A Zero-watermarking Algorithm for Vector Geographic Data Based on Feature Invariants

Shuai Wang
Faculty of Geomatics, Lanzhou Jiaotong University
Li-Ming Zhang (zlm@lzjtu.edu.cn)
Faculty of Geomatics, Lanzhou Jiaotong University
Qi-Hang Zhang
Faculty of Geomatics, Lanzhou Jiaotong University
Yu Li
School of Resource and Environmental Sciences, Wuhan University

Method Article

Keywords: zero-watermarking algorithm, projection transformation, vector geographic data, feature invariant, robustness

Posted Date: September 14th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-2030350/v1

A Zero-watermarking Algorithm for Vector Geographic Data Based on Feature Invariants

Shuai Wang [1,2,3], Li-Ming Zhang [1,2,3*], Qi-Hang Zhang [1,2,3], and Yu Li [4]

[1] Faculty of Geomatics, Lanzhou Jiaotong University, Lanzhou 730070, China;
[2] National Local Joint Engineering Research Center of Technologies and Application for National Geographic State Monitoring, Lanzhou 730070, China
[3] Gansu Provincial Engineering Laboratory for National Geographic State Monitoring, Lanzhou 730070, China
[4] School of Resource and Environmental Sciences, Wuhan University, Wuhan 430079, China;
[*] Correspondence: zlm@lzjtu.edu.cn; Tel.: +86-136-3932-8110

Abstract: Most researches on zero-watermarking algorithms for vector geographic data focus on improving the robustness against geometrical attacks, compression attacks and object attacks. However, there are few zero-watermarking algorithms against projection transformation. We proposed a zero-watermarking algorithm for vector geographic data based on feature invariants. After any projection transformation of vector geographic data, the number of vertices and relative storage order of objects does not change. Therefore, the number of vertices and relative storage order of objects can be considered as the feature invariants. Firstly, according to relative storage order of objects, the watermark bit is determined by comparing the number of vertices between any two objects. Secondly, the watermark index is calculated by the number of vertices of two objects. Then, a feature matrix is constructed combining the watermark bit and the watermark index. Finally, the XOR operation is performed between the feature matrix and the scrambled watermark image to generate the zero-watermark image. The experiments show that the watermark can be detected from the vector geographic data after any projection transformation. And this algorithm can effectively against geometrical attacks, object attacks and precision reduction attacks, showing superior performance compared with previous algorithms.

Keywords: zero-watermarking algorithm; projection transformation; vector geographic data; feature invariant; robustness

1 Introduction

With the rapid development of geographic information science, vector geographic data plays an important role in the national economy, urban national security, and environmental protection [1-3]. The production cost of vector geographic data is high, the production cycle is long, and the potential value is high. Therefore, the security of vector geographic data has always been concerned [4,5]. However, with the growing demand for vector geographic data sharing, the illegal use and infringement of vector geographic data frequently occur, and effective technologies are urgently needed to protect vector geographic data. At present, digital watermarking technology is widely used for copyright protection and traceability of vector geographic data [6-9]. Traditional digital watermarking techniques embeds watermark information by modifying coordinate values in the spatial domain [10-13] or frequency domain [14-17], which will reduce the accuracy and is not suitable for high-fidelity vector geographic data [18-20]. The emergence of zero-watermarking technology has solved this problem very well. Zero-watermarking technology constructs watermarking information by extracting important features of the data itself without any modification on the original data [21-23]. Compared with traditional watermarking technology, zero-watermarking technology is more suitable for high-precision vector geographic data. At the same time, the zero-watermarking technology also balances the contradiction between watermark invisibility and robustness [24,25].

At present, most zero-watermarking algorithms of vector geographic data are targeted at the robustness to geometrical attacks, compression attacks, and object attacks. For example, the zero-watermarking image was constructed based on the distance ratio of feature vertices, and this algorithm has good robustness against geometrical attacks, compression attacks and object attacks [23]. Li et al constructed zero-watermarking image by modulating the slopes of adjacent feature points. This algorithm can effectively against geometrical attacks and vertex attacks [26]. Xi et al proposed a multiple zero-watermarking algorithm. In this algorithm, feature points and non-feature points are divided firstly, then two zero-watermarking images are constructed respectively according to feature points and non-feature points. This algorithm has a good watermark capacity and overall robustness [27]. Zhu et al proposed a zero-watermarking algorithm based on minimum bounding rectangle and singular value decomposition. This algorithm has good robustness against translation attack, compression attacks and object deletion attack [28]. Ren et al proposed a zero-watermarking algorithm based on concentric circles [29]. This algorithm has good robustness against geometrical attacks, compression attacks, and object attacks. These zero-watermarking algorithms mainly focus on the robustness to geometrical attacks, object attacks, vertex attacks, few algorithms consider the robustness of projection transformation.

Projection transformation is often used in vector geographic data processing and application [24,30]. Therefore, in view of the poor robustness of current vector geographic data zero-watermarking algorithms to projection transformation, a zero-watermarking algorithm based on vector geographic data feature invariants is proposed, which can resist any projection transformation.

The remainder of this paper is organized as follows. Section 2 is how to use feature invariants. Section 3 is the basic ideas and details of the algorithm. Section 4 presents the experimental design. Then Section 5 describes the experimental analyses and results. Finally, Section 6 presents discussion and Section 7 draws the conclusions.

2 Preliminaries

Before introducing the algorithm in this paper, there are three problems to be solved: (1) What feature invariants do vector geographic data have after projection transformation; (2) How to keep the watermark synchronization by using the feature invariants; (3) How to use the feature invariants to construct the feature matrix. These three questions are the key points of this algorithm.

2.1 Feature Invariants of Projection Transformation

Projection transformation is an important part of map projection and map compilation. It mainly studies the theory and method of transforming one map projection into another map projection. The projection can be divided into four types: the equal area projection, the conformal projection, the equidistant projections, and compromise projection. All different map projections change the relative position and geometry of the vector geographic data. Therefore, choosing the suitable feature invariants of vector geographic data to projection transformation is the key point for the zero-watermarking algorithm in this paper. In summary, we find that the number of vertices is a feature invariant for the projection transformation, regardless of any projection transformation. Thus, the number of object vertices is a suitable feature invariant.

At the same time, the relative storge order of objects is also a feature invariant for vector geographic data [31]. In general, few people notice this feature and therefore this feature invariant is rarely attacked. In addition, the relative storage order of the objects always remains after geometrical attacks, compression attacks and projection transformations. Therefore, the relative storage order of the objects can also be used as a feature invariant. Figure 1 shows that the relative storage order of objects does not change after object addition and object deletion.

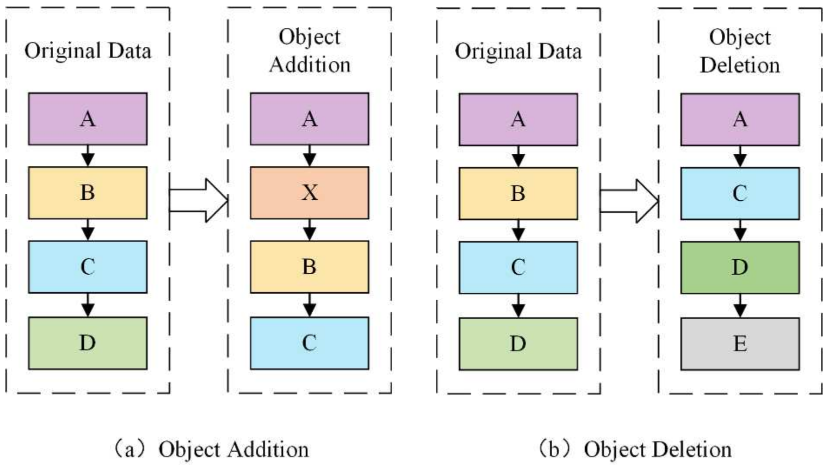


Figure 1. Relative storge order after object addition and object deletion

Figure 1(a) shows object addition, where A, B, C and D are the storage order of the original data, and when an X is added, the object storage order becomes A, X, B, C and D. Figure 1(b) shows object deletion, where when we delete B from the original data, the object storage order becomes A, C, D and E. Figure 1 shows that the relative storage order does not change in any way after object addition and object deletion. Likewise, the relative storge order of objects is also a stable characteristic under other types of attack. Therefore, we choose the number of object vertices and the relative storage order as the feature invariants, and the following is how we use these two feature invariants to design the algorithm.

2.2 Rules for Generating Watermark index Based on the Number of Object Vertices

In order to ensure the synchronization of the watermark, the numbers of object vertices of any two objects are operated to calculate the watermark bits in this paper. Firstly, this paper uses a multiplication operation to expend the range of values. Secondly, to ensure the uniform distribution of watermark embedding bits, the number of vertices of the previous object is multiplied once more to obtain more results. Finally, the obtained results are subjected to remainder operation with the original watermark length to obtain the watermark index of any two objects. This can be calculated by the Equation (1).

$$index_{ij} = (N_i^2 \times N_j)\%L \tag{1}$$

where $index_{ij} \in [0, L-1]$, N_i and N_j mean the number of vertices of any two objects in the relative storage order, and L means the length of original watermark information.

2.3 Rules for Generating Watermark bit Based on feature invariants

Since the relative storage order and the number of object vertices are two feature invariants to the projection transformation, it is crucial to construct the watermark by using these two feature invariants. In general, the watermark is a binary sequence generated by 0 and 1. The watermark bit is determined by judging the number of vertices of any two objects. The rule is: if the number of vertices of the former object is larger than the number of vertices of the latter object, the watermark bit is 1, otherwise the watermark bit is 0. This way, we generate a watermark sequence containing only 1 and 0. The length of the watermark information depends on the number of object vertices. It can be expressed as the Formula (2).

$$m = \sum_{i=2}^{n} i - 1 \tag{2}$$

Where n indicates the number of object vertices and m means the length of the watermark. As an example, when n is 4, the watermark length is 6.

3 Methodology

3.1 Basic Idea

In order to solve the three problems in Section 2, the following three aspects are proposed to design the zero-watermarking algorithm: (1) The number of object vertices and the relative storage order are used as two feature invariants for the projection transformation. (2) The numbers of two objects vertices are used to determine the watermark index. (3) The numbers of two objects vertices in the two relative storage orders are used to generate the watermark bit.

In Section 3, we detail the zero-watermarking scheme based on the two feature invariants. The scheme mainly includes three parts: the generation of original watermark information, the construction of the zero-watermark image and the detected of the zero-watermark image. The detailed descriptions of each part are shown below.

3.2 The Scrambled of Original Watermark Information

In order to improve the security of the original watermark information in practical applications, the watermark information is preprocessed by scrambling transformation before the construction of zero-watermark image. In this paper, we choose the Arnold transform for watermark scrambling [32, 33]. The calculate of the Arnold transform can be mathematically expressed as the following Equation (3).

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mathrm{mod}(N), x, y \in \{0,1,2,\cdots,N-1\} \tag{3}$$

In Equation (3), (x, y) is the coordinate of each pixel in the original watermark image; (x', y') is the coordinate of the corresponding pixel after the Arnold transform; N is the image size, when the length and width of the image are equal, then N takes this value, when the length and width are not equal, N_1 and N_2 take the length and width respectively, as shown in Equation (4).

$$\begin{cases} x' = (x+y)\,\mathrm{mod}(N_1) \\ y' = (x+2y)\,\mathrm{mod}(N_2) \end{cases} \tag{4}$$

Take a watermark image of size 32×64 as an example. Figure 3 shows original watermark, the watermark with 1, 12, 24 and 32 times of transform, respectively. As can be seen from Figure 3 (e), when the image is transformed 32 times, the scrambled image is restored to the original image, so the period of the Arnold transform of this image is 32 times.

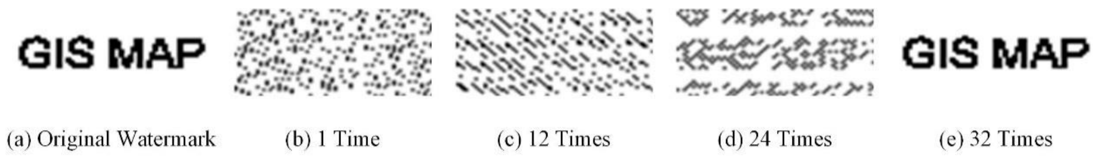


Figure 2. Original watermark information and scrambling

3.3 The Construction of Zero-watermark Image

The process of constructing a zero-watermark image is shown below: Firstly, the numbers of any two objects' vertices in the relative storage order are counted to determine the watermark bit. Secondly, the watermark index is determined by performing several certain operations on numbers of any two objects vertices. Thirdly, the feature matrix is constructed by combining the watermark bits, watermark indices and voting principle. Figure 1 shows the basic idea of the algorithm. Finally, the XOR operation is performed on the scrambled watermark image and the feature matrix to get a zero-watermark image.

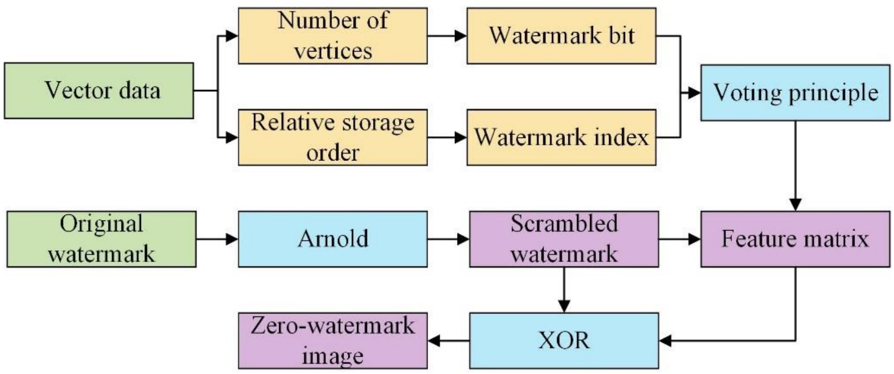


Figure 3. The basic idea of proposed method

The following are the specific steps to construct a zero-watermark image.

Step 1: Read the object sequence $\{F_n\}$ of vector geographic data according to the storage order, expressed by $F_n = \{f_1, f_2, \cdots, f_n\}$, and n is the number of objects.

Step 2: Read the binary original watermark information W and the Arnold transformed watermarked image is noted as W'.

Step 3: Calculate the number of objects' vertices and get the sequence of the number of object vertices S_n, expressed by $S_n = \{s_1, s_2, \cdots, s_n\}$.

Step 4 The numbers of any two objects' vertices are operated and indexed with the length of watermark, as shown in Equation (1). Then the index sequence $\{Index_i\}$ is obtained, expressed by $\{Index_i = index_1, index_2, \cdots, index_i\}$.

Step 5: The watermark bit is determined according to the numbers of any two objects' vertices. The rule is that if the number of vertices of the former object is larger than the number of vertices of the latter object, the watermark bit is 1, otherwise the watermark bit is 0, then the watermark sequence $\{W_i\}$ is obtained, expressed by $W_i = \{w_1, w_2, \cdots w_m\}$. And m is the total length of the watermark, which can be determined by Equation (2).

Step 6: Since the number of $\{Index_m\}$ is much larger than the length of the watermark, there will be a situation that the watermark indices of any two objects are the same. Therefore, the voting principle is used to determine the watermark bit. The method is: define a one-dimensional sequence of equal length to the length of watermark. The value of the same watermark bit $B(k)$ is determined jointly by $\{W_i\}$ and $Index_i$, as shown in Equation (5).

$$B(k) = B(k) + b'(i) \tag{5}$$

Where $b'(i)$ is determined by $b(i)$. The rule is: if $b(i) = 0$, then $b'(i) = -1$, otherwise $b'(i) = 1$. Finally, if $B(k) > 0$, then the corresponding watermark is 1, otherwise the watermark is 0.

Step 7: The extracted watermark sequence is converted from one-dimensional to two-dimensional to obtain the final binary feature matrix M.

Step 8: The zero-watermark image W^* is obtained by XOR operation between the binary feature matrix M and the scrambled watermark image W', as shown in Equation (6). Then register W^* to a third-party intellectual property rights (IPR) repository.

$$W^* = M \oplus W' \tag{6}$$

3.4 The Detection of Zero-watermark Image and Copyright

The steps of zero-watermark detection and zero-watermark generation are the same.

The feature matrix is extracted from the suspicious data, then a XOR operation is performed between the feature matrix and the original zero-watermark image to get the copyright information. The specific processes of copyright detection are as follows:

Step 1: Repeat Step 1 to Step 7 in section 3.3 to generate the feature matrix of the suspicious data.

Step 2: The scrambled watermark information is generated by XOR operation between the feature matrix and the zero-watermark image registered in IPR.

Step 3: The scrambled watermark information is restored by Arnold transform to generate the watermark information.

Step 4: The copyright information is determined by comparing the watermark information with the original watermark information.

4 Experiments

4.1 Dataset

In order to evaluate the performance of the algorithm, we performed experiments by Python3.7 in Windows10. The proposed algorithm in this paper is suitable for polylines and polygons. Four vector geographic data with the same scale of 1:400,000 are used. The format of the four experimental data is the ESRI Shapefile. These four data are different types of vector geographic data from different regions, namely, rivers, highways, administrative divisions of prefectural boundary, and administrative divisions of county boundary. Figure 4 shows the four pieces of experimental data.

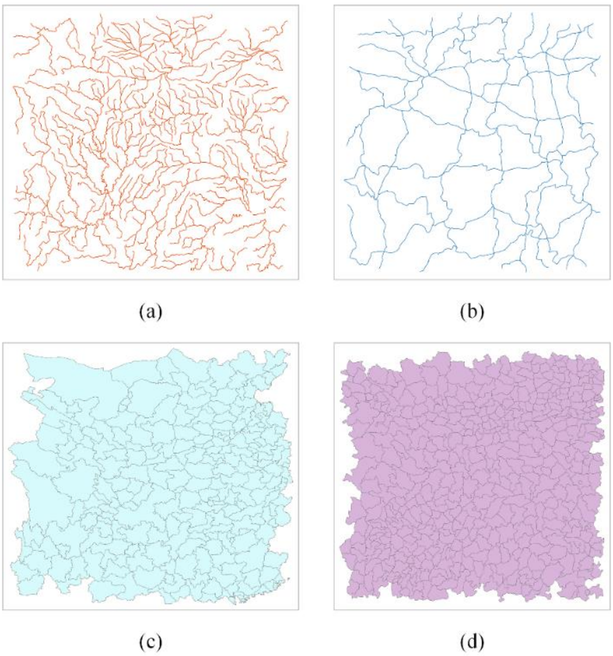


Figure 4. The experimental data. (a)River, (b) Highway, (c) Administrative divisions of prefectural boundary, (d) Administrative divisions of county boundary.

At the same time, Table 1 shows the basic information of experimental data, including data name, data type, number of objects, number of vertices and file size.

Table 1. Basic Information of Experimental Data

Data Name	Data Type	Number of Objects	Number of Vertices	File Size/KB
(A)	Polyline	622	20122	349KB
(B)	Polyline	453	9845	179KB
(C)	Polygon	238	39905	647KB
(D)	Polygon	498	26240	439KB

The watermark information is a 32×64 image containing GIS MAP. The watermark image is scrambled by Arnold transform.

4.2 Experiment Design and Implementation

This section is to perform attack experiments with different types and intensities to verify the robustness of the proposed algorithm. The possible attacks in the actual use of vector geographic data are listed, including geometrical attack, object attack, precision reduction attacks and projection transformation. The proposed algorithm will focus on these attacks as an important aspect of the robustness evaluation. Geometrical attack includes translation, scaling and rotation, object attack includes object addition and object deletion, and there are four types of map projection on projection transformation attack, namely the equal area projection, the conformal projection, the equidistant projection, and the compromise projection. A qualified zero-watermarking algorithm can against the above attacks, the detailed attack settings for every type of attack will be given later. Table 2 shows the corresponding sub-types of different attack types

Table 2. The types of attack experiments

Attack types	Sub-type
Geometrical attacks	Translation Scaling

	Rotation
Object attacks	Object addition Object deletion
Precision reduction attack	Precision reduction
Projection transformation attacks	Equal area projection Conformal projection Equidistant projection Compromise projection

At the same time, two algorithms are selected for comparative experiments, referred to as Wang [25] and Zhu [28] separately. The algorithm proposed by Wang constructs concentric rings of all vertices and then constructs zero-watermark image by quantifying the number of vertices in each ring. The algorithm proposed by Zhu divides the vector geographic data into average blocks and calculates the singular values in the X and Y directions of each block respectively to construct zero-watermark image.

In addition, in order to highlight the robustness of projection transformation attacks, we select four different data for experiment and display the results in the projection transformation attack. In view of the limited space of the article, the other experiments only show the experimental results of data (D).

4.2.1 Geometrical Attacks

In general, geometrical attacks include translation, scaling, and rotation. In translation attack experiments, the experimental data is simultaneously translated in both X and Y directions. The translation distance ranges from 0 m to 3000 m with a gap of 500 m. Scaling attacks are divided into uniform scaling and non-uniform scaling. Uniform scaling means that the scale factor is the same in both X and Y directions, denoted as Sx, Sy. Non-uniform scaling means that the scale factor is not the same in the X and Y directions, which also leads to shape distortion. In the rotation attack experiments, the experimental data rotates clockwise with the data center by a rotation angle from 0° to 360° with a step of 60°. The partial attack results are shown in Figure 5.

4.2.2 Object Attacks

Object attacks include object addition and object deletion. Object attack will change the number of objects, with no effect on the basic shape of objects. The addition rate and deletion rate are equal from 0% to 50% of the original object number, with the step of 10%. Figure 6 shows object addition and Figure 7 shows object deletion.

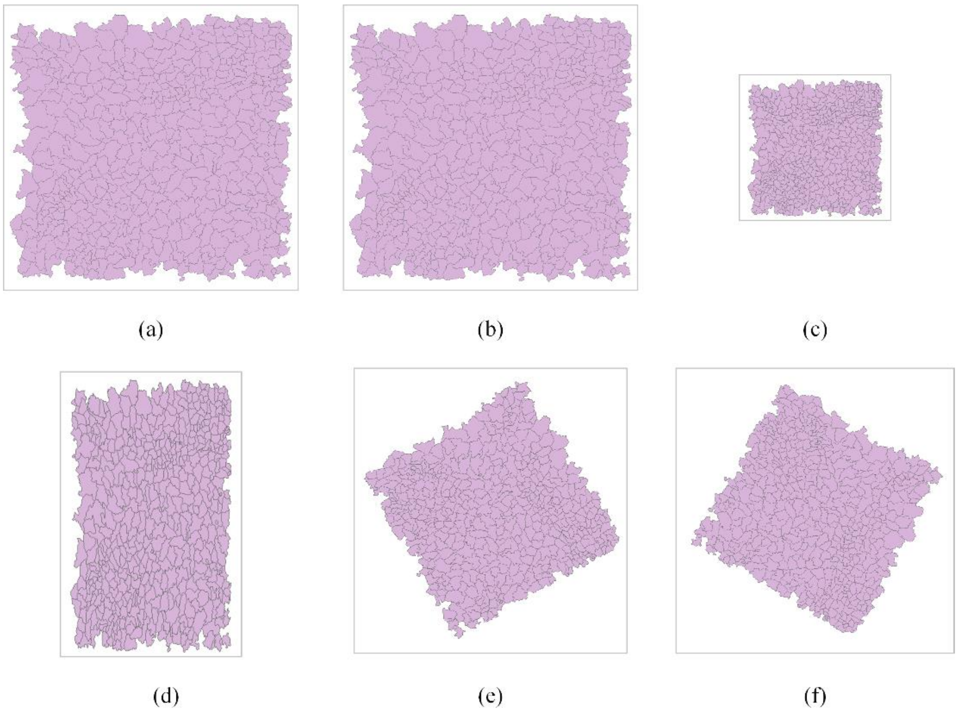


Figure 5. Data after geometrical attacks. (a) Translation distance=500m, (b) Translation distance=1000m, (c) $Sx=0.5$, $Sy=0.5$, (d) $Sx=0.6$, $Sy=1$, (e) Rotation angle=60°, (f) Rotation angle=120°.

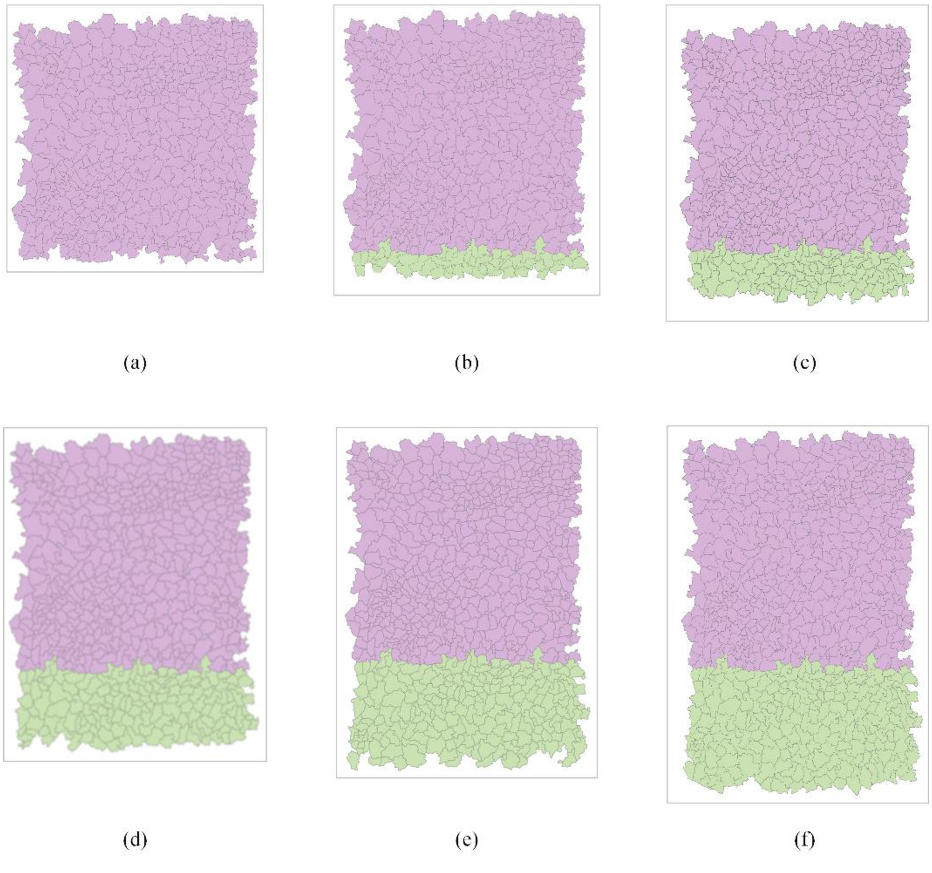


Figure 6. The original data after object addition attacks. (a) Original data, (b) Addition radio=10%, (c) Addition radio=20%, (d) Addition radio=30%, (e) Addition radio=40%, (f) Addition radio=50%.

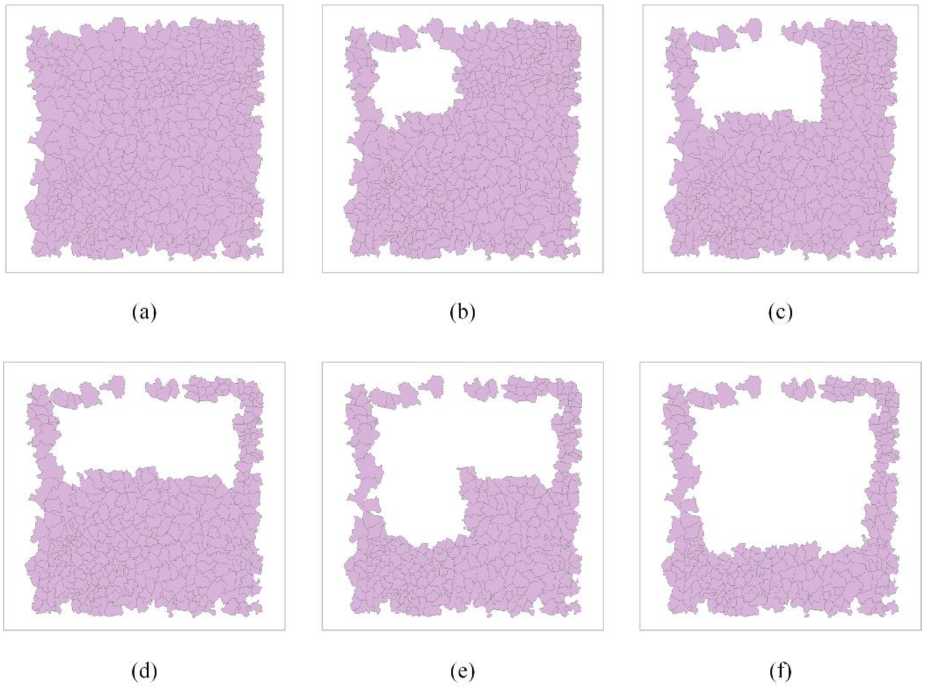


Figure 7. The original vector geographic data after object deletion attacks. (a) Original data, (b) Deletion radio=10%, (c) Deletion radio=20%, (d) Deletion radio=30%, (e) Deletion radio=40%, (f) Deletion radio=50%.

4.2.3 Precision Reduction Attacks

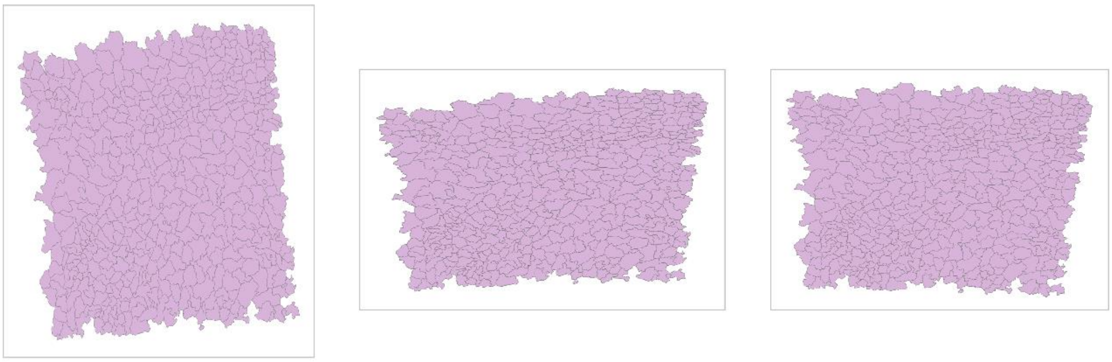
Precision reduction attack refers to an attack by reducing the accuracy of data without affecting the use of data. The effective decimal digit of vector geographic data used in this paper is 11 digits, and each attack is reduced by one digit until there are no decimal digits.

4.2.4 Projection Transformation Attacks

A good zero-watermarking algorithm should be against any projection transformations. To evaluate the robustness of the proposed algorithm to projection transformations, four different projection types are employed. Three subtypes are selected for each type of projection, for a total of 12 projection transformations. This is also to verify the feasibility of the proposed method as much as possible. Table 3 gives the specific projection types and subtypes. Figures 8-11 are schematic diagrams of four projections respectively, taking the data (D) Administrative divisions of county boundary as an example.

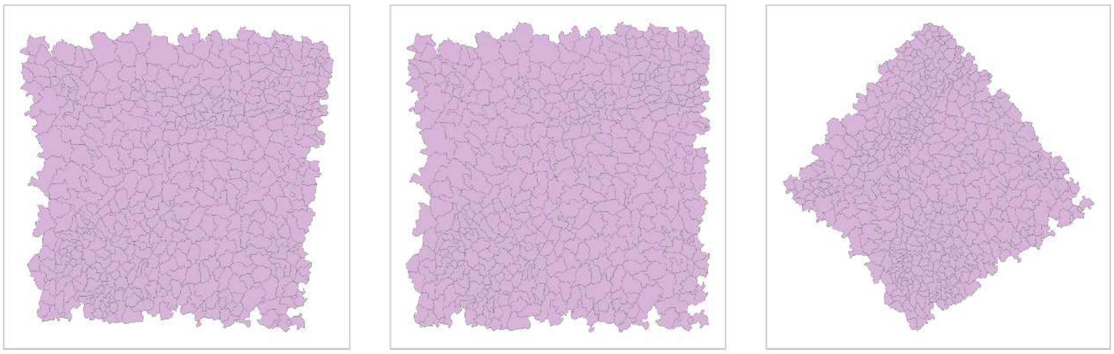
Table 3. Projection transformation

Projection Type	Projection Name	Projection Number
	Asia North Albers Equal Area conic Projection	1
Equal Area Projection	Asia South Albers Equal Area conic Projection	2
	Cylindrical Equal Area Projection	3
	Mercator Projection	4
Conformal Projection	Lambert Conformal Conic Projection	5
	Stereographic Projection	6
	Equidistant Azimuthal Projection	7
Equidistant Projection	Equidistant Cylindrical Projection	8
	Equidistant Conic Projection	9
	Robinson Projection	10
Compromise Projection	Winkel I Projection	11
	Aitoff Projection	12



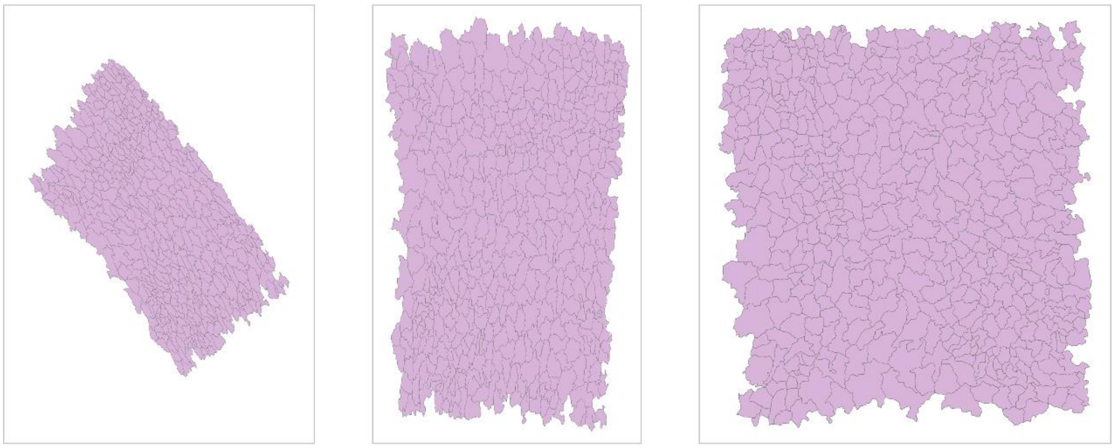
(a) (b) (c)

Figure 8. Equal Area Projection. (a) Asia North Albers Equal Area conic Projection, (b) Asia South Albers Equal Area conic Projection, (c) Cylindrical Equal-Area Projection.



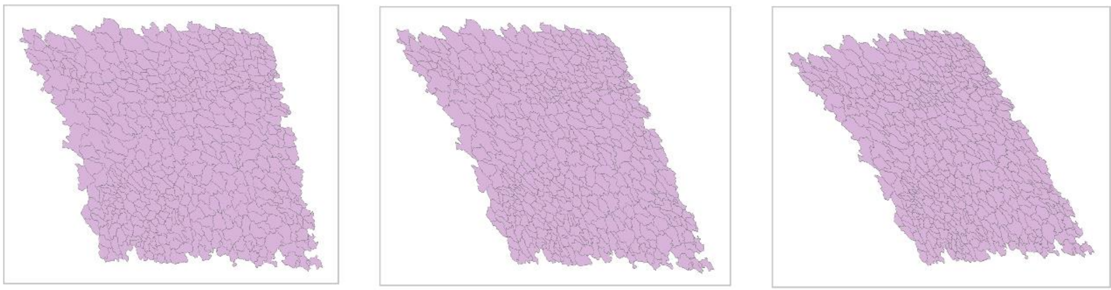
(a) (b) (c)

Figure 9. Conformal Projection. (a) Mercator Projection, (b) Lambert Conformal Conic Projection, (c) Stereographic Projection.



(a) (b) (c)

Figure 10. Equidistant Projection. (a) Equidistant Azimuthal Projection, (b) Equidistant Cylindrical Projection, (c) Equidistant Conic Projection.



(a) (b) (c)

Figure 11. Compromise Projection. (a) Robinson Projection, (b) Winkel I Projection, (c) Aitoff Projection.

4.3 Evaluation

In this step, it is necessary to compare the detected watermark image with the original watermark image. Normalized correlation (NC) is often used as a method to evaluate watermark quality. In this paper, we set the threshold value of NC as 0.80. If the value of NC is higher than 0.80, the copyright information will be detected successfully, otherwise, it will be detected failed. The mathematical equation of NC is as follows:

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} XNOR(W(i,j), W'(i,j))}{M \times N} \tag{7}$$

Where $W(i,j)$ and $W'(i,j)$ denote the original watermark image and the detected watermark image respectively; $M \times N$ is the size of the watermark image.

5 Robustness and Analyses

5.1 The Robustness of Geometrical Attacks

Figure 12 shows the result of geometrical attack. The algorithm proposed by Wang and Zhu has the same effect as the proposed algorithm in this paper in terms of translation attack, but it lacks robustness in scaling and rotation attack. Specifically, in the non-uniform scaling attack, the robustness of the algorithm proposed by them has been declining with the reduction of X direction and the increase of magnification, which cannot meet the requirements. In terms of rotation attacks, the algorithm proposed by Zhu is not robust to rotation attacks, because the grid division itself cannot against rotation attacks. The algorithm proposed by Wang has good robustness against rotation attacks because of the advantages of concentric rings. As can be seen from the figure, the NC value detected by the algorithm proposed in this paper is 1, so it has good robustness to geometrical attacks.

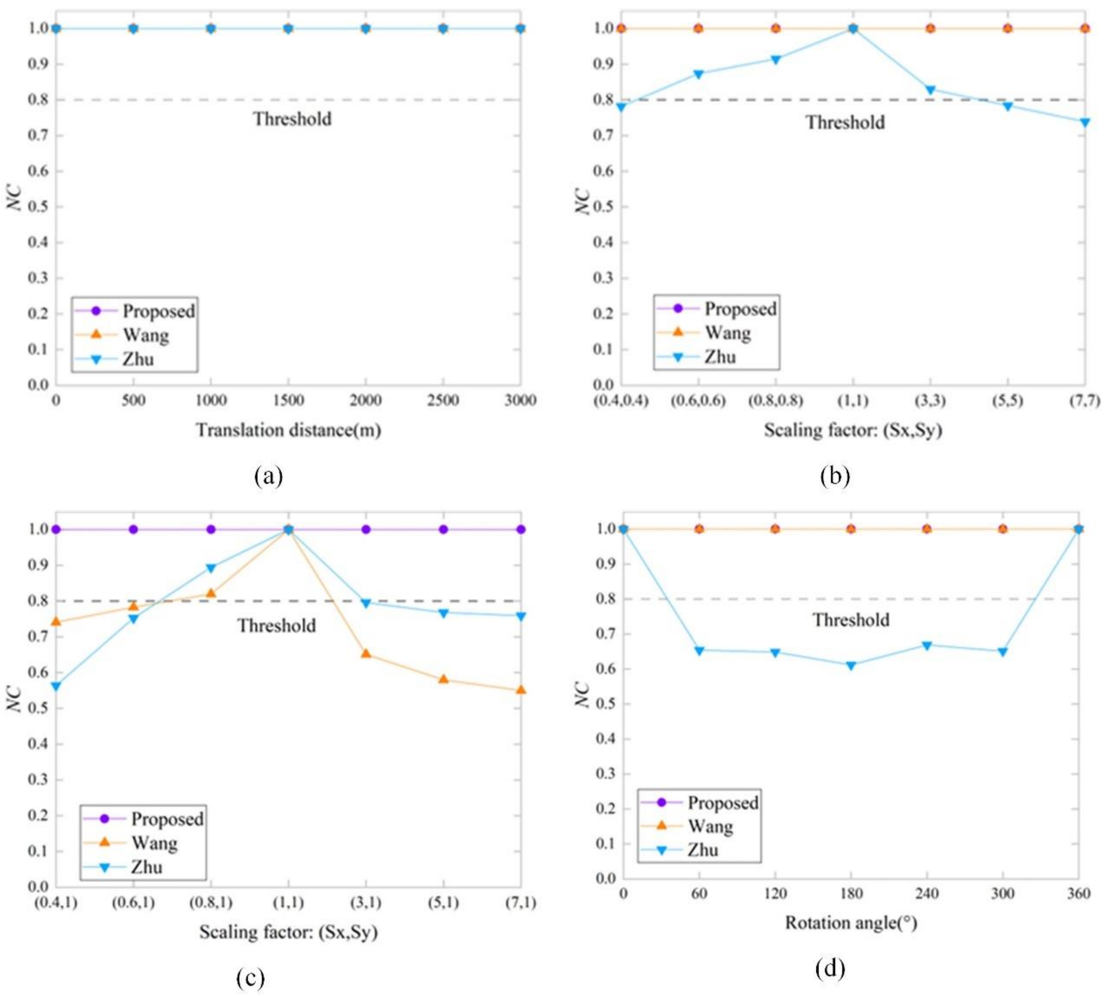
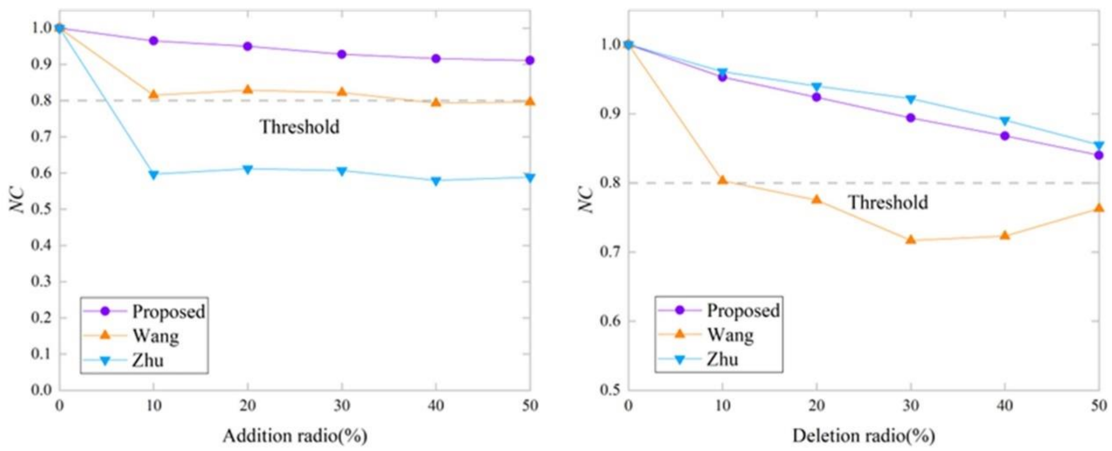


Figure 12. The robustness of geometrical attacks. (a) The robustness of translation attacks, (b) The robustness of uniform scaling attacks, (c) The robustness of non-uniform scaling attacks, (d) The robustness of rotation attacks.

5.2 The Robustness of Object Attacks

The result of object attack is shown in Figures 13. The NC values of object addition and object deletion vary with the ratio of addition and deletion. For object addition attacks, the NC value of both the proposed algorithm and the comparison algorithm decreases with the increase rate. Object addition attack has certain randomness, and different addition will produce different results. In this attack addition experiment, the minimum NC values of the proposed method and the algorithm proposed by Wang and Zhu are 0.965, 0.815 and 0.597, respectively. It can be seen from the figure that the fluctuation range of the algorithm proposed by Wang is large, and the algorithm proposed and Wang's algorithm have good robustness in the aspect of object addition. For object deletion attacks, the NC values of the algorithm in this paper and the other two algorithms will decrease with the increase of the deletion ratio. However, the algorithm in this paper and Zhu's algorithm can still detected NC values greater than 0.8 even if 50% of the objects are deleted, which is more advantageous than Wang's algorithm. In summary, the algorithm proposed in this paper has good robustness in object addition and object deletion attacks, and is better than Wang and Zhu's algorithm.



(a) (b)

Figure 13. The robustness of object attack. (a) The robustness of object addition attacks, (b) The robustness of object deletion attacks.

5.3 The Robustness of Precision Reduction Attacks

The precision reduction attack results are shown in Figure 14. Since the effective decimal places of the data are 11, the following 6 decimal places are discarded from the data under the premise of guaranteeing availability. The algorithm proposed by Wang relies on the number of vertices in concentric circles, and discarding a few decimal places has almost no effect on the calculation of the number of vertices. Zhu's algorithm is also against precision reduction attacks because singular value decomposition can have a good effect on small perturbations of the matrix. The algorithm proposed in this paper completely depends on the number of vertices on the line element or the surface element. The precision reduction attack will not cause any change in the number of vertices, so it can also completely against the precision reduction attack. It can be seen from the figure that the NC values of the three algorithms are all 1, which further shows that the three algorithms have good robustness to precision reduction attacks.

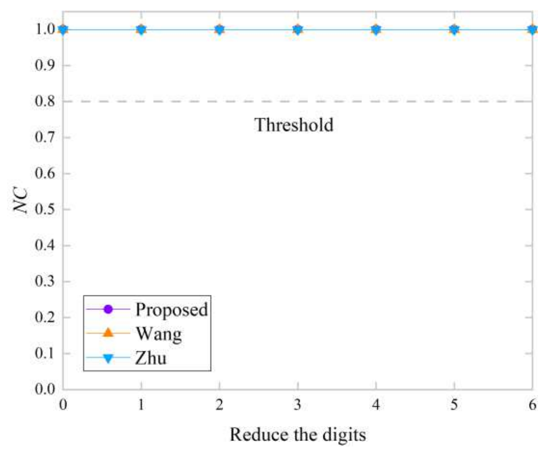


Figure14. The robustness of precision reduction attacks

5.4 The robustness of Projection Transformation Attacks

The result of the projection transformation is shown in Figure 15. The four figures are the experimental results of four kinds of data. As can be seen from the figures, the algorithm proposed by Wang has an overall NC value of about 0.8, which can meet the needs of projection transformation in most cases, but is not robust in individual projection transformations, so it is not perfect. The algorithm proposed by Zhu is completely different. Since the projection transformation can deform the data to different degrees, it has a great impact on the grid division. Therefore, the NC value is basically less than 0.8, and only some of them satisfy the projection transformation. Therefore, the method proposed by Zhu is basically not robust to projection transformations.

But the algorithm proposed in this paper only uses the relative storage order and the number of vertices, which are feature invariants after projection transformation, so it has good robustness to projection transformation in theory. At the same time, the experiment also proves that the detected NC value of the algorithm proposed in this paper remains at 1 for 12 different projection types. Therefore, it can be shown that the algorithm proposed has a good effect on projection transformation attacks and is more effective than other algorithms.

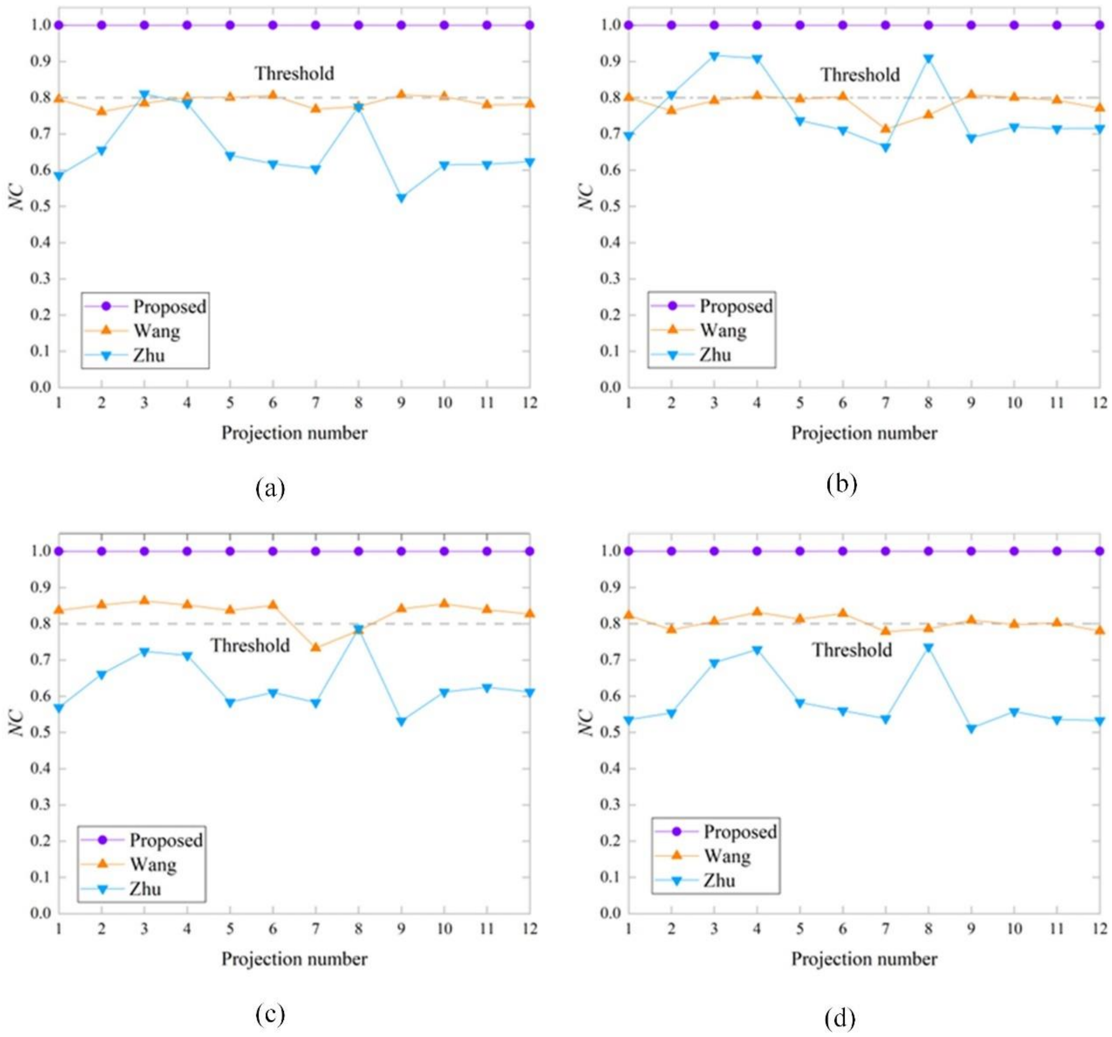


Figure 15. The robustness of projection transformation. (a) The robustness of data (A) river, (b) The results of data (B) highway, (c) The robustness of data (C) administrative divisions of prefectural boundary, (d) The robustness of data (D) administrative divisions of county boundary.

6 Discussions

The experimental results show that the proposed algorithm has strong robustness in many types of attacks, especially in projection transformation, which has a greater advantage than other algorithms. In order to better illustrate the advantages of the algorithm in this paper, the following three aspects will be discussed

6.1 Feature Invariants of Projective Transformation

Vector geographic data will be deformed to different degrees after projection transformation. For previous algorithms, most of them use features such as distance and angle to construct feature matrices, and these often cannot against the projection transformation. The proposed algorithm by using the number of vertices and relative storage order as feature invariants against projection transformation. Geometrical attacks and precision reduction attacks will change the coordinate values of vector geographic data, but will not affect the number of vertices on the objects, while cropping, although making the number of features decrease, will not affect the relative storage order of vector geographic data.

In addition, the projection transformation also only distorts the data, but does not affect the number of vertices and the relative storage order, which are feature invariants. The experimental results also prove that these feature invariants used in the four types of projection transformation, not just in one of them. Thus, the algorithm can completely against any projection transformation.

6.2 The Analysis of the Watermark Index and Watermark bit

The number of vertices as a feature invariant of the projection transformation, the mathematical operation of the number of vertices to establish the watermark index with the original watermark information is stable. However, the operation of adding vertices or deleting vertices to the features will make the watermark index not work correctly, which is also a shortcoming of the algorithm in this paper.

Secondly, since each watermark bit is used multiple times, the voting principle also used multiple times in this algorithm. The voting principle can modify the wrong result induced object addition and deletion and greatly improve the probability of watermark detection. Therefore, the voting principle plays an important role in object addition and object deletion, which has also been well proved in the experiment.

6.3 Applicable Data Type

In this algorithm, the number of vertices of polyline or polygon is used to establish the index between the original watermark and the watermark information is determined according to the number of vertices. The number of vertices determines the whole process of generating the feature matrix. It is because any polyline and polygon have different number of vertices that the generation of feature matrix can be guaranteed. However, it is not suitable for point data. The reason is that a point object has only one vertex, and the watermark index and watermark bit generated in the relative storage order are single. Therefore, the watermark index between and the original watermark information cannot be constructed effectively.

7 Conclusions

At present, few zero-watermarking algorithms of vector geographic data can against projection transformation, the problem is that it is difficult to find the feature invariant of projection transformation. Two feature invariants are introduced in this paper, namely the number of vertices and the relative storage order. The former is used to determine the watermark index, and the latter is used to determine the watermark bit, which is the basis of the algorithm in this paper. Experimental results show that the algorithm can against arbitrary projection transformation and is robust to geometrical attack, object attack and precision reduction. The proposed algorithm also provides a new exploration for zero-watermarking algorithm of vector geographic data against projection transformation. However, the limitation of this algorithm is not applicable to point data. A feasible approach is to construct Voronoi diagrams so that each point has a Thiessen polygon, but the number of vertices of the Thiessen polygon is also limited and cannot be completely applicable. This will also be central to further work.

Declarations Section:

Author's Contributions: SW conceived and designed the experiments; SW and LZ carried out the method; SW performed the analysis and wrote the paper; LZ, QZ and YL reviewed and edited the manuscript. All authors read and approved the final manuscript.

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

Availability of Data and Materials: Please contact me if you want to request the data. (11200866@stu.lzjtu.edu.cn)

Funding: This study was supported by the National Natural Science Foundation of China (Project NO. 41761080), Industrial Support and Guidance Project of Universities in Gansu Province (Project NO. 2019C-04) and by LZJTU EP (Project NO. 201806).

References

1. Zhang L, Yan H, Zhu R, et al. Combinational spatial and frequency domains watermarking for 2D vector maps[J]. Multimedia tools and applications, 2020, 79(41): 31375-31387.
2. Xi X, Zhang X, Sun Y, et al. Topology-preserving and geometric feature-correction watermarking of vector maps[J]. IEEE Access, 2020, 8: 33428-33441.
3. Yang C, Zhu C, Wang Y, et al. A robust watermarking algorithm for vector geographic data based on QIM and matching detection[J]. Multimedia Tools and Applications, 2020, 79(41): 30709-30733.
4. Hou X, Min L, Yang H. A reversible watermarking scheme for vector maps based on multilevel histogram modification[J]. Symmetry, 2018, 10(9): 397.
5. Yan H, Zhang L, Yang W. A normalization-based watermarking scheme for 2D vector map data[J]. Earth Science Informatics, 2017, 10(4): 471-481.
6. Lopez C. Watermarking of digital geospatial datasets: a review of technical, legal and copyright issues[J]. International Journal of Geographical Information Science, 2002, 16(6): 589-607.
7. Zhu C. Research progresses in digital watermarking and encryption control for geographical data[J]. Acta Geodaetica et Cartographica Sinica, 2017, 46(10): 1609.
8. Abubahia, A.; Cocea M. Advancements in GIS map copyright protection schemes-a critical review[J]. Multimedia Tools and Applications, 2017, 76(10): 12205-12231.
9. Peng F, Lin Z X, Zhang X, et al. Reversible data hiding in encrypted 2D vector graphics based on reversible mapping model for real numbers[J]. IEEE transactions on information forensics and security, 2019, 14(9): 2400-2411.
10. Voigt, M.; Busch C. Feature-based watermarking of 2D vector data[C]//Security and Watermarking of Multimedia Contents V. SPIE, 2003, 5020: 359-366.
11. Yan H, Li J, Wen H. A key points-based blind watermarking approach for vector geo-spatial data[J]. Computers, Environment and Urban Systems, 2011, 35(6): 485-492.
12. Wang Y, Yang C, Zhu C, et al. An efficient robust multiple watermarking algorithm for vector geographic data[J]. Information, 2018, 9(12): 296.

13. Ren N, Wang Q, Zhu C. Selective authentication algorithm based on semi-fragile watermarking for vector geographical data[C]//2014 22nd International Conference on Geoinformatics. IEEE, 2014: 1-6.
14. Wang X, Huang D, Zhang Z. A DCT-based blind watermarking algorithm for vector digital maps[C]//Advanced Materials Research. Trans Tech Publications Ltd, 2011, 179: 1053-1058.
15. Shen T, Xu D, Li C, et al. Watermarking GIS data for digital map copyright protection[C]//Proceedings of 24th International Cartographic Conference. 2009, 1: 1-9.
16. Xu D, Zhu C, Wang Q. A Construction of Digital Watermarking Model for the Vector Geospatial Data Based on Magnitude and Phase of DFT[J]. Journal of Beijing University of Posts and Telecommunications, 2011, 34(5): 25.
17. Xu D, Wang Q. The study of watermarking algorithm for vector geospatial data based on the phase of DFT[C]//2010 IEEE International Conference on Wireless Communications, Networking and Information Security. IEEE, 2010: 625-629.
18. Wang X, Shao C, Xu X, et al. Reversible data-hiding scheme for 2-D vector maps based on difference expansion[J]. IEEE Transactions on information forensics and security, 2007, 2(3): 311-320.
19. Cao L, Men C, Ji R. High-capacity reversible watermarking scheme of 2D-vector data[J]. Signal, Image and Video Processing, 2015, 9(6): 1387-1394.
20. Ren N, Zhou Q, Zhu C, et al. A Lossless Watermarking Algorithm Based on Line Pairs for Vector Data[J]. IEEE Access, 2020, 8: 156727-156739.
21. Wen Q, SUN T, Wang S. Concept and application of zero-watermark[J]. ACTA ELECTONICA SINICA, 2003, 31(2): 214.
22. Wang X, Huang D, Zhang Z. A robust zero-watermarking algorithm for 2D vector digital maps[M]//Computer, Informatics, Cybernetics and Applications. Springer, Dordrecht, 2012: 533-541.
23. Peng Y, Yue M. A zero-watermarking scheme for vector map based on feature vertex distance ratio[J]. Journal of Electrical and Computer Engineering, 2015, 2015.
24. Zhou Q, Zhu C, Ren N, et al. Zero Watermarking Algorithm for Vector Geographic Data Based on the Number of Neighboring Features[J]. Symmetry, 2021, 13(2): 208.
25. Wang X, Huang D, Zhang Z. A robust zero-watermarking algorithm for vector digital maps based on statistical characteristics[J]. Softw. Appl. Econ. Anal. Bus. Manag, 2012, 7: 2349.
26. Li W, Yan H, Wang Z, et al. A zero-watermarking algorithm for vector linear feature data[J]. J. Geomat. Sci. Technol, 2016, 33: 94-98.
27. Xi X, Zhang X, Liang W, et al. Dual zero-watermarking scheme for two-dimensional vector map based on delaunay triangle mesh and singular value decomposition[J]. Applied Sciences, 2019, 9(4): 642.
28. Zhu C, Xu D, Ren N, et al. Model and implementation of geographic data transaction certificate and copyright protection based on blockchain and digital watermarking[J]. Acta Geodaetica et Cartographica Sinica, 50(12): 1694.
29. Ren N, Zhao Y, Zhu C, et al. Copyright Protection Based on Zero Watermarking and Blockchain for Vector Maps[J]. ISPRS International Journal of Geo-Information, 2021, 10(5): 294.
30. Yan J, Song X, Gong G. Averaged ratio between complementary profiles for evaluating shape distortions of map projections and spherical hierarchical tessellations[J]. Computers & Geosciences, 2016, 87: 41-55.
31. Zhou Q, Ren N, Zhu C, et al. Blind Digital Watermarking Algorithm against Projection Transformation for Vector Geographic Data[J]. ISPRS International Journal of Geo-Information, 2020, 9(11): 692.
32. Zhang Z, Wu L, Yan Y, et al. An improved reversible image watermarking algorithm based on difference expansion[J]. International Journal of Distributed Sensor Networks, 2017, 13(1): 1550147716686577.
33. Saadi, S.; Merrad, A.; Benziane A. Novel secured scheme for blind audio/speech norm-space watermarking

by Arnold algorithm[J]. Signal Processing, 2019, 154: 74-86.