

High-Capacity and Robust Watermarking Scheme for Small-Scale Vector Data

Deyu Tong¹, Changqing Zhu^{2,3,4*}, Na Ren^{2,3,4} and Wenzhong Shi⁵

¹ College of Information Engineering, Nanjing University of Finance and Economics, Nanjing, Jiangsu 210023, China

[e-mail: tdyforweb@163.com]

² Key Laboratory of Virtual Geographic Environment (Nanjing Normal University), Ministry of Education, Nanjing, Jiangsu 210023, China

³ State Key Laboratory Cultivation Base of Geographical Environment Evolution (Jiangsu Province), Nanjing, Jiangsu 210023, China

⁴ Jiangsu Center for Collaborative Innovation in Geographical Information Resource Development and Application, Nanjing, Jiangsu 210023, China

[e-mail: zcq88@263.net, renna1026@163.com]

⁵ Department of Land Surveying and Geo-Informatics, The Hong Kong Polytechnic University, Kowloon, Hong Kong, China;

[e-mail: lswzshi@polyu.edu.hk]

*Corresponding author: Changqing Zhu

*Received July 4, 2018; revised January 9, 2019; accepted July 4, 2019;
published December 31, 2019*

Abstract

For small-scale vector data, restrictions on watermark scheme capacity and robustness limit the use of copyright protection. A watermarking scheme based on robust geometric features and capacity maximization strategy that simultaneously improves capacity and robustness is presented in this paper. The distance ratio and angle of adjacent vertices are chosen as the watermark domain due to their resistance to vertex and geometric attacks. Regarding watermark embedding and extraction, a capacity-improved strategy based on quantization index modulation, which divides more intervals to carry sufficient watermark bits, is proposed. By considering the error tolerance of the vector map and the numerical accuracy, the optimization of the capacity-improved strategy is studied to maximize the embedded watermark bits for each vertex. The experimental results demonstrated that the map distortion caused by watermarks is small and much lower than the map tolerance. Additionally, the proposed scheme can embed a copyright image of 1024 bits into vector data of 150 vertices, which reaches capacity at approximately 14 bits/vertex, and shows prominent robustness against vertex and geometric attacks for small-scale vector data.

Keywords: Digital watermarking, capacity, robustness, vector data, small-scale data

This research was supported by Jiangsu Province Surveying and Mapping Geographic Information Research Project under grant No JSCHKY201902, National Natural Science Foundation of China under grant No 41301413, the Priority Academic Program Development of Jiangsu Higher Education Institutions, Six Talent Peaks Project in Jiangsu Province and Outstanding Innovation Team in Colleges and Universities in Jiangsu Province.

1. Introduction

As an important data type and form of geographic information system (GIS), geographical vector data have been widely used for research in many industries. Due to the high accuracy and copyright value of vector data, data piracy and leakage have become security issues that severely threaten data owners. Although the study of GIS has moved into the big data era [1, 2], the data volume of geographical vector data may be very small, e.g., tiled vector map used in online map service, observation points near country borders and objects in military usage, etc. The low volume feature makes the vector data easier to duplicate, distribute and modify. Hence, it is important to protect the copyright of vector data, especially for small-scale data.

Digital watermarking is an effective method for copyright identification and usage tracking, which means embedding copyright information into media secretly without degrading data fidelity [3, 4]. It has been studied and applied in copyright protection for a variety of multimedia data [5-12], including vector data [13-30]. However, in terms of small-scale vector data, both the watermarking capacity and robustness have been the key factors in watermarking algorithm research. The watermarking capacity determines whether the copyright information can be successfully embedded into small-scale data, while the robustness provides the watermark resistance against various kinds of attacks. Although some researches concerning about watermarking vector data have been conducted, the robustness and watermark capacity are not sufficiently high and applicable for small-scale vector data. The detailed analysis of this drawback is clarified in section 2.

To improve the capacity and robustness of watermarking algorithm for small-scale vector data, a high-capacity and robust watermarking scheme is proposed in this paper. The main contributions are summarized as follows:

(1) The distance ratio and angle formed by adjacent vertices are chosen as the robust geometric features carrying watermark information. As the stability of the geometric features under vertex attacks and geometric attacks, the proposed watermarking algorithm is essentially robust against those attacks.

(2) The capacity-improved strategy is proposed based on quantization index modulation (QIM) and geometric constraints. By dividing more intervals in QIM and optimizing the interval parameter under constraints, the capacity is increased into a much higher level.

The remaining parts of this paper are arranged as follows. In section 2, the related work is reviewed. Section 3 discusses and analyzes the robust geometric features, where watermark is embedded and extracted. The capacity-improved strategy is proposed in section 4, and its optimization is given in section 5. Based on the robust geometric features and capacity-improved strategy, the proposed watermarking scheme is demonstrated in section 6, and the experimental results are presented in section 7. Finally, conclusions are drawn in section 8.

2. Related Work

The watermarking method consists of three steps. First, the data is converted in watermark domain and watermark is embedded into it. Then, watermarked data is distributed or shared by its owners. Finally, if there is any suspect data, watermark is extracted from its watermark domain and copyright identification is realized according to the extracted watermark. The whole procedure is illustrated in Fig. 1.

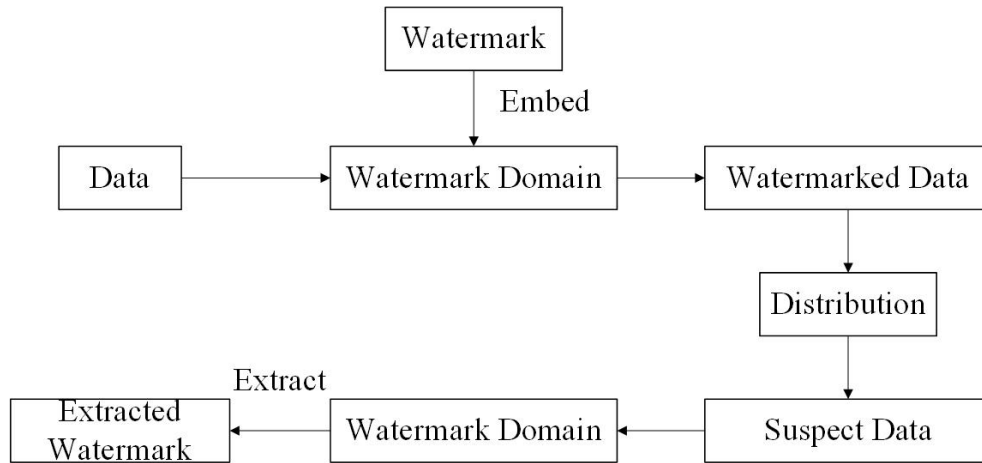


Fig. 1. The watermarking procedure

From the perspective of embedding domain, watermarking algorithms for vector data can be divided into the spatial domain and the transformation domain. Watermarking algorithms based on spatial domain embed watermark into spatial coordinates [15, 16, 18, 20, 23, 28, 31], statistical indices [14, 32-34], metric measurements [22], angles [35], areas [36], arc lengths [25], geometric coordinates [26, 37, 38], etc. Generally, watermarking methods considering geometric feature factors have more resistance against rotation, scaling and translation (RST) attack. Furthermore, transformation-based watermarking methods embed watermark in the coefficients after transformations such as discrete Fourier transformation [26, 37, 38] and discrete wavelet transformation [19]. Transformation-based methods are more robust against several types of global attack, including noise addition or filtering. Apart from the embedding domain, these research also proposed different embedding strategies to enhance the watermark robustness against various types of attack.

It can be seen from the above research, more attention has been paid on robustness rather than watermark capacity. As another key factor of watermarking schemes, watermark capacity determines how many watermark bits can be embedded into the small-scale vector data. Commonly, the capacity is measured as the number of bits that each vertex can provide. If the watermarking capacity is low, the copyright information cannot be completely embedded in small-scale vector data, which leads to watermark extraction failure.

Until now, few researchers contributed to the study of high-capacity watermarking. Wang compressed watermark with vertex properties and embed them into coordinates directly with the capacity of nearly 0.3 bits/vertex [18]. Yamada offered an embedding strategy that inserts new vertices into polylines; the capacity reached 500 bytes for less than 500 vectors [20]. In fact, this mechanism can provide an arbitrary capacity as long as the accuracy is high enough. However, inserting new vertices changes the vertex number and increases the data volume, making it easy to remove the embedded watermark and degrading data fidelity. Cao proposed a watermarking strategy which embeds watermark iteratively into the median value of coordinate sequence [32, 34]. The capacity of this method exceeded 5 bits/vertex with some visible distortions. The methods provided in [23, 33] embed watermarks according to a histogram of the coordinates and result in a capacity of approximately 0.8 bits/vertex. Xiao improved the quantization modulation scheme by setting more quantization intervals, which resulted in a capacity of 2 bits/vertex [28]. Wang split the distance into several intervals to

represent more state values [26]. In this scheme, each vertex can carry at least 2 bits, and the capacity is proportional to the number of subintervals.

However, the problems of watermarking small-scale vector data, namely the watermark capacity and robustness, have not been comprehensively addressed. Most of the previous methods, either focusing on robustness [13-15, 19, 21, 22, 25] or reversibility [18, 23, 28, 33], fail to handle small-scale vector data as the capacity less than 4 bits/vertex. For example, embedding a 32×32 binary image into a vector data with 150 vertices is difficult for them. Although the capacity of some proposed watermark schemes is high enough for small-scale vector data [26, 32, 34], low robustness of those watermarking schemes means that watermark cannot be properly extracted after data manipulation. This is because the embedding strategies or domains of them, attaching importance to reversibility [18, 23, 26, 32-34], are not resisted towards attacks including vertex deletion, vertex insertion, vertex update, rotation, etc. Hence, the high watermark capacity and robustness have not been achieved at the same time to watermark small-scale vector data.

In this paper, a watermarking algorithm intended for improving watermark capacity and robustness simultaneously have been studied and verified.

3. Robust Geometric Features

3.1 Features Chosen

Prior to study watermark embedding strategies, the watermark embedding domain or position needs to be studied first. Several high-capacity watermarking methods directly embed watermarks into the coordinates of vector data. In contrast with these embedding domains, geometric features are considered in the proposed watermarking method. Here, the distance ratio and angle of adjacent lines are chosen to carry the watermark information.

According to the structure of the geographical vector data, polylines are similar to polygons; hence, the features are easily determined by their adjacent relationship in topology. For discrete points, the adjacent relationship can refer to the object index in data file. Specifically, the distance ratio and angle of adjacent polylines are denoted as R and A , respectively. P represents a polyline, polygon or a set of points. Suppose P consists of n vertices recorded as $V_i(x_i, y_i)(i=1, 2, \dots, n)$, where x_i and y_i are the coordinates of each vertex. Then, the computation of the distance ratio $R_i(i=2, 3, \dots, n-1)$ is:

$$R_i = \frac{|V_i V_{i+1}|}{|V_{i-1} V_i|} = \frac{\sqrt{(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2}}{\sqrt{(x_i - x_{i-1})^2 + (y_i - y_{i-1})^2}} \quad (1)$$

and the computation of angle A_i is:

$$\begin{aligned} A_i &= \angle V_{i-1} V_i V_{i+1} = \arccos \left(\frac{\overrightarrow{V_i V_{i-1}} \cdot \overrightarrow{V_i V_{i+1}}}{|V_i V_{i-1}| \times |V_i V_{i+1}|} \right) \\ &= \arccos \left(\frac{(x_{i-1} - x_i)(x_{i+1} - x_i) + (y_{i-1} - y_i)(y_{i+1} - y_i)}{\sqrt{(x_{i-1} - x_i)^2 + (y_{i-1} - y_i)^2} \sqrt{(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2}} \right) \end{aligned} \quad (2)$$

Fig. 2 illustrates these features.

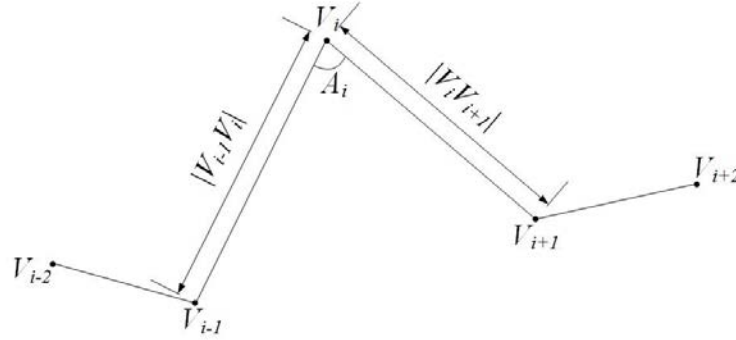


Fig. 2. Illustration of the distance ratio and the angle of the adjacent lines

3.2 Feature Properties

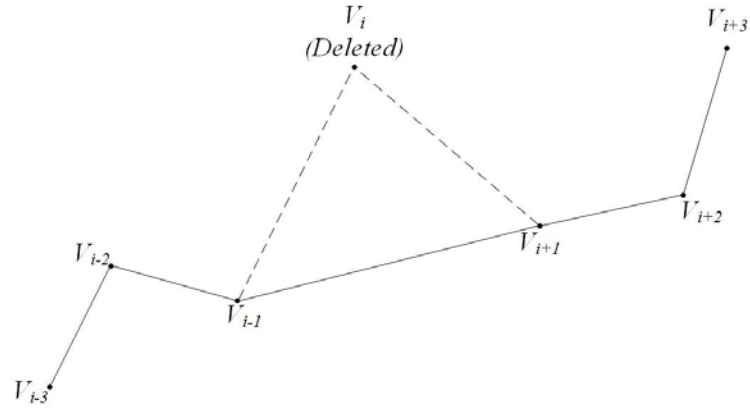
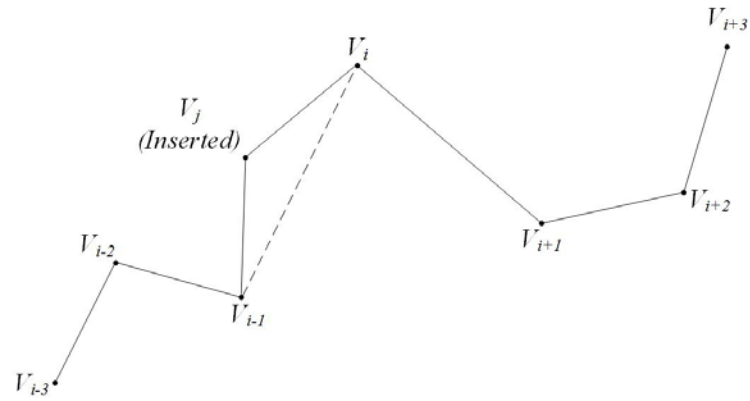
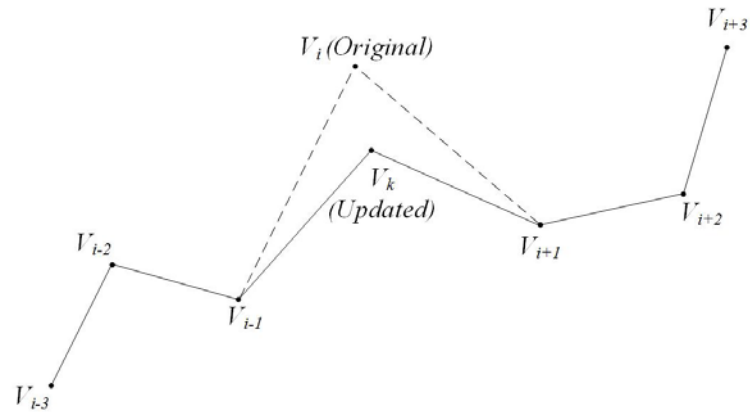
In the proposed watermarking scheme, the distance ratio R and the angle A carry watermark information because watermark capacity and robustness are related to their characteristics. These feature properties are discussed and analyzed here.

1) Independence. The distance ratio and angle provide two types of watermark carriers. As watermark embedding changes the feature values, conflicts caused by the changes should be avoided. Otherwise, watermarks will be embedded improperly due to conflicts. Thus, the independence of the features should be guaranteed first.

To clearly demonstrate the independence of the distance ratio and angle, polar coordinates are used instead of Cartesian coordinates. The symbols used in [Fig. 2](#) are also used here. For each distance ratio R_i and angle A_i , the origin of the polar coordinate is set to point V_i , and the unit length is $|V_i V_{i+1}|$. Then, the coordinates of V_{i+1} are (R_i, A_i) . Consequently, the process of watermark embedding changes $V_{i+1}(R_i, A_i)$ to $V_{i+1}'(R_i + \Delta R, A_i + \Delta A)$. As polar coordinates can be mapped into Cartesian coordinates, the position of the watermarked vertex V_{i+1}' can be determined accurately and uniquely. From this perspective, the independence of the distance ratio from the angle is clarified clearly.

2) Robustness against geometric attack. Common geometric attacks of GIS vector data include translation, scaling and rotation. It is easy to deduce that the distance ratio and angle of adjacent lines are invariant in these geometric transformations. Then, for each vertex V_i , the watermarked coordinates $V_{i+1}'(R_i + \Delta R, A_i + \Delta A)$ remain unchanged and the watermark can be extracted without distortion. Hence, the features essentially and naturally provide robustness against geometric attacks.

3) Robustness against vertex attacks. Vertex editing is widely used to process GIS vector data, which affects watermark extraction. Common vertex attacks include vertex deletion, vertex insertion and vertex update. These three types of attacks are shown in [Fig. 3–5](#).

**Fig. 3.** Vertex deletion attack**Fig. 4.** Vertex insertion attack**Fig. 5.** Vertex update attack

For the vertex deletion attack in **Fig. 3**, the deletion of vertex V_i will only change the original distance ratios $\frac{|V_{i-1}V_i|}{|V_{i-2}V_{i-1}|}$, $\frac{|V_iV_{i+1}|}{|V_{i-1}V_i|}$, $\frac{|V_{i+1}V_{i+2}|}{|V_iV_{i+1}|}$ and the angles $\angle V_{i-2}V_{i-1}V_i$, $\angle V_{i-1}V_iV_{i+1}$, $\angle V_iV_{i+1}V_{i+2}$; the other features remain the same. In watermark extraction, incorrect watermark information

will be extracted by distance ratios $\frac{|V_{i-1}V_{i+1}|}{|V_{i-2}V_{i-1}|}$, $\frac{|V_{i+1}V_{i+2}|}{|V_{i-1}V_{i+1}|}$ and angles $\angle V_{i-2}V_{i-1}V_i$, $\angle V_{i-2}V_{i-1}V_i$.

However, this type of error, which can be reduced or eliminated by the mapping mechanism of the proposed scheme in section 6, is not considered here. The analysis here focuses on the remaining watermark capacity after attacks. If a geometric object P consists of n vertices $V_i (i=1,2,...,n)$, the watermark capacity that each distance ratio and angle can provide is denoted as a and b bits, respectively. Then, the watermark capacity provided by P is $(a+b)(n-2)$ bits. After the watermarked vertex $V_i (i=3,4,...,n-2, n \geq 5)$ is deleted, the remaining watermark capacity provided by P is $(a+b)(n-5)$ bits. If m consequent vertices have been deleted in P , the watermark capacity becomes $(a+b)(n-m-4)$ bits. In the worst situation, the watermark capacity is still greater than $(a+b)(n-3m-2)$ bits after deleting m vertices from each interval containing 3 vertices (e.g., the vertices $V_{3i} (i=1,2,...,m)$ are deleted). This nearly linear relationship demonstrates that the features are robust against vertex deletion.

The features robustness against vertex insertion and updating are analyzed in the same way. For vertex insertion attack, inserting n consequent vertices reduces the capacity to $(a+b)(n-4)$ bits, which is a constant value. For vertex update attacks, the relationship between the updated vertex count and capacity is the same as that of vertex deletion. Hence, the watermark capacity with a number of inserted or updated vertices is also nearly linearly dependent.

Taking these properties into consideration, the distance ratio and angle are robust against geometric and vertex attacks. Hence, in the proposed watermarking scheme, watermark will be embedded in these features, which carry watermark in a stable and robust way.

4. Capacity-Improved Watermarking Strategy

In the proposed watermarking scheme, watermark is embedded in and extracted from the features mentioned above. Quantization index modulation (QIM), which proves to be effective and robust [39], is adopted as the watermark embedding and extracting method. As the watermark capacity is limited for small-scale vector data, a capacity-improved watermarking strategy based on QIM is studied here to embed as much watermark as possible.

4.1 Introduction to QIM

QIM divides the value space into two types of intervals, where each interval represents a watermark value, and modulates the original value into the section corresponding to the embedded watermark value. Specifically, if a binary watermark bit $w (w \in \{0,1\})$ is embedded into the numerical value c and the quantization interval length is l , then the numerical value c is modulated to c' according to:

$$\begin{cases} c' = c & \text{if } x \% 2l < l \text{ and } w = 0 \\ c' = c - l & \text{if } x \% 2l \geq l \text{ and } w = 0 \\ c' = c - l & \text{if } x \% 2l < l \text{ and } w = 1 \\ c' = c & \text{if } x \% 2l \geq l \text{ and } w = 1 \end{cases} \quad (3)$$

Here, % represents the modulo operation. The watermark embedding process based on QIM is illustrated in Fig. 6.

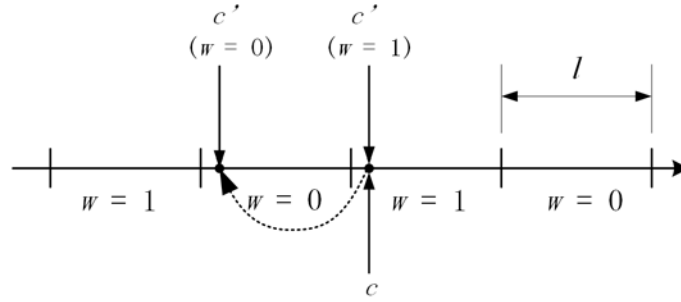


Fig. 6. Illustration of the watermark-embedding process based on QIM

Then, the watermark bit w can be extracted by:

$$\begin{cases} w = 0 & \text{if } c' \% 2l < l \\ w = 1 & \text{if } c' \% 2l \geq l \end{cases} \quad (4)$$

4.2 Capacity-Improved QIM

The two types of intervals in QIM correspond to the binary watermark bits. To carry more watermark bits, the value range can be divided into more types of intervals with shorter lengths. When the number of interval types changes from 2 to k , the corresponding watermark becomes $w (w \in \{0, 1, 2, \dots, k-1\})$. Then, the watermark embedding process using QIM is expected to modulate the value from current interval into watermark value interval. For example, the original value c is laid on the interval representing value p , embedding watermark “2” means moving the value c into the interval indicating $w = 2$, which is shown in **Fig. 7**.

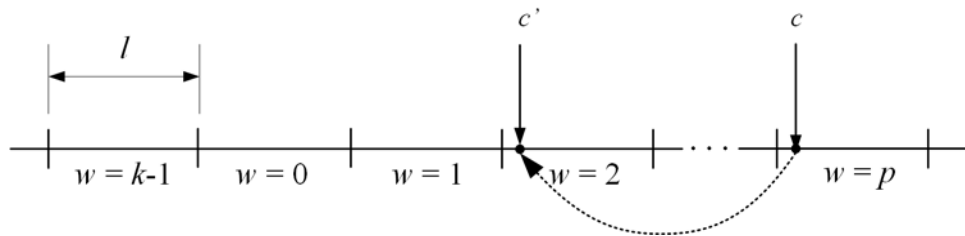


Fig. 7. Illustration of embedding watermark “2” by capacity-improved QIM

Generally, embedding the watermark $w (w \in \{0, 1, 2, \dots, k-1\})$ into value c is the procedure that first calculates the value p indicated by the current interval:

$$p = \left\lfloor \frac{c - \left\lfloor \frac{c}{kl} \right\rfloor \times kl}{l} \right\rfloor \quad (5)$$

and then modulate value c into c' :

$$c' = c + l \times (w - p) \quad (6)$$

The operation $\lfloor \cdot \rfloor$ rounds the number down to the nearest integer.

Then, extracting watermark $w (w \in \{0, 1, 2, \dots, k-1\})$ from value c' yields:

$$w = \left\lfloor \frac{c' - \left\lfloor \frac{c'}{kl} \right\rfloor \times kl}{l} \right\rfloor \quad (7)$$

Hence, the capacity-improved QIM increases the watermark capacity from 1 bit to $\lfloor \log_2 k \rfloor$ bits for each watermarked value c' .

4.3 Distortion Reduction

In the embedding process of capacity-improved QIM, the maximum distortion on numerical value c is kl because the modulation is only in one direction according to Equation (6). To further enhance the watermark capacity under the same distortion tolerance, the embedding process can be optimized to modulate in dual directions, as the intervals are repeated and continuous along the value axis. For example, if the original value c laid on the interval representing value p , embedding watermark “1” is to move the value c into the interval indicating $w = 1$, the moving direction is determined by the shortest modulation length. The modulation process is shown in Fig. 8.

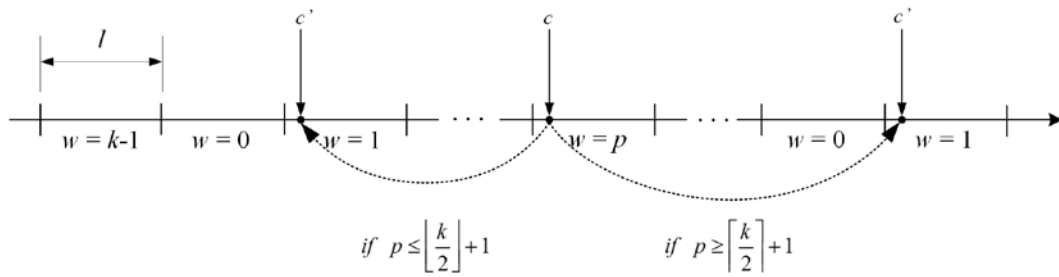


Fig. 8. Modulation by reducing distortions

In this circumstance, the maximum distortion Δ_{\max} for each watermarked value is reduced to:

$$\Delta_{\max} = \left\lfloor \frac{k}{2} \right\rfloor l \quad (8)$$

Generally, the modulation of distortion reduction is expressed as:

$$\begin{cases} c' = c + (w - p) \times l & \text{if } |p - w| \leq \left\lfloor \frac{k}{2} \right\rfloor \\ c' = c + (w - p + k) \times l & \text{if } w - p + k \leq \left\lfloor \frac{k}{2} \right\rfloor \text{ and } p \geq w \\ c' = c + (w - p - k) \times l & \text{if } p - w + k < \left\lfloor \frac{k}{2} \right\rfloor \text{ and } p < w \end{cases} \quad (9)$$

The extraction formula is the same as Equation (7). If the distortion tolerance stays the same, then the maximum capacity will increase 1 bit for each watermarked value c' compared with the method in section 4.2.

5. Capacity Maximization under Constraints

5.1 Two Constraints

The distance ratio R and angle A studied in section 3 are used to carry information, and the distortion-reduced QIM discussed in section 4.3 is adopted to embed watermark into these features. However, the watermark capacity cannot be infinitely large and is strictly constrained by two aspects: numerical accuracy limitations and vector data tolerance. Hence this section mainly consider how to maximize the capacity under the constraints.

The numerical accuracy limitation is due to the finite precision of the floating number in computer systems. Specifically, numerical accuracy is denoted as γ . If the floating numbers x_1 and x_2 satisfy $|x_1 - x_2| < \gamma$, then these two numbers are considered to be equal in computer

systems ($x_1 = x_2$). In the process of embedding watermarks, the numerical accuracy implies that the minimum interval l in QIM should meet the requirement:

$$l \geq \gamma \quad (10)$$

The vector data tolerance means that after embedding watermark, the modifications of the vertex coordinates should be limited in a small range. Otherwise, the usability of vector data will be cracked. The vector data tolerance is denoted as τ . If the vertex becomes $V'(x', y')$ after watermarking, it should satisfy:

$$\sqrt{(x' - x)^2 + (y' - y)^2} \leq \tau \quad (11)$$

5.2 Capacity-Improved QIM under Constraints

Considering the above constraints, the parameters in distortion-reduced QIM would be optimized to maximize the watermark capacity. Suppose the original distance ratio R and the angle A become R' and A' after watermark embed, the vertices related to R and A are then denoted as $V_1(x_1, y_1)$, $V_2(x_2, y_2)$ and $V_3(x_3, y_3)$. Besides, the coordinates of vertex V_1 and V_2 remain invariant and vertex $V_3(x_3, y_3)$ becomes $V'_3(x'_3, y'_3)$. The modulations of R and A are denoted as ΔR and ΔA ($\Delta A \ll \frac{\pi}{2}$), respectively. Because there are each two directions of modulation on R and A , the spatial relationship between watermarked vertex $V'_3(x'_3, y'_3)$ and original vertex $V_3(x_3, y_3)$ has four possible situations. In each situation, the watermarked vertex $V'_3(x'_3, y'_3)$ is denoted as v_1, v_2, v_3, v_4 respectively, as shown in Fig. 9.

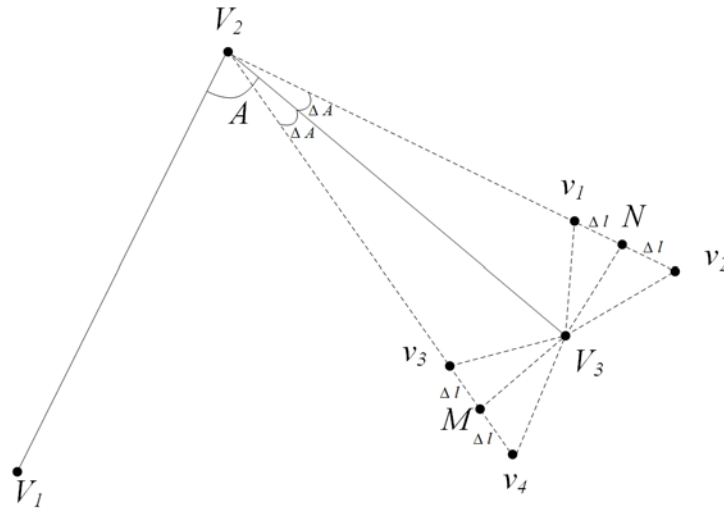


Fig. 9. The modulation of vertex V_3

In Fig. 9, the auxiliary points M and N are labeled, which means the modulation moves V_3 to M or N first and then moves N to v_1 or v_2 . In addition, M is moved to v_3 or v_4 . Hence, because $|V_2V_3| = |V_2M| = |V_2N| = R|V_1V_2|$ and the length of $|Nv_1|$ is denoted as Δl , there is $|Nv_1| = |Nv_2| = |Mv_3| = |Mv_4| = \Delta l = \Delta R|V_1V_2|$.

According to the law of sines:

$$|V_3 N| = \frac{\sin \Delta A |V_2 V_3|}{\sin(\frac{\pi - \Delta A}{2})} \quad (12)$$

and based on the law of cosines, the distance between V_3 and v_1, v_2, v_3, v_4 is calculated as:

$$|V_3 v_1| = |V_3 v_3| = \sqrt{\Delta l^2 + |V_3 N|^2 - 2\Delta l |V_3 N| \cos(\frac{\pi - \Delta A}{2})} \quad (13)$$

$$|V_3 v_2| = |V_3 v_4| = \sqrt{\Delta l^2 + |V_3 N|^2 - 2\Delta l |V_3 N| \cos(\frac{\pi + \Delta A}{2})} \quad (14)$$

The interval lengths of the modulation on distance ratio R and angle A are denoted as l_R and l_A , and the interval counts are k_R and k_A , respectively. According to the analysis in section 4.2, the maximum capacity for each vertex is $\lfloor \log_2 k_R \rfloor + \lfloor \log_2 k_A \rfloor$. Considering the numerical accuracy constraint and vector data tolerance, the optimization of maximizing watermark capacity is:

$$\max \lfloor \log_2 k_R \rfloor + \lfloor \log_2 k_A \rfloor \quad (15)$$

$$s.t. \ l_R \geq \gamma, l_A \geq \gamma \quad (16)$$

$$\gamma \leq |V_3 v_1| \leq \tau, \gamma \leq |V_3 v_2| \leq \tau \quad (17)$$

$$l_R \leq \Delta R \leq \left\lfloor \frac{k_R}{2} \right\rfloor l_R, l_A \leq \Delta A \leq \left\lfloor \frac{k_A}{2} \right\rfloor l_A \quad (18)$$

When γ is very small [26] (e.g. 10^{-10}), $\sin \gamma \approx \gamma$ and $\cos \gamma \approx 1$. Hence, $|V_3 v_1| = |V_3 v_2|$ and Equation (17) is converted to:

$$\gamma \leq \sqrt{\Delta R^2 + \Delta A^2 R^2} |V_1 V_2| \leq \tau \quad (19)$$

It is clear that the capacity becomes maximized when $l_R = \gamma, l_A = \gamma$ because $|V_2 V_3| = R |V_1 V_2|$. Thus, Equation (19) equals:

$$\sqrt{\left\lfloor \frac{k_R}{2} \right\rfloor |V_1 V_2|^2 + \left\lfloor \frac{k_A}{2} \right\rfloor |V_2 V_3|^2} \leq \frac{\tau}{\gamma} \quad (20)$$

From Equation (20), the interval counts k_R and k_A are related to the lengths of the adjacent lines $|V_1 V_2|$ and $|V_2 V_3|$.

5.3 Optimization Solution

Theoretically, the optimization of Equation (15) under the constraints in Equation (20) is related to the vector data properties, meaning that the vector data should be analyzed first. Moreover, if k_R and k_A are determined from specific vector data, these parameters must be stored in the watermark extraction process so the watermarking scheme is not fully blind. To directly and conveniently use the specific parameters k_R and k_A , the optimization solution based on the common properties of vector data is given as follows.

In the extreme situation when both $|V_1 V_2|$ and $|V_2 V_3|$ achieve the maximum length, then:

$$\max |V_1 V_2| = \max |V_2 V_3| \leq \alpha \tau \quad (21)$$

where parameter α is the maximum line length L_{\max} divided by vector data tolerance τ :

$$\alpha = \frac{L_{\max}}{\tau} \quad (22)$$

The interval counts k_R and k_A are then calculated by:

$$k_R = k_A \leq \frac{1}{\alpha^2 \gamma^2} + 1 \quad (23)$$

Parameter α can be determined empirically by considering extreme situations. First, assume the map scale of vector data is small. For example, for vector data of China with a map scale of 1:1 000 000 in the geographic coordinate system, the maximum distance of the adjacent vertices is often less than 5° . According to the map standards [40], map tolerance is usually no higher than 5×10^{-3} ; in this situation, parameter $\alpha = 10^3$. Another situation is when the map scale becomes large, such as a residential area with a map scale of 1:1000 in the projected coordinate system. In this case, the maximum distance of the adjacent vertices is often less than 7500 m, and the map tolerance is often smaller than 0.1 m. Parameter α is then determined as 7.5×10^4 . Combining these two situations, the larger value 7.5×10^4 , which satisfies the stronger requirement, is a candidate value for parameter α .

For the numerical accuracy γ , Wang suggested that $\gamma = 10^{-15}$ [26]. The number 15 may be deduced from the IEEE 754 specifications [41]. Here, a stricter condition is considered when the integer part of a number exceeds 10^7 in the project coordinate system. Thus, the numerical accuracy γ becomes 10^{-8} . In addition, some of the least significant digits may change under data manipulation, such as vector data format exchange. Hence, to ensure accuracy, two least significant digits are eliminated and γ is determined as 10^{-6} .

When $\alpha = 7.5 \times 10^4$ and $\gamma = 10^{-6}$, the interval counts are calculated by:

$$k_R = k_A \leq \frac{1}{\alpha^2 \gamma^2} + 1 \approx 179 \quad (24)$$

When $k_R = k_A = 2^n, n \in \mathbb{Z}$, the watermark capacity denoted by Equation (15) is an integer. For convenience in computation, the candidate values for the interval counts k_R and k_A are both 128. The theoretical watermark capacity then becomes 14 bits/vertex.

6. Watermarking Scheme

6.1 Watermark Embedding

Watermark embedding consists of the following steps:

- 1) Convert the binary watermark information into a sequence W based on β , $\beta = \lfloor 1 + \log_2 k_R \rfloor$. The watermark sequence W then becomes $W = \{w_j, j = 0, 1, 2, \dots, M-1\}$ with $w_j \in \{0, 1, 2, \dots, \beta-1\}$, and M denotes the watermark length.
- 2) Read the vertices sets $V_i (i = 1, 2, \dots, n)$ of the vector data. For discrete points, read the vertices in the storage order.
- 3) Starting from $i = 2$, calculate the distance ratio R_i and angle A_i according to Equations (1) and (2).
- 4) The mapping mechanism is used to establish a robust relationship between the embedded watermark index j and embedded domain. First, obtain the first q digits IR_i from R_i , which means:

$$IR_i = \lfloor R_i \times 10^q \rfloor \quad (25)$$

Five is a candidate value for q to distinguish the first q digits of R_i with other numbers. Then, the relationship between IR_i and the watermark index j is established by:

$$j = \text{hash}(IR_i) \% M \quad (26)$$

where *hash* is a random hash function, for example, the Logistic chaos function. The relationship between IA_i and the watermark index j is established in the same way.

5) Embed the watermark w_j into R_i using the capacity-improved QIM strategy according to Equation (9). The interval counts and length are the same as those provided in section 5.3. A_i is then embedded in the same way. After watermark embedding, V_{i+1} is moved to V'_{i+1} .

6) Update V_{i+1} with V'_{i+1} in the vertex sets $V_i (i = 1, 2, \dots, n)$ and continue to embed until all the vertices have been watermarked.

6.2 Watermark Extraction

The watermark extraction procedure is the inverse of the watermark-embedding procedure and consists of the following steps:

1) Read the vertices sets $V_i (i = 1, 2, \dots, n)$ and perform the calculations in the same way as for watermark embedding.

2) Starting from $i = 2$, calculate the distance ratio R_i and the angle A_i according to Equations (1) and (2).

3) Establish the same mapping mechanism as that in watermark embedding. Parameter q is also the same here.

4) Extract the watermark value according to Equation (7) and the watermark index j using the mapping mechanism. Record the extracted watermark information.

5) For each watermark index j , the corresponding watermark value is determined by the larger count of records. Combining this majority principle and the mapping mechanism, the error introduced by the new generated features mentioned in section 3.2 is reduced to a minor level.

6) Convert the extracted watermark sequence into binary information and determine the copyright of the vector data.

7. Experimental and Analysis

Experiments have been conducted to verify the imperceptibility, capacity and robustness of the proposed watermarking scheme. The experiments are performed mainly on ArcMap 10.4 and MATLAB 2016a.

7.1 Experimental Data

In the experiments, two small-scale vector datasets and one medium-scale vector dataset, denoted as Data(A), Data(B) and Data(C), respectively, are used to carry the watermarks. The experimental data properties are listed in [Table 1](#).

Table 1. The experimental data properties.

Vector data	Data type	Coordinate system	Vertices	Scale	Accuracy tolerance
Data(A)	Point	Gauss Kruger	100	1:1000	0.1 m
Data(B)	Polyline	Gauss Kruger	150	1:2000	0.2 m
Data(C)	Polygon	WGS84	3079	1:100 000	10^{-4}

The experimental data are shown in [Fig. 10](#).

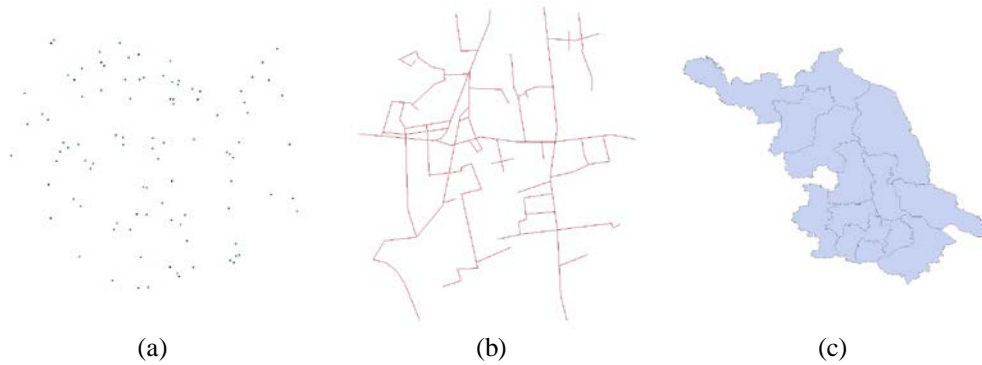


Fig. 10. The experimental data: (a) Data(A); (b) Data(B); (c) Data(C)

A 32×32 binary image, shown in **Fig. 11**, is used as the copyright image in the experiment.



Fig. 11. The copyright image

7.2 Extracted Watermark

Using the proposed watermarking method, the copyright image is embedded in the experimental data and then extracted. The correctness ratio (CR), is defined here to measure the similarity between the extracted copyright image and the original. If $W' = \{w'_j, j = 0, 1, 2, \dots, M - 1\}$ represents the extracted watermark and the original watermark is $W = \{w_j, j = 0, 1, 2, \dots, M - 1\}$, then the index CR is deduced from the bit error ratio (BER) and is calculated as:

$$CR = 1 - BER = \frac{1}{M} \sum_{i=1}^M XNOR(w'[i], w[i]) \quad (27)$$

where $XNOR$ represents the exclusive OR operation. The extracted watermarks and their CR s are shown in **Table 2**.

Table 2. The extracted watermarks.

Vector data	Data(A)	Data(B)	Data(C)
Vertices	100	150	3079
Extracted watermark			
CR	0.9561	1	1

According to the extracted watermark results, although some minor differences exist in the watermark image extracted from Data(A), its content can be easily recognized, and the CR is greater than 0.9. Hence, the proposed watermarking method can embed most of the watermark

image into the vector data of only 100 vertices and identify the copyright successfully. The extracted watermark for Data(B) demonstrates that the proposed watermarking method can embed and extract the copyright image without error when the vertex count slightly increases. Additionally, the method is also applicable to medium-scale or large-scale vector data, as deduced from the result of Data(C).

7.3 Imperceptibility

The watermarked experimental data are shown in Fig. 12.

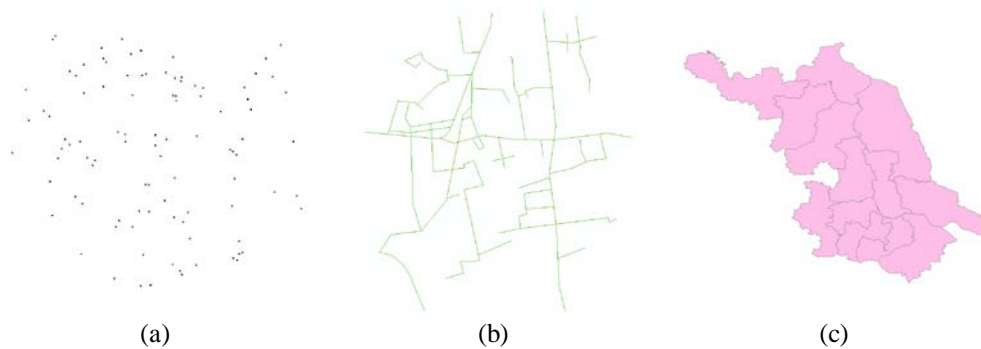


Fig. 12. Watermarked experimental data: (a) Watermarked Data(A); (b) Watermarked Data(B); (c) Watermarked Data(C)

No visual difference can be seen between the watermarked data in Fig. 12 and the original data in Fig. 10. To quantitatively measure the distortions introduced by the watermark, statistical indices, including maximum (Max), mean (Mean), and standard deviation (Std), are calculated according to the spatial distances between the watermarked vertices and the original vertices. Table 3 lists the statistical results.

Table 3. Distortion Statistics.

Watermarked vector data	Accuracy tolerance	Distortion statistics index		
		Max	Mean	Std
Data(A)	0.1 m	1.545×10^{-5} m	3.628×10^{-6} m	3.274×10^{-6} m
Data(B)	0.2 m	4.015×10^{-5} m	8.242×10^{-6} m	7.282×10^{-6} m
Data(C)	10^{-4}°	$4.327 \times 10^{-7}^\circ$	$7.722 \times 10^{-8}^\circ$	$1.634 \times 10^{-7}^\circ$





















From the distortion statistics, it is clear that the maximum distortions introduced by the watermark are far below the accuracy tolerances. In addition, the distortions remain stable according to the standard deviations. For the geographic coordinate system, the distortion is very small and satisfies the accuracy requirement because the proposed capacity-improved QIM strategy takes the distortions into consideration and controls the maximum distortion to be strictly less than the data tolerance. Hence, the effectiveness in error control and the superior imperceptibility of the proposed watermarking method have been proven.

7.4 Capacity

For the capacity experiments, the small-scale Data(B) is chosen to delete or insert vertices to generate small-scale data consisting of 100, 150, 200 and 300 vertices. After embedding and extracting the watermark, the CR of the extracted image and the capacity are calculated according to the vertex count and the embedded watermark bits. Thus, the capacity index is measured based on the number of bits/vertex. The comparison methods include two high-capacity watermarking methods and two robust watermarking methods. The

high-capacity watermarking methods are described in [26] and [34] and are denoted as Method(A) and Method(B), respectively. The robust methods are referred to in [25] and [38] and are denoted as Method(C) and Method(D), respectively. To apply the same conditions of data tolerance and numerical accuracy, the value of parameter c is set to 4 in Method(A) and the value of t is set to 10 in Method(B). The value of parameter m in Method(C) is set to 1 to increase the capacity. The experimental capacity results are listed in Table 4.

Table 4. Watermark capacity experimental results.

Method	Index	100 Vertices	150 Vertices	200 Vertices	400 Vertices
Proposed Method	Extracted Watermark				
	CR	0.9502	1	1	1
	Capacity	13.72	13.81	13.86	13.93
Method(A)	Extracted Watermark				
	CR	0.9365	1	1	1
	Capacity	7.840	7.893	7.920	7.960
Method(B)	Extracted Watermark				
	CR	0.8955	0.9492	1	1
	Capacity	5.600	5.693	5.735	5.762
Method(C)	Extracted Watermark				
	CR	0.7402	0.7422	0.7441	0.7559
	Capacity	0.0900	0.1267	0.1225	0.1038
Method(D)	Extracted Watermark				
	CR	0.7852	0.8154	0.8369	0.9424
	Capacity	1.960	1.973	1.980	1.990

From Table 4, the proposed method can embed almost 14 watermark bits into each vertex, and the extracted watermark from data with 100 vertices is clear. Other high-capacity watermarking methods, including Method(A) and Method(B), the capacity index is lower than the proposed one. In addition, the watermark capacities of Method(C) and Method(D), which paid more attention to robustness, are lower than 2 bits/vertex. In conclusion, the proposed method outperforms the other methods in watermarking capacity.

In fact, the key advantage of the proposed algorithm is the capacity-improved watermarking strategy. Unlike classical QIM only using two interval types, the capacity-improved watermarking strategy divides much more intervals to carry watermark information, meaning that each interval represents more watermark bits, instead of one bit. Based on the capacity maximization optimization, 128 interval types can contain approximately 7 bit watermark information in QIM. Thus the watermark capacity achieves 14 bits/vertex as angles and distance ratios both carry watermarks. Combine the theoretical analysis and experiment result, the proposed watermark method is proven to meet the capacity requirement of copyright protection for small-scale data.

7.5 Robustness

In the robustness experiments, the robustness of the proposed method and the comparison algorithms is verified for small-scale and medium-scale vector data. The small-scale vector dataset Data(B) consists of 150 vertices and the medium-scale vector data Data(C) consists of 3079 vertices. The attack types are divided into vertex and geometric attacks. The vertex attacks consist of vertex deletion, vertex insertion and vertex updating, while geometric attacks include rotation, scaling and translation. Regarding the robustness index, CR is used to measure the robustness of different methods.

7.5.1 Robustness against Vertex Attacks for Small-Scale Vector Data

The experimental results of robustness against vertex attack for small-scale Data(B) are shown in Fig. 13–15.

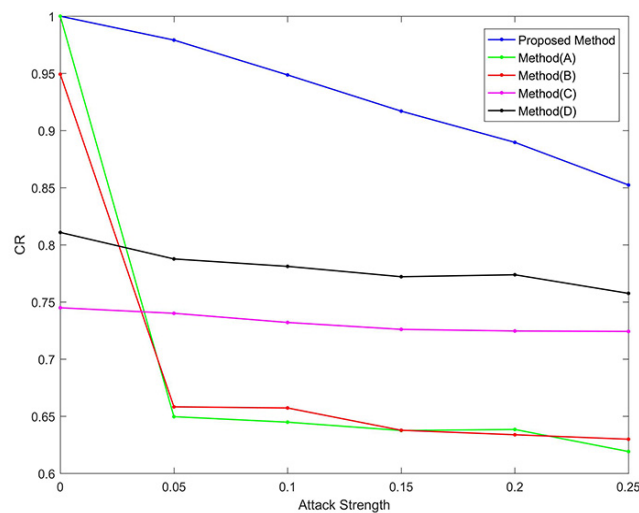


Fig. 13. Robustness against vertex deletion for small-scale vector data

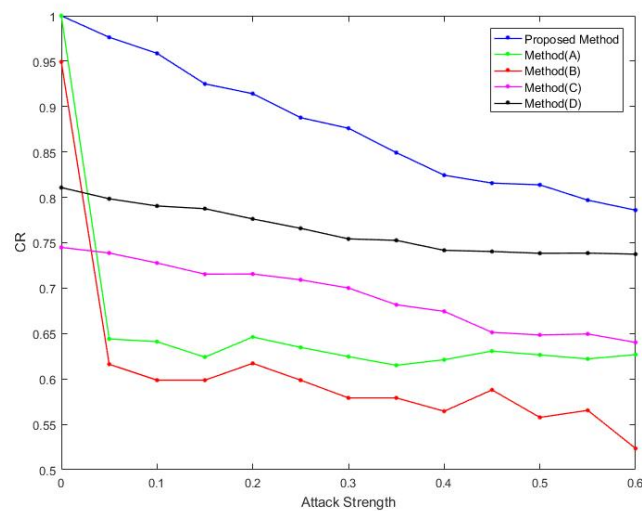


Fig. 14. Robustness against vertex insertion for small-scale vector data

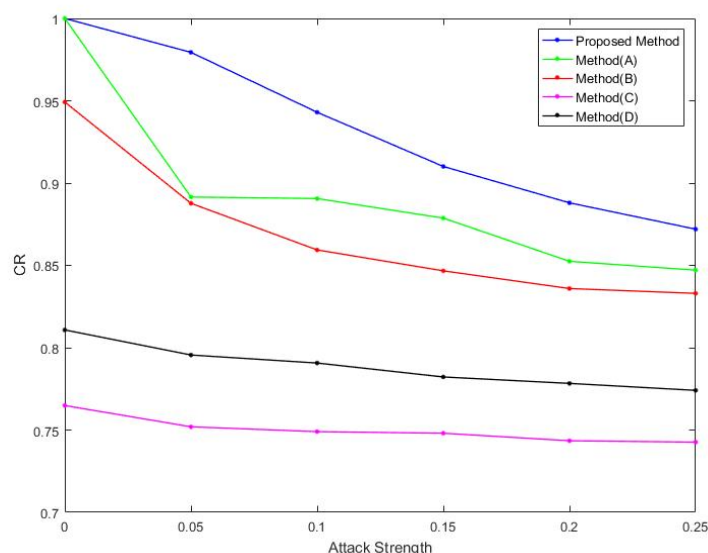


Fig. 15. Robustness against vertex update for small-scale vector data

From **Fig. 13–15**, it is obvious that the robustness of the proposed watermarking method is better than that of the compared methods. When no attack has been conducted on the watermarked data, the *CR* values of Method(A) and Method(B) are higher than those of Method(C) and Method(D) because the former methods are designed as high-capacity watermarking methods. However, when some degree of attacks, such as vertex deletion, vertex insertion or vertex update, has occurred on the watermarked data, the robustness of Method(A) and Method(B) decrease rapidly due to a lack of robustness against vertex attack. Although the decreases in the robustness of Method(C) and Method(D) are not severe, their watermark capacity limits the embedded watermark bits in small-scale vector data; thus, the *CR* values of these two methods are still not high enough.

Moreover, the robustness of the proposed watermarking method outperforms other methods because the combination of robust geometric features and capacity-improved strategy has been used. From the experimental results, the decline of the proposed method robustness is slow and nearly linear, which is consistent with the analysis results presented in section 3.2. Furthermore, this phenomenon proves that the incorrectly extracted watermark bits introduced by vertex attacks are reduced, as mentioned in section 3.2. In summary, the robustness of the proposed watermarking method has been verified by experiments when applied to small-scale vector data.

7.5.2 Robustness against Vertex Attacks for Medium-scale Vector Data

The experimental results of robustness against vertex attack for medium-scale Data(C) are shown in **Fig. 16–18**.

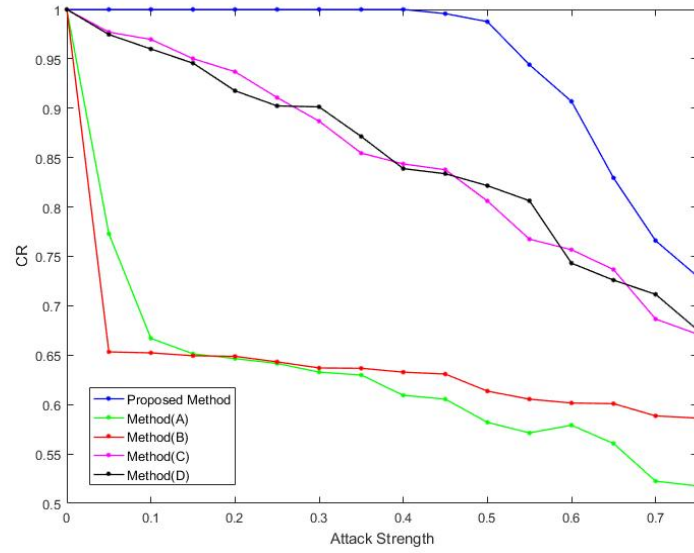


Fig. 16. Robustness against vertex deletion for medium-scale vector data

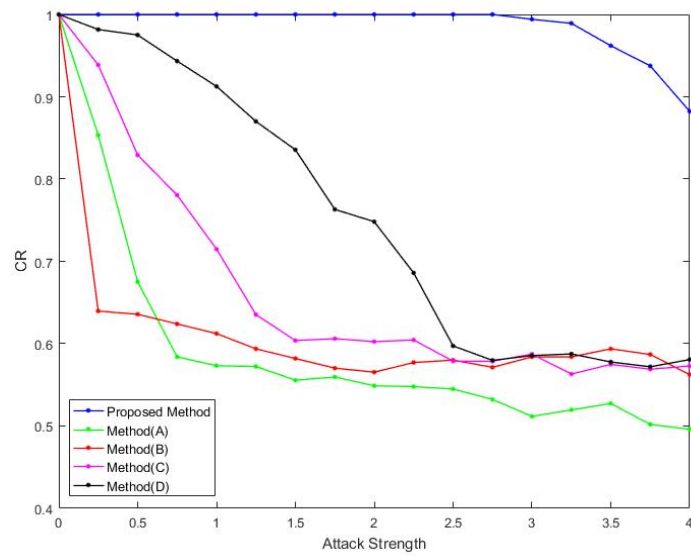


Fig. 17. Robustness against vertex insertion for medium-scale vector data

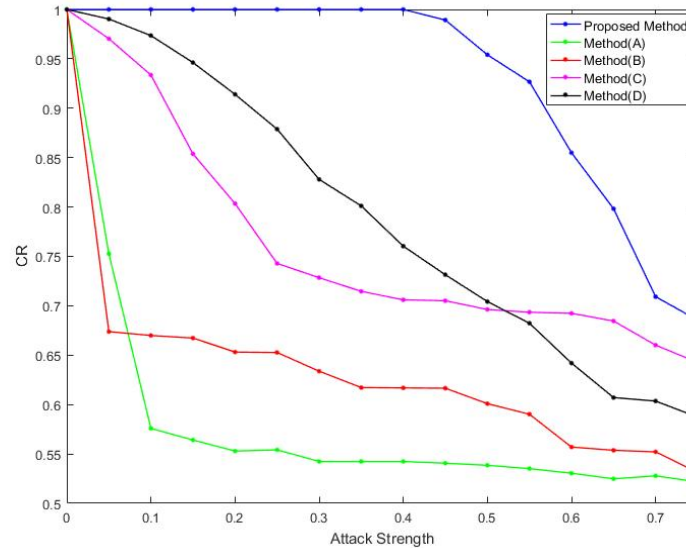


Fig. 18. Robustness against vertex update for medium-scale vector data

When handling medium-scale vector data, the superiority of the robustness of the proposed watermarking method can also be deduced from [Fig. 16–18](#). For example, after deleting 60%, inserting 375% or updating 55% of the vertices, the *CR* of the proposed method is still higher than 0.9, which implies that the watermark is extracted successfully and identifies the copyright information clearly. However, in this situation, the *CR* of the other methods are lower than 0.9. Moreover, the maximized capacity watermarking strategy enables more watermark bits to be embedded compared to other methods. Thus, the redundancy of the watermark bits will help the watermarking method resist vertex attacks.

7.5.3 Robustness against Geometric Attacks

As geometric transformations are other common operations used for vector data, robustness against them is vital when evaluating the watermarking method. The robustness of the proposed method and the comparisons are shown in [Table 5](#). The resistance to geometric attack is denoted as “√” or “×”, representing the robustness against attack or not, respectively.

Table 5. Robustness against geometric attack.

Geometric Attack	Proposed Method	Method(A)	Method(B)	Method(C)	Method(D)
Translation	√	√	√	√	√
Scaling	√	×	×	√	√
Rotation	√	×	×	√	×

From [Table 5](#), the proposed method and Method(C) are resistant towards translation, scaling or rotation attack, while the other methods are not completely robust against these attacks. The geometric attack results also demonstrate the high robustness of the proposed algorithm.

Considering the above robustness experimental results, the superior robustness of the proposed method benefits from two aspects, naming the watermarking domain and

watermarking strategy. The performance of watermark domain is analyzed in section 2, as the distance ratio and angle provide resistance against vertex attacks and geometric attacks. Besides, the capacity-improved watermarking strategy increases the embedded watermark bits in vector data. This means the higher watermark redundancy and probability of watermark extraction against vertex attacks. Thus, the whole algorithm robustness is improved by these two mechanisms at the same time.

8. Conclusion

This paper presents a high-capacity and robust watermarking scheme for vector data aimed at copyright protection for small-scale vector data. The proposed watermarking scheme is based on the robust geometric features of vector data, which provide robustness against vertex and geometric attacks. A capacity maximization watermarking strategy is also proposed to improve capacity by optimizing the watermark-embedding parameters under the constraints of numerical accuracy and map tolerance. Experiments have been conducted to verify the effectiveness of the proposed watermarking scheme. The tiny map distortions introduced by the watermark demonstrate the good imperceptibility of the proposed scheme, as the error is strictly controlled by the watermarking strategy. Regarding the capacity, the proposed scheme can successfully embed an image of 1024 bits into vector data with 150 vertices, and the capacity reaches nearly 14 bits/vertex, which is superior to other high-capacity watermarking and robust schemes. In addition, the experimental results also prove that the proposed scheme is more robust against vertex deletion, vertex insertion, vertex update, rotation, scaling and translation attacks, than the other watermarking schemes. In conclusion, the proposed watermark scheme, which improves the watermark capacity and robustness simultaneously, is able to protect the copyright for small-scale vector data.

References

- [1] J. Thatcher, "Big data, big questions| Living on fumes: Digital footprints, data fumes, and the limitations of spatial big data," *International Journal of Communication*, vol. 8, pp. 1765-1783, 2014. [Article \(CrossRef Link\)](#)
- [2] H. J. Miller and M. F. Goodchild, "Data-driven geography," *GeoJournal*, vol. 80, no. 4, pp. 449-461, 2015. [Article \(CrossRef Link\)](#)
- [3] G. C. Langelaar, I. Setyawan and R. L. Lagendijk, "Watermarking digital image and video data - a state-of-the-art overview," *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 20-46, 2000. [Article \(CrossRef Link\)](#)
- [4] T. Hai, C. Li, J. M. Zain and A. N. Abdalla, "Robust image watermarking theories and techniques: A review," *Journal of Applied Research and Technology*, vol. 12, pp. 122-138, 2014. [Article \(CrossRef Link\)](#)
- [5] P. Zhu, F. Jia and J. Zhang, "A copyright protection watermarking algorithm for remote sensing image based on binary image watermark," *Optik*, vol. 124, no. 20, pp. 4177-4181, 2013. [Article \(CrossRef Link\)](#)
- [6] Q. Su and G. Wang, "An improved color image watermarking algorithm based on QR decomposition," *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 707-729, 2017. [Article \(CrossRef Link\)](#)
- [7] G. Doerr and J. L. Dugelay, "A guide tour of video watermarking," *Signal Processing-Image Communication*, vol. 18, no. 4, pp. 263-282, 2003. [Article \(CrossRef Link\)](#)
- [8] R. O. Preda and D. N. Vizireanu, "A robust digital watermarking scheme for video copyright protection in the wavelet domain," *Measurement*, vol. 43, no. 10, pp. 1720-1726, 2010. [Article \(CrossRef Link\)](#)

- [9] D. Kirovski and H. S. Malvar, "Spread-spectrum watermarking of audio signals," *IEEE Transactions on Signal Processing*, vol. 51, No. 4, pp. 1020-1033, 2003. [Article \(CrossRef Link\)](#)
- [10] M. Arnold, X. Chen, P. Baum, U. Gries and G. Doerr, "A Phase-Based audio watermarking system robust to acoustic path propagation," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 411-425, 2014. [Article \(CrossRef Link\)](#)
- [11] H. M. Meral, B. Sankur, A. S. Ozsoy, T. Gungor and E. Sevinc, "Natural language watermarking via morphosyntactic alterations," *Computer Speech and Language*, vol. 23, no. 1, pp. 107-125, 2009. [Article \(CrossRef Link\)](#)
- [12] K. Jawad and A. Khan, "Genetic algorithm and difference expansion based reversible watermarking for relational databases," *Journal of Systems and Software*, vol. 86, no. 11, pp. 2742-2753, 2013. [Article \(CrossRef Link\)](#)
- [13] V. Solachidis and I. Pitas, "Watermarking polygonal lines using Fourier descriptors," *IEEE Computer Graphics and Applications*, vol. 24, no. 3, pp. 44-51, 2004. [Article \(CrossRef Link\)](#)
- [14] C. Shao, H. Wang, X. Niu and X. Wang, "A shape-preserving method for watermarking 2D vector maps based on statistic detection," *IEICE Transactions on Information and Systems*, vol. E89D, no. 3, pp. 1290-1293, 2006. [Article \(CrossRef Link\)](#)
- [15] P. Jia, Y. Chen, J. Ma and D. Zhu, "Digital watermark-based security technology for geo-spatial graphics data," *Chinese Geographical Science*, vol. 16, no. 3, pp. 276-281, 2006. [Article \(CrossRef Link\)](#)
- [16] Y. Pu, W. Du and I. Jou, "Perceptually transparent polyline watermarking based on normal multi-resolution representation," *IEICE Transactions on Information and Systems*, vol. E89D, no. 12, pp. 2939-2949, 2006. [Article \(CrossRef Link\)](#)
- [17] V. R. Doncel, N. Nikolaidis and I. Pitas, "An optimal detector structure for the Fourier descriptors domain watermarking of 2D vector graphics," *IEEE Transactions on Visualization and Computer Graphics*, vol. 13, no. 5, pp. 851-863, 2007. [Article \(CrossRef Link\)](#)
- [18] X. Wang, C. Shao, X. Xu and X. Niu, "Reversible data-hiding scheme for 2-d vector maps based on difference expansion," *IEEE Transactions On Information Forensics And Security*, vol. 2, no. 3, pp. 311-320, 2007. [Article \(CrossRef Link\)](#)
- [19] D. Im, H. Lee, S. Ryu and H. Lee, "Vector watermarking robust to both global and local geometrical distortions," *IEEE Signal Processing Letters*, vol. 15, pp. 789-792, 2008. [Article \(CrossRef Link\)](#)
- [20] T. Yamada, Y. Fujii, S. Tezuka and N. Komoda, "Line-Division-Based digital watermarking system for facilitating fair use of Small-Size vector map content," *Electronics and Communications in Japan*, vol. 91, no. 9, pp. 11-19, 2008. [Article \(CrossRef Link\)](#)
- [21] H. Yan, J. Li and H. Wen, "A key points-based blind watermarking approach for vector geo-spatial data," *Computers, Environment and Urban Systems*, vol. 35, no. 6, pp. 485-492, 2011. [Article \(CrossRef Link\)](#)
- [22] C. Wang, Z. Peng, Y. Peng, L. Yu, J. Wang and Q. Zhao, "Watermarking geographical data on spatial topological relations," *Multimedia Tools and Applications*, vol. 57, no. 1, pp. 67-89, 2012. [Article \(CrossRef Link\)](#)
- [23] P. Fei, C. Li and L. Min, "A reversible watermark scheme for 2D vector map based on reversible contrast mapping," *Security and Communication Networks*, vol. 6, no. 9, pp. 1117-1125, 2013. [Article \(CrossRef Link\)](#)
- [24] S. Lee, S. Kwon and K. Kwon, "Robust hashing of vector data using generalized curvatures of polyline," *IEICE Transactions on Information and Systems*, vol. E96D, no. 5, pp. 1105-1114, 2013. [Article \(CrossRef Link\)](#)
- [25] S. Lee, X. Huo and K. Kwon, "Vector watermarking method for digital map protection using arc length distribution," *IEICE Transactions on Information and Systems*, vol. E97.D, no. 1, pp. 34-42, 2014. [Article \(CrossRef Link\)](#)
- [26] N. Wang, H. Zhang and C. Men, "A high capacity reversible data hiding method for 2D vector maps based on virtual coordinates," *Computer-Aided Design*, vol. 47, pp. 108-117, 2014. [Article \(CrossRef Link\)](#)

- [27] Z. Peng, M. Yue, X. Wu and Y. Peng, "Blind watermarking scheme for polylines in vector geo-spatial data," *Multimedia Tools and Applications*, vol. 74, no. 24, pp. 11721-11739, 2015. [Article \(CrossRef Link\)](#)
- [28] D. Xiao, S. Hu and H. Zheng, "A high capacity combined reversible watermarking scheme for 2-D CAD engineering graphics," *Multimedia Tools and Applications*, vol. 74, no. 6, pp. 2109-2126, 2015. [Article \(CrossRef Link\)](#)
- [29] X. Niu, C. Shao and X. Wang, "A survey of digital vector map watermarking," *International Journal of Innovative Computing Information and Control*, vol. 2, no. 6, pp. 1301-1316, 2006. [Article \(CrossRef Link\)](#)
- [30] A. Abubahia and M. Cocea, "Advancements in GIS map copyright protection schemes - a critical review," *Multimedia Tools and Applications*, vol. 76, no. 10, pp. 12205-12231, 2017. [Article \(CrossRef Link\)](#)
- [31] Y. Wang, C. Yang and C. Zhu, "A multiple watermarking algorithm for vector geographic data based on coordinate mapping and domain subdivision," *Multimedia Tools and Applications*, vol. 77, no. 15, pp. 19261-19279, 2017. [Article \(CrossRef Link\)](#)
- [32] L. Cao, C. Men and Y. Gao, "A recursive embedding algorithm towards lossless 2D vector map watermarking," *Digital Signal Processing*, vol. 23, no. 3, pp. 912-918, 2013. [Article \(CrossRef Link\)](#)
- [33] F. Peng, Y. Liu and M. Long, "Reversible watermarking for 2D CAD engineering graphics based on improved histogram shifting," *Computer-Aided Design*, vol. 49, pp. 42-50, 2014. [Article \(CrossRef Link\)](#)
- [34] L. Cao and C. Men, "High-capacity reversible watermarking scheme of 2D-vector data," *Signal, Image and Video Processing*, vol. 9, no. 6, pp. 1387-1394, 2015. [Article \(CrossRef Link\)](#)
- [35] L. Cao, C. Men and R. Ji, "Nonlinear scrambling-based reversible watermarking for 2D-vector maps," *Visual Computer*, vol. 29, no. 3, pp. 231-237, 2013. [Article \(CrossRef Link\)](#)
- [36] S. Lee and K. Kwon, "Vector watermarking scheme for GIS vector map management," *Multimedia Tools and Applications*, vol. 63, no. 3, pp. 757-790, 2013. [Article \(CrossRef Link\)](#)
- [37] N. Wang, "Reversible watermarking for 2D vector maps based on normalized vertices," *Multimedia Tools and Applications*, vol. 76, no. 20, pp. 20935-20953, 2017. [Article \(CrossRef Link\)](#)
- [38] H. Yan, L. Zhang and W. Yang, "A normalization-based watermarking scheme for 2D vector map data," *Earth Science Informatics*, vol. 10, no. 4, pp. 471-481, 2017. [Article \(CrossRef Link\)](#)
- [39] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423-1443, 2001. [Article \(CrossRef Link\)](#)
- [40] Regulation State Administration for Market, "Basic requirements for products of digital topographic map," *GB/T 17278-2009, Standards Press of China*, 2009. [Article \(CrossRef Link\)](#)
- [41] IEEE Std 754-2008, "IEEE Standard for Floating-Point Arithmetic," pp. 1-70, 2008. [Article \(CrossRef Link\)](#)



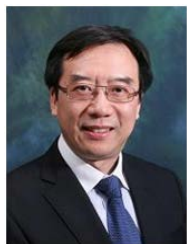
Deyu Tong received the Ph.D. degree in cartography and geographic information system at Nanjing Normal University, Nanjing, China, in 2018. He is now a lecturer at Nanjing University of Finance and Economics. His research interests include information security and Internet of Things.



Changqing Zhu received the Ph.D. degree in mathematics from the Information Engineering University, Zhengzhou, China, in 1997. He is now a Professor at Nanjing Normal University, Nanjing, China. His research interests include theories and methods of geographic information system and digital image processing, with a focus on spatial information security.



Na Ren received the Ph.D. degree in cartography and geographic information system at Nanjing Normal University, Nanjing, China, in 2011. She is now an Associate Professor at Nanjing Normal University, Nanjing, China. Her research interests include copyright protection and security for geographic information.



Wenzhong Shi is the Head and Chair Professor in the Department of Land Surveying and Geoinformatics at the Hong Kong Polytechnic University. His research interests include GIScience and remote sensing, focusing on uncertainties and quality control of spatial data, satellite images and LiDAR data, 3D modeling, and human dynamics.