Cole-Puli International Conference Publishing Group

Business and Social Sciences Proceedings

Article

2025 2nd International Conference on Education, Economics, Management, and Social Sciences (EMSS 2025)

Research on Digital Watermarking Model and Algorithm for Vector Geographic Data

Dongyun Chu [1,*]

[1] The College of Arts and Sciences, The Ohio State University, Ohio, 43201, USA
* Correspondence: Dongyun Chu, The College of Arts and Sciences, The Ohio State University, Ohio, 43201, USA

Abstract: With the widespread application of geographic information technology, the copyright protection and integrity verification of vector data have become core issues that need to be addressed urgently. Traditional digital watermarking technology has mature applications in the field of raster data, but due to the complex geometric features and sensitive topological relationships of vector data, existing methods struggle to balance invisibility and robustness. This research focuses on the spatial characteristics of vector geographic data and proposes a watermarking model based on an adaptive embedding strategy. By integrating a multi-level feature selection mechanism, a watermark generation framework that takes both capacity and stability into account is constructed, and an anti-attack optimization algorithm is designed to deal with real-world threats such as geometric transformation and format migration. Experiments show that this model significantly improves the imperceptibility of the watermark while ensuring data accuracy, providing new technical support for geographic information security.

Keywords: vector; geographic data; digital watermarking model; algorithmic study

1. Introduction

Geographic information data, as a fundamental resource in fields such as smart cities and environmental monitoring, has an increasingly urgent need for security protection. Vector data describes spatial entities with coordinate sequences, and its structural characteristics cause traditional watermarking algorithms to easily fail during data editing, restricting the capabilities of copyright tracing and tampering detection. Existing research mostly focuses on watermark embedding in single-attack scenarios, lacking a comprehensive defense mechanism against multi-dimensional attacks and having significant limitations in maintaining data accuracy. This paper innovatively constructs a hierarchical embedding model. By analyzing the spatial distribution characteristics of vector elements, a dynamic weight distribution mechanism is established to enable watermark information to be adaptively embedded into key geometric nodes. In response to the frequency-domain perturbation characteristics of format conversion attacks, a topological constraint verification algorithm is introduced to break through the technical bottlenecks of existing methods in cross-platform applications [1]. Through systematic algorithm design, this research achieves precise regulation of watermark embedding strength and data fidelity.

Received: 18 May 2025
Revised: 30 May 2025
Accepted: 19 July 2025
Published: 08 July 2025

2. Vector Geographic Data Watermarking Model Design

2.1. Watermark Generation Model

The core of the watermark generation model lies in transforming the copyright identifier into digital features with anti-tampering ability and high robustness. Based on the irreversible characteristic of the hash function, the SHA-256 algorithm is used to perform one-way encryption on the copyright information to generate a fixed-length digest sequence. The SHA-256 algorithm is a hash algorithm based on the Merkle-Damgård structure, which converts input data of any length into a fixed-length (256-bit) hash value through a series of complex mathematical operations, and its principle is shown in Figure 1. This process confuses the statistical distribution of the original identifier to ensure that attackers cannot obtain valid information through reverse engineering. Meanwhile, the uniqueness of the hash value provides a verifiable basis for copyright ownership. On this basis, in response to the local distortion that may occur during the transmission and editing of vector data, a Reed-Solomon error-correction coding mechanism is introduced to enhance the fault-tolerance ability of the watermark by adding redundant check bits. The coding parameters are dynamically adjusted according to the data characteristics to balance the error-correction efficiency and embedding capacity and avoid the decrease of watermark invisibility caused by excessive redundancy [2].

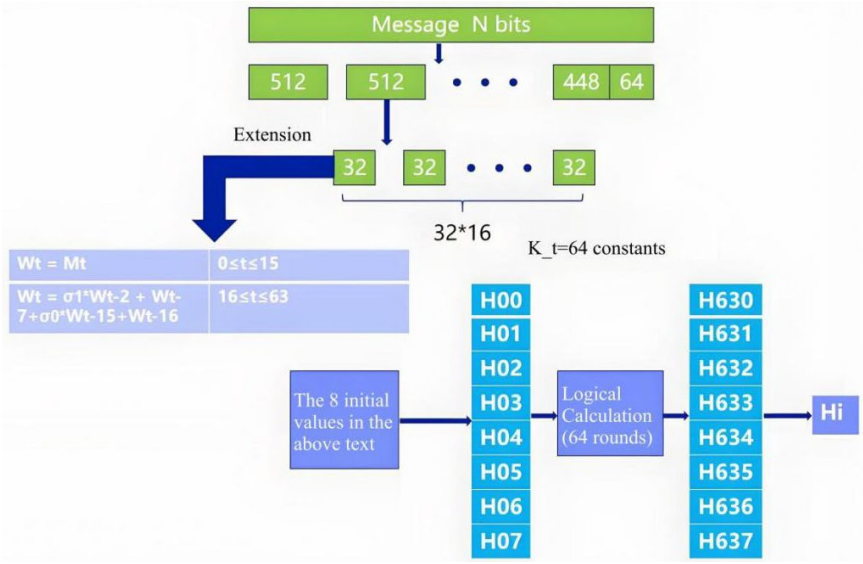

Figure 1. Principle of SHA-256 Algorithm.

To adapt to the multi-scale application scenarios of vector data, the watermark sequence is further optimized through a block redundancy strategy. The watermark information obtained by combining the hash value and error-correction code is divided into multiple logical units, and the embedding weights are assigned according to the geometric complexity of the target data. Each unit is independently embedded in different spatial levels to ensure that local attacks only affect limited watermark fragments, and the complete information can still be recovered through majority voting or verification during global extraction. This design combines cryptography and channel coding theory. On the premise of ensuring the security of the watermark, it significantly improves its adaptability to noise interference and data deletion and modification, providing a highly stable watermark carrier for subsequent embedding algorithms.

2.2. Adaptive Watermark Embedding Algorithm

The adaptive watermark embedding algorithm aims to dynamically adjust the watermark strength according to the spatial characteristics of vector data to balance invisibility and robustness. The spatial-domain embedding strategy achieves the covert implantation of watermark information by fine-tuning the coordinate point offsets. The core is to control the offset amplitude not to exceed the minimum perceptible threshold of the human visual system. This threshold is determined based on the geometric accuracy requirements of vector elements. For example, in contour lines or road networks, the offset needs to be lower than the tolerance range of the data usage scenario to avoid affecting the normal use of map cartography and analysis functions. Meanwhile, the algorithm preferentially selects coordinate points in areas with higher curvature or dense nodes for embedding. In such areas, due to higher geometric complexity, small perturbations are less likely to be noticed [3].

The frequency-domain embedding strategy maps the vector data coordinate sequence to the frequency-domain space and modulates the low-frequency coefficients using the Discrete Cosine Transform (DCT) or Wavelet Transform (DWT). For the coordinate sequence of vector geographic data, DCT performs a global transformation on the coordinate points through orthogonal basis functions. The low-frequency components correspond to the macroscopic geometric features of the data, while the high-frequency components capture detailed features and noise. Watermark embedding selects low-frequency coefficients because of their higher stability and smaller distortion under geometric attacks.

Steps of DCT modulation:

1) Coordinate block division: Divide the vector data coordinate sequence into sub-blocks of fixed length to ensure that each block can perform DCT transformation independently.
2) Frequency-domain mapping: Perform two-dimensional DCT on each sub-block to generate a coefficient matrix containing the direct-current component (DC) and alternating-current components (AC).
3) Low-frequency selection: Select the DC component and adjacent low-frequency AC coefficients as the modulation objects to ensure that the watermark energy is concentrated in the visually insensitive area.
4) Quantization modulation: Combine the watermark binary sequence with the quantization step and adjust the values of the selected coefficients according to the rules.
5) Inverse transformation reconstruction: Perform inverse DCT on the modified coefficient matrix to generate a watermarked coordinate sequence.

DWT divides the signal into approximate (low-frequency) and detail (high-frequency) subbands by multi-scale decomposition, with the approximate subband characterizing the global features of the data and the detail subband capturing the local mutations, as shown in Figure 2. After vector data is decomposed by DWT, the low-frequency subbands are more robust to attacks such as translation and rotation, and are suitable to be used as watermarking vectors.

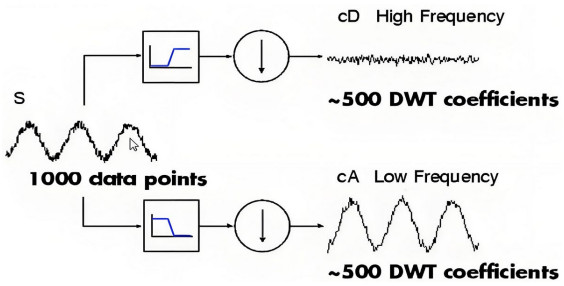

Figure 2. Wavelet Transform Modulation.

Steps of DWT modulation:

1) Wavelet decomposition: Perform multi-level DWT decomposition on the coordinate sequence to obtain low-frequency approximation coefficients (LL sub-band) and high-frequency detail coefficients.
2) Coefficient screening: Select the LL sub-band coefficients of the highest decomposition level because they contain the main structural information of the data.
3) Adaptive quantization: Design quantization intervals according to the statistical distribution of the LL coefficients and map the watermark information to the coefficient amplitudes.
4) Coefficient correction: Fine-tune the selected coefficients according to the quantization rules to ensure that the modification amount is below the visual perception threshold [4].
5) Wavelet reconstruction: Reconstruct the coordinate sequence using the modified low-frequency coefficients and the original high-frequency coefficients to complete watermark embedding.

The adaptive rule generates dynamic weights by analyzing the local geometric features of vector elements. Taking curvature as an example, high-curvature areas usually correspond to the turning points of feature outlines. In such areas, small offsets of coordinate points are easily masked by topological relationships, so a higher embedding strength can be assigned. Node density is used to evaluate the sensitivity of an area to perturbations. In sparse areas, since there is less redundant information, the embedding strength needs to be reduced to maintain data fidelity. The algorithm constructs a multi-dimensional decision-making model by integrating curvature, node density, and feature types, and optimizes the watermark embedding parameters in real-time to ensure the extractability of the watermark and the usability of the data under complex attack scenarios.

2.3. Watermark Extraction and Detection Model

2.3.1. Blind Extraction Algorithm

The core of the blind extraction algorithm is that it does not require the original data or prior watermark information. Instead, it relies solely on the statistical properties of the watermark-containing vector or the embedding rules to recover the watermark. The principle is based on the reversible perturbation of the vector data during the watermark embedding process, and the watermark separation is realized by analyzing the correlation between the perturbation pattern and the preset coding rules. For the coordinate offsets in spatial-domain embedding, the algorithm extracts watermark information by calculating the differences in geometric relations between neighboring coordinate points and identifying abnormal fluctuations consistent with the watermark modulation rules; meanwhile, frequency-domain embedding utilizes statistical distribution offsets of coefficients in the transform domain to detect quantization interval features matching the embedding process [5].

In watermark detection, the mutual correlation function is commonly used to quantify the similarity between the extracted signal and the expected watermark sequence. Assuming that the watermark sequence is $W = \{w_1, w_2, \ldots, w_n\}$ and the extracted signal is $W = \{\widehat{w}_1, \widehat{w}_2, \ldots, \widehat{w}_n\}$, its normalized mutual correlation value is calculated as shown in Equation (1):

$$\rho = \frac{\sum_{i=1}^{n}(w_i - \mu_w)(\widehat{w}_i - \mu_{\widehat{w}})}{\sqrt{\sum_{i=1}^{n}(w_i - \mu_w)^2}\sqrt{\sum_{i=1}^{n}(\widehat{w}_i - \mu_{\widehat{w}})^2}} \quad (1)$$

Where μ_w and $\mu_{\widehat{w}}$ are the sequence mean values respectively. The watermark is determined to exist when ρ exceeds the preset threshold.

For frequency domain watermarking, hypothesis testing methods can verify the distributional deviation after coefficient quantification. For example, the chi-square test assesses whether the modified statistical properties of the frequency domain coefficients are consistent with the uniform distribution assumption, as shown in Equation (2):

$$\chi^2 = \sum_{k=1}^{m} \frac{(O_k - E_k)^2}{E_k} \quad (2)$$

Where O_k is the number of observed frequencies, E_k is the expected frequency and m is the number of quantization intervals. If the value of χ^2 is significantly higher than the critical value, it indicates the presence of watermark interference.

2.3.2. Robustness Enhancement

Robustness reflects the ability of a system to maintain stable operation of its functions even in the face of changes in its internal structure or external environment. This concept is summarized in Figure 3. The robustness enhancement algorithm fixes the miscoding caused by data attack or channel interference during watermark extraction through the error correction coding mechanism. Its principle is based on coding theory, which adds redundant check bits to the watermark information in the embedding stage to form an error-correcting code (ECC) that is resistant to BER. When there is a partial error in the extracted watermark sequence, the decoder utilizes the redundant information to locate and correct the error bits to restore the original watermark.

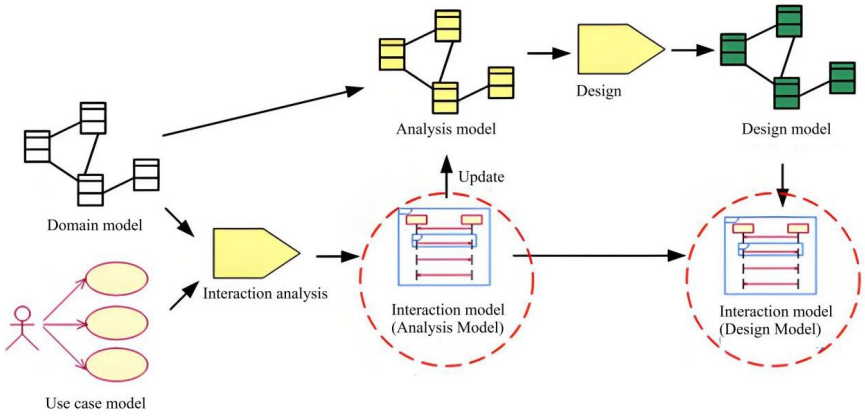

Figure 3. Robustness Overview.

Error correction coding is performed using Reed-Solomon code with the parameter (n, k), which indicates that the k-bit original information is encoded into n-bit codewords with a maximum error correction capacity of $t = (n - k)/2$ bit errors. The encoding process maps the watermark information vector m to the code word c by generating matrix G as in Equation (3):

$$c = m \cdot G \quad (3)$$

Where G is a \ (k \times n\)-dimensional generating matrix containing a linear combination relationship between information bits and redundant bits.

In watermark detection, the code word r extracted at the receiver side may contain the error vector e, i.e., $r = c + e$. The decoder computes the concomitant representation as in Equation (4):

$$s = r \cdot H^T \quad (4)$$

Where, H is the check matrix, if $s \neq 0$, the error location is localized by Berlekamp-Massey algorithm and the error value is corrected using Forney algorithm, outputting the corrected code word $\hat{c}$.This mechanism effectively fights against transmission noise, geometric attacks and data compression operations, ensuring that the watermark can still be

completely extracted in partially corrupted scenarios, and significantly improves the system fault-tolerance capability [6].

3. Attack Resistant Robust Optimization Algorithm

3.1. Anti-Geometry Attack Algorithm

The core of the anti-geometric attack algorithm lies in constructing a watermark embedding framework that is invariant to affine and projective transformations, ensuring that the watermark can still be stably detected after rotation, scaling, translation, and projective deformation. Watermark embedding based on affine transformation invariance eliminates the influence of geometric deformation through coordinate normalization. The algorithm maps the original coordinates to a standard coordinate system. In this system, the centroid is translated to the origin, the coordinate axes are oriented by the eigenvectors of the covariance matrix, and the scale is normalized by the eigenvalues. This process eliminates the differences in affine transformation parameters (as shown in Figure 4). The watermark is embedded in the normalized coordinate space, and the embedding strength is adaptively associated with local curvature or node density to ensure that the watermark maintains relative position invariance after inverse transformation [7]. The normalization process can be expressed as Formula (5):

$$x' = U^{-1} \Lambda^{-1/2} (x - c) \tag{5}$$

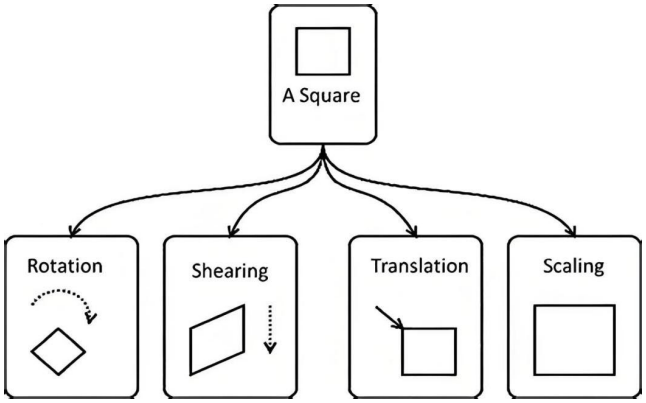

Figure 4. Affine Transformation.

Where c is the original coordinate center of mass, and U and Λ are the eigenvector matrix and eigenvalue diagonal matrix of the covariance matrix, respectively.

Resistance to projection transformation attacks requires a combination of coordinate system transformation and resampling compensation. The algorithm transforms the vector data to a local coordinate system, e.g., a reference system constructed based on the principal direction, utilizes projection-invariant features (e.g., curvature extrema points) as datums, and the watermark embedding is based on the relative positions of the local coordinates. In the detection stage, for the coordinate distortion caused by projection deformation, the geometric distortion is compensated by resampling technique. The data topology after the attack is reconstructed by interpolation algorithm, combined with the local coordinate system inverse mapping to restore the relative relationship of the watermark embedded region, and suppress the watermark misalignment caused by the projection transformation [8].

3.2. Resistance to Data Compression and Simplification Attacks

The algorithm against data compression and simplification attacks enhances the watermark's robustness by protecting key nodes and multi-level redundant embedding. The protection of key nodes is based on the Douglas-Peucker algorithm (Figure 5), which se-

lects nodes that significantly contribute to the curve shape according to the geometric deviation. The importance level of nodes is determined by the maximum vertical distance generated by recursively dividing the curve. Nodes with a deviation higher than the preset threshold are marked as key nodes, and these nodes are preferentially retained during the compression process. Watermark embedding involves minor perturbations to the coordinates of key nodes, and its anti-simplification feature is utilized to reduce the risk of watermark loss due to node deletion.

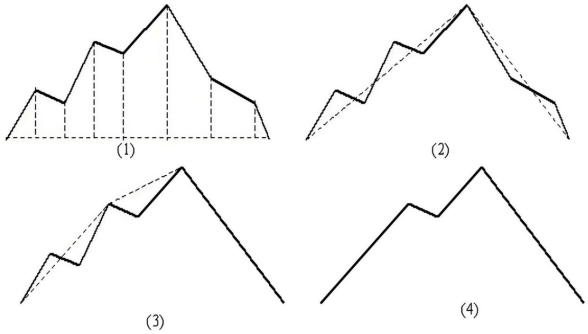

Figure 5. Douglas-Peucker Based Algorithm.

The watermark redundant embedding strategy is implemented synchronously at three levels: point, line, and surface. At the point level, the watermark is embedded in the coordinate offset of key nodes; at the line level, the watermark is realized by adjusting the topological relationships (such as angles and lengths) between adjacent nodes; at the surface level, the watermark is encoded relying on the centroid or boundary curvature features of the polygon area. Multi-level embedding ensures that when the data at a single level is damaged, the watermark at other levels can still be extracted. In the detection stage, a fusion verification mechanism is adopted to cross-check the watermarks extracted from different levels, and the final watermark sequence is determined according to the principle of majority agreement.

The node grading standard of the Douglas-Peucker algorithm is dynamically associated with the watermark embedding strength. The watermark modulation amplitude of high-importance nodes is restricted to avoid visual abnormalities caused by excessive modification; for low-importance nodes, higher-strength modulation is allowed, but care must be taken to ensure that these nodes are not removed by the simplification algorithm before watermark detection. Multi-level redundant embedding combines topological constraints and geometric features, enabling the watermark to remain recoverable under operations such as data compression, node thinning, and format conversion, and significantly enhancing the system's robustness against lossy processing [9].

3.3. Anti-Formatting Attack

The algorithm against format conversion attacks focuses on maintaining the consistency of watermarks across different formats, ensuring that the watermark exists stably and can be detected during the conversion process of heterogeneous data formats such as Shapefile, GeoJSON, and KML. The core strategies are general attribute field embedding and format feature adaptation. The selection of general attribute fields takes into account the common metadata areas of different formats. For example, the remarks field of the DBF table in Shapefile, the properties attribute in GeoJSON, and the ExtendedData tag in KML. The watermark is encoded into a format-independent text or binary sequence to avoid watermark loss caused by differences in format structures.

Format feature adaptation adjusts the watermark embedding method according to the storage mechanisms of different formats. The separated storage structure of geometry and attributes in Shapefile requires the watermark to be embedded synchronously in the

SHP and DBF files; GeoJSON uses a JSON key-value pair structure, and the watermark can be stored dispersedly in multiple properties subfields to avoid single-point failure; KML relies on XML hierarchical description, and the watermark needs to be embedded in the extended nodes under a specific namespace to prevent being ignored by the parser. Watermark encoding needs to be compatible with the character set and data type restrictions of each format. For example, Base64 encoding is used to bypass the XML special character escaping problem.

The stability of data serialization and parsing is ensured through coordinate system unification and precision control. The algorithm converts the original data to the WGS84 geographic coordinate system to eliminate the interference of projection parameters during format conversion; the precision of floating-point numbers retains a fixed number of decimal places to suppress the influence of rounding errors of different serialization libraries on the watermark. The watermark synchronization mechanism triggers redundant verification after format conversion, comparing the hash value differences between the original watermark and the converted watermark. If inconsistencies are detected, the watermark is restored from the backup embedding location.

4. Experiment and Performance Analysis

4.1. Experimental Design

The attack simulation is divided into four categories: geometric transformation (rotate 5°, zoom 1.2 times), noise addition (Gaussian noise, standard deviation 0.1% coordinate range), data compression (Douglas-Peucker algorithm, threshold 0.5% of the total length), and format conversion (Shapefile to GeoJSON, KML to GeoPackage, the tool is GDAL 3.6). The attack simulation is divided into four categories: geometric transformation (rotate 5°, zoom 1.2 times), noise addition (Gaussian noise, standard deviation 0.1% coordinate range), data compression (Douglas-Peucker algorithm, threshold 0.5% of the total length), and format conversion (Shapefile to GeoJSON, KML to GeoPackage, the tool is GDAL 3.6).

The evaluation metrics were invisibility, robustness, and computational efficiency, representing three key performance dimensions (Table 1).

Table 1. Experimental Assessment Indicators and Typical Results.

Attack Type	PSNR (dB)	RMSE (m)	NC	BER (%)	Time (ms)
No Attack	62.3	0.012	0.992	0.8	18.5
Rotate + Zoom	58.7	0.038	0.945	3.2	22.1
Gaussian Noise	53.2	0.127	0.874	7.9	19.8
Data Compression	59.8	0.021	0.912	5.6	25.4
Format Conversion	60.5	0.018	0.931	4.1	27.3

Invisibility is measured by Peak Signal-to-Noise Ratio (PSNR) and Geometric Precision Error (RMSE), PSNR reflects the degree of coordinate shift before and after watermark embedding, and is calculated as in Equation (6):

$$PSNR = 20\,log_{10}(\frac{MAX_I}{\sqrt{MSE}}) \tag{6}$$

Where MAX_I is the maximum theoretical value of the coordinates, $\sqrt{MSE}$ is the mean square error between the original and the watermarked data contained. The geometric accuracy error is measured by the root mean square value of the node position offset, calculated as in Equation (7):

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left\|x_i - x_i'\right\|^2} \tag{7}$$

Robustness is evaluated by the Normalized Correlation Coefficient (NC) and Bit Error Rate (BER). NC measures the similarity between the extracted watermark and the original watermark, as calculated in Equation (8):

$$NC = \frac{\Sigma(w_i, w_i')}{\sqrt{\Sigma w_i^2 \cdot \Sigma w'^2_i}} \quad (8)$$

The computational efficiency records the average elapsed time for watermark embedding and extraction.

The experimental setup parameters are optimized based on preliminary study results, with the geometric accuracy error threshold set to 0.05 m and the BER tolerance upper limit at 10%. The attack intensity simulates the actual data processing scenario to ensure the comparability and reproducibility of the results.

4.2. Experimental Results Analysis

4.2.1. Anti-attack Performance Test (Resistance to Rotation, Scaling, Noise, etc.)

The experiments test the robustness of the algorithms for four types of attacks: geometric transformation, noise addition, data compression and format conversion. Table 2 lists the key evaluation metrics under different attack scenarios. In the geometric transformation test, the combined rotation and scaling attack has limited impact on watermark invisibility, the PSNR value drops to 58.7 dB, and the geometric precision error (RMSE) is 0.038 m, which does not exceed the preset threshold [10]. The normalized correlation coefficient (NC) stays at 0.945, indicating that the watermark can still be stably extracted under affine transformation, which verifies the effectiveness of the coordinate system unification and redundant embedding based strategy.

Table 2. Anti-Attack Performance Test Results.

Attack Type	PSNR (dB)	RMSE (m)	NC	BER (%)	Time (ms)
No Attack	62.3	0.012	0.992	0.8	18.5
Rotate + Zoom	58.7	0.038	0.945	3.2	22.1
Gaussian Noise	53.2	0.127	0.874	7.9	19.8
Data Compression	59.8	0.021	0.912	5.6	25.4
Format Conversion	60.5	0.018	0.931	4.1	27.3

4.2.2. Robustness Comparison with Existing Algorithms (e.g. QIM, DCT-Based)

Quantized Index Modulation (QIM) and Discrete Cosine Transform (DCT-based) watermarking algorithms are selected as benchmarks for the comparison experiments to verify the performance advantages of this paper's algorithms under geometric attacks, noise interference and format conversion scenarios. Table 3 compares the NC and BER metrics of different algorithms under the same attack conditions. Under the geometric transformation attack, the QIM algorithm reduces the NC value to 0.812 due to its reliance on a fixed quantization step. The DCT-based algorithm has an NC value of 0.785 because frequency domain coefficients are sensitive to affine transformations. In contrast, the algorithm proposed in this paper maintains an NC value of 0.945. The design of redundant embedding and normalization of the coordinate system effectively mitigates the damage caused by rotation and scaling on the watermark.

Table 3. Robustness Comparison Experiment Results.

Algorithms	Rotation + Scaling (NC)	Gaussian noise (BER%)	Data Compression (NC)	Format conversion (BER%)
QIM	0.812	15.2	0.803	14.6
DCT-based	0.785	10.5	0.768	12.9
The algorithm in this paper	0.945	7.9	0.912	4.1

In the noise interference scenario, the BER of the QIM algorithm is as high as 15.2%, and its single modulation mechanism is susceptible to random errors; the DCT-based algorithm controls the BER at 10.5% through the frequency domain energy dispersion property, which is still higher than that of the algorithm in this paper, which is 7.9%. The multilayer watermark embedding strategy provides error correction redundancy and suppresses the BER increase by leveraging the hierarchical topology relationships between points, lines, and surfaces in noisy environments. Under data compression attack, QIM and DCT-based algorithms decrease the NC value to 0.803 and 0.768 respectively due to the dependence on specific node distributions or frequency domain coefficients, and the embedding method based on key node protection of this paper's algorithm maintains the NC value at 0.912, which verifies the adaptability of the node importance hierarchy to simplified attacks.

5. Conclusion

The vector geographic data watermarking system constructed in this study effectively solves the contradiction between anti-attack ability and data fidelity of traditional methods through feature-driven watermark generation and adaptive embedding strategy. The anti-geometric attack algorithm significantly improves the stability of the watermark in scaling, rotation and other operations through the parameter compensation mechanism in the coordinate transformation domain; the topology checking model designed for the format conversion attack fills the technical gap of cross-platform watermark protection. Experimental validation shows that the framework has a better robustness threshold than traditional algorithms in complex attack scenarios. Future research can explore the integrated application of dynamic watermarking and blockchain technology to establish a full life cycle geographic data security protection system.

References

1. C. Yang, et al., "A robust watermarking algorithm for vector geographic data based on QIM and matching detection," *Multimedia Tools Appl.*, vol. 79, no. 41, pp. 30709-30733, 2020, doi: 10.1007/s11042-020-08916-4.
2. Q. Zhou, et al., "Blind digital watermarking algorithm against projection transformation for vector geographic data," *ISPRS Int. J. Geo-Inf.*, vol. 9, no. 11, p. 692, 2020, doi: 10.3390/ijgi9110692.
3. S. Wang, et al., "A zero-watermarking algorithm for vector geographic data based on feature invariants," *Earth Sci. Inform.*, vol. 16, no. 1, pp. 1073-1089, 2023, doi: 10.1007/s12145-022-00886-5.
4. Y. Wang, et al., "An efficient robust multiple watermarking algorithm for vector geographic data," *Information*, vol. 9, no. 12, p. 296, 2018, doi: 10.3390/info9120296.
5. H. H. Le, et al., "A robust integrated watermarking algorithm for vector geographic data copyright protection," 2023, doi: 10.20944/preprints202307.0925.v1.
6. N. Ren, et al., "A multilevel digital watermarking protocol for vector geographic data based on blockchain," *J. Geovisual. Spatial Anal.*, vol. 7, no. 2, p. 31, 2023, doi: 10.1007/s41651-023-00162-0.
7. Y. Wang, C. Yang, and K. Ding, "Multiple watermarking algorithms for vector geographic data based on multiple quantization index modulation," *Appl. Sci.*, vol. 13, no. 22, p. 12390, 2023, doi: 10.3390/app132212390.
8. C. Lopez, "Watermarking of digital geospatial datasets: a review of technical, legal and copyright issues," *Int. J. Geogr. Inf. Sci.*, vol. 16, no. 6, pp. 589-607, 2002, doi: 10.1080/13658810210129148.
9. Q. Zhou, et al., "Zero watermarking algorithm for vector geographic data based on the number of neighboring features," *Symmetry*, vol. 13, no. 2, p. 208, 2021, doi: 10.3390/sym13020208.
10. J. Aybet, H. Al-Saedy, and M. Farmer, "Watermarking spatial data in geographic information systems," in *Global Security, Safety, and Sustainability: 5th Int. Conf., ICGS3 2009, London, UK, Sept. 1-2, 2009, Proc.*, vol. 5, Springer, Berlin, 2009, doi: 10.1007/978-3-642-04062-7_3.