引文格式:张明旺,张黎明,闫浩文,等.面向OpenDRIVE格式高精地图的DNA动态加密算法[J].武汉大学学报(信息科学版),2026,51(6):1263-1272.DOI:10.13203/j.whugis20240304

Citation: ZHANG Mingwang, ZHANG Liming, YAN Haowen, et al. A DNA Dynamic Encryption Algorithm for High-Definition Maps of OpenDRIVE[J]. Geomatics and Information Science of Wuhan University, 2026, 51(6):1263-1272.DOI:10.13203/j.whugis20240304

面向OpenDRIVE格式高精地图的DNA动态加密算法

张明旺[1,2,3] 张黎明[1,2,3] 闫浩文[1,2,3] 谭 涛[1,2,3] 汪 磊[1,2,3] 刘帅康[1,2,3]

1 兰州交通大学测绘与地理信息学院,甘肃 兰州,730070

2 地理国情监测技术应用国家地方联合工程研究中心,甘肃 兰州,730070

3 甘肃省测绘科学与技术重点实验室,甘肃 兰州,730070

摘 要:针对高精地图在存储、传输中的安全问题,基于脱氧核糖核酸(deoxyribonucleic acid, DNA)编码,提出了一种面向OpenDRIVE格式高精地图的动态加密算法,该算法包括置乱和扩散两部分。首先,应用混沌系统产生随机序列,通过该序列将DNA碱基组合与高精地图中的参数化三次曲线建立映射,再应用碱基互补规则对曲线参数进行置乱;然后,扩散曲线参数,通过对DNA碱基编码,由随机序列建立各曲线与编码方案的映射,并对曲线参数进行二进制下的碱基编码;最后,按照映射的编码方案进行DNA加法运算,将运算结果转化为十进制得到密文数据。实验结果验证了所提算法可以实现选择性加解密,平均加密效率为2.654 MB/s,平均解密效率为2.588 9 MB/s。加密算法的信息熵随数据量增大而增大,实验数据的最大信息熵达到29 101,且能抵抗裁剪攻击,可用于智能网联汽车高精地图的安全存储和传输。

关键词:高精地图;OpenDRIVE;DNA动态加密;选择性解密

中图分类号:P208 **文献标识码**:A **收稿日期**:2025-05-29

DOI:10.13203/j.whugis20240304 **文章编号**:1671-8860(2026)06-1263-10

A DNA Dynamic Encryption Algorithm for High-Definition Maps of OpenDRIVE

ZHANG Mingwang[1,2,3] *ZHANG Liming*[1,2,3] *YAN Haowen*[1,2,3] *TAN Tao*[1,2,3]
WANG Lei[1,2,3] *LIU Shuaikang*[1,2,3]

1 Faculty of Geomatics, Lanzhou Jiaotong University, Lanzhou 730070, China

2 National-Local Joint Engineering Research Center of Technologies and Applications for National Geographic State Monitoring, Lanzhou 730070, China

3 Gansu Province Key Laboratory of Science and Technology in Surveying & Mapping, Lanzhou 730070, China

Abstract: **Objectives**: High-definition (HD) maps are essential infrastructure for autonomous driving, characterized by high collection costs, significant economic value, and containing a substantial amount of sensitive geographic and road information. Ensuring their security and privacy protection has become an urgent priority. As the foundation of data security, encryption technology can provide the technical support necessary for the secure storage and transmission of HD maps. To address the security protection issues of HD maps during storage and transmission, a dynamic encryption algorithm for high-definition maps in OpenDRIVE format was proposed based on the data characteristics of HD maps and deoxyribonucleic acid (DNA) dynamic coding. **Methods**: The algorithm consists of two main components: scrambling and diffusion. During the scrambling process, a random sequence is first generated using the SHA-512 hash algo-

基金项目:国家自然科学基金(42271430,41761080);甘肃省高等学校科研项目(2026CYZC-036);甘肃省知识产权计划项目(25ZSC-QG042)。

第一作者:张明旺,博士生,研究方向为地理信息安全。18809366269@163.com

通信作者:张黎明,博士,教授。zlm@lzjtu.edu.cn

rithm in conjunction with a two-dimensional chaotic system. Next, the parameterized cubic curves representing elevation, superelevation, and lanes in the HD map are mapped to corresponding base combinations using this random sequence. The parameters within the curves are then scrambled according to the principle of base complementarity. In the diffusion operation, the DNA bases are first encoded, and a stable index relationship between each curve and the encoding scheme is established through a random sequence. Second, the parameters of the curve are base-encoded in binary. Third, the DNA addition operation is performed according to the index encoding scheme. Finally, the operation result is converted into decimal to obtain the ciphertext data. **Results**: The experiment demonstrates that the algorithm provides high security, with a large key space and strong key sensitivity. The encryption algorithm demonstrates effective performance, enabling selective encryption and decryption. Additionally, in the event of cropping attacks on the HD map, the unaffected portions of the data can still be successfully decrypted. **Conclusions**: The algorithm is suitable for the secure storage and transmission of HD maps in intelligent connected vehicles. Its selective encryption and decryption capabilities make it adaptable to various application scenarios, offering strong practicality.

Key words: HD map; OpenDRIVE; DNA dynamic encryption; selective decryption

随着智能交通和自动驾驶技术的快速发展,高精地图逐渐成为智能网联汽车关键组成部分[1]。高精地图不仅有传统地图的基本地理信息,还包含了更加详细且精确的道路数据、交通标志、道路曲率、坡度等信息[2]。详细且高精度的数据使得自动驾驶车辆能够更准确地感知周围环境,实现更安全高效的路径规划和驾驶决策[3]。然而,随着高精地图在智能交通和自动驾驶中的应用,一系列复杂的安全问题随之而来[4]。高精地图中包含大量敏感信息,如道路基础设施布局和交通信息,若被不法分子利用,可能对公共安全和个人隐私构成威胁[5]。因此,研究用于高精地图安全的加密算法,保护数据免受未经授权的访问或篡改,具有重要的现实意义和紧迫性。

目前,加密是数据安全保护的主流方式之一,可以为高精地图存储、传输提供安全保护,防止数据被非法获取和篡改。OpenDRIVE是目前国际上广泛使用的高精地图标准格式之一,包含了自动驾驶所需的静态道路交通网络[6-7]。此类数据以可扩展标记语言(extensible markup language, XML)进行存储,扩展名为xodr。因此,针对OpenDRIVE格式的高精地图加密算法研究,必须考虑其数据文件的存储特征。

现有的加密算法可以分为经典密码体制[8-12]、频率域[13-15]和空间域[16-18]3类。基于经典密码体制的加密算法可以分为对称加密和非对称加密。其中,对称加密技术包括数据加密标准[9]和高级加密标准[10]等,非对称加密技术包括李维斯特-沙米尔-阿德曼加密算法[11]和Paillier[12]等。这些经典加密算法的安全性高,应用广泛,但在加密时需要将整个数据进行二进制加密,存在加密效率低、可用性差等问题。此外,这些经典加密算法的加密方式会破坏高精地图的原始结构和属性特征,并不适用于OpenDRIVE格式的高精地图。基于频率域的加密算法相较于经典加密算法具有更高的加密效率,且不破坏数据本身的结构和特征。文献[14]对矢量地图进行Haar小波变换,先对变换后的系数进行加密,再进行逆变换得到加密后的矢量地图;文献[15]先对矢量地图的折线和多边形数据进行离散余弦变换,再在离散余弦变换域中进行加密。OpenDRIVE格式的高精地图数据以XML文件存储,包含大量的节点和属性,这些信息在时域中表现为高度结构化和层次化的数据,而频率域加密算法通常更适合处理图像和音频等均匀连续的数据。直接将频率域算法应用于这种复杂的结构化数据可能会导致效率低下和加密不完全,甚至会导致高精地图中某些关键信息的丢失或误解。因此,此类加密算法也不适用于OpenDRIVE格式的高精地图。基于空间域的加密算法可以通过改变数据的原始值来达到加密的效果。文献[17]对矢量数据进行极坐标转换,并通过流密码对极坐标的数值进行加密。此外,空间域的加密算法还可以改变数据的物理位置达到加密效果,文献[18]通过混沌系统对矢量地图中坐标的存储顺序进行置换加密。高精地图通常需要保持极高的数据精度和完整性,以确保其在自动驾驶等应用中的准确性。空间域的加密方案能够维持数据的完整性,且具备较高的加密效率,适用

于高精地图加密算法设计。

近年来,由于脱氧核糖核酸(deoxyribonucleic acid, DNA)分子的高信息存储密度和复杂的组合特性,DNA 编码逐渐成为信息加密领域的重要研究方向[19]。如动态编码[20]、DNA 序列混沌映射[21]等。这些方法在加密强度和抗攻击性方面具有明显优势,尤其在处理大数据加密时表现出较高的效率[22]。

综上所述,空间域加密算法能够有效保持数据的结构与精度,维护数据完整性,同时具备较高的安全性、可逆性、计算效率及兼容性,适用于高精地图的加密需求。针对高精地图的安全保护难题,本文以 DNA 碱基互补配对与动态编码为基础,结合 OpenDRIVE 格式高精地图的数据特征,提出了一种动态加密算法。

1　基于 DNA 动态编码的加密算法

1.1　算法思想

OpenDRIVE 格式的高精地图数据是一种基于 XML 的结构化文本文件,通过大量的节点与属性来描述道路、交叉口及交通标志等复杂的路网信息。该格式采用模块化结构,对道路、车道、几何形状以及信号标志等路网要素进行分类表达。在 OpenDRIVE 标准中,高程、超高和车道宽度等信息的数学描述方式基本一致。具体而言,高程信息描述道路的纵向高度变化,超高信息描述模拟弯道的横向倾斜度变化,这两者均包含起点距离 S 以及参数化三次曲线的 4 个系数 a、b、c、d。此外,车道模块中的宽度信息也采用了相同的表达逻辑,包含起始偏移距离 S_{Offset} 及上述 4 个曲线系数。为避免对整个文件进行加密从而影响数据的可用性,可对这些显著的数据特征进行加密,在保证数据完整性和可用性的同时提高加密效率。

在现代密码学中,置乱机制可以防止攻击者利用统计分析或简单数学模型破解密文,而扩散机制则用于掩盖密文中可能保留的明文模式与结构。因此,本文通过 DNA 动态编码将置乱和扩散原则相结合,在保证安全性的同时实现了选择性加解密和抗裁剪攻击。

1.2　DNA 的编码与解码

相较于采用固定密钥与算法的传统静态加密,动态加密技术通过在加密过程中动态更新密钥、算法或相关参数来保障数据安全。DNA 动态编码正是利用多种编码规则的切换来实现这一效果,其加密过程涵盖了密钥与算法的双重动态变换。

DNA 包含腺嘌呤(adenine, A)、胸腺嘧啶(thymine, T)、胞嘧啶(cytosine, C)和鸟嘌呤(guanine, G)4 种碱基,且严格遵循 A-T 与 C-G 的互补配对原则。由于这 4 种碱基在信息承载机制上与计算机二进制数据类似的特性,因此可通过特定的映射规则实现二进制信息向 DNA 序列的转换。一种典型的映射方式是将每两位二进制数映射为单一 DNA 碱基。例如,将 00、01、10、11 分别映射为 A、C、G、T。根据此映射规则,DNA 碱基可以有 8 种有效编码方案,编码规则如表 1 所示。

表 1　DNA 的编码方案

Table 1　DNA Coding Scheme

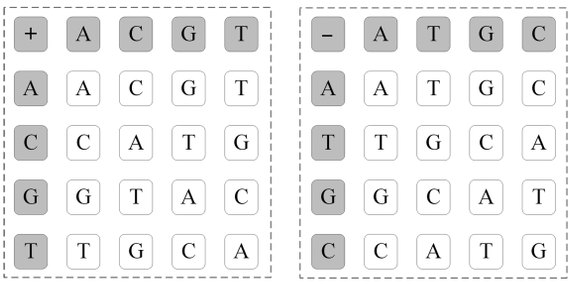
方案	00	01	10	11
1	A	C	G	T
2	A	G	C	T
3	C	A	T	G
4	C	T	A	G
5	G	A	T	C
6	G	T	A	C
7	T	G	C	A
8	T	C	G	A

通过这种映射编码,可以将 DNA 序列转化为二进制数据,从而能够在 DNA 碱基上执行类似于二进制加法和减法的操作。该操作可以理解为将两个 DNA 序列进行逐碱基相加或相减。以 A(00)和 C(01)为例,A+C=00+01=01=C,C−A=01−00=01=C。在加法和减法中,进位和借位是关键的操作。DNA 加法中的进位类似于传统的二进制加法,当两位相加超过“1”时产生进位。减法中的借位则与二进制借位规则类似,当无法直接减去时,需要向高位借位。

以表 1 中的编码方案 1 为例,将 A(00)、C(01)、G(10)、T(11)基于二进制进行加减运算可以获得 8 种不同的 DNA 编码,对应的加法和减法运算规则如图 1 所示。

1.3　高精地图加密

基于 DNA 动态编码的高精地图加密过程分为置乱和扩散两部分。在置乱部分,首先利用 4 种 DNA 碱基 A、T、C、G 的全排列生成 24 种组合方式;随后,引入混沌系统生成的随机序列,将高程、超高及车道宽度等节点中参数化三次曲线的参数 a、b、c、d 动态映射至上述 24 种碱基组合之一,并结合碱基互补原则实现参数的空间。在扩



(a) 加法 (b) 减法

图1 DNA编码的加法和减法运算规则

Fig. 1 Rules for DNA Addition and Subtraction Operations

散部分,首先,确定DNA碱基编码规则,利用随机序列为每条曲线建立与特定编码方案的索引关系;其次,将曲线参数转换为二进制形式并进行DNA编码;然后,根据索引指向的编码方案执行DNA加法运算;最后,将运算结果逆转换为十进制数值,生成最终的高精地图密文。

1)对DNA碱基进行排列组合,一共有24种组合,记为P。

2)使用高精地图数据的相关信息,采用SHA-512散列算法生成512 bit的散列值,并进行0和1的二值化。以8个为一组,划分成64组并进行十进制转换。

3)将64个十进制数与它们的均值进行比较,若大于均值,则设为1,否则设为0,得到64位0和1的序列,并均分为8组,记为$K_i=\{K_1,K_2,\cdots,K_8\}$。

4)计算二维Henon-Sine映射的密钥(x_0,y_0,μ,δ),计算式为:

$$\begin{cases} x_0=(\text{bin2dec}(K_1\oplus K_2)/256)\times(-1)^{k_1} \\ y_0=(\text{bin2dec}(K_3\oplus K_4)/256)\times(-1)^{k_2} \\ \mu=(\text{bin2dec}(K_5\oplus K_6)/256)\times(-1)^{k_3} \\ \delta=(\text{bin2dec}(K_7\oplus K_8)/256)\times(-1)^{k_4} \end{cases} \tag{1}$$

式中,$k_1\sim k_4$是用于控制密钥正负的随机整数;bin2dec( )是二进制转换十进制的函数;x_0、y_0为二维Henon-Sine映射的迭代初始值;μ、δ为二维Henon-Sine映射的超参数。

5)使用二维Henon-Sine映射生成两个随机序列A和B。二维Henon-Sine映射的定义如下:

$$\begin{cases} x_{i+1}=\text{mod}((1-\mu\sin^2 x_i+y_i),1) \\ y_{i+1}=\text{mod}(\delta x_i,1) \end{cases} \tag{2}$$

式中,x_i、y_i为迭代值,其取值范围都是$(-\infty,+\infty)$,初始值为x_0、y_0;mod( )为求余函数。

6)使用随机序列A作为控制参数,建立每一条参数三次曲线与碱基组合的索引,计算式为:

$$I=\text{mod}(\text{int}(S\times l_i\times 10^k),24) \tag{3}$$

式中,I为曲线与碱基组合之间的索引;int为取整函数;l_i为随机序列A中的随机数;k为放大参数;S为高程、超高的起始距离,在用于车道段时,表示其起始偏移距离。

7)确定每条曲线与碱基组合P的对应关系后,按照DNA碱基互补配对原则确定其互补链,如一条参数三次曲线中4个参数a、b、c、d对应的碱基组合为A、G、C、T,那么它的互补链为T、C、G、A,按此排列方式进行置乱。

8)对曲线中4个参数进行二进制转换,转换标准为IEEE754,由符号位(1位)、指数位(11位)和小数位(52位)组成。通过随机序列B计算每个节点采用的编码方案的公式为:

$$I'=\text{mod}(n\times l_i'\times 10^k,8) \tag{4}$$

式中,I'为编码方案;l_i'为随机序列B中的随机数;n为每个节点下曲线的数量。

9)每个节点下的加密密钥K_p'的计算式为:

$$K_p'=K_p'[\text{mod}(n^2,460),\text{mod}(n^2,460)+52] \tag{5}$$

式中,K_p为SHA-512散列算法生成的512 bit 0和1的集合。

10)将参数a、b、c、d进行二进制转换,并根据表1中的编码方案对4个参数的小数位和当前节点的加密密钥K_p'进行编码,并按照表2对编码后的小数位和K_p'进行加法运算。以方案1为例,二进制0010110111110010经过编码后为AGTCTTAG。

11)根据表1中的编码方案对加密结果进行解码,得到解密后的小数位,经过十进制转换后得到加密后的高精地图。

上述加密过程如图2所示,其中置乱操作过程与扩散操作过程顺序可以进行交换,不存在先后顺序。

1.4 高精地图解密

高精地图的解密过程是加密的逆过程,高精地图的解密流程如图3所示。(1)通过SHA-512散列算法生成相同的密钥。再通过二维Henon-Sine映射生成相同的随机序列A和B;(2)先使用随机序列A确定每一条参数化三次曲线所对应的碱基组合,然后根据碱基推导出它对应的互补碱基,最后按互补碱基的排列方式对参数三次曲线中4个参数a、b、c、d进行解密并替换;(3)通过式(4)、式(5)确定每个节点的编码方案和加密

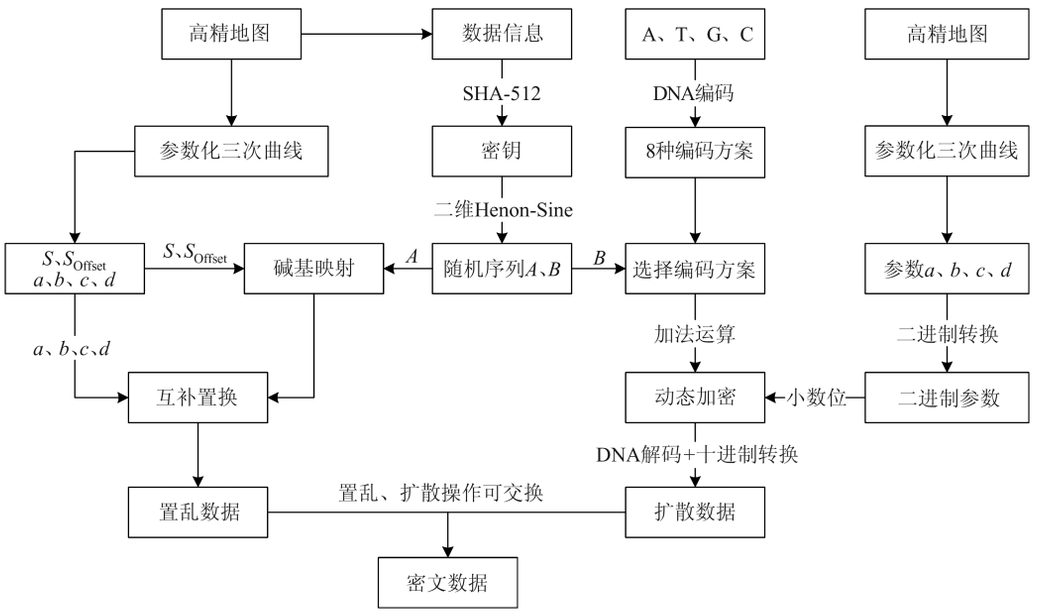


图 2　高精地图加密过程

Fig. 2　Encryption Process of HD Map

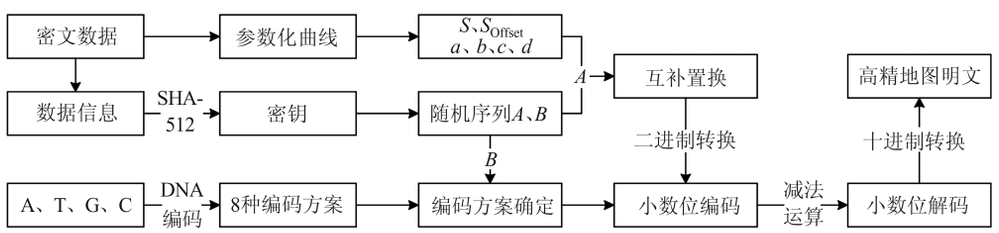


图 3　高精地图解密过程

Fig. 3　Decryption Process of HD Map

密钥,并对曲线中的参数进行二进制转换;(4)对参数的二进制小数位和对应的加密密钥进行编码,按照图 1 中的规则进行减法运算,得到解码后的小数位;(5)经过十进制转换后得到解密的高精地图。

2　高精地图加密实验与分析

为了验证加密算法的安全性以及其对 OpenDRIVE 格式的高精地图的适用性,选取了 4 个 OpenDRIVE 格式的高精地图作为实验数据。这些实验数据的详细信息如表 2 所示,包括数据的大小,每一个数据中高程、超高、车道的节点数量。实验部分包括加密和解密实验,分析部分包括加密、解密效率分析、抗裁剪攻击分析、选择性解密分析和安全性分析。本文中所有脚本均以 Python3.9 编写,在 Intel(R) Core(TM) i5-9300HCPU@2.40 GHz 的 Windows 系统上运行。实验数据的可视化结果如图 4 所示。

表 2　高精地图的详细信息

Table 2　Detailed Information of Experimental Data

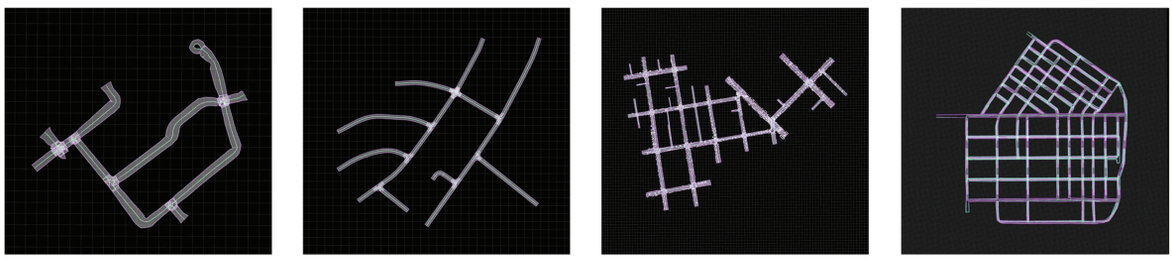
数据	大小/kB	高程节点/个	超高节点/个	车道节点/个
1	394	33	33	33
2	210	0	0	84
3	6 239	243	243	322
4	26 722	1 055	0	1 147

2.1　加密与解密

在加密实验中,采用§1.1 中的加密方案对 4 个不同的高精地图数据进行加密。其加密结果可视化如图 5 所示,加密后数据隐藏了原始道路的高程、超高及车道宽度等关键几何特征,未授权者无法从中获取任何有效的路网结构信息。

有效的加密算法需要将高精地图进行完全解密。对图 5 中加密后的实验数据进行解密,结果如图 6 所示,所有高精地图均能被正确还原,且与原始数据完全一致。

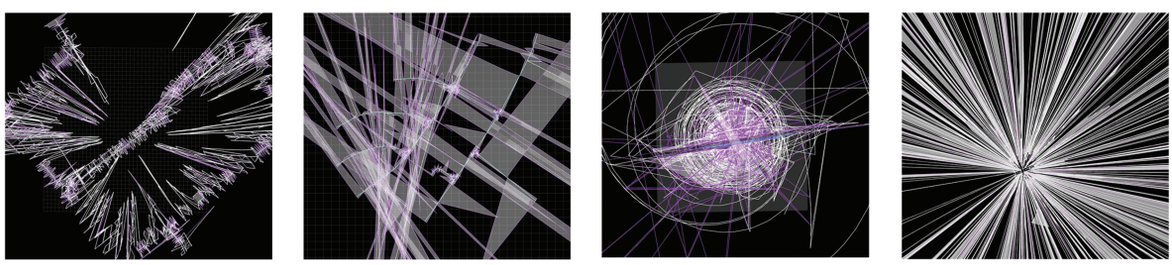
本文加密算法的加密对象为描述高程、超高与车道信息的参数化三次曲线,为了验证算法



(a) 数据1 (b) 数据2 (c) 数据3 (d) 数据4

图4 实验数据可视化

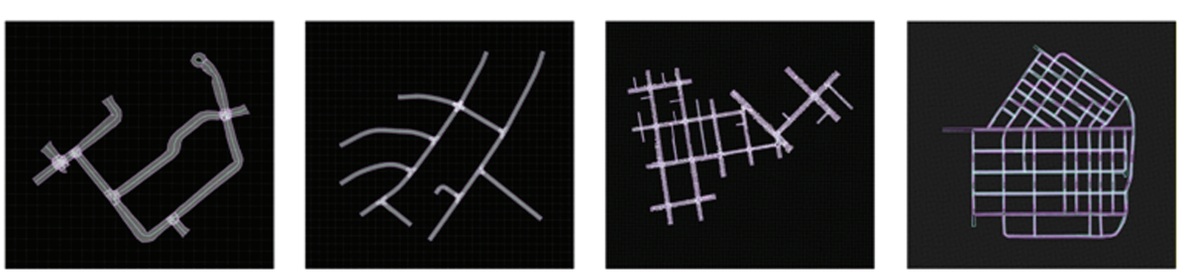
Fig. 4 Visualization of Experimental Data



(a) 数据1 (b) 数据2 (c) 数据3 (d) 数据4

图5 高精地图加密结果可视化

Fig. 5 Visualization of Encryption Results of HD Map



(a) 数据1 (b) 数据2 (c) 数据3 (d) 数据4

图6 高精地图的解密结果可视化

Fig. 6 Visualization of Decryption Results of HD Map

是无损的,对解密后的高精地图(图5)和原始高精地图(图3)进行均方根误差(root mean square error,RMSE)的计算,其计算式为:

$$E_{\mathrm{RMSE}}=\sqrt{\frac{1}{n}\sum_{i=1}^{n}(f_i'-f_i)^2} \tag{6}$$

式中,f_i'为解密后的高精地图中表示高程、超高和车道信息的参数化三次曲线的4个参数;f_i为原始高精地图中对应的相关参数。

经过计算,3个加密对象的RMSE计算结果均为0,因此本文提出的加密算法具有无损性。

2.2 算法性能分析

1)算法效率。算法对数据的加密和解密效率在现实世界中非常重要,对实验数据进行加密和解密效率的实验分析统计结果如表3所示,经过均值计算,实验所用数据的平均加密效率为2.654 MB/s,平均解密效率为2.589 MB/s。加密和解密效率良好。

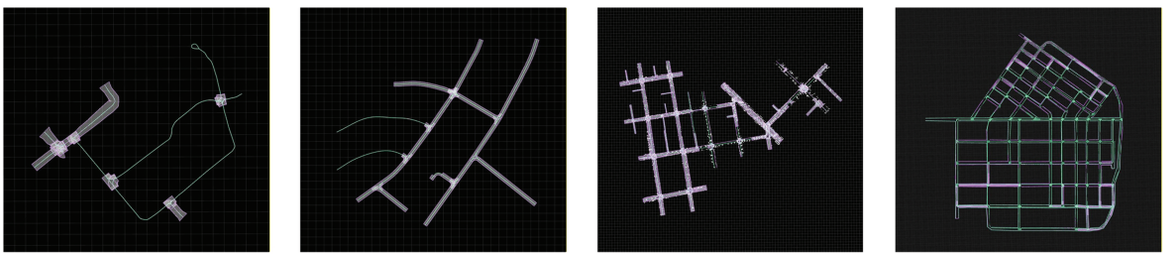
表3 加密和解密效率的统计表

Table 3 Statistics of Encryption and Decryption Efficiency

数据	大小/kB	曲线数量/个	参数数量/个	加密时间/s	解密时间/s
1	394	1 818	7 072	0.175 1	0.199 1
2	210	512	2 048	0.047 8	0.045 9
3	6 239	27 566	110 264	2.965 3	3.115 1
4	26 722	124 781	539 124	12.579 0	13.051 0

2)抗裁剪攻击。高精地图的加密是通过对参数三次曲线依次进行互补置换加密来实现的。对高精地图进行裁剪攻击,即删除节点中的全部或部分参数三次曲线。为了验证这一操作是否会影响高精地图的解密,分别对实验数据进行不同程度的随机裁剪。裁剪比例分别设置为10%、

20%、40% 和 65%，并对攻击后的高精地图密文进行解密，结果如图 7 所示。可以看出，受到不同程度的裁剪攻击后，未被攻击的部分仍然能够正常解密，证明本文的加密算法可以抵抗裁剪攻击。

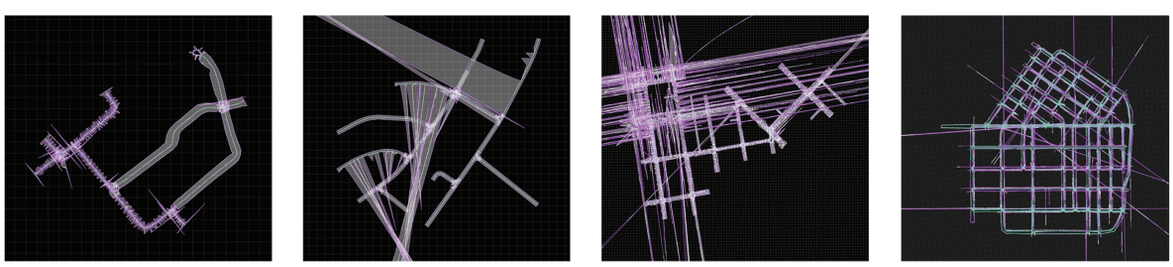


(a) 数据1　(b) 数据2　(c) 数据3　(d) 数据4

图 7　受到裁剪攻击后的解密结果

Fig. 7　Decryption Results After Cropping Attack

3）选择性解密。根据不同场景的需求，可能需要对加密的高精地图进行选择性解密。如部分地图信息可能涉及隐私或敏感数据时，通过选择性解密可以有效保护这些敏感数据，避免在不需要时暴露。在车辆跨越多个地理区域时，选择性解密可以确保只解密当前所处区域的数据，避免冗余数据处理，提升系统效率。本文分别对 4 个加密的实验数据进行选择性解密实验，为了直观展示选择性解密结果，先将实验数据的高程和超高进行完全解密，然后对车道信息进行选择性解密，解密结果如图 8 所示。可以看出，所提加密算法可以选择性地对高精地图进行加密或解密。



(a) 数据1　(b) 数据2　(c) 数据3　(d) 数据4

图 8　选择性解密的可视化结果

Fig. 8　Visualization Results of Selective Decryption

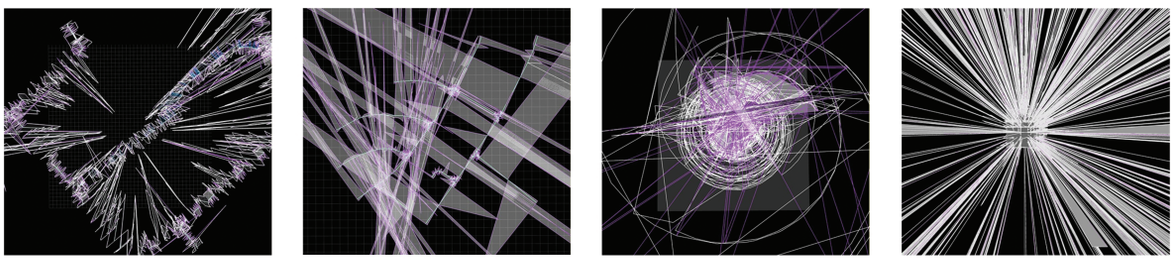
2.3　安全性分析

有效的加密算法应该有足够大的密钥空间来抵御计算机的穷举破解[23]。此外，加密使用的密钥也需要具有较高的敏感性，即相似的密钥是无法正常解密密文地图[24]。

1）密钥空间。有效高精地图加密算法需要有足够的密钥空间，才可以防止被计算机暴力破解。对高精地图进行加密时，采用了 SHA-512 散列算法生成二维混沌系统的密钥，其密钥空间为 2^{512}，远大于 2^{100}，可以有效防止计算机的穷举破解攻击[25]。

2）密钥敏感性。密钥需要较高的敏感度，发生任何改变都不能正常解密。SHA-512 散列算法和混沌系统本身都对初始信息具有较高的敏感性。本文中加密时采用 SHA-512 散列算法生成混沌系统的密钥。原始密钥为 2024.07.20，通过 SHA-512 生成的混沌系统密钥为 x_0=0.156 25、y_0=0.765 625、μ=1.410 156 25、δ=−1.277 343 75，将其修改为 2024.07.21，新生成的混沌系统密钥为 x_0=0.191 406 25、y_0=0.101 562 5、μ=1.507 812 5、δ=1.0，可以发现，用于生成随机序列的混沌密钥发生了较明显的变化。使用修改后的密钥去解密加密后的高精地图，结果如图 9 所示。修改后的密钥无法正常解密高精地图，证明本文提出的加密算法具有良好的密钥敏感性。

3）信息熵。信息熵定义为一个随机变量所有可能取值的概率分布的平均不确定性。当一个事件发生的概率越小时，包含的信息量越大；相反，发生概率越大的事件，其包含的信息量越小。信息熵常用于评估密码系统的安全性，熵值越高，密码的随机性越大，破解难度越高，其计算式如下：



(a) 数据1 (b) 数据2 (c) 数据3 (d) 数据4

图9 使用修改密钥解密的可视化结果

Fig. 9 Visualization of Decryption Results Using Modified Keys

$$H_L=\left|\sum_{i=1}^{n}\left(|L|\log_2\frac{1}{|K|}+|P_i|\log_2\frac{1}{|P_i|}\right)\right| \tag{7}$$

式中,$|L|$为密文数据中参数化三次曲线的基数;$|P_i|$为每个参数化三次曲线的基数;$|K|$为密钥的基数,本文中$|K|$为512。

由表4可知,本文算法的信息熵随实验数据量的增加而显著提升,其数值从5 146增长至29 101。考虑到高精地图本身具备数据量大、节点多等特性,根据信息熵的理论定义,该变化趋势表明本文提出的算法具有较高的安全性。

表4 实验数据的信息熵统计表

Table 4 Information Entropy Statistics of Experimental Data

数据	大小/kB	节点数量/个	参数数量/个	信息熵/个
1	394	99	7 072	5 264
2	210	84	2 048	5 146
3	6 239	808	110 264	12 425
4	26 722	2 202	539 124	29 101

2.4 对比分析

为了进一步验证本文算法的优越性,将其与3种现有的矢量地图加密算法进行对比分析,分别为文献[12]、文献[18]与文献[26]中算法。其中文献[12]算法将数据整数变换后采用Paillier同态加密,虽然安全性较高,但加密后会导致高精地图的数据精度降低。文献[18]算法和文献[26]算法均为置换加密方法,其中文献[18]算法通过对线和面数据中的坐标位置进行两次随机映射来达到加密效果;文献[26]算法先将矢量地图中的坐标点划分到一个方形矩阵中进行列的置换,再用置换后的坐标值替代原始矢量地图。这两种算法均可以应用于OpenDRIVE格式高精地图,实现无损解密,但是不支持选择性加解密,且加密算法的置换顺序单一,安全性较低。4种算法的比较结果如表5所示,可以看出本文算法不仅兼顾了其余3种算法的优势,还进一步弥补了它们的不足,为OpenDRIVE格式高精地图的数据保护提供了一种高效、可靠的新思路。

表5 与现有相关算法的对比结果

Table 5 Comparison Results with Existing Related Algorithms

算法	针对OpenDRIVE	抗穷举攻击	选择性加解密	无损	动态加密
文献[12]	×	√	×	×	×
文献[18]	×	√	×	√	×
文献[26]	×	√	×	√	×
本文算法	√	√	√	√	√

3 结 语

本文提出了一种基于DNA动态编码的高精地图加密算法,旨在提升数据在存储、传输过程中的安全性。该算法针对OpenDRIVE格式的高精地图设计,能够在加密过程中确保数据精度无损。实验结果表明,该加密机制在遭受裁剪攻击时,仍能有效解密并恢复未受损的数据区域,展现出良好的鲁棒性与实用性。此外,本文算法支持选择性加解密,可根据具体应用场景进行灵活处理,提升加密效率。本文算法为高精地图的安全防护提供了一种切实可行的解决方案。

本文算法也存在一定的局限性,目前主要聚焦于高精地图核心道路信息,尚未完全覆盖OpenDRIVE格式中包含的道路几何形状、交通标志等其他敏感信息。同时鉴于高精地图数据量大,在未来研究中,设计兼顾轻量化与高安全性的加密算法将是进一步探索的重要方向。

参 考 文 献

[1] JO K, KIM C, SUNWOO M. Simultaneous Localization and Map Change Update for the High Defi-

nition Map-Based Autonomous Driving Car [J]. *Sensors*, 2018, 18(9): 3145.

[2] 李必军，郭圆，周剑，等. 智能驾驶高精地图发展与展望[J]. 武汉大学学报(信息科学版)，2024，49(4)：491-505.
LI Bijun, GUO Yuan, ZHOU Jian, et al. Development and Prospects of High Definition Map for Intelligent Vehicle [J]. *Geomatics and Information Science of Wuhan University*, 2024, 49(4): 491-505.

[3] LI J Y, JIANG F L, YANG J, et al. Lane-DeepLab: Lane Semantic Segmentation in Automatic Driving Scenarios for High-Definition Maps [J]. *Neurocomputing*, 2021, 465: 15-25.

[4] 陈会仙，章炜，杨蒙蒙，等. 面向无人驾驶的高精地图公开应用趋势研究[J]. 武汉大学学报(信息科学版)，2024，49(4)：537-545.
CHEN Huixian, ZHANG Wei, YANG Mengmeng, et al. Open Application Trend of High Definition Map for Unmanned Driving[J]. *Geomatics and Information Science of Wuhan University*, 2024, 49(4): 537-545.

[5] 肖晓，胡挺，李巧霞，等. 高精度地图对地理信息管理的变革需求研究[J]. 测绘地理信息，2026，51(2)：57-61.
XIAO Xiao, HU Ting, LI Qiaoxia, et al. Research on the Geographic Information Management Transformation Requirements of High-Precision Maps [J]. *Journal of Geomatics*, 2026, 51(2): 57-61.

[6] 袁天洋，朱长青，陈会仙，等. 面向 OpenDRIVE 格式高精地图的脆弱水印法[J]. 武汉大学学报(信息科学版)，2026，51(2)：403-412.
YUAN Tianyang, ZHU Changqing, CHEN Hui xian, et al. Fragile Watermarking Algorithm for High-Definition Map of OpenDRIVE Format [J]. *Geomatics and Information Science of Wuhan University*, 2026, 51(2): 403-412.

[7] 詹骄，郭迟，雷婷婷，等. 自动驾驶地图的数据标准比较研究[J]. 中国图象图形学报，2021，26(1)：36-48.
ZHAN Jiao, GUO Chi, LEI Tingting, et al. Comparative Study on Data Standards of Autonomous Driving Map [J]. *Journal of Image and Graphics*, 2021, 26(1): 36-48.

[8] 楼燕敏，刘阳，何曼丽. “车路云一体化”高精度地图安全应用的浙江探索与实践[J]. 测绘地理信息，2026，51(2)：127-131.
LOU Yanmin, LIU Yang, HE Manli. Zhejiang's Exploration and Practice of Safety Applications in “Vehicle-Road-Cloud Integration” High-Precision Map[J]. *Journal of Geomatics*, 2026, 51(2): 127-131.

[9] 汤任君，段竞哲，邓洪敏. Logistic 混沌序列和 DES 算法的图像加密方法[J]. 计算机应用，2017，37(S1)：89-92.
TANG Renjun, DUAN Jingzhe, DENG Hongmin. Image Encryption Algorithm Based on Logistic Chaotic Sequence and DES [J]. *Journal of Computer Applications*, 2017, 37(S1): 89-92.

[10] 闫乐乐，李辉. 基于复合混沌序列的动态密钥 AES 加密算法[J]. 计算机科学，2017，44(6)：133-138.
YAN Lele, LI Hui. Dynamic Key AES Encryption Algorithm Based on Compound Chaotic Sequence [J]. *Computer Science*, 2017, 44(6): 133-138.

[11] 耿建勇，鲁士文. 基于 XML 加密规范的安全数据交换的实现[J]. 计算机应用与软件，2005，22(2)：99-101.
GENG Jianyong, LU Shiwen. Safe Data Exchange Based on XML Encryption [J]. *Computer Applications and Software*, 2005, 22(2): 99-101.

[12] 刘永轩，董明，杨伯钢，等. 高精度地图众源更新安全监管研究与路径探析[J]. 北京测绘，2024，38(2)：189-194.
LIU Yongxuan, DONG Ming, YANG Bogang, et al. Research and Path Analysis on Safety Supervision of Multi-source Update of High-Precision Map [J]. *Beijing Surveying and Mapping*, 2024, 38(2): 189-194.

[13] REN N, ZHAO M, ZHU C Q, et al. Commutative Encryption and Watermarking Based on SVD for Secure GIS Vector Data [J]. *Earth Science Informatics*, 2021, 14(4): 2249-2263.

[14] WANG X L, YAN H W, ZHANG L M, et al. An Encryption Algorithm for Vector Maps Based on the Gaussian Random and Haar Transform [J]. *Journal of Spatial Science*, 2023, 68(2): 303-318.

[15] Pham N G, Kwon K R, Lee S H, et al. Selective Encryption Algorithm for Vector Map Using Geometric Objects in Frequency Domain[J]. *Journal of Korea Multimedia Society*, 2017, 20(8): 1312-1320.

[16] TAN T, ZHANG L M, ZHANG M W, et al. Commutative Encryption and Watermarking Algorithm Based on Compound Chaotic Systems and Zero-Watermarking for Vector Map[J]. *Computers & Geosciences*, 2024, 184: 105530.

[17] REN N, TONG D Y, CUI H C, et al. Congruence and Geometric Feature-Based Commutative Encryption-Watermarking Method for Vector Maps [J].

Computers & Geosciences, 2022, 159: 105009.

[18] LI Y, ZHANG L M, WANG X L, et al. A Novel Invariant Based Commutative Encryption and Watermarking Algorithm for Vector Maps[J]. *ISPRS International Journal of Geo-Information*, 2021, 10(11): 718.

[19] CHEN J X, ZHU Z L, ZHANG L B, et al. Exploiting Self-Adaptive Permutation-Diffusion and DNA Random Encoding for Secure and Efficient Image Encryption[J]. *Signal Processing*, 2018, 142: 340-353.

[20] ZHANG T S, ZHU B B, MA Y Q, et al. A Novel Image Encryption Algorithm Based on Multiple Random DNA Coding and Annealing[J]. *Electronics*, 2023, 12(3): 501.

[21] DONG H, BAI E J, JIANG X Q, et al. Color Image Compression-Encryption Using Fractional-Order Hyperchaotic System and DNA Coding[J]. *IEEE Access*, 2020, 8: 163524-163540.

[22] SONG C Y, QIAO Y L. A Novel Image Encryption Algorithm Based on DNA Encoding and Spatio-temporal Chaos[J]. *Entropy*, 2015, 17(10): 6954-6968.

[23] 王小龙, 张黎明, 闫浩文, 等. 利用哈尔变换和高斯随机数进行矢量空间数据坐标加密[J]. 武汉大学学报(信息科学版), 2022, 47(11): 1946-1955.
WANG Xiaolong, ZHANG Liming, YAN Haowen, et al. A Coordinate Encryption Algorithm for Vector Spatial Data Using Haar Transform and Gaussian Random Number[J]. *Geomatics and Information Science of Wuhan University*, 2022, 47(11): 1946-1955.

[24] 吴柏燕, 柳范硕, 刘曦. 一种矢量地图同态加密域可逆水印方法[J]. 地理科学, 2025, 45(4): 699-710.
WU Baiyan, LIU Fanshuo, LIU Xi. A Reversible Watermarking Algorithm in Homomorphic Encrypted Domain for Vector Map Data[J]. *Geographical Science*, 2025, 45(4): 699-710.

[25] ALVAREZ G, LI S J. Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems[J]. *International Journal of Bifurcation and Chaos*, 2006, 16(8): 2129-2151.

[26] 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.
LI Anbo, WANG Hairong, ZHOU Wei. Scrambling Encryption of Vector Digital Map Based on 2D Chaos System[J]. *Journal of China University of Mining & Technology*, 2015, 44(4): 747-753.