武汉大学学报(信息科学版)
Geomatics and Information Science of Wuhan University
ISSN 1671-8860,CN 42-1676/TN

《武汉大学学报(信息科学版)》网络首发论文

题目：面向 OpenDRIVE 格式高精地图 DNA 动态加密算法
作者：张明旺，张黎明，闫浩文，谭涛，汪磊，刘帅康
DOI：10.13203/j.whugis20240304
收稿日期：2024-10-29
网络首发日期：2024-11-07
引用格式：张明旺，张黎明，闫浩文，谭涛，汪磊，刘帅康．面向 OpenDRIVE 格式高精地图 DNA 动态加密算法[J/OL]．武汉大学学报(信息科学版).
https://doi.org/10.13203/j.whugis20240304

DOI:10.13203/j.whugis20240304
引用格式：
张明旺, 张黎明, 闫浩文, 等. 面向 OpenDRIVE 格式高精地图 DNA 动态加密算法[J]. 武汉大学学报（信息科学版）, 2024, DOI:10.13203/J.whugis20240304（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, 2024, DOI:10.13203/J.whugis20240304）

面向 OpenDRIVE 格式高精地图 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和传输中的安全问题，基于 DNA 编码，提出了一种面向 OpenDRIVE 格式高精地图动态加密算法，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。随后对曲线参数进行扩散，首先对 DNA 碱基进行编码，并通过随机序列建立各曲线与编码方案的映射，其次对曲线参数进行二进制下的碱基编码，然后按照映射的编码方案进行 DNA 加法运算，后将运算结果转化为十进制得到密文数据。实验验证了本研究可以实现选择性加解密，平均加密效率 2.654 MB/S，平均解密效率 2.5889 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 29101，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；XML

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. Aiming at the security protection problem of high-precision maps in storage and transmission, a dynamic encryption algorithm for high-definition maps in OpenDrive format was proposed based on

收稿日期：2024-10-29
基金项目：国家自然科学基金（42271430，41761080）；甘肃省高等学校产业支撑项目(2019C-04)。
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

the data characteristics of HD maps and 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 algorithm 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 curve 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. Secondly, the parameters of the curve are base-encoded in binary. Then, 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 demonstrated that the algorithm provides high security, with a large key space and strong key sensitivity. The encryption algorithm demonstrated 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 high-definition maps in intelligent connected vehicles. Its selective encryption and decryption capabilities make it adaptable to various application scenarios, offering strong practicality.

Key Words: high-definition map; OpenDRIVE; DNA dynamic encryption; selective decryption; XML

随着智能交通和自动驾驶技术的快速发展，高精地图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，还包含了更加详细和精确的道路数据、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，实现更安全和高效的路径规划和驾驶决策[3]。然而，随着高精度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要技术之一，可以为高精地图存储和传输提供安全保护，防止对数据的非法获取和篡改。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]。这种数据以文本形式存储，是以 xodr 为拓展名的 XML 文件。因此，针对 OpenDrive 格式的高精地图加密算法研究，需顾及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]三类。

1) 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 DES[9]和 AES[10]等，非对称加密技术包括 RSA[11]和 Paillier[12]等。这些经典的加密算法安全性高，应用广泛，但是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，此类加密算法并不适用于 OpenDrive 格式的高精地图。

2) 基于频率域的加密算法相较于经典加密算法，其加密效率较高，且不破坏数据本身的结构和特征。如 Wang 等[14]对矢量地图进行 Harr 小波变换，然后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。Pham 等[15]对矢量地图的折线和多边形数据进行 DCT 变换，然后在 DCT 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连续和均匀的数据，如图像和音频。因此，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，可能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。

3) 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。如 Ren 等[17]对矢量数据进极坐标转换，并通过流密码对极坐标的数值进行加密。空间域的加密算法还可以通过改变数据的物理位置达到加密效果，如 Li 等[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，且加密效率是三类中最高的，适用于高精地图加密算法设计。

近年来，由于 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，现有的加密算法中，空间域加密可以有效地保持数据的结构和精度，维护数据的完整性，同时提供较高的安全性和可逆性。且计算效率高、兼容性好，可以应用于高精地图的加密。因此本文针对高精地图的安全保护难题，以 DNA 碱基互补和动态编码为基础，结合 OpenDrive 格式高精地图的数据特征，提出了一种安全加密算法。

1 基于 DNA 动态编码的加密方案

1.1 算法思想

OpenDrive 格式的高精地图数据是基于 XML 的结构化文本文件，包含大量的节点和属性，描述了道路、交叉口、交通标志等复杂的道路网络信息。OpenDrive 使用模块化结构将道路网络的不同部分进行分类和描述，包括道路、车道、几何形状、标志和信号等。在 OpenDrive 格式的高精地图中，高程信息使用元素 <elevation> 来描述道路沿纵向的高度变化。该元素中包含 5 个属性，起点距离“s”和参数化三次曲线的 4 个系数“a，b，c，d”。超高信息使用元素 <superelevation> 来描述道路的横向倾斜度变化，用于模拟弯道处的倾斜，其属性内容域高程相同。车道信息包含大量的子元素，包括车道的标志信息、速度限制、宽度信息等。其中宽度信息使用子元素 <width> 描述，同样包含了 5 个属性。起始偏移距离“sOffset”，即相对于车道段起点，以及参数化三次曲线的 4 个系数“a，b，c，d”。OpenDrive 格式的高精地图中对高程、超高及宽度信息的描述方式一致。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。

在现代加密算法中，置乱可以防止攻击者通过统计分析或简单的数学模型来破解加密内容，扩散可以避免密文中保留明文的模式和结构。基于 DNA 编码的加密方案在加密强度和抗攻击性方面具有明显优势，因此本研究通过 DNA 动态编码将置乱和扩散原则相结合，保证安全性的同时可以实现选择性加解密和抗裁剪攻击。

1.2 DNA 的编码与解码

与传统的静态加密方法使用固定的密钥和算法不同，动态加密是一种通过在加密过程中不断改变密钥、算法或加密参数来保护数据安全的加密技术。DNA 动态编码通过多种编码规则改变来达到动态加密的效果，数据加密过程中包含密钥变化和算法变化。

DNA 的碱基有四种：腺嘌呤(A)、胸腺嘧啶(T)、胞嘧啶(C)和鸟嘌呤(G)，其中腺嘌呤总是与胸腺嘧啶配对，胞嘧啶总是与鸟嘌呤配对。DNA 碱基的四种字符(A、T、C、G)在信息传递方面具有与二进制数据类似的特性。为了将二进制信息转化为 DNA 信息，需要通过一定的映射规则将二进制数与 DNA 碱基对应。一种常见的映射方式是将每两个二进制位映射到一个 DNA 碱基，例如“00”代表 A，“01”代表 C，“10”代表 G，“11”代表 T。根据此种映射规则，DNA 碱基可以有 8 种有效的编码方案，编码规则如表 1 所示。

表 1 DNA 的编码方案

Tab.1 DNA Coding Scheme

方案	1	2	3	4	5	6	7	8
00	A	A	C	C	G	G	T	T
01	C	G	A	T	A	T	G	C
10	G	C	T	A	T	A	C	G
11	T	T	G	G	C	C	A	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。可以理解为将两个 DNA 序列进行逐碱基相加或相减的操作。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，即将 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表 2 和表 3 所示。

表 2 DNA 的加法运算规则

Tab.2 Rules for DNA Addition Operations

加法	A	C	G	T
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	C	A

表 3 DNA 的减法运算规则

Tab.3 Rules for DNA Addition Operations

减法	A	T	G	C
A	A	T	G	C
T	T	G	C	A
G	G	C	A	T
C	C	A	T	G

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，首先对四个碱基(A、T、C、G)进行排列组合，一共有 24 种组合方式。其次通过混沌系统生成的随机序列，将各高程、超高及车道宽度节点中的参数化三次曲线随机映射为 24 种碱基组合之一，然后按照碱基互补原则对曲线中(a, b, c, d)的参数进行置乱。在扩散操作中，首先对 DNA 碱基进行编码，并通过随机序列建立各曲线与编码方案的索引。其次对曲线参数进行二进制下的碱基编码。然后按照索引的编码方案进行 DNA 加法运算。最后将运算结果进行十进制转换得到高精地图密文。加密流程如图 1 所示，详细的加密步骤如下。

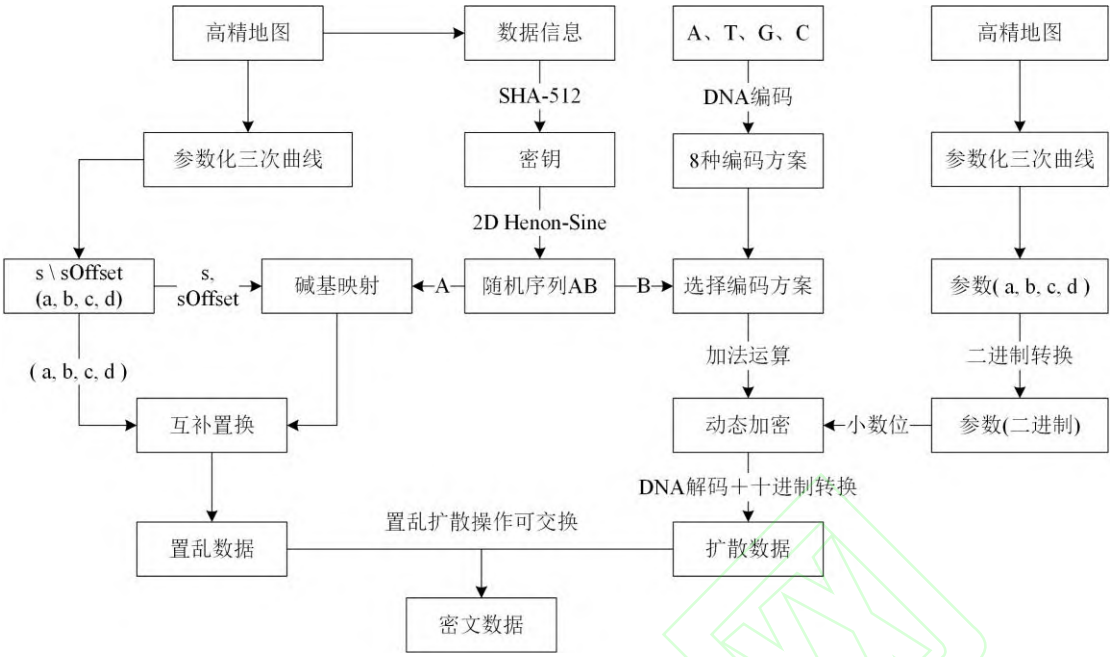


图 1 高精地图加密过程

Fig. 1 Encryption Process of HD Map

Step 1: 对 DNA 碱基进行排列组合，一共有 24 种组合记为 $P=\{[ATGC],[ACTG],\cdots,[TCGA]\}$。

Step 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 比特的散列值，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。

Step 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$K_i=\{K_1,K_2,\cdots,K_8\}$。

Step 4: 使用式(1)生成二维 Henon-Sine 映射的密钥(x_0,y_0,μ,δ)。其中k_1-k_4是用于控制密钥正负的随机整数，$bin2dec()$为二进制转换十进制的函数。

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

Step 5: 使用二维 Henon-Sine 映射生成两个随机序列L_1和L_2。二维 Henon-Sine 映射的定义如下式(2)所示，其中μ和δ为参数，x_i和y_i为迭代值，它们的取值范围都是$(-\infty,+\infty)$，mod为求余函数。

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

Step 6: 使用随机序列 A 作为控制参数，按式(3)建立每一条参数三次曲线与碱基组合的索引。其中$index$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为分别高程和超高的起始距离、车道段的起始偏移距离。

$$index=mod(int(s\times l_i\times 10^k),24),l_i\in A \tag{3}$$

Step 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四个参数(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。

Step 8: 对曲线中四个参数进二进制转换，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 和式(4)确定每个节点下所采用的编码方案。其中$index'$代表编码方案，l_i'为随机序列 B 中的随机数，sum为每个节点下曲线的数量。并根据公式(5)确定每个节点下的加密密钥K_p'，K_p为 SHA-512 散列算法生成的 512 比特 0 和 1 的集合。

$$index' = mod(sum \times l_i' \times 10^k, 8), l_i \in B \tag{4}$$

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

Step 9: 将参数(a,b,c,d)进行二进制转换，并根据表 1 中的编码方案对四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 为例子，二进制 0010110111110010 经过编码后为 AGTCTTAG。

Step 10: 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。

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 2 所示。

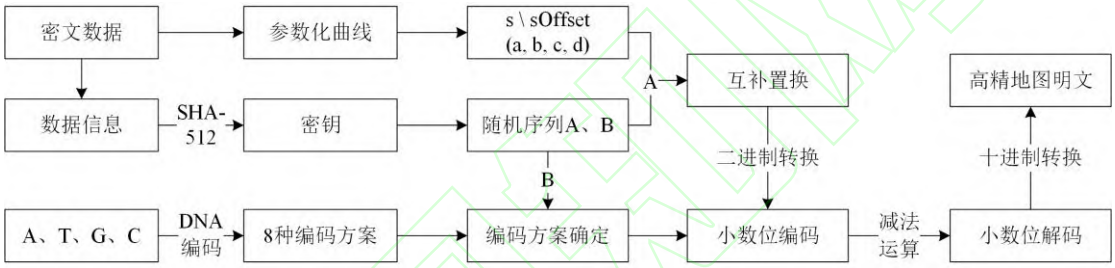


图 2 高精地图解密过程

Fig. 2 Decryption Process of HD Map

Step 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。

Step 2: 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四个参数(a,b,c,d)进行解密并替换。

Step 3: 通过式(8)-(9)确定每个节点的编码方案和加密密钥，并对曲线中的参数进行二进制转换。

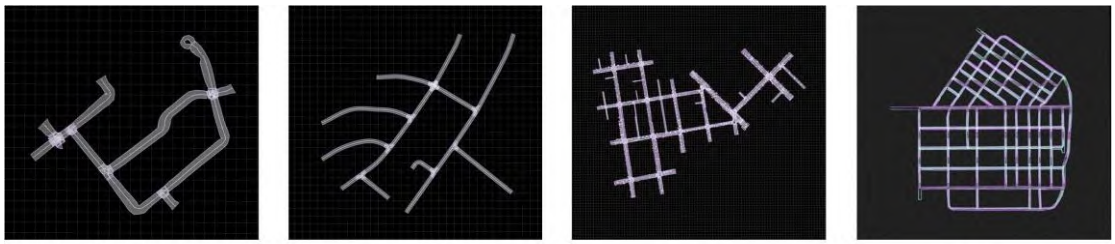
Step 4: 对参数的二进制小数位和对应的加密密钥进行编码，按照表 3 中规则进行减法运算，得到解码后的小数位。

Step 5: 经过十进制转换后得到解密的高精地图。

2 实验与分析

为了验证加密算法的安全性以及对 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。这些实验数据的大小、各节点数据均不相同。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) i5-9300H CPU @ 2.40GHz 的 Windows 系统上运行。

本文所选用的 4 个的高精地图实验数据的详细信息如表 4 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。实验数据的可视化结果如图 3 所示。



(a) 数据 A　(b) 数据 B　(c) 数据 C　(d) 数据 D

图 3 实验数据可视化

Fig. 3 Visualization of Experimental Data

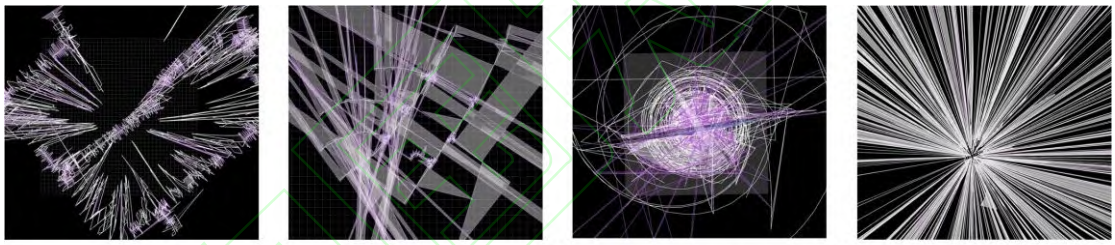
表 4 高精地图的详细信息

Tab. 4 Detailed Information of Experimental Data

数据	大小 (kB)	高程节点数	超高节点数	路段节点数
A	394	33	33	33
B	210	0	0	84
C	6239	243	243	322
D	26722	1055	0	1147

2.1 加密与解密

在加密实验中，采用 1.1 节中的加密方案对 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 4 所示，本文算法具有良好的加密效果。

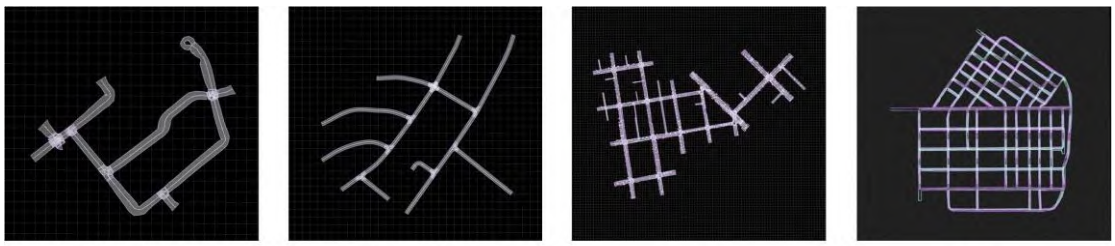


(a) 数据 A　(b) 数据 B　(c) 数据 C　(d) 数据 D

图 4 高精地图加密结果可视化

Fig. 4 Visualization of the Encryption Results of the HD Map

有效的加密算法需要将高精地图进行完全解密，将图 4 中加密后的 4 个高精地图实验数据进行解密。解密结果如图 5 示，所有的高精地图可以被正确解密，本文提出加密算法具有可行性和有效性。



(a) 数据 A　(b) 数据 B　(c) 数据 C　(d) 数据 D

图 5 高精地图的解密结果可视化

Fig. 5 Visualization of the Decryption Results of HD Map

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，为了验证算法是无损的，本节对解密后的高精地图（图 5）和原始高精地图(图 3)进行均方根误差的

计算，计算公式如式(6)。其中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 个参数和，f_i为原始高精地图中对应的相关参数。均方根误差的计算结果如表 5 所示，三个加密对象的均方根误差计算结果均为 0，因此本文加密算法具有无损性。

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

表 5 RMSE 计算结果

Tab. 5 Calculation Results of RMSE

RMSE	数据 A	数据 B	数据 C	数据 D
高程	0	0	0	0
超高	0	0	0	0
车道	0	0	0	0

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，因此本节对 4 个实验数据进行加密和解密效率的实验分析。统计结果如表 6 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 2.589MB/S。加密和解密效率良好。

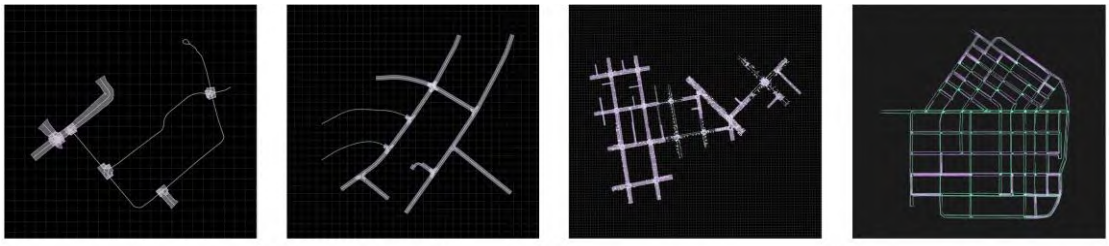
表 6 加密和解密效率的统计表

Tab. 6 Statistics of Encryption and Decryption Efficiency

数据	大小(kB)	曲线数量	参数数量	加密(s)	解密(s)
A	394	1818	7072	0.1751	0.1991
B	210	512	2048	0.0478	0.0459
C	6239	27566	110264	2.9653	3.1151
D	26722	124781	539124	12.579	13.051

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。对高精度地图进行裁剪攻击，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，裁剪比例为 10%-65%，并对攻击后的高精地图密文进行解密。结果如图 6 所示，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。因此，本文提出的加密方案可以抵抗裁剪攻击。



(a) 数据 A　(b) 数据 B　(c) 数据 C　(d) 数据 D

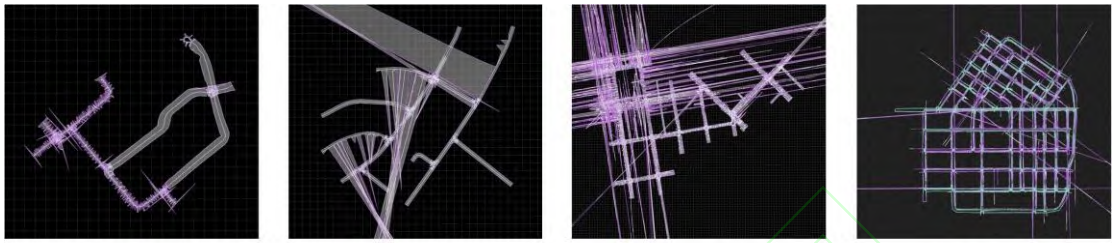
图 6 受到裁剪攻击后的解密结果

Fig. 6 Decryption Result 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清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。本文提出的加密方案可以在保证足够的安全性和加密效率的同时，满足不同场景的解密需求。为了验证这一结论，本节对 4 个加密的实验数据进行了选择性解密实验。为了可以直观的展示出选择性解密的结果，本节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 7 所示。结果表明，本文提出的加密方案可以选择性地对高清地图进行加密或解密。



(a) 数据 A　(b) 数据 B　(c) 数据 C　(d) 数据 D

图 7 选择性解密的可视化结果

Fig. 7 Visualization Results of Selective Decryption

2.3 安全性分析

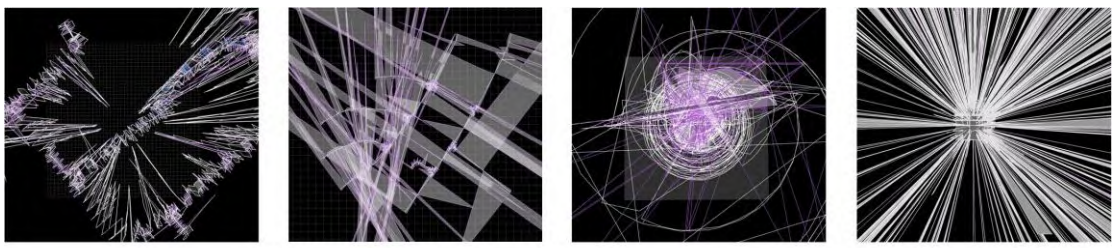
有效的加密算法应该有足够大的密钥空间来抵御计算机的穷举破解[23]。此外，加密使用的密钥也需要具有较高的敏感性，即相似的密钥是无法正常解密密文地图[24]。

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用于高精地图的解密。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$(x_0 = 0.15625, y_0 = 0.765625, \mu = 1.41015625, \delta = -1.27734375)$，将其修改为 2024.07.21，新生成的混沌系统密钥为$(x_0 = 0.19140625, y_0 = 0.1015625, \mu = 1.5078125, \delta = 1.0)$。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，然后使用修改后的密钥去解密加密后的高精度地图，本文中所用的四个高精地图数据的解密结果如图 8 所示。修改后的密钥无法正常解密高精地图，因此本文的加密算法具有良好的密钥敏感性。



(a) 数据 A　(b) 数据 B　(c) 数据 C　(d) 数据 D

图 8 使用修改密钥解密的可视化结果

Fig. 8 Visualization of Decryption Results Using Modified Keys

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，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。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。信息熵用公式(7)表示，其中$abs()$是绝对值函数，$|L|$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 7 可知，本文算法的信息熵随着实验数据的数据量增大而增大，由 5146 增加至 29101，而高精地图数据具有数据量大，节点多等特点。从信息熵的定义来看，本算法具有较高的安全性。

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

表 7 实验数据的信息熵统计表

Tab. 7 Information Entropy Statistics Table of Experimental Data

数据	大小(kB)	节点数量	参数数量	信息熵
A	394	99	7072	5264
B	210	84	2048	5146
C	6239	808	110264	12425
D	26722	2202	539124	29101

2.4 对比分析

为了进一步验证本文算法的优势，将本文算法与现有的 3 个矢量地图加密算法文献进行比对分析，包括文献[12]、文献[18]和文献[26]。这 3 个加密方法可以应用于 OpenDrive 格式高精地图中有关数字部分的加密，并且均可以抵抗穷举攻击。对比内容包括是否可应用与高精地图、能否抵抗计算机的穷举攻击、能够进行选择性加密和解密、加密是否造成高精地图数据体积膨胀以及是否影响高精地图数据精度。其中文献[12]通过将数据整数变换后采用 Paillier 同态加密，虽然该方案虽然安全性较高，但加密后会导致高精地图的数据精度降低。文献[18]和文献[26]均为置换加密方法，其中文献[18]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]通过将矢量地图中的坐标点划分到一个方形矩阵中进行和列的置换，再将置换后的坐标值替代原始矢量地图。这两个方案均可以应用于 OpenDrive 格式高精地图，并且实现无损解密，但是不支持选择性加解密，且这两种加密方案的置换的顺序单一，安全性较低。本文算法与这些现有方法的比较结果如表 8 所示，本文提出的针对 OpenDrive 格式高精地图的加密算法不仅可以兼顾对比算法的优势，还能弥补这些现有算法的不足，为 OpenDrive 格式高精地图的保护提供了一种有效的思路。

表 8 与现有相关算法的对比结果

Tab. 8 Comparison Results with Existing Related Algorithms

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

3 总结与展望

本文提出了一种基于 DNA 编码的高精地图动态加密算法，旨在提升高精地图在存储与

传输过程中的安全性。该算法针 OpenDrive 格式的高精地图，可以确保在数据加密的过程中不损失数据精度。实验验证了本文提出的新的加密机制在面对裁剪攻击时仍能有效解密未受攻击的数据，展现了出色的鲁棒性和实用性。此外，该算法支持选择性加解密，能够根据不同需求和应用场景对高精地图进行灵活处理，显著提高了加密效率和效果。这为高精地图数据的安全存储和传输提供了一种切实可行的解决方案，具备较高的实际应用价值。

然而，OpenDrive 格式中除道路信息外，还包含道路几何形状和交通标志等敏感信息，本文提出的算法尚未覆盖这些数据。此外，高精地图数据量大，设计轻量化和安全性高的加密算法是未来研究的重要目标。

参考文献

[1] Jo K, Kim C, Sunwoo M. Simultaneous localization and map change update for the high-precision map-based autonomous driving car[J]. Sensors, 2018, 18(9): 3145.

[2] Zhang Pan, Liu Jingnan. A generalized data model of high definition maps[J]. Acta Geodaetica et Cartographica Sinica, 2021,50(11):1432-1446. (张攀,刘经南.通用化高精地图数据模型[J].测绘学报,2021,50(11):1432-1446.)

[3] Li J, Jiang F, Yang J, et al. Lane-deeplab: Lane semantic segmentation in automatic driving scenarios for high-precision maps[J]. Neurocomputing, 2021, 465: 15-25.

[4] 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(04):537-545. (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(04):537-545.)

[5] Meng Liqiu. Yesterday，today and tomorrow of autonomous navigation maps[J], Acta Geodaetica et Cartographica Sinica, 2022,51(06):1029-1039. (孟立秋.自主导航地图的昨天、今天和明天[J].测绘学报,2022,51(06):1029-1039.)

[6] Lyu Xuchao, Ren Na, Zhou Qifei, et al. A digital watermark algorithm suitable for OpenDrive format at high precision maps under invisible characters[J]. Journal of Geo-information Science. (吕旭超,任娜,周齐飞,等.不可见字符下适用于 OpenDrive 格式高精地图的数字水印算法[J/OL].地球信息科学学报,1-12[2024-07-19].)

[7] Zhan Jiao，Guo Chi，Lei Tingting， et al． Comparative study on data standards of autonomous driving map. Journal of Image and Graphics,2021,26(01): 0036-0048. (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(01):36-48.)

[8] Zhu Changqing, Ren Na, Xu Dingjie. Geo－information security technology：progress and prospects[J], Acta Geodaetica et Cartographica Sinica, 2022,51(06):1017-1028. (朱长青,任娜,徐鼎捷.地理信息安全技术研究进展与展望[J].测绘学报,2022,51(06):1017-1028.)

[9] Tang Ren Jun, Duan Jingzhe, Deng Hongming. Image encryption algorithm based on Logistic chaotic sequence and DES[J]. Journal of Computer Applications, 2017,37(S1):89-92. (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.)

[10] Yan Lele, Li Hui. Dynamic Key AES Encryption Algorithm Based on Compound Chaotic Sequence [J]. Computer Science, 2017,44(06):133-138+160. (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(06):133-138+160.)

[11] Geng Jianyong, Lu Shiwen. Safe Data Exchange Based on XML Encryption[J]. Computer Applications and Software, 2005,(02):99-101. (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,(02):99-101.)

[12] Wu Baiyan, Dai Qianyi, Peng Yiwei, et al. Robust vector map watermarking algorithm in homomorphic encrypted domain[J]. Journal of Geo-information Science, 2022,24(6):1120-1129. (吴柏燕,戴千一,彭煜玮,等.矢量地图同态加密域鲁棒水印算法[J].地球信息科学学报,2022,24(06):1120-1129.)

[13] Ren N, Zhao M, Zhu C, et al. Commutative encryption and watermarking based on SVD for secure GIS vector data. Earth Science Informatics, 2021, 14:2249-2263.

[14] Wang X, Yan H, Zhang L, 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, Zhang M, 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, Cui H, 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, Wang X, 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, Zhu Z, Zhang L, 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, Zhu B, Ma Y, 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, 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, Qiao Y. A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos[J]. Entropy, 2015, 17(10): 6954-6968.

[23] 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. (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.)

[24] Ding Chen, Peng Cheng, Tang Jianbo, et al. A Local Encryption Menthod for Vector Maps Based on Multileve Spatial index Structure[J]. Acta Geodaetica et Cartographica Sinica, 2024,53(03):569-581. (丁晨,彭程,唐建波,等.顾及多级空间索引结构的矢量地图局部加密方法[J].测绘学报,2024,53(03):569-581.)

[25] Alvarez, G.; Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. International journal of bifurcation and chaos 16(08), 2129-2151 (2006).

[26] Li A B, Wang H R, Zhou W. Scrambling Encryption of Vector Digital Map Based on 2D chaos System[J], Journal of China University of Mining & Technology,2015,44(04):747-753. (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(04):747-753.)

网络首发：

标题：面向 OpenDRIVE 格式高精地图 DNA 动态加密算法

作者：张明旺, 张黎明, 闫浩文, 谭涛, 汪磊, 刘帅康

收稿日期：2024-10-29

DOI:10.13203/j.whugis20240304

引用格式：

张明旺, 张黎明, 闫浩文, 等. 面向 OpenDRIVE 格式高精地图 DNA 动态加密算法[J]. 武汉大学学报（信息科学版）, 2024, DOI:10.13203/J.whugis20240304（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, 2024, DOI:10.13203/J.whugis20240304）