据加密。生成要素点集的矩阵和混沌序列的矩阵之后，将对地理空间要素的加密转换为对要素点集矩阵的置乱。首先是对行置乱，根据索引序列 IA 中 $\{ix_i|i=0,1,\ldots m-1\}$，将要素点集矩阵 $\boldsymbol{N}$ 的第 i 行的所有点换成第 ix_i 行的所有点，得到中间矩阵 $\boldsymbol{N}_1$。然后对 $\boldsymbol{N}_1$ 进行列置乱，根据索引序列 IB 中 $\{iy_j|j=0,1,\ldots n-1\}$，将要素点集矩阵 $\boldsymbol{N}_1$ 中第 j 列的所有点置换为第 iy_j 列的点要素，置换完成之后得到全局置乱的要素矩阵 $\boldsymbol{N}_2$。然后根据前面记录的要素的个数和每个要素坐标点的数量，将矩阵中的点集再次写入到地理空间数据中，完成加密工作。

4 实验结果与分析

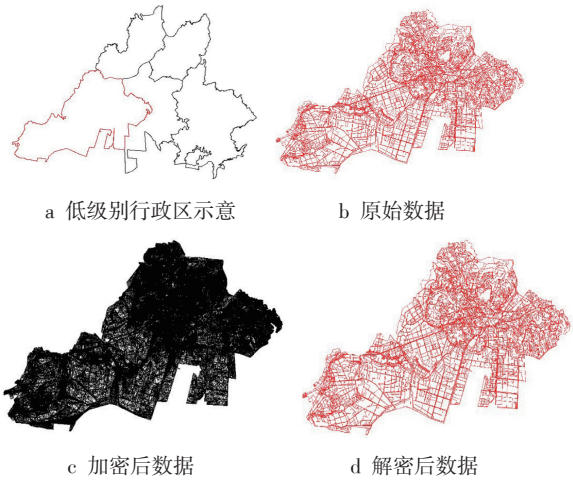
为验证本文提出的算法，选择某县级国土调查数据中地类图斑图层及其辖区乡镇开展加密与解密实验，并对解密后数据开展误差分析，相关算法使用Java语言开发。

图1为某县级行政区域数据加密与解密结果，从图1b和图1c可以看出，置乱是在图层的空间范围内进行的，置乱加密在完成加密的同时，不会改变数据的格式和数据的组织结构。对比图1a和图1d可以发现，加密和解密之后的数据一致。图2展示了图1所示区域低一个级别的行政区域，对比图2b和图2c可以看出，置乱是在局部区域内完成的，区域的加解密能够配合访问控制的工作，很好地与访问控制结合，保证用户在需要访问数据时，解密在一定的用户空间范围内进行，保证了加解密的效率，同时避免用户无权限的区域被解密而导致数据的泄漏。



a 原始数据　b 加密后数据　c 原始数据与加密数据叠加　d 解密后数据

图1 县级行政区域数据加密与解密效果



a 低级别行政区示意　b 原始数据　c 加密后数据　d 解密后数据

图2 低级别行政区域加密与解密效果

在加解密的过程中存在坐标信息与混沌系统生成的序列之间的运算操作，在运算过程中会产生精度的

表3 部分数据解密后坐标与原始坐标对比

原始X坐标	解密X坐标	误差	原始Y坐标	解密Y坐标	误差
37 606 890.802 3	37 606 890.802 3	0	3 555 026.313 3	3 555 026.313 3	0
37 606 904.790 9	37 606 904.790 9	0	3 554 809.066 9	3 554 809.066 9	0
37 606 885.936 2	37 606 885.936 2	0	3 555 025.823 4	3 555 025.823 4	0
37 606 885.758 7	37 606 885.758 7	0	3 555 025.465 1	3 555 025.465 1	0
37 606 890.802 3	37 606 890.802 3	0	3 555 026.313 3	3 555 026.313 3	0
37 606 895.856 7	37 606 895.856 7	0	3 555 032.368 3	3 555 032.368 3	0

损失，表3列出了数据中部分坐标点在解密前后的差异，从表中数据可以看出，本算法在计算机精度范围内对坐标精度的坐标误差为0，解密后的数据与原始数据相同，表明本算法能够保证数据的精度，不会破坏数据的可用性。

5 结　语

本文设计了针对国土调查数据的加密算法。考虑国土调查数据的特征，分别对属性数据和空间数据设计加密算法。针对属性数据单一字段下属性值有较高重复率、国土调查数据的属性信息具有较高统计价值的特点，设计了基于AES算法的敏感字段变密钥加密算法。采取变密钥的加密算法，一次一密，保证无法通过密文的统计特征破解密文。设计的加密算法简单高效，实验结果表明该算法非常适合运算能力较弱的移动设备。针对国土调查数据具有行政区域的特点并结合访问控制的需求，设计基于混沌系统的空间数据置乱加密算法。该算法以行政区划为边界，对坐标信息的置乱加密在一定的行政边界内进行，能够配合访问控制时权限分配的要求，同时混沌系统具有非线性和伪随机性，能够保证密文的安全性。

参考文献

[1] 闵连权.矢量地图数据的加密算法[J]. 海洋测绘,2005,24(2):55-57

[2] 李安波,王海荣,周卫. 基于二维混沌系统的矢量数字地图置乱加密[J]. 中国矿业大学学报,2015,44(4):747-753

[3] Wu F,Cui W,Chen H. A Compound Chaos-based Encryption Algorithm for Vector Geographic Data Under Network Circumstance[C]//IEEE,2008

[4] 李孟婷,赵泽茂. 一种新的混沌伪随机序列生成方法[J]. 计算机应用研究,2011,28(1):341-344

[5] 张翰林,王青山,邹永初. 复合混沌系统的矢量数据加密研究[J].测绘科学,2012,37(5):87-89

[6] 钟尚平,高庆狮. 网络环境下地图的混沌加密实用算法[J]. 计算机辅助设计与图形学学报,2004,15(2):238-242

[7] 王相生,甘骏人. 一种基于混沌的序列密码生成方法[J].计算机学报,2002,24(4):351-356

[8] 国务院第三次全国土地调查领导小组办公室.第三次全国国土调查总体方案[Z].

[9] 祁琼,张莉,裴利利,等. 一种基于RBAC的国土调查数据访问控制模型[J]. 地理空间信息,2025,23(1):17-20

[10] 国务院第三次全国土地调查领导小组办公室. 土地利用数据库标准(试行)[S].

[11] 翟兴华,邓少平. 三调成果的建设用地审查报批地类认定关键方法研究[J]. 地理空间信息,2024,22(6):84-88

[12] 赖权有,唐欣. 面向国土空间规划需求的国土调查优化研究[J]. 自然资源情报,2023,23(12):19-25

[13] Kelber, Kristina, Schwarz, et al. General Design Rules for Chaos-based Encryption Systems[C]//International Symposium on Nonliner Theory and Its Applications,2005

（上接第9页）

多尺度云检测[J]. 地理空间信息,2024,22(7):54-58

[8] 乔志勇. 基于改进DeepLabV3+的高分辨率遥感影像建筑物提取[J]. 地理空间信息,2024,22(12):69-73

[9] Zhang Y. Optimisation of Building Detection in Satellite Images by Combining Multispectral Dlassification and Texture Filtering[J]. SPRS Journal of Photogrammetry & Remote Sensing, 1999, 54(1): 50-60

[10] Chen D, Shang S, Wu C. Shadow-based Building Detection and Segmentation in High-resolution Remote Sensing Image[J]. Journal of Multimedia,2014,9(1):181-188

[11] 柳杨,赵泉华,李玉,等. 融合注意力的轻量级遥感影像村落提取方法[J]. 测绘科学,2023,48(6):161-171

[12] Renxi C, Xinhui L, Jonathan L. Object-based Features for House Detection from RGB High-resolution Images[J]. Remote Sensing,2018,10(3):451

[13] 张合欣,张赫雷. 基于U-Net与Model Builder的建筑物属性信息提取方法[J]. 地理空间信息,2024,22(12):98-101

[14] Senaras C, Ozay M, Yarman V F T. Building Detection With Decision Fusion[J]. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing,2013,6(3):1 295-1 304

[15] 杨桢,段雨昕,李鑫,等. 基于2D-SPWVD与PCA-SSA-RF的超宽带雷达人体跌落动作辨识方法[J]. 电子测量与仪器学报,2024,38(10):147-158

[16] 张立志,王冬雪,陈永超,等. 基于GMRF和KNN算法的人脸表情识别[J]. 计算机应用与软件,2020,37(10):214-219

[17] Hinton G E, Osindero S, Teh Y W. A Fast Learning Algorithm for Deep Belief Nets[J]. Neural Computation, 2006, 18(7):1 527-1 554

[18] 王顺,陈小月,林中杰,等. 运用U-Net++模型的遥感影像多尺度云检测[J]. 地理空间信息,2024,22(7):54-58