International Journal of
Geo-Information

Article

A Blockchain Copyright Protection Model Based on Vector Map Unique Identification

Heyan Wang [1,2,3], Nannan Tang [4], Changqing Zhu [1,2,3], Na Ren [1,2,3,*] and Changhong Wang [4]

[1] Key Laboratory of Virtual Geographic Environment, Nanjing Normal University, Ministry of Education, Nanjing 210023, China; 221301023@njnu.edu.cn (H.W.); 09322@njnu.edu.cn (C.Z.)
[2] State Key Laboratory Cultivation Base of Geographical Environment Evolution, Nanjing 210023, China
[3] Jiangsu Center for Collaborative Innovation in Geographical Information Resource Development and Application, Nanjing 210023, China
[4] Hunan Engineering Research Center of Geographic Information Security and Application, Changsha 410004, China; tnngeo@163.com (N.T.); wangchgeo@163.com (C.W.)
* Correspondence: 09359@njnu.edu.cn

Abstract: Combining blockchain technology with digital watermarking presents an efficient solution for safeguarding vector map files. However, the large data volume and stringent confidentiality requirements of vector maps pose significant challenges for direct registration on blockchain platforms. To overcome these limitations, this paper proposes a blockchain-based copyright protection model utilizing unique identifiers (BCPM-UI). The model employs a distance ratio-based quantization watermarking algorithm to embed watermark information into vector maps and then generates unique identifiers based on their topological and geometric parameters. These identifiers, rather than the vector maps themselves, are securely registered on the blockchain. To ensure reliable copyright verification, a bit error rate (BER)-based matching algorithm is introduced, enabling accurate comparison between the unique identifiers of suspected infringing data and those stored on the blockchain. Experimental results validate the model's effectiveness, demonstrating the high uniqueness and robustness of the identifiers generated. Additionally, the proposed approach reduces blockchain storage requirements for map data by a factor of 200, thereby meeting confidentiality standards while maintaining practical applicability in terms of copyright protection for vector maps.

Keywords: vector map copyright protection; blockchain; unique identification; geometric feature; topological feature

Academic Editors: Wolfgang Kainz, Jun Feng and Changqing Luo

Received: 20 November 2024
Revised: 23 January 2025
Accepted: 28 January 2025
Published: 30 January 2025

Citation: Wang, H.; Tang, N.; Zhu, C.; Ren, N.; Wang, C. A Blockchain Copyright Protection Model Based on Vector Map Unique Identification. *ISPRS Int. J. Geo-Inf.* **2025**, *14*, 53. https://doi.org/10.3390/ijgi14020053

Copyright: © 2025 by the authors. Published by MDPI on behalf of the International Society for Photogrammetry and Remote Sensing. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Vector map data form a cornerstone of geographic information systems (GISs) and various mapping applications, serving as a fundamental component for advancing geospatial technologies and their diverse societal applications [1]. As a critical foundation for geospatial data sharing and urban planning, vector maps facilitate efficient data exchange, integration, and decision-making in domains such as transportation management, environmental monitoring, and land-use planning. Given their importance, safeguarding the copyright of vector maps is paramount.

Digital watermarking technology plays a pivotal role in the copyright protection of vector maps by embedding watermark information into the data without altering its appearance or quality [2–4]. When map data are leaked or unlawfully replicated, the embedded watermark can be extracted and verified using decoding algorithms, enabling the identification of the source and legitimacy of the data [5]. However, conventional watermark verification systems often rely on centralized servers or third-party institutions, which introduce vulnerabilities. Centralized systems are susceptible to failures and cyberattacks that can compromise the entire verification process [6,7]. Furthermore, the inclusion of personal or sensitive information in watermarks [8] raises concerns about potential misuse or unauthorized access by third-party institutions.

The emergence of blockchain technology offers a transformative solution for the secure and reliable verification of digital watermarks [9]. Blockchain's distributed and decentralized architecture ensures data integrity and trustworthiness by storing watermark information on multiple nodes across the network [10]. As an immutable distributed ledger, blockchain encrypts and hashes data records, making them resistant to tampering or deletion once registered [11]. Additionally, blockchain facilitates the tracing of watermark propagation paths, recording every instance of data copying or dissemination. This traceability enables copyright holders to quickly identify infringements and take legal action to protect their rights [12].

Despite these advantages, the unique characteristics of vector map data introduce challenges for blockchain-based copyright protection. Vector maps comprise extensive geographic information [13], including coordinates, line segments, and polygons. These data demand substantial storage capacity when registered on blockchain nodes. Moreover, the high confidentiality requirements of vector maps render direct registration impractical. Therefore, a mathematical approach is urgently needed to construct unique identifiers from vector maps, allowing these identifiers—rather than the full maps—to be registered on the blockchain. This approach not only reduces storage demands but also facilitates the efficient verification and traceability of map data origins and integrity.

Currently, unique identifiers for vector maps are often generated using hash algorithms, which ensure strong differentiation between datasets [14,15]. However, hash algorithms are inherently sensitive to data tampering, with even minor modifications leading to significant changes in the hash value. This lack of robustness poses challenges in reconstructing unique identifiers for disrupted data. There is a critical need for a new method to generate unique identifiers that combine strong uniqueness with exceptional robustness, enabling them to reliably represent vector maps on blockchain platforms.

To address these issues, this paper proposes a blockchain-based copyright protection model using unique identifiers (BCPM-UI). This model embeds watermark information into vector maps using a distance ratio-based quantization watermarking algorithm. Unique feature identifiers are subsequently constructed based on both the geometric and topological characteristics of the watermarked vector maps. Geometric features are extracted by calculating angles between geographic entities using techniques such as Delaunay triangulation, forming a geometric feature vector that represents the map. Topological features are derived by analyzing spatial relationships—such as proximity, connectivity, and containment—between geographic elements. The Hausdorff distance is employed to evaluate the spatial configuration and closeness of features, ensuring robust topological representation. The combined geometric and topological features are used to generate a unique identifier for each vector map. This identifier, along with watermark information, timestamps, and user details, is recorded on the blockchain instead of the full vector map. This approach reduces blockchain storage requirements by a factor of 200 while maintaining the confidentiality of vector maps. The unique identifiers are robust against common geometric transformations, such as rotation, scaling, and translation, ensuring their reliability. In cases of suspected infringement, unique identifiers are constructed from the infringing data and matched with those stored on the blockchain to identify the corresponding original map. Watermark information is extracted and compared between the suspected infringing data and the original map files to verify their correlation. This combined use of unique identifiers and watermark information provides definitive evidence for determining infringement and supports subsequent legal arbitration.

The structure of this paper is as follows: Section 2 reviews related work, while Section 3 introduces the preliminaries. The proposed BCPM-UI model is detailed in Section 4. Experimental results and discussions are presented in Sections 5 and 6, respectively, and Section 7 concludes the paper.

2. Related Work

2.1. Research on Copyright Protection Technology for Vector Maps Combining Blockchain and Digital Watermark

With the rapid development of the internet, the widespread dissemination of digitized content over networks has exacerbated the issue of digital piracy. In terms of addressing the challenges of copyright protection for digital works, the integration of blockchain technology with digital watermarking has emerged as a promising solution [16,17]. Unlike conventional methods, blockchain offers inherent advantages such as tamper-resistant on-chain records and irrefutability. On-chain records refer to data entries that are permanently stored within a blockchain network, ensuring their immutability and verifiability. These records are instrumental in securely storing watermark-related information, including timestamps, copyright details, and transaction histories, thereby providing a decentralized and transparent framework for copyright protection [18,19].

While blockchain-based copyright protection methods have been extensively explored for common data formats, like images and videos, research focusing on vector maps remains relatively nascent. Ren et al. pioneered the integration of vector map watermarking with blockchain by proposing a framework that constructs zero-watermark information based on the angular features of vector maps. This framework stores both the zero-watermark information and associated copyright details on the blockchain, enabling secure and immutable copyright registration [12]. Zhu et al. advanced this field by introducing a geographic data trading and copyright protection model that combines zero-watermarking, InterPlanetary File System (IPFS), and smart contract technologies. This model eliminates dependence on third-party intermediaries and ensures permanent proof of transaction information on the blockchain through smart contract design, thereby facilitating timestamp authentication for watermark registration [20]. These studies indicate that the combination of digital watermarking and blockchain technology can effectively protect the copyright of vector maps. However, vector map data have a large scale and high confidentiality requirements [21], making them unsuitable for direct deployment on blockchain platforms. Further research is needed to design blockchain-based copyright protection methods tailored to the characteristics of vector map data.

2.2. Research on Methods for Constructing Vector Map Unique Identifiers

Currently, methods for constructing unique feature identifiers in vector maps can be broadly categorized into approaches based on fragile hashing, approaches based on frequency domain coefficient analysis, approaches based on geometric feature extraction, and approaches based on topological feature extraction. The fragile hashing approach generates unique and irreversible identifiers for map features by utilizing hash functions, effectively verifying the integrity and authenticity of map data while preventing unauthorized modifications or tampering [14,22]. This method is versatile as it does not rely on specific geometric or semantic features [15]. However, its robustness is limited, as even minor edits or geometric transformations in the data can invalidate the hash. In contrast, methods based on frequency domain coefficient analysis involve transforming vector maps into the frequency domain to extract features using techniques such as Fourier transform and wavelet transform [23]. These methods excel at capturing periodicity and frequency-related characteristics in map data, making them particularly effective for handling periodic changes [24]. However, they exhibit limitations in sensitivity to non-periodic features and face high computational complexity when applied to large-scale or intricate vector maps [25].

Geometric feature extraction, a fundamental technique, focuses on identifying and leveraging essential geometric attributes from spatial data, such as vertex counts [26], angles [27], and distances [28,29]. This approach provides an intuitive representation of spatial information, effectively capturing the shape and directional characteristics of geographic entities. Geometric features exhibit strong robustness against transformations, such as scaling, rotation, and translation. Nevertheless, methods that rely solely on individual geometric features may be susceptible to specific attacks, such as feature distortion, which can compromise their robustness. Therefore, combining geometric features with other attributes could enhance the robustness of unique identifier construction. Topological feature extraction, on the other hand, emphasizes the relational properties between geographic entities, such as adjacency, intersection, and containment [30]. By constructing unique identifiers based on these topological relationships, this approach effectively captures the connectivity and relational structure of vector data [31]. Such methods are particularly resilient to data cropping and merging attacks and remain unaffected by format conversions [32].

From the existing research, it is evident that geometric feature extraction and topological feature extraction possess distinct advantages in robustness, effectively addressing various attack patterns. Future research will likely focus on integrating these two approaches to construct unique identifiers for vector maps, aiming to achieve enhanced robustness and applicability in diverse scenarios.

3. Basic Idea and Preliminaries

3.1. Basic Idea

In this paper, a novel model for vector map copyright protection is proposed, where the core innovation lies in replacing traditional methods of storing entire datasets into the blockchain with the use of unique identifiers (UIDs), as shown in Figure 1. These UIDs are constructed based on the geometric and topological features of vector maps, capturing the essential characteristics of the data in a compact and robust manner. Instead of registering large map files on the blockchain, this model only registers the UIDs and relevant metadata, significantly reducing the storage overhead on the blockchain.

The UIDs are derived through a process that analyzes the geometric and topological relationships inherent in the vector map dataset. By leveraging geometric relationships and topological relationships, a unique and robust identifier is created for each vector map. This identifier not only ensures uniqueness but also maintains robustness against changes in the map's structure due to transformations such as rotation, scaling, and translation. The UID construction process is computationally efficient, which makes it suitable for large-scale datasets.

Once constructed, these UIDs, along with associated metadata, including watermark information, user information, and timestamps, are independently registered on the blockchain. The blockchain serves as a decentralized and immutable ledger that ensures the traceability and verifiability of each map's copyright status, while the map data are stored off-chain using the InterPlanetary File System (IPFS). This approach provides a scalable solution for map copyright management, where only essential identifiers and metadata are stored on-chain, thus enhancing both efficiency and security.

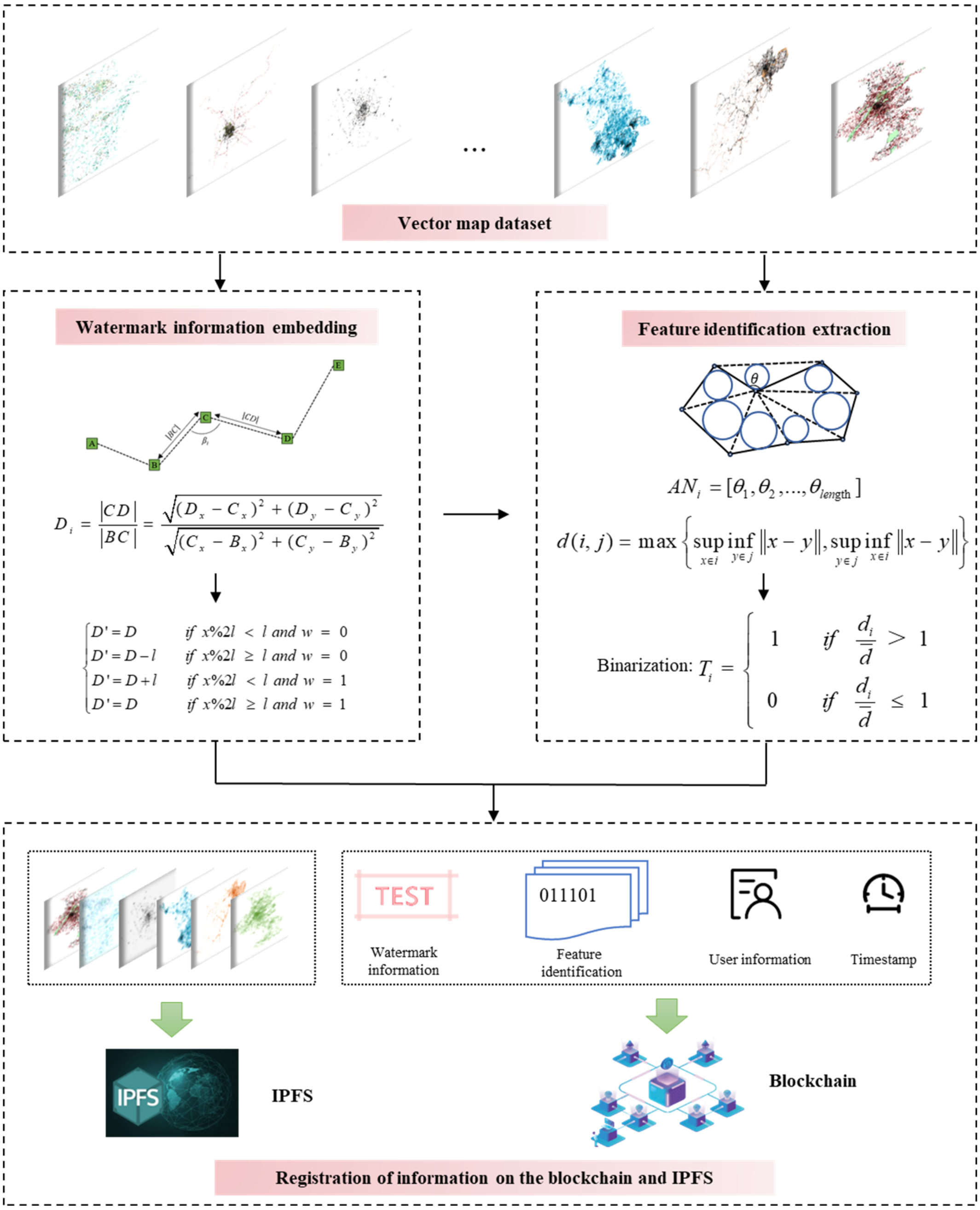

Vector map dataset
Watermark information embedding
A
B
C
D
E
|BC|
|CD|
β_i
$D_i = \frac{|CD|}{|BC|} = \frac{\sqrt{(D_x - C_x)^2 + (D_y - C_y)^2}}{\sqrt{(C_x - B_x)^2 + (C_y - B_y)^2}}$
$\begin{cases} D' = D & \text{if } x\%2l < l \text{ and } w = 0 \\ D' = D - l & \text{if } x\%2l \geq l \text{ and } w = 0 \\ D' = D + l & \text{if } x\%2l < l \text{ and } w = 1 \\ D' = D & \text{if } x\%2l \geq l \text{ and } w = 1 \end{cases}$
Feature identification extraction
θ
$AN_i = [\theta_1, \theta_2, \ldots, \theta_{length}]$
$d(i, j) = \max\left\{\sup_{x \in i} \inf_{y \in j} \|x - y\|, \sup_{y \in j} \inf_{x \in i} \|x - y\|\right\}$
Binarization: $T_i = \begin{cases} 1 & \text{if } \frac{d_i}{d} > 1 \\ 0 & \text{if } \frac{d_i}{d} \leq 1 \end{cases}$
TEST
Watermark information
011101
Feature identification
User information
Timestamp
IPFS
IPFS
Blockchain
Registration of information on the blockchain and IPFS

Figure 1. Copyright registration process in the BCPM-UI model: feature identifier construction, watermark embedding, and blockchain registration.

3.2. AntChain Combined with IPFS for Vector Map Copyright Protection

In the realm of vector map copyright protection, leveraging blockchain technology offers a promising solution to secure ownership, verify authenticity, and enable the efficient management of copyright information. The model proposed in this paper combines AntChain, a private blockchain platform, with the InterPlanetary File System (IPFS) to form an integrated framework for securing vector map datasets while maintaining system scalability and confidentiality, as shown in Figure 2. The primary advantage of this integration lies in the ability to store essential metadata and unique identifiers on-chain, while off-chain storage solutions like IPFS are utilized for managing large-scale data such as complete vector map files [33].

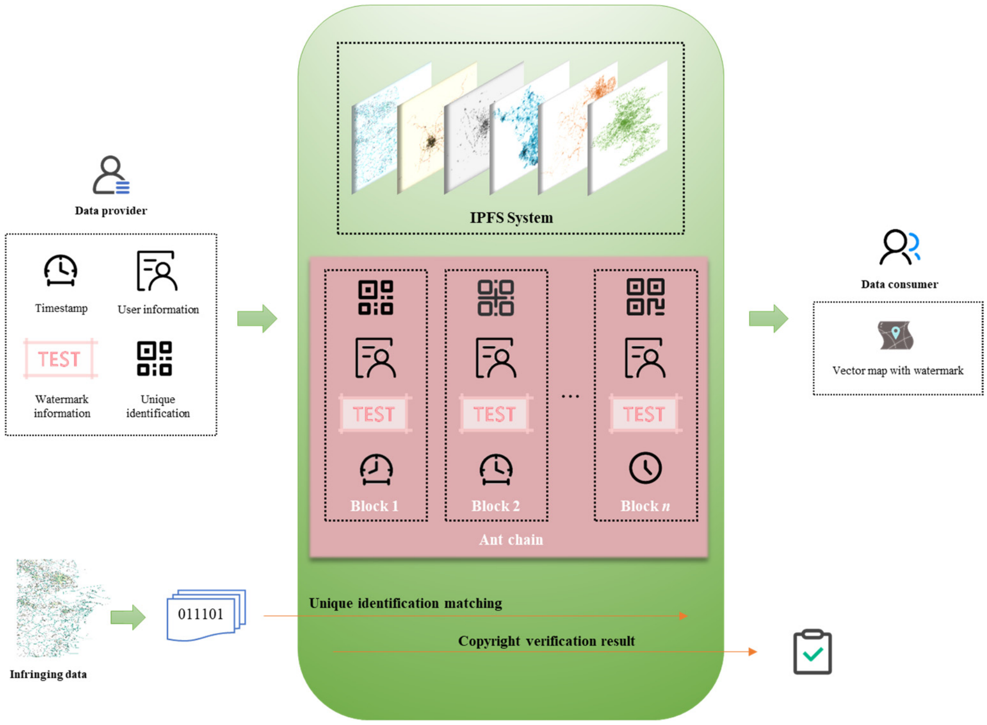


Figure 2. Antchain combined with IPFS for vector map copyright protection.

AntChain, a consortium blockchain, is selected as the blockchain platform due to its support for high throughput, low latency, and flexibility, features which are critical for the effective management of vector map copyrights. A blockchain is fundamentally a distributed ledger that consists of a sequence of blocks, each containing a set of transactions [34]. These blocks are cryptographically linked, ensuring the immutability and traceability of the recorded data. In a consortium blockchain like AntChain, the network is permissioned, meaning only pre-authorized entities can participate in transaction validation and block creation. AntChain's modular architecture allows for tailored consensus mechanisms, such as PBFT (Practical Byzantine Fault Tolerance), which optimize transaction processing for specific application requirements. This ensures that the transaction load is distributed efficiently, with strong privacy and security guarantees provided by the permissioned framework. Within this blockchain structure, important data such as unique identifiers, watermark information, timestamps, and user details are recorded directly on the blockchain [35]. This on-chain information serves as a secure and immutable reference for map ownership, ensuring the traceability of vector map data from creation to use while minimizing the risk of data tampering [36].

In contrast to public blockchains, which suffer from scalability issues due to high transaction costs and slow processing speeds when handling large datasets, AntChain facilitates faster transaction processing by utilizing optimized consensus protocols and parallel transaction execution. This makes it well suited for applications such as vector map copyright protection, where the efficiency of blockchain transactions is crucial for real-time verification. Additionally, the modular nature of AntChain allows for seamless integration with off-chain storage systems such as IPFS, which handles the large-scale storage of vector map files.

IPFS, a decentralized file storage system, is integrated to complement the blockchain by providing a robust and scalable solution for storing complete vector map datasets. IPFS operates on a peer-to-peer (P2P) network, where files are distributed across various nodes, and data are retrieved using content hashes rather than specific node addresses. This method ensures the integrity and uniqueness of map data while alleviating the storage burden on the blockchain. Using IPFS allows for efficient and fast data retrieval, which is critical for handling large vector map files. In the proposed model, vector map files are stored off-chain in IPFS, and only their corresponding unique identifiers and associated metadata are recorded on AntChain, preserving both security and privacy.

Upon receipt of a transaction request, data providers generate unique identifiers for vector maps, embedding watermark information and registering these identifiers on the AntChain blockchain [37]. The blockchain records the relevant metadata, including the unique identifiers, watermark details, user information, and timestamps, ensuring that these data are securely stored in a tamper-proof ledger. Meanwhile, the complete vector map files are uploaded to IPFS. In the event of a copyright infringement, the process involves constructing the unique identifiers from the alleged infringing data and performing a similarity check against the identifiers stored on AntChain. If a match is found, the watermark information is compared to verify infringement. This decentralized model allows for efficient copyright enforcement while significantly reducing the storage requirements on the blockchain, ensuring both scalability and confidentiality.

This integration of AntChain and IPFS offers a balanced approach to vector map copyright protection, combining the strengths of both technologies to address the challenges posed by large-scale geographic data management. By leveraging AntChain's high performance and secure on-chain data storage capabilities, along with IPFS's scalable off-chain storage, the proposed model ensures the efficient, secure, and transparent copyright management of vector maps.

3.3. Vector Map Unique Identification Based on Geometric and Topological Relationships

As the ID number of a map, unique identification is obtained by computing the unique characteristic values of a vector map. The purpose of this is to replace the cumbersome map files registered on the blockchain platform while ensuring uniqueness and robustness, thereby replacing the traditional deployment method of map files on the blockchain platform. The construction approach of unique identification in this paper is as follows: utilizing geometric relationships [38], such as angles between geographical features, a quantitative description of the map structure is obtained through mathematical calculations and geometric measurements. Simultaneously, based on the topological feature relationships [39] of the vector map dataset, an analysis of proximity, connectivity, and containment relationships between geographic entity features is conducted to abstract the mathematical expressions of topological relationships [40]. Ultimately, by combining geometric and topological features, unique feature identification is performed for the map, ensuring not only the uniqueness of the identification but also resistance to changes in geographic features and geometric attributes.

Firstly, all coordinate points of the vector map dataset are obtained, after which a Delaunay triangulation T is constructed. Subsequently, all circles inscribed in triangles adjacent to each coordinate point P_i are identified. The minimum radius of these inscribed circles corresponds to the angle θ, as illustrated in Figure 3.

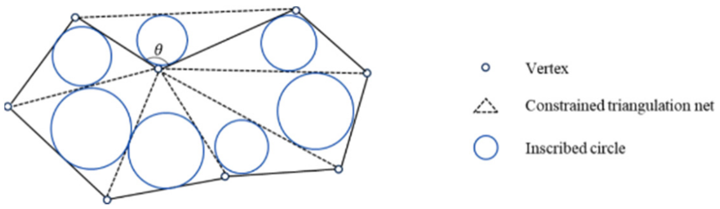


Figure 3. Schematic diagram of angle feature parameter acquisition.

Working according to the aforementioned approach, it is necessary to obtain the angular value θ for each geographical feature, forming the geometric feature vectors of the vector map.

$$AN_i = [\theta_1, \theta_2, \ldots, \theta_{length}] \tag{1}$$

where *length* denotes the number of geographical features in the vector map dataset.

As depicted in Equation (2), by mapping the angle values, a quantitative expression of geometric features is achieved, thereby obtaining the geometric feature parameter H_{ijk}.

$$H_{ijk} = floor[(AN_i)^{\frac{1}{p}} \times (n-1)] + 1 \tag{2}$$

where p serves as an adjustable parameter that modulates the weighting effect, with smaller values of p amplifying the weighting effect, while larger values diminish it. n denotes the length of subsequent unique identification sequences. The floor(x) function is utilized to obtain the largest integer less than or equal to x.

Subsequently, each geographical feature in the vector map dataset is traversed. It is necessary to consider the entire vector dataset S, which includes a set of points P, a set of polylines L, and a set of polygons A. Using the R-tree index R, it is necessary to perform nearest non-intersecting heterogeneous feature queries for each feature i, leveraging spatial indexing to accelerate distance computations. The algorithm for nearest neighbor non-intersecting heterogeneous feature queries across diverse feature types is outlined as follows:

$$NN(i) = \arg \min_{j \in S, j \neq i, type(i) \neq type(j)} d(i,j) \tag{3}$$

where type(i) denotes the type of feature i. The distance $d(i, j)$ is measured by using the Hausdorff distance as the metric for different types of features. Assuming that feature i and feature j belong to different subsets of S (i.e., $i \in P$ and $j \in L$ or A, or $i \in L$ and $j \in P$ or A, or $i \in A$ and $j \in P$ or L), the distance computation formula is as follows:

$$d(i,j) = \max\left\{ \underset{x \in i}{\text{sup}} \underset{y \in j}{\text{inf}} \|x-y\|, \underset{y \in j}{\text{sup}} \underset{x \in i}{\text{inf}} \|x-y\| \right\} \tag{4}$$

where $\|\cdot\|$ denotes the Euclidean distance. To facilitate understanding, we illustrate the distance measurement using Figure 4. Let us suppose that, in the dataset, the similar features to feature A are Points 1 and 2, while the dissimilar features are Polyline 1, Polyline 2, and Polygon 1. Among these, only Polyline 1 and Polygon 1 are disjointed and do not intersect with A. By calculating the Hausdorff distance between feature A and Polyline 1, as well as between feature A and Polygon 1, and then taking the minimum value, we obtain the nearest non-intersecting heterogeneous feature, $NN(A)$.

It is necessary to utilize the R-tree spatial index to find the nearest candidate features; this should be followed by an exact Hausdorff distance calculation for the candidate set. Assuming the candidate set for feature i is C_i, the precise calculation process is as follows:

$$\forall j \in C_i, if\ d(i,j) = \min_{k \in C_i} d(i,k),\ then\ record\ d(i,j) \tag{5}$$

For each feature I, it is necessary to record the nearest non-intersecting heterogeneous feature $d(i{,}NN(i))$ into the result sequence D. The sequence is formatted as follows:

$$D = \{d(i, NN(i)) | i \in S\} \tag{6}$$

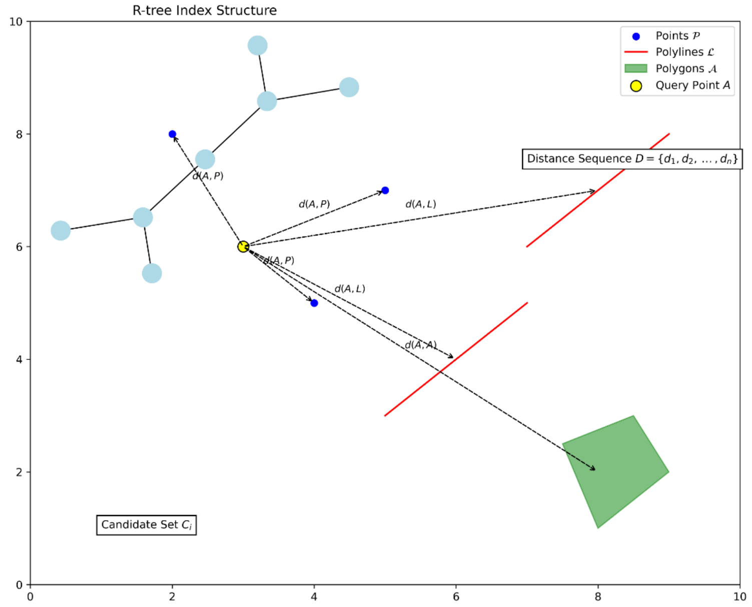


Figure 4. Schematic of nearest neighbor non-intersecting heterogeneous feature query based on Hausdorff distance.

After obtaining the distance sequence D, we need to calculate the mean value of the sequence D. Let D contain n distance values, denoted as $D = \{d_1, d_2, \ldots d_n\}$. The formula for calculating the mean $\overline{d}$ is as follows:

$$\overline{d} = \frac{1}{n}\sum\nolimits_{i=1}^{n} d_i \tag{7}$$

In the formula, d_i is the i-th distance value in the sequence D, and n is the length of the sequence D (i.e., the total number of features).

Ultimately, by comparing the specific distance of each geographical feature with the global mean, the correlation between geographical features is quantified in a binary manner to obtain the topological feature parameters of the vector map dataset.

$$T_i = \begin{cases} 1 & if \ \frac{d_i}{\overline{d}} > 1 \\ 0 & if \ \frac{d_i}{\overline{d}} \leq 1 \end{cases} \tag{8}$$

where T_i represents the topological feature parameter in the i-th position of the unique identifier.

Finally, by using the geometric feature parameter H_{ijk} as the index and the topological feature parameter T_i as the feature value, the unique identifier of the vector map can be constructed.

Continuing with the example of rotational transformation, we focus on analyzing the stability of geometric and topological feature parameters amidst geometric transformations like rotation, scaling, and translation (RST). For the geometric feature parameter H_{ijk}, the calculation of the angle after rotation is independent of the rotation itself. According to Equation (9), the geometric feature parameter H_{ijk} remains unchanged after rotation. According to Equation (10), distance calculation only involves positional information and is unaffected by rotation. Therefore, the topological feature parameter T_i also remains unchanged after rotation transformation.

$$H_{ijkr} = f(\theta_{1r}, \theta_{2r}, \ldots, \theta_{lenr}) = f(\theta_1, \theta_2, \ldots, \theta_{len}) = H_{ijk} \tag{9}$$

$$T_i\ (r) = d_{ir}/\overline{d_r} = d_i/\overline{d} = T_i \tag{10}$$

where H_{ijkr} and $T_i(r)$ represent the geometric and topological feature parameters, respectively, after rotation transformation. θ_{1r}, θ_{2r}, and θ_{lenr} denote the angle values of each geographical feature in the vector map dataset after rotation, while d_{ir} indicates the distance between each geographical feature after rotation and the nearest dissimilar feature. d_r represents the global mean distance of the vector map dataset after rotation.

Similarly, under scaling and translation transformations, geometric and topological feature parameters retain their integrity, ensuring robust and consistent representations across diverse geometric transformations of vector map data.

4. Blockchain Copyright Protection Model Based on Vector Map Unique Identification

The BCPM-UI model is a blockchain-based framework designed to ensure secure registration and the reliable verification of vector map copyrights. At its core, the model integrates digital watermarking and unique identifier construction with blockchain technology to provide a robust solution for copyright protection. Watermark information is embedded into the vector map in a manner that ensures imperceptibility and robustness. Simultaneously, unique feature identifiers are derived from the geometric and topological characteristics of the watermarked map. These identifiers, along with associated metadata, are securely recorded on the blockchain. By combining the immutability of blockchain with the resilience of watermarks and identifiers, the model achieves traceability, confidentiality, and accountability, offering a comprehensive solution for vector map copyright management.

The implementation of the model is divided into two primary processes: the copyright registration process and the copyright verification process. During registration, watermark information is embedded into the vector map and unique identifiers are constructed. Both of these are securely registered on the blockchain, along with relevant metadata. The verification process focuses on identifying potential copyright infringements by constructing unique identifiers and watermark data from suspected infringing datasets and comparing them with blockchain records. This ensures the precise and reliable validation of ownership and infringement detection, providing robust evidence for arbitration and accountability in vector map transactions.

4.1. Copyright Registration Process

As the ID number of a map, unique identification is obtained by computing the unique characteristic values of vector maps. Its purpose is to replace the cumbersome map files registered on the blockchain platform while ensuring uniqueness and robustness, thereby replacing the traditional deployment method of map files on the blockchain platform. The construction approach of unique identification used in this paper is as follows: utilizing geometric relationships, such as angles between geographical features, a quantitative description of the map structure is obtained.

The copyright registration process comprises two parts: watermark embedding and unique identification construction.

4.1.1. Watermark Embedding

The basic steps for watermark embedding are as follows:

Step 1: Generate a binary watermark sequence W from the copyright binary image, where $W = \{w_j, j = 0, 1, 2, ..., M - 1\}$. M represents the length of the transformed watermark information.

Step 2: Read the coordinate points V_i (i = 1, 2, ..., n) in the vector map according to the order of the coordinate points in line and polygon features. Coordinate points of point features are read based on the order stored in the file. Calculate the corresponding distance ratio D_i according to Equation (11), as shown in Figure 5.

$$D_i = \frac{|CD|}{|BC|} = \frac{\sqrt{(D_x - C_x)^2 + (D_y - C_y)^2}}{\sqrt{(C_x - B_x)^2 + (C_y - B_y)^2}} \tag{11}$$

where B_x, C_x, and D_x represent the abscissa of the coordinate point V_i, and B_y, C_y, and D_y denote the ordinate of the coordinate point V_i.

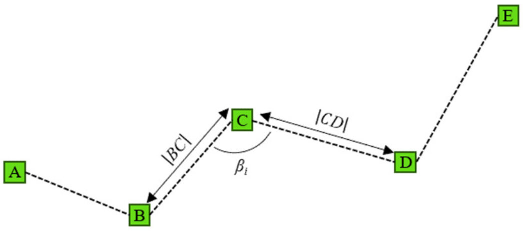


Figure 5. Calculation diagram of distance ratio.

Step 3: Establish the mapping relationship between the watermark values and the watermark indices based on the mapping mechanism. Taking the distance ratio D_i as an example, stable numerical ID_i values are obtained by taking the first n digits of D_i.

$$ID_i = D_i \times 10^n \tag{12}$$

The watermark synchronization mechanism is established as follows:

$$Watermark_{index} = Hash(ID_i)\%M_N \tag{13}$$

where $Watermark_{index}$ represents the watermark position to be embedded, M_N is the number of watermark bits, and $Hash$ denotes the hash function, such as the logistic chaotic function.

Step 4: Currently, prevalent methods for embedding and extracting watermarks in vector maps encompass classical techniques such as LSB (least significant bit), additive multiplicative methods, and spreadspectrum methods, among others. To meet the requirements for blind watermark extraction and robustness, a quantization mechanism is embraced for watermark embedding and extraction. Let the quantization step be denoted as l, and the watermark information to be embedded denoted as W = 0 or 1. Consequently, the watermark embedding process based on the distance ratio D unfolds as follows:

$$\begin{cases} D' = D & if\ x\%2l < l\ and\ w = 0 \\ D' = D - l & if\ x\%2l\ \geq\ l\ and\ w = 0 \\ D' = D + l & if\ x\%2l < l\ and\ w = 1 \\ D' = D & if\ x\%2l\ \geq\ l\ and\ w = 1 \end{cases} \tag{14}$$

where % denotes the modulo operation. The watermark embedding process is illustrated in Figure 6.

The index of the watermark value to be embedded is derived from the mapping mechanism in Step 3. Based on the change in the distance ratio, it is necessary to calculate the coordinates of $V_i{}'$ after embedding the watermark.

Step 5: Update the coordinates of $V_i{}'$ to the set of coordinates V_i (i = 1, 2, ..., n), and repeat Step 4 iteratively until all coordinates complete watermark embedding.

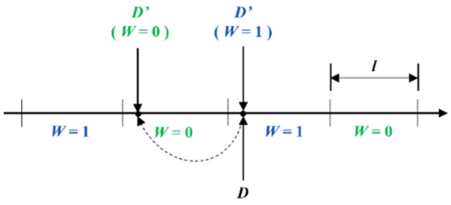


Figure 6. Quantization mechanism watermark embedding diagram.

4.1.2. Unique Identification Construction

In this paper, we define the unique identifier as a fixed-length binary sequence composed of information values represented by 0 and 1. Utilizing the quantized index of geometric features from the vector map dataset and information values obtained through topological feature quantization identifiers, the precise procedure for constructing the unique identification unfolds as follows:

Step 1: Retrieve the vector map file containing the watermark and iterate through all geographical features within the dataset. Employ the Douglas–Peucker (DP) algorithm to extract feature points of vector maps, thereby improving the robustness of subsequent unique identification construction processes.

Step 2: For each geographical feature, construct the Delaunay triangulation T and obtain all circumcircles of triangles adjacent to the coordinate point P_i. Record the smallest radius of the circumcircle corresponding to the angle θ of the triangle and map this angle value to a hash value, thereby achieving a quantitative representation of geometric relationships. Consequently, abstract the relationships between features into indices of unique identifiers.

$$FI_i = Hash(key \times AF_i)\%FI_{len} \tag{15}$$

where *Hash*() is the normalized hash function, *key* is the encryption key, AF_i represents the most significant bit of the angle feature parameter of the i-th feature, FI_{len} is the length of the identification sequence, and FI_i is the unique identification mapping index obtained from quantizing the i-th feature.

Step 3: For every geographical feature, determine the distance to the nearest dissimilar feature based on Equation (4), and establish a distance matrix accordingly. Compute the average of the distance matrix using Equation (7) to attain a comprehensive assessment of spatial correlation.

Step 4: By contrasting the distance from each geographical feature to the closest dissimilar counterpart with the mean of the distance matrix, encode the correlation between geographical features in binary format as per Equation (8). Distances exceeding the mean value are denoted as 1, whereas those falling below the mean value are denoted as 0, thereby finalizing the generation of unique identifiers.

Step 5: Leverage the unique identifiers, watermark information, user details, timestamps, and additional data as transaction inputs. Utilize smart contracts to record the information into the unique identification repository on the blockchain, thereby finalizing the copyright registration procedure.

4.2. Copyright Verification Process

The copyright verification process comprises two parts: unique identification matching and watermark extraction.

4.2.1. Unique Identification Matching

The unique identification matching process ensures reliable copyright verification by sequentially comparing the constructed unique identifications from suspicious data with the records stored in the blockchain. Initially, the identifications are constructed from suspicious data based on topological and geometric characteristics, as described in Section 4.1. These constructed identifications are then compared against the unique identification repository recorded on the blockchain. The comparison is performed by calculating the similarity between each constructed identification and every blockchain-stored identification using the bit error rate (BER), defined as the proportion of differing bits between two standardized bit strings. For each constructed identification, the blockchain-stored identification with the highest similarity (i.e., the lowest BER) is selected as the most probable match. This approach not only ensures accurate matching but also enhances the robustness of the system against potential alterations in suspicious data, as the identification process prioritizes the closest match, reducing the risk of false negatives in cases of the partial distortion or modification of the embedded identifiers.

Step 1: Convert the constructed unique identifications and blockchain identifications into bit string representations. Let u_i and b_j be bit strings of length k. Assume u_i and b_j are standardized to bit strings of the same length.

Step 2: For each pair of identifications (u_i, b_j), calculate the bit error rate (BER). The BER is defined as the proportion of differing bits between two bit strings. The specific formula is as follows:

$$BER(u_i, b_j) = \frac{1}{k}\sum_{l=1}^{k} \delta({u_i}^l, {b_j}^l) \tag{16}$$

Step 3: Calculate $BER(u_i, b_j)$ for each pair of identifications (u_i, b_j). If $BER(u_i, b_j) < BER_{threshold}$, consider it a successful match and add the pair (u_i, b_j) to the result set M.

Step 4: Traverse all combinations of constructed identifications u_i and stored identifications b_j, and record the matching pairs (u_i, b_j) for all successful matches. Output the matching result set M.

$$M = \left\{(u_i, b_j) \middle| BER(u_i, b_j) < BER_{threshold}, \forall u_i \in U, b_j \in B\right\} \tag{17}$$

4.2.2. Watermark Extraction

Watermark extraction is the inverse process of watermark embedding used to extract the hidden watermark information from the suspicious data, as detailed below:

Step 1: Read the coordinate points V_i (i = 1, 2, ..., n) in the vector map according to the order of the coordinate points in line and polygon features. Coordinate points of point features are read based on the order stored in the file. Calculate the corresponding distance ratio D_i according to Equation (14).

Step 2: In the geometric feature domain for extraction, apply Step 3 of the watermark embedding algorithm to establish a synchronization relationship between the watermark values and indices.

Step 3: For the distance ratio D_i, extract the watermark according to Equation (18). The index of the watermark value to be extracted is determined by the mapping mechanism in Step 3. Then, record the extracted watermark value and index.

The watermark extraction process based on the distance ratio D is as follows:

$$\begin{cases} w' = 0 & if \;\; D'\%2l < l \\ w' = 1 & if \;\; D'\%2l \geq l \end{cases} \tag{18}$$

Step 4: Employ the majority rule to derive the watermark sequence from the extracted watermark information. Convert this sequence into a binary format and utilize it to authenticate the copyright information linked with the identifier.

Given that a watermark bit might be extracted multiple times, the majority rule is utilized to ascertain the watermark information for each individual watermark bit. The majority decision rule is outlined as follows:

$$W_i' = \begin{cases} 1, & if\ F_i(w_1) > F_i(w_0) \\ 0, & if\ F_i(w_1) \leq F_i(w_0) \end{cases} \tag{19}$$

where $F_i(w_0)$ denotes the number of times the watermark information "0" is extracted for the i-th bit, and $F_i(w_1)$ denotes the number of times the watermark information "1" is extracted for the i-th bit. Using this method, the extracted watermark information $W_i{}'$ is obtained. Based on the size of the original watermark image, the one-dimensional sequence $W_i{}'$ is reconstructed into a two-dimensional watermark image W_{image}.

5. Experiment Results and Analysis

5.1. Experimental Dataset

To comprehensively assess the effectiveness of the proposed BCPM-UI model, we selected six shapefile datasets representing vector maps from key urban areas—Shanghai, Beijing, Chengdu, Jiangsu Province, Hangzhou, and Nanjing. These datasets exhibit diverse characteristics in terms of coordinate systems, layer complexities, and geographic feature densities, providing a robust evaluation framework. The experimental setup operates on a Windows 10 platform equipped with an Intel i7-9700 CPU and 16 GB RAM, ensuring reliable execution. The unique identification construction was implemented using MATLAB R2023a, leveraging robust computational and visualization capabilities. The blockchain infrastructure employed was the Ant Open Alliance Chain, a consortium blockchain platform that supports high throughput and secure data recording. Integration with MATLAB involved the generation of unique identifiers, which were exported and recorded in the blockchain through API calls facilitated by Python scripts. The development of blockchain smart contracts was carried out within the Cloud IDE provided by Ant Open Alliance Chain. Solidity 0.8.18 was used for contract design and deployment, ensuring compatibility with the platform's virtual machine. The Cloud IDE's integrated environment streamlined the process, from contract development and testing to deployment. This setup ensures reproducibility, as all tools and configurations are well documented and accessible.

The data in the proposed model were utilized in multiple critical stages. This included constructing unique identifiers based on the geometric and topological characteristics of vector maps, embedding watermark information into the datasets, and recording these identifiers and watermarks on the blockchain. The dataset's diverse attributes allowed us to test the model's adaptability and robustness across different map structures and complexities. Furthermore, the experimental datasets were used to evaluate the integrity and resilience of watermark extraction and identifier matching under various levels of distortion or modification, ensuring comprehensive performance validation.

In evaluating the adaptability of the model to diverse and complex vector map datasets, this paper selected datasets with varying numbers of layers, geographic feature counts, and coordinate systems, as shown in Figure 7. Table 1 provides detailed information on the experimental datasets, including the vector map names, coordinate systems, layer numbers, and geographic feature counts. Furthermore, to optimize the practical application of watermark information, this paper utilized meaningful binary information, sized at 64 × 64, as watermark data. This ensures substantive watermark information while providing a benchmark closer to real-world applications for subsequent model evaluations, as depicted in Figure 8. Through systematic dataset selection and watermark information settings, the relevance of the model's performance can be more accurately tested, thereby enhancing the practicality and generalizability of the research.

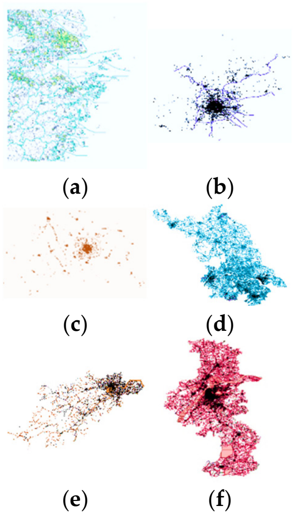

(**a**) (**b**)
(**c**) (**d**)
(**e**) (**f**)

Figure 7. The dataset used in the experiment: (**a**) Shanghai dataset; (**b**) Beijing dataset; (**c**) Chengdu dataset; (**d**) Jiangsu dataset; (**e**) Hangzhou dataset; (**f**) Nanjing dataset.

Table 1. Detailed information about the experimental dataset.

Name of Vector Map	Quantity of Map Layers			Quantity of Features	Coordinate System
	Point Layer	Line Layer	Polygon Layer		
Shanghai dataset	1	1	1	6214	WGS 1984 Albers
Beijing dataset	2	1	1	16,343	GCS Beijing 1954
Chengdu dataset	3	1	1	18,769	WGS 1984 Albers
Jiangsu dataset	2	2	1	22,168	GCS WGS 1984
Hangzhou dataset	9	4	2	64,810	WGS 1984 Albers
Nanjing dataset	10	6	3	53,660	WGS 1984 Albers

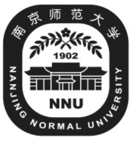


Figure 8. Watermark images used in the experiment.

5.2. Evaluation Index

5.2.1. Evaluation Index for Vector Map Imperceptibility

Evaluation metrics for the imperceptibility of vector maps include the average distance, maximum distance, and standard deviation. Among these, the average distance and maximum distance provide quantitative evaluations of the shape changes in the map after embedding the watermark, while the standard deviation can measure the stability of the map after watermark embedding. Therefore, this paper evaluates the error between the original vector map and the vector map containing the watermark using the average distance D_{mean}, the maximum distance D_{max}, and the standard deviation σ. It is assumed that the original data points of the vector map are (x_i, y_i), and the data points of the vector map containing the watermark are $(x_i{}', y_i{}')$.

The maximum distance error D_{max} represents the maximum distance between the data points with watermark and the original data points, calculated using Equation (20).

$$D_{max} = \max\sqrt{(x_i - x_i')^2 + (y_i - y_i')^2} \quad (20)$$

The average distance error D_{mean} is the average distance between the data points with watermark and the original data points, as shown in Equation (21).

$$D_{mean} = \frac{1}{n}\sum\nolimits_{i=1}^{n} \sqrt{(x_i - x_i')^2 + (y_i - y_i')^2} \quad (21)$$

where n represents the number of data points.

The standard deviation σ, calculated as the standard deviation of errors between the data points with watermark and the original data points, represents the dispersion of errors, as derived from Equation (22).

$$\sigma = \sqrt{\frac{1}{n}\sum\nolimits_{i=1}^{n} (\sqrt{(x_i - x_i')^2 + (y_i - y_i')^2} - D_{mean})^2} \quad (22)$$

5.2.2. Evaluation Index for Watermark Correlation

When authenticating map data, it is imperative to compare the extracted watermark with the original watermark stored in the blockchain to validate its authenticity. The evaluation of watermark similarity primarily encompasses metrics such as the Normalized Correlation Coefficient (NC), Structural Similarity Index (SSIM), Signal-to-Noise Ratio (SNR), among others. Notably, the NC index holds significant relevance in the domain of digital watermarking [41]. Hence, this paper adopts NC as the metric for assessing watermark correlation, with its calculation formula presented as Equation (23).

$$NC = \frac{\sum\limits_{i=1}^{M}\sum\limits_{j=1}^{N} XNOR(W(i,j), W'(i,j))}{M \times N} \quad (23)$$

In the equation, $W(i,j)$ and $W'(i,j)$ respectively, represent the original watermark information stored in the blockchain and the extracted watermark information from the infringing data, while $M \times N$ denotes the size of the copyright information. The XNOR operation involves performing a logical XOR operation on two pixels and then inverting the result.

The Normalized Correlation Coefficient (NC) serves as a metric for assessing similarity, ranging from 0 to 1. A higher NC value, approaching 1, signifies greater similarity between the extracted watermark and the original watermark. Following a comprehensive analysis of extensive datasets and referencing established practices in digital watermarking, this paper sets 0.75 as the optimal NC threshold for watermark extraction. This threshold effectively balances robustness and imperceptibility, ensuring reliable detection of watermarks under various conditions while maintaining minimal visual distortion, consistent with benchmarks reported in related studies [42].

5.2.3. Evaluation Index for Unique Identification Similarity

When assessing whether map data have been infringed upon, it is crucial to compare the similarity between the identifiers of the potentially infringing data and the original data to accurately match the unique identifiers. The assessment of unique identifier similarity primarily incorporates metrics such as Hamming distance (HD), signal-to-noise ratio (SNR), and bit error rate (BER). Among these, the bit error rate directly quantifies the error rate of unique identifiers during transmission or processing, offering an intuitive and straightforward measure of the similarity between unique identifiers. Consequently, this paper opts to use the bit error rate (BER) as the metric for evaluating similarity between two unique identifiers. Specifically, the bit error rate (BER) denotes the ratio of unequal values between the unique identifier in the blockchain identifier library and the constructed unique identifier to the total number of values, as depicted in Equation (16).

The bit error rate (BER) is a critical metric in evaluating the similarity between unique identifiers, with values ranging from 0 to 1. A higher BER signifies lower similarity between two unique identifiers, thereby reflecting the model's stronger uniqueness but potentially weaker robustness. Drawing on extensive experimental data, as well as insights from related studies such as those by Lu [43] and Num et al. [44], this paper determines a threshold of 0.1 for BER. Through initial experiments and benchmarking against other approaches, a threshold of 0.1 was established to strike an optimal balance between robustness and accuracy. When the BER remains below 0.1, the blockchain system can reliably and efficiently match unique identifiers, ensuring both effective copyright protection and practical applicability. This selection ensures a solid practical performance across diverse scenarios while aligning with theoretical considerations in digital watermarking and data integrity applications.

5.3. Experiment

This section is dedicated to comprehensively evaluating the performance of the BCPM-UI model through various experiments. Simultaneously, this paper selects a blockchain-based vector map copyright protection model [42] and three vector map unique identification construction methods [15,32,45] for comparison to underscore the advantages of this research. In particular, our blockchain storage experiments are compared with Ren's model, while the experiments related to unique identifier construction are compared with the methods proposed by Lee, Li, and Zhou. Among these, Ren's proposed blockchain-based vector map copyright protection model involves deploying vector maps entirely on the blockchain platform without utilizing the approach of replacing on-chain data with unique identifiers. Additionally, the unique identification construction methods differ significantly in their approach. Lee employs GMM clustering to derive multi-line curvature hashes from vector maps, generating final binary hashes through binarization. In contrast, Li integrates the spatial autocorrelation index (SAI) to combine spatial topology and geometric information for unique identification construction. Zhou, on the other hand, utilizes the neighborhood features of vector maps to construct unique identifiers. In this paper, the length of the unique identifiers was carefully selected as 1500 bits to balance uniqueness, computational efficiency, and storage requirements. This length is sufficient to ensure minimal collision probability while maintaining practicality in real-world applications. The choice was further informed by experimental data and theoretical considerations, highlighting its suitability for achieving precise and robust matching in diverse vector map datasets. Table 2 provides detailed experimental arrangements, including the selected vector map datasets and corresponding attack scenarios, to systematically validate the model's adaptability and robustness.

Table 2. Detailed summary of experiments.

Experiments Name	Attack Type	Vector Map Data
Vector map storage experiment	-	Chengdu dataset, Jiangsu dataset, Hangzhou dataset, Nanjing dataset
Uniqueness experiment	-	Shanghai dataset, Beijing dataset, Chengdu dataset, Jiangsu dataset, Hangzhou dataset

Table 2. *Cont.*

Experiments Name	Attack Type	Vector Map Data
Imperceptibility experiment	-	All datasets
Geometric attacks	Rotation Scaling Translation	Shanghai dataset, Jiangsu dataset
Cropping and merge attacks	Cropping Merging	Jiangsu dataset
Object attacks	Object addition Object deletion	
Layer attacks	Layer addition Layer deletion	
Format conversion attack	Dwg E00 Gdb	Chengdu dataset, Nanjing dataset, Shanghai dataset
Reordering attack	Reordering	Nanjing dataset

5.3.1. Storage Space of Vector Maps

This experiment aims to assess the space-saving effectiveness of unique identification compared to full map data in blockchain storage, ensuring the practical applicability of the model. Four map files are selected to ensure applicability across different maps, from which corresponding unique identifications are constructed. Initially, following Ren's comparative algorithm, full map data are deployed onto the blockchain. Subsequently, according to the proposed BCPM-UI model, unique identifications of vector maps are constructed and deployed onto the blockchain, recording the respective storage space requirements. A comparison of the storage space utilization between the two methods is conducted, and the experimental results are presented in Figure 9. Figure 9 shows that unique identifications with small data volumes exhibit significant space-saving effects compared to the use of full map data in blockchain storage. Using this method, for smaller-scale datasets, approximately 200 times more storage space can be saved, while for larger-scale datasets, around 5000 times more storage space can be conserved. The experiments demonstrate that the proposed BCPM-UI model effectively reduces the storage of map data in the blockchain.

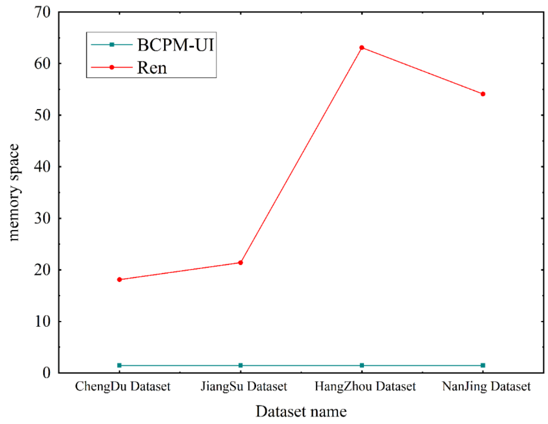


Figure 9. The amount of memory space occupied in the blockchain.

5.3.2. Uniqueness Experiment of Unique Identification

In this experiment, different data should result in entirely different unique identifications in order to prevent mutual denial between trading parties. Vector map unique identifications are constructed from six datasets using the method outlined in Section 4, and the correlation between every pair of data identifications is compared. We evaluate the correlation between two identifications using the bit error rate (BER). Generally, if the BER between two identifications is greater than 0.2, it indicates significant differences between them, implying substantial disparities in unique identifications at certain positions.

As shown in Table 3, the lowest BER is 0.34, suggesting considerable differences between the unique identifications. This could be attributed to variations in geographical features, changes in feature distribution, or other factors influencing unique identification. Moreover, it indicates that the unique identifications constructed through the BCPM-UI model possess strong uniqueness, enabling the differentiation of unique identifications constructed from different vector map datasets. This helps to prevent the erroneous matching of unique identification information in the blockchain.

Table 3. Uniqueness experiment results (BER).

Dataset	Shanghai	Beijing	Chengdu	Jiangsu	Hangzhou	Nanjing
Shanghai	0.00	0.42	0.39	0.42	0.38	0.39
Beijing	0.42	0.00	0.36	0.44	0.38	0.37
Chengdu	0.39	0.36	0.00	0.50	0.34	0.45
Jiangsu	0.42	0.44	0.50	0.00	0.50	0.42
Hangzhou	0.38	0.38	0.34	0.50	0.00	0.41
Nanjing	0.39	0.37	0.45	0.42	0.41	0.00

5.3.3. Imperceptibility Experiment of Vector Maps

In this experiment, imperceptibility refers to the embedding of watermark information not having an impact on the accuracy of the original vector map. Watermark embedding is conducted on various map datasets to obtain watermarked data. The coordinate errors between the watermarked data and the original data are statistically analyzed, including metrics such as maximum distance, mean value, and standard deviation. Figure 10 presents the maps after watermark embedding, while Table 4 presents the statistical results of the errors. From the error statistics, it is evident that the proposed BCPM-UI model ensures that the error introduced by watermark embedding remains well below the spatial accuracy requirement of the data (0.1 m). Moreover, the stable standard deviation values indicate that the errors are consistently maintained at a stable level without significant fluctuations. Therefore, the proposed BCPM-UI model exhibits excellent imperceptibility.

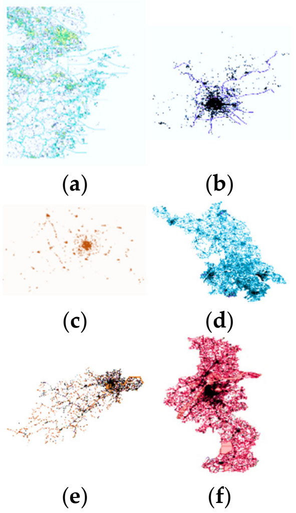


Figure 10. Watermarked vector map: (**a**) Shanghai dataset; (**b**) Beijing dataset; (**c**) Chengdu dataset; (**d**) Jiangsu dataset; (**e**) Hangzhou dataset; (**f**) Nanjing dataset.

Table 4. Error statistics of data.

Watermarked Vector Map	Data Accuracy	Error Index		
		Maximum Distance	Mean Distance	Standard Deviation
Shanghai dataset	0.1 m	3.20×10^{-4} m	1.61×10^{-5} m	6.54×10^{-6} m
Beijing dataset	0.1 m	4.00×10^{-4} m	2.94×10^{-5} m	2.28×10^{-5} m
Chengdu dataset	0.1 m	3.70×10^{-4} m	2.03×10^{-5} m	1.42×10^{-5} m
Jiangsu dataset	0.1 m	2.75×10^{-4} m	1.35×10^{-5} m	5.80×10^{-6} m
Hangzhou dataset	0.1 m	2.85×10^{-4} m	1.69×10^{-5} m	7.34×10^{-6} m
Nanjing dataset	0.1 m	4.02×10^{-4} m	2.67×10^{-5} m	2.02×10^{-5} m

5.3.4. Robustness Experiment

Robustness is a critical property that measures a model's ability to maintain the integrity of both the unique identifiers and the embedded copyright information under intentional or accidental tampering. To comprehensively evaluate the robustness of the proposed BCPM-UI model, extensive experiments were conducted across six diverse vector map datasets: the Shanghai dataset, Beijing dataset, Chengdu dataset, Jiangsu dataset, Hangzhou dataset, and Nanjing dataset. These datasets encompass varying geographic features and complexities, providing a rigorous validation of the model's robustness. The experiments systematically assessed the model's performance under various attack scenarios, including geometric transformations [46], object addition or deletion, layer modification, cropping and merging, format conversion, and reordering attacks. Both the robustness of the unique identifiers and the accurate extraction of copyright information were evaluated to ensure comprehensive protection.

To test robustness against geometric transformations, experiments were designed to evaluate the effects of rotation, scaling, and translation (RST). These transformations are common in GIS applications, such as coordinate system adjustments or data visualization. The rotation experiment applied increments of 30°, ranging from 30° to 150°. Translation experiments shifted data in 100 m intervals up to 300 m, while scaling experiments adjusted data from 60% to 140% of the original size in 20% increments. The results, presented in Figure 11a–c, demonstrate that the BCPM-UI model achieved a bit error rate (BER) of 0 and a normalized correlation (NC) value of 1 across all transformations. These findings confirm that the model is invariant to geometric manipulation, ensuring robustness in practical GIS scenarios that involve frequent RST operations.

Object addition or deletion simulates the dynamic evolution of geographic data, where features such as points, lines, and polygons may be modified [47]. To emulate real-world changes, the experiments incrementally added or deleted 10% to 50% of objects in the map. Figure 11d,e and Table 5 show that as the proportion of objects added or deleted increased, the BER rose across all models. However, the BCPM-UI model exhibited the slowest increase in BER. This was attributable to its use of geometric feature parameters, which quantify angular relationships among spatial features, and topological feature parameters, which calculate overall correlations. These features remain largely unaffected by object-level modifications, ensuring resilience against such tampering.

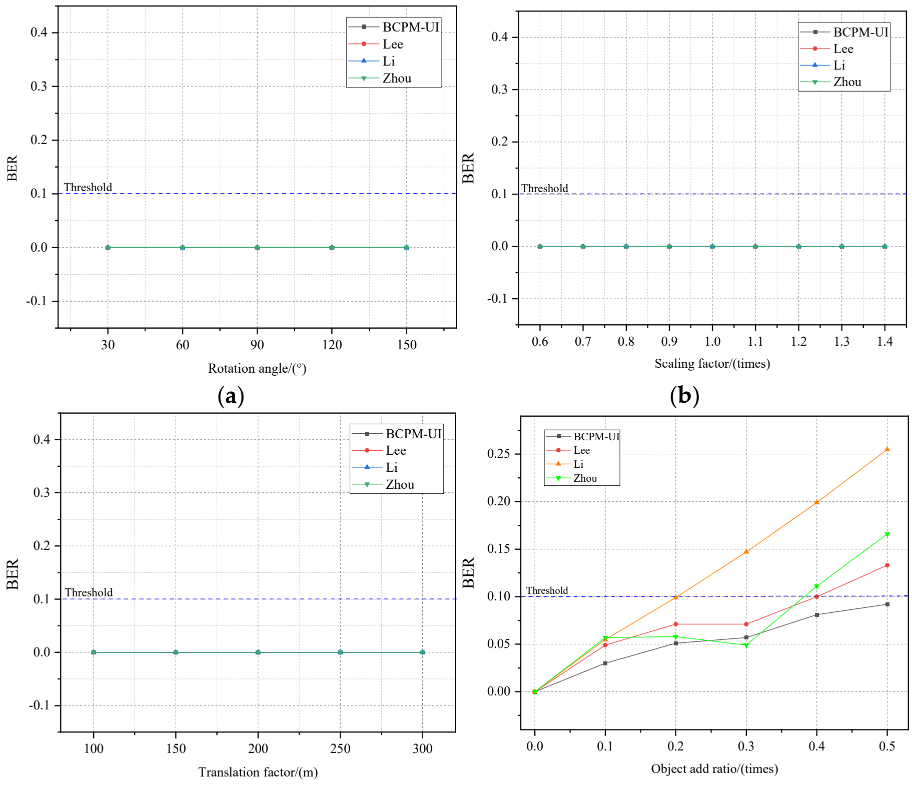
Layer attacks, which involve adding or removing one to five layers, assess the model's sensitivity to structural changes in GIS data. These modifications are common in GIS workflows and involve events such as merging datasets or updating map layers. Figure 11f,g and Table 5 reveal that while the BER increased with the addition or removal of more layers, the BCPM-UI model demonstrated the most gradual increase. Even after the removal of five layers, the BCPM-UI model maintained a BER below 0.1, meeting robustness requirements for unique identification. This resilience stems from the geometric and topological parameters, which are designed to handle the global relationships between layers, mitigating the impact of layer-level changes.

Table 5. Experimental results of layer addition and deletion attacks.

Dataset	Degree of Attack	BER	NC	Unique Identification Match Result
	Add 50%	0.09	0.93	Match
	Delete 50%	0.09	0.90	Match
	Add 5 layers	0.10	0.96	Match
	Delete 5 layers	0.10	0.88	Match
	Cropping 50%	0.06	0.91	Match
	Merge 50%	0.05	0.91	Match

Cropping and merging operations are frequently performed in GIS when focusing on specific regions or integrating datasets [48]. Experiments incrementally applied these operations at 10% intervals, ranging from 10% to 50%. The results, shown in Figure 11h,i and Table 5, indicate that although BER increased with higher cropping and merging ratios, the BCPM-UI and Lee's models exhibited the slowest growth. This robustness is due to the model's reliance on geometric and topological invariants, which remain stable under partial data modifications.

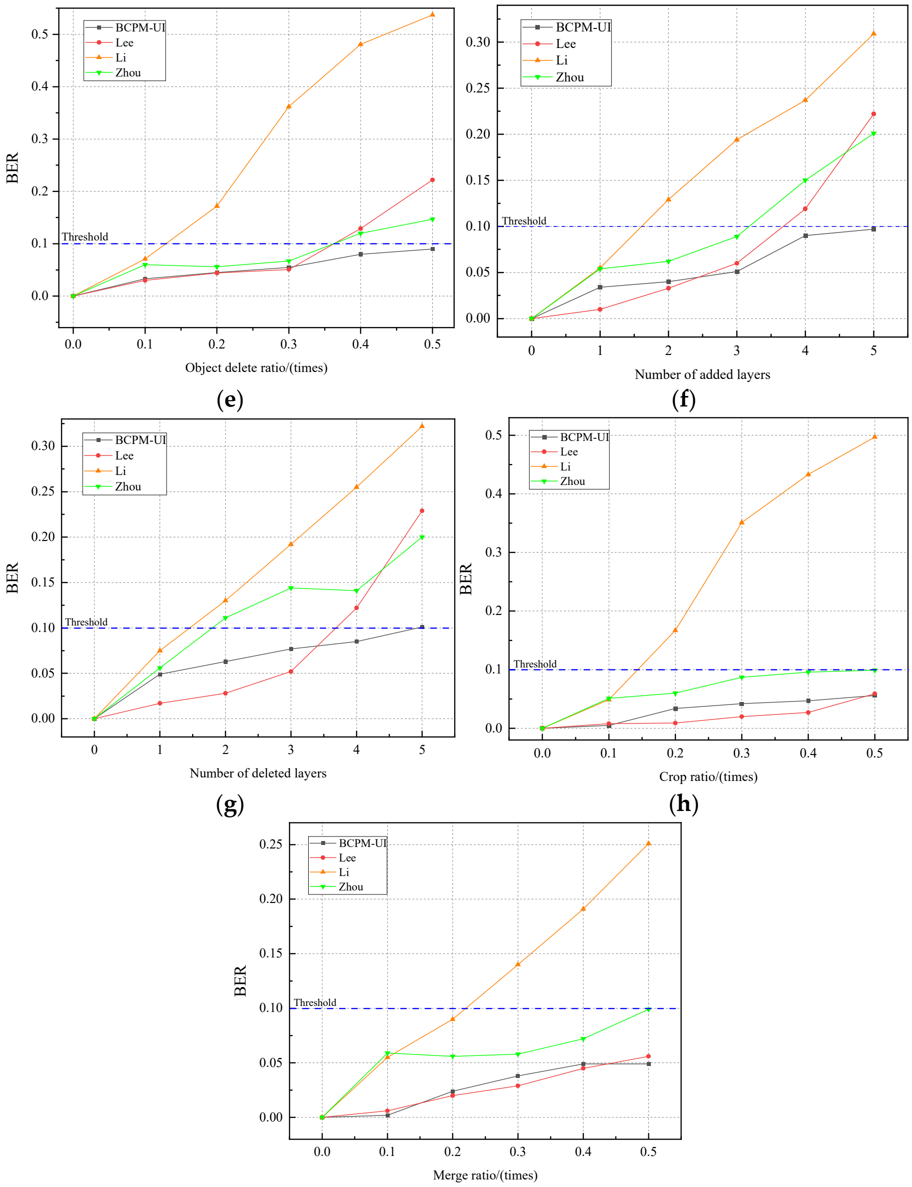
Format conversion is a practical consideration for GIS platforms, where data interoperability often requires conversion between formats. Watermarked maps were converted into DWG, E00, and GDB formats and reverted to Shapefile format for extraction. Table 6 summarizes the results, showing that unique identifiers and watermark information were successfully retrieved in all cases. The NC values consistently remained at 1, and BER values stood at 0, demonstrating robustness across diverse formats.



(**a**) (**b**)

(**c**) (**d**)

Figure 11. *Cont.*



(**e**) (**f**) (**g**) (**h**) (**i**)

Figure 11. Robustness experiment results: (**a**) rotation attack; (**b**) scaling attack; (**c**) translation attack; (**d**) object-add attack; (**e**) object-delete attack; (**f**) layer-add attack; (**g**) layer-delete attack; (**h**) cropping attack; (**i**) merge attack.

Table 6. The robustness results of format conversion attacks.

Data Format	NC			BER		
	Chengdu Dataset	Nanjing Dataset	Shanghai Dataset	Chengdu Dataset	Nanjing Dataset	Shanghai Dataset
dwg	1.00	1.00	1.00	0.00	0.00	0.00
e00	1.00	1.00	1.00	0.00	0.00	0.00
gdb	1.00	1.00	1.00	0.00	0.00	0.00

Reordering attacks simulate scenarios where the storage order of geographic features is altered [49], a frequent occurrence during data processing or transmission. The BCPM-UI model embeds watermarks and constructs unique identifiers based on index positions and values, rendering it immune to such alterations. The experimental results confirmed that reordering geographic features had no impact on the constructed identifiers or watermarks, with NC values consistently at 1.

The rationale behind selecting these specific tampering scenarios lies in their prevalence and relevance to real-world GIS applications. Geometric transformations, object and layer modifications, cropping, merging, format conversions, and reordering represent common operations and potential attack vectors in GIS workflows. By addressing these challenges, the BCPM-UI model demonstrates its robustness and adaptability, making it suitable for reliable unique identification and copyright protection in complex and dynamic GIS environments.

5.3.5. Computational Complexity Analysis

The computational complexity of the proposed BCPM-UI model is a critical aspect of its evaluation, particularly when processing vector maps with intricate structures and large numbers of elements. This section examines the model's performance through an analysis of copyright registration and verification times across six datasets, as summarized in Table 7.

Table 7. The results of efficiency comparison experiments.

Name of Vector Map	Quantity of Map Layers			Quantity of Features	Registration Time (s)	Verification Time (s)
	Point Layer	Line Layer	Polygon Layer			
Shanghai dataset	1	1	1	6214	66.9	65.7
Beijing dataset	2	1	1	16,343	80.4	80.2
Chengdu dataset	3	1	1	18,769	101.7	105.1
Jiangsu dataset	2	2	1	22,168	112.4	108.0
Hangzhou dataset	9	4	2	64,810	166.0	157.6
Nanjing dataset	10	6	3	53,660	188.0	180.9

The experimental results reveal that the time required for registration and verification tasks increases with the complexity of the vector map, as indicated by the number of layers and features. For relatively simple datasets, such as the Shanghai dataset, with 6214 features distributed across one point layer, one line layer, and one polygon layer, the registration and verification times are 66.9 s and 65.7 s, respectively. In contrast, for the more complex Nanjing dataset, which contains 10 point layers, 6 line layers, and 3 polygon layers encompassing 53,660 features, these tasks take 188.0 s and 180.9 s, respectively.

The scalability of the model is further evidenced by the near-linear growth of processing times with the increase in the number of features. This suggests that the proposed algorithm is capable of accommodating datasets of varying sizes and complexities without significant performance degradation. Nevertheless, further efforts to optimize the model are warranted. Future work will explore the use of parallel processing techniques to accelerate feature extraction and watermark embedding.

To further clarify the distinctions between the proposed method (BCPM-UI) and existing approaches, Table 8 provides a detailed comparison in terms of blockchain storage capacity and the robustness of feature identifiers against various attack scenarios. As shown in the table, the proposed model achieves minimal blockchain storage usage while exhibiting robust resistance to geometric attacks, feature addition/deletion, layer addition/deletion, and cropping and merging attacks. In contrast, Ren's blockchain-based model incurs significant storage requirements due to the lack of an off-chain mechanism for data management. Among the identifier construction methods, Lee, Li, and Zhou's approaches demonstrate resilience to geometric attacks, but only BCPM-UI effectively addresses the challenges posed by feature and layer modifications. These results underscore the comprehensive adaptability and efficiency of the proposed model for real-world vector map copyright protection.

Table 8. Comparison between the BCPM-UI model and the contrast model.

Model	Blockchain Storage Capacity	Robustness to Geometric Attacks	Robustness to Feature Addition/Deletion	Robustness to Layer Addition/Deletion	Robustness to Cropping and Merging Attacks
BCPM-UI	Minimal	Yes	Yes	Yes	Yes
Ren	Significant	N/A	N/A	N/A	N/A
Lee	N/A	Yes	No	No	Yes
Li	N/A	Yes	No	No	No
Zhou	N/A	Yes	No	No	Yes

6. Discussion

6.1. Impact of Character Length on the Uniqueness and Robustness of Unique Identification

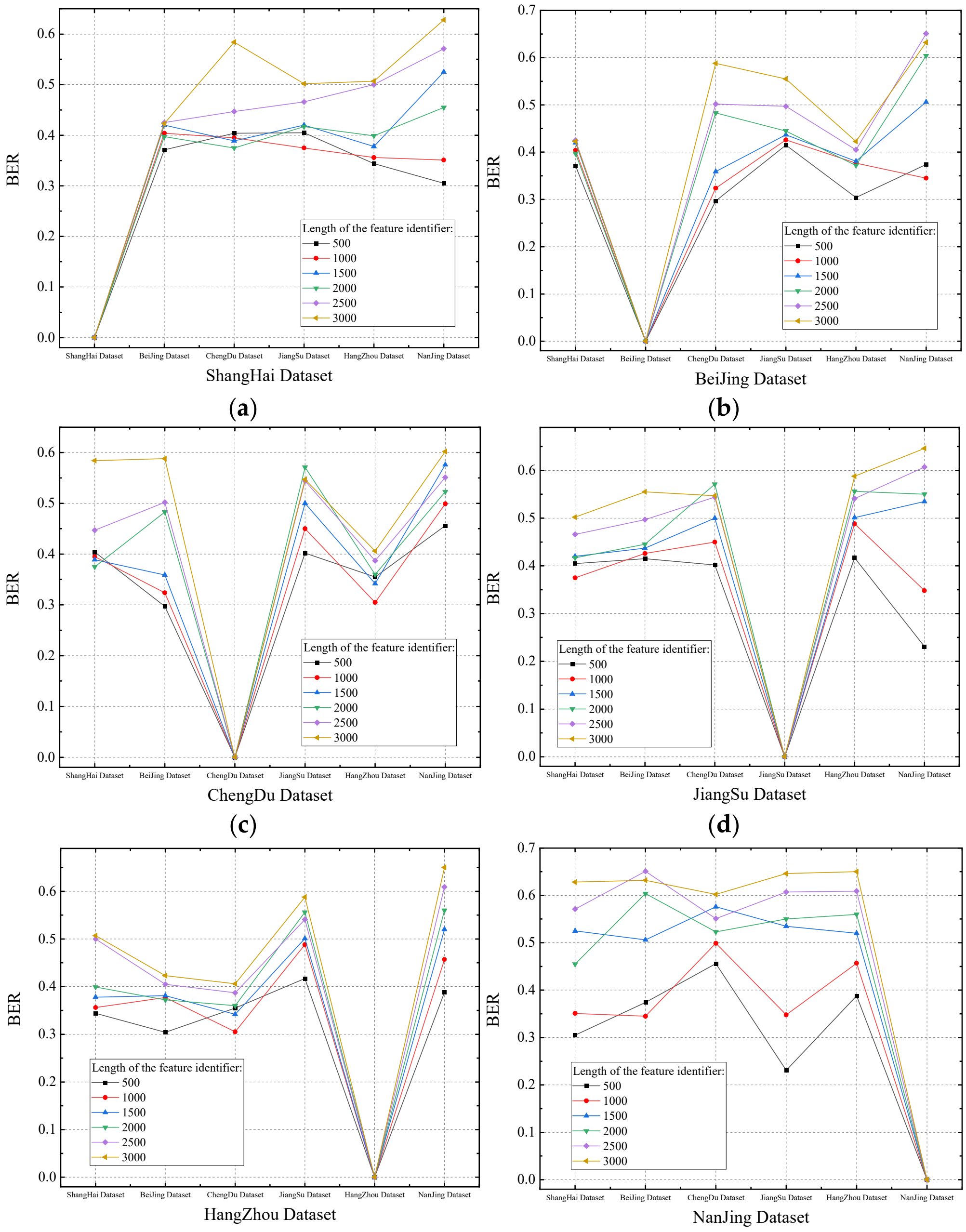
In Section 5, a unique identifier length of 1500 is selected. However, different lengths of unique identifiers demonstrate varying degrees of uniqueness and robustness. This section delves into the impact of character length on the uniqueness and robustness of unique identifiers to ascertain the appropriate range for constructing such identifiers.

Initially, uniqueness experiments are conducted, wherein unique identifiers of different lengths are generated for six datasets, encompassing character lengths of 500, 1000, 1500, 2000, 2500, and 3000. Subsequently, the bit error rate (BER) between unique identifiers of varying lengths for each dataset is computed to assess the uniqueness. The experimental findings, illustrated in Figure 12, reveal that as the length of unique identifiers increases, the BER values between pairs of identifiers gradually rise. This indicates that the identifiers become increasingly dissimilar, reflecting stronger uniqueness and distinctiveness, which are essential for ensuring reliable copyright protection and differentiation.

Similarly, robustness experiments are conducted. This involves unique identifiers of various character lengths, ranging from 500 to 3000 characters, across the same datasets. Various degrees of attacks, such as cropping, feature deletion, and layer deletion, are applied to these identifiers. The BER values between the constructed unique identifiers from the disrupted data and the original unique identifiers are then calculated to evaluate robustness. As depicted in Figure 13, the results indicate that as the character length of unique identifiers increases, the BER values also escalate, implying diminished robustness.

Analysis derived from the uniqueness and robustness experiments suggests that overly short character sequences may result in identical sequences across different map areas, thus compromising uniqueness. This occurs because identical feature sequences might manifest in diverse map areas, posing challenges in accurately distinguishing between geographical locations. Additionally, short sequences may fail to encapsulate the intricate structures and features of vector maps adequately, potentially leading to critical information loss during unique identifier generation. Conversely, longer sequences are more susceptible to noise, deformation, and environmental changes, thereby reducing robustness. Prolonged sequences may excessively react to minor variations, deeming slight differences in geographical locations as significant.

Therefore, to strike a balance between uniqueness and robustness, it is imperative to select a moderately sized character sequence length. This ensures the precise identification of distinct map areas while maintaining the requisite level of robustness against noise and variations. Based on a comprehensive analysis of the experimental outcomes, performed from Figures 12 and 13, it is concluded that unique identifiers spanning a character length of 1500–2000 meet the criteria for both uniqueness and robustness. Hence, they are deemed suitable for deployment on blockchain platforms.



(**a**) (**b**) (**c**) (**d**) (**e**) (**f**)

Figure 12. Experimental results of uniqueness between datasets with different unique identification lengths: (**a**) Shanghai dataset; (**b**) Beijing dataset; (**c**) Chengdu dataset; (**d**) Jiangsu dataset; (**e**) Hangzhou dataset; (**f**) Nanjing dataset.

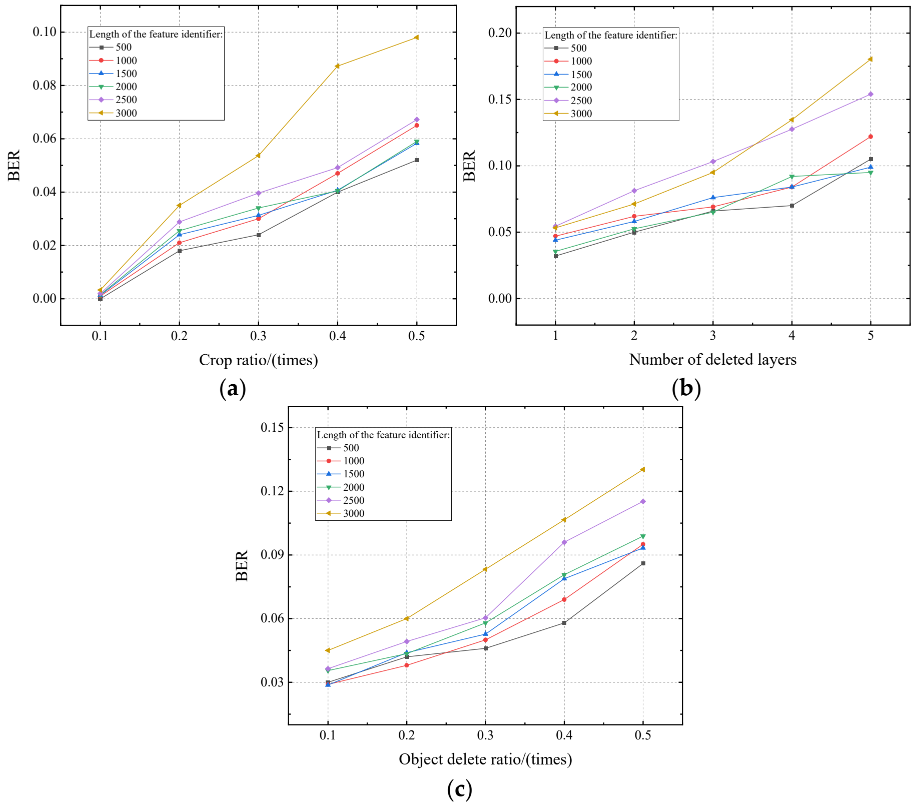


Figure 13. Experimental results of robustness with different unique identification length: (**a**) cropping attack; (**b**) layer-delete attack; (**c**) object-delete attack.

6.2. Applicability of the BCPM-UI Model to Small-Scale Vector Maps

In small-scale vector map datasets, typically comprising limited data such as essential geographic features like roads, water bodies, and buildings, the representation tends to be less detailed [50]. These datasets are commonly utilized in straightforward applications like route planning and location positioning. In this paper, we discovered that the BCPM-UI model not only suits large-scale vector map datasets with high precision but also proves effective for small-scale ones.

In this section, we conducted experiments using local vector map datasets from Chongqing and Xi’an to showcase the algorithm’s adaptability to small-scale datasets. The Chongqing dataset encompasses 450 features, while the Xi’an dataset includes 1012 features, as depicted in Figure 14. The constructed unique identifiers have a length of 1500.

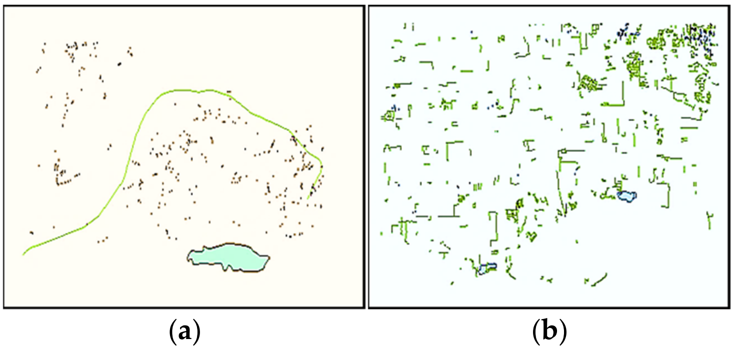


Figure 14. Vector map dataset with small data volume: (**a**) Chongqing dataset; (**b**) Xi’an dataset.

Figure 15 exhibits the BER of the model under various types of attacks. Notably, even in the face of varying degrees of RST, object deletion, and cropping attacks, the BER values remain below the 0.10 threshold. These experimental findings underscore the significant applicability of the BCPM-UI model in handling small-scale vector map datasets. This offers valuable insights into exploring and researching watermark algorithms tailored for such datasets and lays a theoretical groundwork for developing more sophisticated and efficient copyright protection models for small-scale vector map datasets in the future.

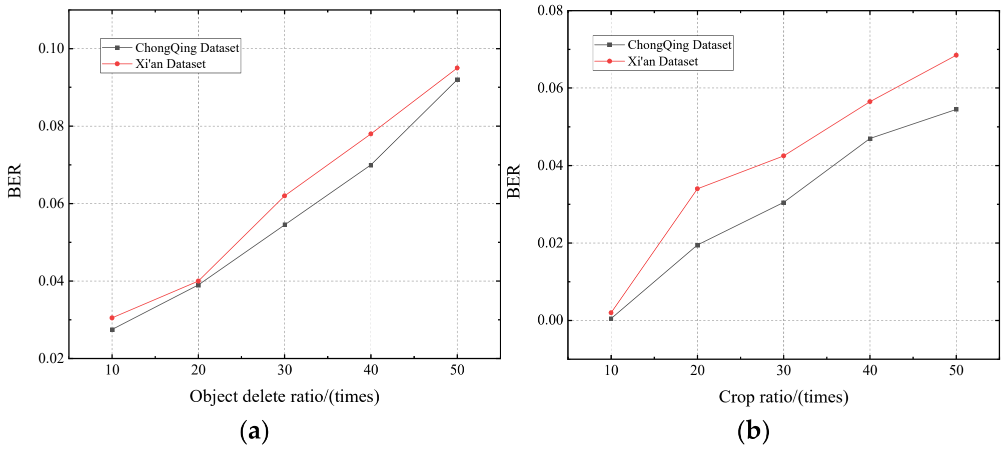


Figure 15. Experimental results of robustness under vector maps with small data volume: (**a**) object-delete attack; (**b**) cropping attack.

7. Conclusions

This paper introduces a blockchain-based copyright protection model for vector maps, termed BCPM-UI. In this model, copyright information is embedded into vector maps through a distance ratio quantization-based watermark embedding algorithm, and unique identifiers are constructed using topological and geometric feature parameters. These unique identifiers, along with watermark information, timestamps, and user details, are securely registered on a blockchain platform. To address potential infringement, a bit error rate-based unique identification matching algorithm is proposed to compare the unique identifiers of suspected infringing data with those stored on the blockchain. Experimental results validate the proposed model's strong uniqueness and robustness, fulfilling data privacy protection requirements. Beyond technical robustness, the BCPM-UI model provides significant societal and environmental benefits by enhancing the security and traceability of geospatial data, which is critical in applications such as urban planning, disaster management, and environmental monitoring. By ensuring reliable copyright protection and data integrity, the model contributes to fostering trust in geospatial data sharing, thus promoting the sustainable and ethical utilization of geospatial resources.

Future research will address the challenge of blockchain's high storage costs by further reducing the data volume of watermark information. As watermark information often necessitates network-wide validation and traceability, future work will focus on developing lightweight watermarking algorithms that minimize computational complexity and on-chain data, enhancing the overall efficiency and scalability of the proposed system. Furthermore, integrating advanced privacy-preserving techniques, such as homomorphic encryption and zero-knowledge proofs, will be explored to reinforce the confidentiality of geospatial data in collaborative environments.

Author Contributions: Conceptualization, Heyan Wang, Nannan Tang and Na Ren; methodology, Heyan Wang, Changqing Zhu and Na Ren; validation, Heyan Wang, Changqing Zhu and Na Ren; formal analysis, Heyan Wang and Changqing Zhu; writing—original draft preparation, Heyan Wang; writing—review and editing, Heyan Wang, Na Ren and Nannan Tang; visualization, Heyan Wang

and Changqing Zhu; supervision, Na Ren, Changhong Wang and Nannan Tang; funding acquisition, Na Ren. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key Research and Development Program of China (No. 2023YFB3907100), the National Natural Science Foundation of China (No. 42471440), and the Hunan Provincial Natural Science Foundation of China (No. 2024JJ8360). Thanks to our project partners and sponsors for their support.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Luo, L.; Hou, X.; Cai, W.; Bin, G. Incremental route inference from low-sampling GPS data: An opportunistic approach to online map matching. *Inf. Sci.* **2020**, *512*, 1407–1423. [CrossRef]
2. Zhou, Q.; Ren, N.; Zhu, C.; Zhu, A. Blind digital watermarking algorithm against projection transformation for vector geographic data. *ISPRS Int. J. Geo-Inf.* **2020**, *9*, 692. [CrossRef]
3. Ren, N.; Zhou, Q.; Zhu, C.; Zhu, A.; Chen, W. A lossless watermarking algorithm based on line pairs for vector data. *IEEE Access* **2020**, *8*, 156727–156739. [CrossRef]
4. Ren, N.; Tong, D.; Cui, H.; Zhu, C.; Zhou, Q. Congruence and geometric feature-based commutative encryption-watermarking method for vector maps. *Comput. Geosci.* **2022**, *159*, 105009. [CrossRef]
5. Guo, S.; Zhu, S.; Zhu, C.; Ren, N.; Tang, W.; Xu, D. A robust and lossless commutative encryption and watermarking algorithm for vector geographic data. *J. Inf. Secur. Appl.* **2023**, *75*, 103503. [CrossRef]
6. Xi, X.; Zhang, X.; Liang, W.; Xin, Q.; Zhang, P. Dual zero-watermarking scheme for two-dimensional vector map based on delaunay triangle mesh and singular value decomposition. *Appl. Sci.* **2019**, *9*, 642. [CrossRef]
7. Qiu, Y.; Sun, J.; Zheng, J. A Self-Error-Correction-Based Reversible Watermarking Scheme for Vector Maps. *ISPRS Int. J. Geo-Inf.* **2023**, *12*, 84. [CrossRef]
8. Lin, Z.; Peng, F.; Long, M. A Low-Distortion Reversible Watermarking for 2D Engineering Graphics Based on Region Nesting. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2372–2382. [CrossRef]
9. Meng, Z.; Morizumi, T.; Miyata, S.; Kinoshita, H. Design Scheme of Copyright Management System Based on Digital Watermarking and Blockchain. In Proceedings of the IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 23–27 July 2018; pp. 359–364.
10. Ma, Z.; Jiang, M.; Gao, H.; Wang, Z. Blockchain for digital rights management. *Future Gener. Comput. Syst.* **2018**, *89*, 746–764. [CrossRef]
11. Xu, D.; Ren, N.; Zhu, C. Integrity Authentication Based on Blockchain and Perceptual Hash for Remote-Sensing Imagery. *Remote Sens.* **2023**, *15*, 4860. [CrossRef]
12. Ren, N.; Zhao, Y.; Zhu, C.; Zhou, Q.; Xu, D. Copyright Protection Based on Zero Watermarking and Blockchain for Vector Maps. *ISPRS Int. J. Geo-Inf.* **2021**, *10*, 294. [CrossRef]
13. Zhou, C.; Lu, H.; Xiang, Y.; Wu, J.; Wang, F. Geohashtile: Vector geographic data display method based on geohash. *Int. J. Geo-Inf.* **2020**, *9*, 418. [CrossRef]
14. Lee, S.; Kwon, S.; Kwon, K. Robust hashing of vector data using generalized curvatures of polyline. *IEICE Trans. Inf. Syst.* **2013**, *96*, 1105–1114. [CrossRef]
15. Lee, S.; Hwang, W.; Kwon, K. Polyline curvatures based robust vector data hashing. *Multimed. Tools Appl.* **2014**, *73*, 1913–1942. [CrossRef]
16. Wang, B.; Shi, J.; Wang, W.; Zhao, P. Image Copyright Protection Based on Blockchain and Zero-Watermark. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 2188–2199. [CrossRef]
17. Yu, F.; Peng, J.; Li, X.; Li, C.; Qu, B. A Copyright-Preserving and Fair Image Trading Scheme Based on Blockchain. *Tsinghua Sci. Technol.* **2023**, *28*, 849–861. [CrossRef]
18. Lizama, M.G.; Huesa, J.; Claudio, B.M. Use of Blockchain technology for the exchange and secure transmission of medical images in the cloud: Systematic Review with Bibliometric Analysis. *ASEAN J. Sci. Eng.* **2024**, *4*, 7. [CrossRef]
19. Xu, D.; Ren, N.; Zhu, C. High-Resolution Remote Sensing Image Zero-Watermarking Algorithm Based on Blockchain and SDAE. *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.* **2024**, *17*, 323–339. [CrossRef]
20. Zhu, C.; Xu, D.; Ren, N.; Cui, H.; Zhao, Y. Model and implementation of geographic data transaction certificate and copyright protection based on blockchain and digital watermarking. *Acta Geod. Cartogr. Sin.* **2021**, *50*, 1694–1704.

21. Liu, H.; Yan, F.; Tian, H. A Vector Map of Carbon Emission Based on Point-Line-Area Carbon Emission Classified Allocation Method. *Sustainability* **2020**, *12*, 10058. [CrossRef]
22. Da, Q.; Sun, J.; Zhang, L.; Kou, L.; Wang, W.; Han, Q.; Zhou, R. A novel hybrid information security scheme for 2D vector map. *Mob. Netw. Appl.* **2018**, *23*, 734–742. [CrossRef]
23. Wang, S.; Zhang, L.; Li, Y.; Qin, R.; Zhang, Q. A zero-watermarking algorithm of vector geographic data using singular value decomposition. *Sci. Surv. Mapp.* **2022**, *47*, 196–203.
24. Li, W.; Yan, H.; Wang, Z.; Zhang, L.; Lu, X. A zero-watermarking algorithm for vector geo-spatial data based on logistic chaotic mapping and DFT. *Sci. Surv. Mapp.* **2017**, *42*, 143–148.
25. Xi, X.; Hua, Y.; Chen, Y.; Zhu, Q. Zero-Watermarking for Vector Maps Combining Spatial and Frequency Domain Based on Constrained Delaunay Triangulation Network and Discrete Fourier Transform. *Entropy* **2023**, *25*, 682. [CrossRef] [PubMed]
26. Wang, S.; Zhang, L.; Zhang, Q.; Li, Y. A zero-watermarking algorithm for vector geographic data based on feature invariants. *Earth Sci. Inform.* **2023**, *16*, 1073–1089. [CrossRef]
27. Peng, F.; Jiang, W.; Qi, Y.; Lin, Z.; Long, M. Separable Robust Reversible Watermarking in Encrypted 2D Vector Graphics. *IEEE Trans. Circuits Syst. Video Technol.* **2020**, *30*, 2391–2405. [CrossRef]
28. Peng, Y.; Yue, M. A zero-watermarking scheme for vector map based on feature vertex distance ratio. *J. Electr. Comput. Eng.* **2015**, *2015*, 421529. [CrossRef]
29. Lyu, W.; Zhang, L. A zero-watermark algorithm for vector data based on distribution center. *Eng. Surv. Mapp.* **2017**, *26*, 50–53+61.
30. Xi, X.; Zhang, X.; Sun, Y.; Jiang, X.; Xin, Q. Topology-Preserving and Geometric Feature-Correction Watermarking of Vector Maps. *IEEE Access* **2020**, *8*, 33428–33441. [CrossRef]
31. Ren, N.; Guo, S.; Zhu, C.; Hu, Y. A zero-watermarking scheme based on spatial topological relations for vector dataset. *Expert Syst. Appl.* **2023**, *226*, 120217. [CrossRef]
32. Li, A.; Zhu, A. Copyright authentication of digital vector maps based on spatial autocorrelation indices. *Earth Sci. Inform.* **2019**, *12*, 629–639. [CrossRef]
33. Khan, P.; Byun, Y. A blockchain-based secure image encryption scheme for the industrial Internet of Things. *Entropy* **2020**, *22*, 175. [CrossRef] [PubMed]
34. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F.Y. Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 2266–2277. [CrossRef]
35. Xu, Y.; Zhang, C.; Zeng, Q.; Wang, G.; Ren, J.; Zhang, Y. Blockchain-Enabled Accountability Mechanism Against Information Leakage in Vertical Industry Services. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 1202–1213. [CrossRef]
36. Abrar, A.; Abdul, W.; Ghouzali, S. Secure Image Authentication Using Watermarking and Blockchain. *Intell. Autom. Soft Comput.* **2021**, *28*, 577–591. [CrossRef]
37. Wang, B.; Shi, J.; Wang, W.; Zhao, P. A Blockchain-based System for Secure Image Protection Using Zero-watermark. In Proceedings of the IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems, Delhi, India, 10–13 December 2020; pp. 62–70.
38. Zou, W.; Long, R.; Zhang, Y.; Liao, M.; Zhou, Z.; Tian, S. Dual geometric perception for cross-domain road segmentation. *Displays* **2023**, *76*, 102332. [CrossRef]
39. Deng, M.; Li, C.; Liu, W. Describing spatial relations between area objects via combining topology with metrization. *Acta Geod. Cartogr. Sin.* **2002**, *31*, 164–169.
40. Chen, J.; Li, C.; Li, Z.; Gold, C. A Voronoi-based 9-intersection model for spatial relations. *Int. J. Geogr. Inf. Sci.* **2001**, *15*, 201–220. [CrossRef]
41. Abubahia, A.; Cocea, M. Evaluating the topological quality of watermarked vector maps. *Appl. Soft Comput.* **2018**, *71*, 849–860. [CrossRef]
42. Ren, N.; Wang, H.; Chen, Z.; Zhu, C.; Gu, J. A multilevel digital watermarking protocol for vector geographic data based on blockchain. *J. Geovisualization Spat. Anal.* **2023**, *7*, 31. [CrossRef]
43. Lu, C.; Hsu, C. Near-optimal watermark estimation and its countermeasure: Antidisclosure watermark for multiple watermark embedding. *IEEE Trans. Circuits Syst. Video Technol.* **2007**, *17*, 454–467. [CrossRef]
44. Nam, S.; Mun, S.; Ahn, W.; Kim, D.; Yu, I.; Kim, W.; Lee, H. NSCT-based robust and perceptual watermarking for DIBR 3D images. *IEEE Access* **2020**, *8*, 93760–93781. [CrossRef]
45. Zhou, Q.; Zhu, C.; Ren, N.; Chen, W.; Gong, W. Zero watermarking algorithm for vector geographic data based on the number of neighboring features. *Symmetry* **2021**, *13*, 208. [CrossRef]
46. Wang, N.; Zhao, X.; Xie, C. RST invariant reversible watermarking for 2D vector map. *Int. J. Multimed. Ubiquitous Eng.* **2016**, *11*, 265–276. [CrossRef]
47. Li, Y.; Zhang, L.; Wang, X.; Zhang, X.; Zhang, Q. A Novel Invariant Based Commutative Encryption and Watermarking Algorithm for Vector Maps. *ISPRS Int. J. Geo-Inf.* **2021**, *10*, 718. [CrossRef]

48. Wang, Y.; Yang, C.; Ding, K. Multiple watermarking algorithms for vector geographic data based on multiple quantization index modulation. *Appl. Sci.* **2023**, *13*, 12390. [CrossRef]
49. Zhou, Q.; Ren, N.; Zhu, C.; Tong, D. Storage feature-based watermarking algorithm with coordinate values preservation for vector line data. *KSII Trans. Internet Inf. Syst. (TIIS)* **2018**, *12*, 3475–3496.
50. Tong, D.; Zhu, C.; Ren, N. Watermarking algorithm applying to small amount of vector geographical data. *Acta Geod. Cartogr. Sin.* **2018**, *47*, 1518.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.