A Robust Zero-Watermarking Algorithm for Vector Digital Maps Based on Statistical Characteristics

Xun WANG
College of Computer Science & Information Engineering
Zhejiang Gongshang University
Hangzhou, China
Email: wx@mail.zjgsu.edu.cn

Dingjun Huang, Zhiyong Zhang
College of Computer Science & Information Engineering
Zhejiang Gongshang University
Hangzhou, China
Email: huangdingjun@163.com, zzy@mail.zjgsu.edu.cn

***Abstract*—This paper presented a new zero-watermarking algorithm for vector digital maps based on statistical characteristics. The watermark information is constructed by utilizing the original data's characteristics. We divide the map into rings by using concentric circles and count the number of vertices in each ring, which is the feature information. A zero watermark image is constructed by using feature information and copyright information. Experiments show that the watermarks are resilient to translation, scaling, vertex deletion and growth, rotation, random noise, objects scrambling and cropping, making it a robust algorithm.**

***Index Terms*—vector map, zero-watermarking, vertex, concentric circles**

I. INTRODUCTION

With the extensive use of Geographic Information System (GIS), vector digital map has been widely adopted in our social life, such as car navigation systems, web-based map services, and geographical information systems for city planning. Just as other digital products, vector digital map is easy to update, duplicate, and distribute. It is also prone to be illegally duplicated and embezzled [1, 2]. With the prevailing trend of highly developed internet technique, it is extremely urgent to find out how to protect the copyright of vector digital mapping effectively and prevent it from being illegally embezzled.

Watermarking technique can be applied to protect the copyright of vector map. At present, the digital watermarking technique on vector map is realized through modifying the original map data, such as spatial watermarking algorithm [3, 4, 5] and frequency-domain watermarking algorithm [6-13]. Spatial watermarking algorithm is used to modify the coordination data within the permitted accuracy range of map data. It is simple to compute, with excellent imperceptibility, and has a certain capacity of watermark embedded etc. However, spatial watermarking algorithm is weak in its robustness, since it cannot deal with some conventional operations or resist hostile attacks on the vector digital map data. In this case, frequency-domain watermarking is robust, but rather complicated to compute because of a large quantity of calculation and unfitting the requirement on data high accuracy. Therefore, direct or indirect modification of map data will always affect the accuracy. And unpredictable attacks may lead it to lose efficacy. Furthermore, the algorithm complexity will increase explosively in order to guarantee the visual effect of the watermark. So even if we can correctly extract the watermark, it can't be applied into practice. To meet the high precision and topology invariance requirements of vector data, it seems that the traditional algorithms of digital watermark are impractical. As a new digital watermark algorithm, zero-watermarking [14, 26, 27] can resolve the conflict between imperceptibility and robustness of digital watermark because it does not change the data to construct watermark information. It is a natural blind watermark algorithm.

However, at present, very few researches have been done on zero-watermarking algorithm [15-18] in the domain of geographical spatial data. Therefore, in this paper, a new zero-watermarking algorithm for 2D vector digital maps is proposed. First, we divide the map into grids by using concentric circles and count the number of vertices in each grid, which is the feature information. And then we construct a watermark image using grids data and copyright information. Experimental results show that the proposed algorithm is resilient to random noise, general geometric transformation and cropping.

Manuscript received May 19, 2011; revised September 15, 2011; accepted October 12, 2011.
*Corresponding author: Dingjun Huang.

doi:10.4304/jsw.7.10.2349-2356

And it can resolve the conflict between imperceptibility and robustness of traditional watermarking algorithm.

The remaining part of this paper is organized as follows: Section 2 presents the main idea of our zero-watermarking scheme, including zero-watermark generation and extraction; Section 3 presents the experiment results to demonstrate our ideas, and the robustness of our algorithm against some attacks is further discussed; Section 4 gives the conclusions and future work.

II. THE WATERMARKING ALGORITHM

A. The Characteristics Definitions of Vector Map

Geographical data is usually stored inside geographical databases such as PostGIS or exchange files in different formats, such as shape files, MIF files, DXF files, etc. There are many formats but in all of them, the geographical data is represented as a composition of geographical objects [19, 20]. A geographical object is composed of two parts: its geometry (point, polyline, polygon, etc.) and attributes. Furthermore, the attributes may contain information of object type and its properties. There is another feature of vector map, namely topology characteristics, which represents the relationship between geometrical objects.

We have to extract certain characters from the vector map when designing a vector map data watermarking algorithm.

First, these data are without inherent orders. Audio and video data are arranged in chronological order. Still image and video frames are arranged in scan lines. When it comes to the vector map data, it is without inherent order. Thus only the storage location would be changed when the data are scrambled, neither the visual effect nor positioning accuracy of the data would be affected.

Second, the vector map includes geometry information, attribute information and meanwhile the implicated topology characteristics.

Third, the representations of the geometrical object are not exclusive. One geographical entity can be represented by various models, which may cause the failure of watermarking detection.

Fourth, the vector data might suffer coordinate transformation, projection transformation, data format transformation, data compression, and other operations. Therefore, these operations will change vector map data or structure, which may influence the results of our watermark information.

In this paper, we will take advantage of the geometry of the geographical objects defined in vector map data and find out a watermarking algorithm which is resilient against many attacks.

In the next section, we will present the main idea of our zero-watermarking algorithm.

B. The Main Idea of Our Algorithm

Algorithm [15] presented a zero-watermarking scheme for vector data. The watermark signal is constructed by using the vector data's topology characteristics. And algorithm [16] also presented a zero-watermarking algorithm for 2D vector maps.

Considering the characteristics of vector map, various data objects are composed of vertex. As we know, vector data might suffer coordinate transformation, projection transformation, data format transformation, data compression, and other operations. Though these operations change the data information or structure, they do not influence the visual content of the map. Therefore, we use the distribution of vertex coordinates to construct zero-watermark information. This method will prevent destroying the watermark information when the original vector map is attacked by the general geometric transformation. In addition, in order to make the watermark resilient to rotation, the vector digital map is divided into several parts according to a statistical method of concentric circles. The main idea of the algorithm is summarized as follows.

First, we calculate the mean coordinate point called *AvePoint*, and mean distance value called *AveDistance*, using all vertices of the vector map. The formulas of calculating the *AvePoint* and *AveDistance* are presented as follows:

$$\overline{x} = \sum_{i=1}^{m} x_i \ . \tag{1}$$

$$\overline{y} = \sum_{i=1}^{m} y_i \ . \tag{2}$$

$$AveDis\tan ce = \frac{\sum_{i=1}^{m} \sqrt{\left(x_i - \overline{x}\right)^2 + \left(y_i - \overline{y}\right)^2}}{m} \ . \tag{3}$$

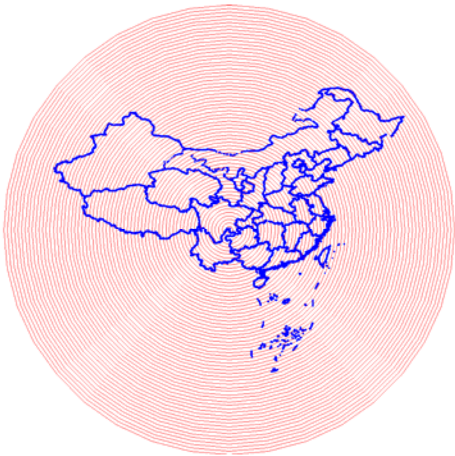
Where $(\overline{x}, \overline{y})$ represents the *AvePoint*'s coordinate value and m means the number of vector map vertices.

Second, we design a circle. The center of circle is *AvePoint* and the radius of the circle is 2 times that of *AveDistance*. Then, we divide this circle into a number of rings by using concentric circles method. The length of rings is l, which is of the binary image size. Seeing from equation (4):

$$l = N \times N \ . \tag{4}$$

In this case, N is of the width or height of the binary image. For example, we use a China vector map to test our division approach by using concentric circles method, which is shown as Fig. 1.

Fig. 1 (a) shows a vector map of China, which is divided into 64 rings; Fig. 1 (b) shows the central part of our China vector map, where the vertices are in their own ring.



(a) The division of China's map by concentric circles

(b) The center part of the concentric circles

Figure 1. The division approach by using concentric circles

At last, we count the number of vertices in each ring as the vector map's characteristics, and then we construct a watermark image using characteristics data and copyright information.

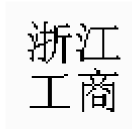
In watermark extraction, we use the reverse process of watermarking construction to detect the copyright authentication.

C. Watermark Scrambling

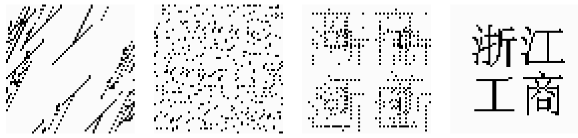
In order to increase the secrecy of the watermark information, the original watermark image scrambling transformation is performed before the construction of zero-watermark. A commonly used scrambling method is Arnold transformation [21], which is applied widely in digital image encryption because of its periodicity, namely cat face scrambling. The Arnold transformation formula of the square image is:

$$\begin{bmatrix} \hat{x} \\ \hat{y} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\bmod N). \quad (5)$$

Where N is the width or height of binary image, (x, y) is the coordinate of original image, $(\hat{x}, \hat{y})$ is the coordinate of new image. This method is to scramble the original image by exchanging the coordinates of image. We can take advantage of the periodicity [22-25] of Arnold transformation to restore the scrambled image. We take a sample showing as Fig. 2:



(a) Original Watermark Image



(b) 1 time (c) 13 times (d) 24 times (e) 48 times

Figure 2. The Image Scrambled by Arnold transformation

Fig. 2 (a) is a 64 × 64 original binary image; Fig. 2 (b) is the scrambled image by Arnold transformation; Fig. 2 (c) is the 13-times scrambled image by Arnold transformation; Fig. 2 (d) is the 24-times scrambled image by Arnold transformation; Fig. 2 (e) is the restored image by Arnold transformation for 48 times, because its periodicity is 48 for a 64 × 64 binary image.

The following sections are the specific steps of the watermark embedding and extraction algorithm.

D. Zero-Watermark Generation

As mentioned above, Zero-watermarking generation algorithm based on the original vector map's features. The specific steps of the algorithm are described as follows:

Step1. To generate scrambled copyright bits. The copyright bits are extracted from a binary image (Watermark image), using secret key and Arnold transform to modulate the copyright bits, which is called binary bit stream w: if the binary image size is $N \times N$, then the length of watermark bits is $l = N \times N$. Arnold transform and key are generated and integrated into the final watermark bit stream, $w = (w_1, w_2, ..., w_i, ..., w_l)$, where $w_i \in \{0,1\}, 0 \le i < l$;

Step2. To generate zero-watermark information. According to the length of binary image, the vector map is divided into several rings by using concentric circles method and then the number of vertices in each ring is count, called array M, then we calculate the average n*umber of all rings* to produce the relationship information between array M and *AveNums*, which is treated as the feature messages, M^*. At last, *XOR* operation is performed on feature messages and scrambled copyright bits to generate zero-watermark information. At last, zero-watermark is registered into IPR depository. The specific steps are:

a. Using equation (1), (2) (3) to calculate the values of *AvePoint* and *AveDistance*.

b. To design a circle. The center of circle is *AvePoint* and the radius of circle is 2 times *that* of *AveDistance*. Then, we divide this circle into a number of rings by using concentric circles method. The length of rings is l, obtained from equation (4), so the interval from each ring is $\frac{2 \times AveDistance}{l}$.

c. To count the number of vertices for each ring. We traverse each vertex in vector map to calculate the distance between the current vertex and the center point-*AvePoint*, and then we classify each vertex to its ring in order to calculate the number of vertices in each ring. The numbers are stored in the array M. M is a one-dimensional array, the length is *l*.

d. To calculate the average number of vertices for all rings, called *AveNums*. And then we use equation (6) to change array M. M^* is feature messages, where $M_i^* \in \{0,1\}, 0 \le i < l$.

$$M_i^* = \begin{cases} 0, & M_i < AveNums \\ 1, & M_i \ge AveNums \end{cases}. \tag{6}$$

e. To generate zero-watermark information using equation (7) as follow. We do *XOR* operation between feature messages and scrambled copyright bits to generate zero-watermark information. I is the zero-watermark information;

$$I = M^* \oplus W. \tag{7}$$

Step3. Zero-watermark registration. Zero-watermark is registered into IPR depository. The producer of original data takes his data production and zero-watermark generated to authority organ, and if the data and watermark pass the censor, they will be registered and published for notarization efficacy.

E. Zero-Watermark Extraction

Zero-watermark can be extracted by watermark extraction method. The watermark extracted will be compared with the registered watermark, and the comparability can be determined. Therefore the copyright of the data might be confirmed and the evidence could be provided. The specific steps of the algorithm are described as follows:

Step1. According to the detect vector map, we check the zero-watermark I from IPR depository.

Step2. To generate scrambled copyright bits. According to the length of binary image, the vector map is divided into several rings by using method described in section 2.2. The specific steps are:

a. Using equation (1), (2) (3) to calculate the values of *AvePoint* and *AveDistance*.

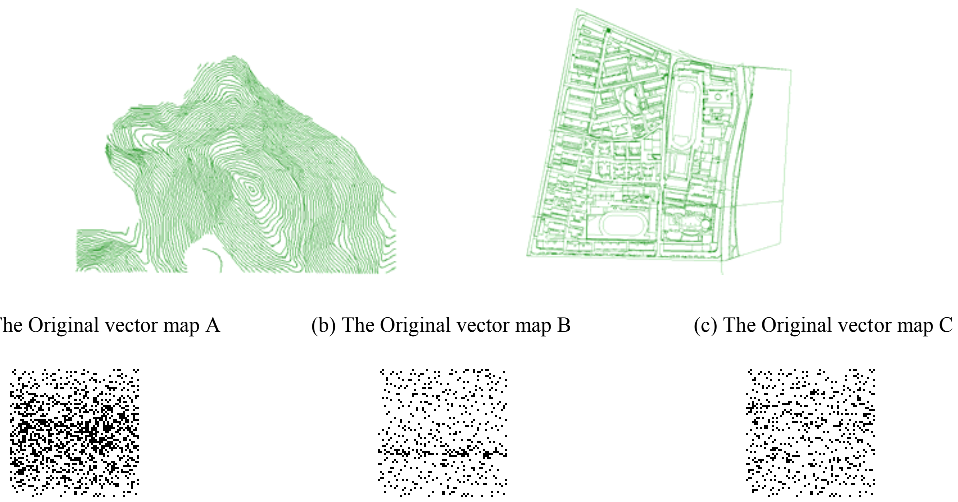
b. To divide rings. The center of circle is *AvePoint* and radius of circle is 2 times of *AveDistance*. Then, we divide this circle into a number of rings by using concentric circles method. The length of rings is l, from equation (4), the interval from each ring is $\frac{2 \times AveDistance}{l}$.

c. To count the number of vertices for each ring. The new numbers are stored in the array M.

d. To calculate the average number of vertices for all rings, and then we use equation (6) as mentioned above to change array M. M^* is the feature messages.

e. To generate watermark image copyright bits using equation (8) as follow. W' is the zero-watermark information;

$$W' = M^* \oplus I. \tag{8}$$



(a) The Original vector map A (b) The Original vector map B (c) The Original vector map C

(d) Zero-watermark from (a) (e) Zero-watermark from (b) (f) Zero-watermark from (c)

Figure 3. The result of zero-watermark generation.

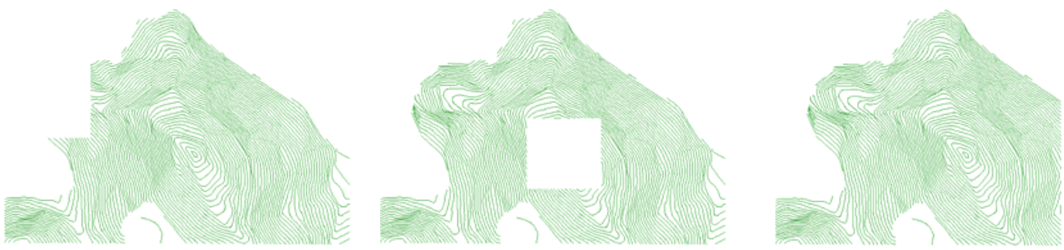
Step3. Copyright bits are generated as a binary image. Before generating watermark binary image, inverse Arnold transform operations are performed and the watermark bits extraction is encrypted with the secret key as described in section 2.4.

III. EXPERIMENTS AND RESULTS

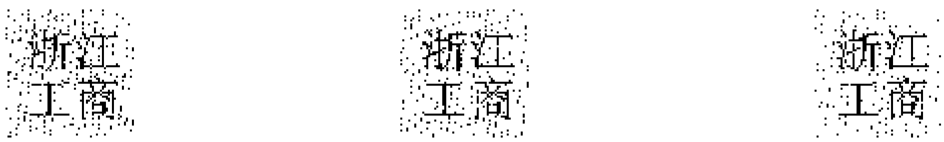
In this experiment, we take three test maps to demonstrate our algorithm. We use the copyright watermark image, which is shown as Fig. 2 (a), it is a 64 × 64 binary image; the test original vector map A is shown as Fig. 3 (a); the test original vector map B is shown as Fig. 3 (b); the test original vector map C is shown as Fig. 3 (c); and their zero-watermark images are shown as Fig. 3 (d), Fig. 3 (e) and Fig. 3 (f), they are generated by test original vector map and the watermark image. The original test vector map A is a contour map, it contains 17065 vertices, the original test vector map B is a figure outline map of China, it contains 81696 vertices, and the original test vector map C is a district map, it contains 383800 vertices.

To test the robustness of the proposed algorithm, we make the following seven attacks to test these three vector digital maps: (1) translation; (2) scaling; (3) rotation; (4) increase or decrease the vertex; (5) cropping, (6) add random noise, (7) objects scrambling.

For (1) attack, all of the vertices are translated to the direction of X and Y or opposite direction respectively; for (2) attack, the region of vector digital map is modified with different scale; for (3) attack, vector digital map is rotated according to different angles. Because of the vector digital maps' own characteristics and our algorithm only using the coordinates of vector digital maps to calculate the number of vertices, the operation of coordinate translation, scaling or rotation will not affect the number of vertices of the rings, so the above three kinds of attacks have no effect on watermark detection, and the extracted watermark image's similarity is 1.

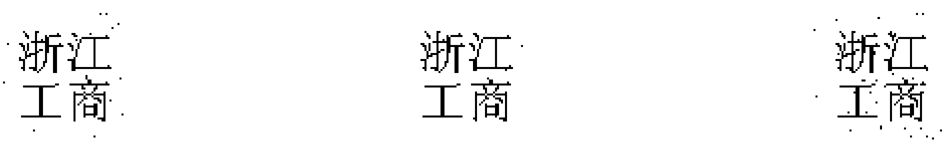


(a) The left cropping of vector map A (b) The center cropping of vector map A (c) The right cropping of vector map A



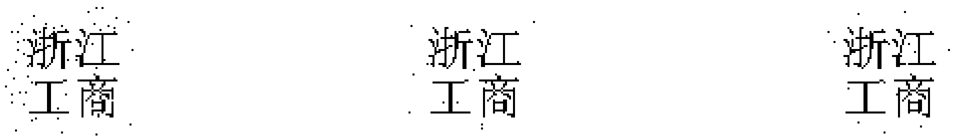
(d) Extracted watermark image from (a) (e) Extracted watermark image from (b) (f) Extracted watermark image from (c)

(g) The left cropping of vector map B (h) The center cropping of vector map B (i) The right cropping of vector map B



(j) Extracted watermark image from (g) (k) Extracted watermark image from (h) (l) Extracted watermark image from (i)

(m) The left cropping of vector map C (n) The center cropping of vector map C (o) The right cropping of vector map C



(p) Extracted watermark image from (m) (q) Extracted watermark image from (n) (r) Extracted watermark image from (o)

Figure 4. The results of extracted watermark image by cropping attack.

For (4) attack, due to increase or decrease the number of vertices, it will directly change the number of count-matrix in the vector digital map, thus affecting the *XOR* operation when extracting the watermark information from the zero-watermarking. Here, p and q are the changed number of vertices, which we will increase or decrease them randomly.

For (5) attack, we are going to crop the test vector digital maps. Fig. 4 shows the experimental results of watermark detection by cutting off the top-left corner, lower-right corner and center of vector digital map, we test vector map A, test vector map B and vector map C. We can see that cropping is more influential than other attacks, but the result of extracted watermark image and watermark image's similarity indicate that our algorithm is still robust.

For (6) attack, we add random noise into coordinates. Due to the change of vertices' coordinates, it will indirectly change the number of count-matrix in the vector digital map, thus also affecting the result of *XOR* operation when extracting the watermark information from the zero-watermarking. Here, r is the percentage of changed number of vertices in the map. In our experiments, we will use r and the value of 10%, 20% and 30%, and we changed the coordinates at a certain range.

For (7) attack, because the algorithm is independent from the order of the geometrical objects in the original vector maps, and the coordinate of vertices will not be changed by scrambling, thus this kind of attack has no effect on watermark detection, so the extracted watermark image's similarity is 1.

To check comparability with the experimental results of extracted watermark image mentioned above, we use similarity (NC) calculation equation (9) to calculate similarity between the extracted watermark image and original watermark image; the results are shown as below table I, table II and table Ш.

$$NC = \frac{\sum_{i,j} f(i,j) f'(i,j)}{\sum_{i,j} f^2(i,j)}. \tag{9}$$

TABLE I.
SIMILARITY ANALYSIS OF THE RESULTS OF WATERMARK DETECTION BASED ON TEST VECTOR MAP A

Attack Mode	Watermark Image Similarity (NC)		
Translation		1.0	
Scaling		1.0	
Rotation		1.0	
Increase vertices (p)	0.9998 (p=100)	0.9979 (p=200)	0.9938 (p=300)
Delete vertices (q)	0. 9958 (q=100)	0.9913 (q=200)	0.9856 (q=300)
Cropping (left)		0.8362	
Cropping (center)		0.8433	
Cropping (right)		0.8658	
Random noise (r)	0.9944 (r=10%)	0.9944 (r=20%)	0.9669 (r=30%)
Objects scrambling		1.0	

TABLE II.
SIMILARITY ANALYSIS OF THE RESULTS OF WATERMARK DETECTION BASED ON TEST VECTOR MAP B

Attack Mode	Watermark Image Similarity (NC)		
Translation		1.0	
Scaling		1.0	
Rotation		1.0	
Increase vertices (p)	0.9881 (p=400)	0.9793 (p=800)	0.9608 (p=1200)
Delete vertices (q)	0. 9784 (q=400)	0.9643 (q=800)	0.9504 (q=1200)
Cropping (left)		0.8965	
Cropping (center)		0.8992	
Cropping (right)		0.8999	
Random noise (r)	0.9888 (r=10%)	0.9778 (r=20%)	0.9654 (r=30%)
Objects scrambling		1.0	

TABLE III.
SIMILARITY ANALYSIS OF THE RESULTS OF WATERMARK DETECTION BASED ON TEST VECTOR MAP C

Attack Mode	Watermark Image Similarity (NC)		
Translation		1.0	
Scaling		1.0	
Rotation		1.0	
Increase vertices (p)	0.9981 (p=2000)	0.9993 (p=4000)	0.9924 (p=6000)
Delete vertices (q)	0. 9998 (q=2000)	0.9996 (q=4000)	0.9993 (q=6000)
Cropping (left)		0.8857	
Cropping (center)		0.8970	
Cropping (right)		0.8958	
Random noise (r)	0.9998 (r=10%)	0.9997 (r=20%)	0.9998 (r=30%)
Objects scrambling		1.0	

In equation (9), $f(i,j)$ and $f^{'}(i,j)$ represent the gray value of two images at (i,j).

Experimental results show that our algorithm have no effects on the objects scrambling, translation, scaling and rotation of vector digital map data. For the deletion and increase of vertex, add random noise and cropping attacks, we can also extract the watermark under certain limits. Thus, watermarking algorithm of this paper has strong robustness, which indicates that the algorithm is feasible and effective.

IV. CONCLUSIONS AND FUTURE WORK

In this paper, we proposed a new zero-watermarking algorithm based on characteristics of 2D vector map. First, we divide the map into grids by using concentric circles and count the number of vertices in each grid, which is the feature information. And then we construct a zero-watermark image which using grids data and copyright watermark image. Experimental results show that the proposed algorithm is resilient to translation, scaling, vertex deletion and growth, rotation and cropping. It can resolve the conflict between imperceptibility and robustness of traditional watermarking algorithm.

As the original vector map data undergoes some normal operations, the data will be changed to be a little different from the original one. Also the latter extracted zero-watermark will not be same with the original one. Therefore, we want to improve the watermark algorithm in our future work to find a comparability measuring for watermark extraction and enhance the robustness of zero-watermark, such as projection transformation, data compression, and other operations.

ACKNOWLEDGMENT

This research is supported by Zhejiang Natural Science Foundation of China (Grant No. Y1101326). And our research is also supported by the Science and Technology Planning Project of Zhejiang Province Grant No.2008C13080 and Grant No. 2010C33150.

REFERENCES

[1] Cox GS, deJager G. A survey of point pattern matching techniques and a new approach to point pattern recognition. In Proceedings of Symposium on Communication and Signal Processing, Lesotho, 1993. 243～248

[2] Johnson Neil F, Duric Zoran, Jajodia Sushil. Information Hiding: Steganography and Watermarking-Attacks and Countermeasures. Portland: Kluwer Academic Publishers, 2000

[3] M. Kurihara, N. Komatsu, H. Arita. Watermarking Vector Digital Maps, Tokyo: Special Interest Group Report Vol. 2000, No. 36, Information Processing Society of Japan

[4] I. Kitamura, S. Kanai, and T. Kishinami, Watermarking vector digital map using wavelet transformation, Proc. Annual Conference of the Geographical Information Systems Association (GISA), Tokyo, pp. 417-421, 2000

[5] R. Ohbuchi, H. Ueda, S. Endoh, Robust watermarking of vector digital maps, in Proc. IEEE Conference on Multimedia and Expo 2002, Lausanne, Switzerland, pp.1-4, 2002

[6] V. Solachidis, N. Nikolaidis, I. Pitas, Watermaking polygonal lines using fourier descriptors. ICASSP2000, Instablul Turkey, 2000. 5-9

[7] N. Nikolaidis, N. Pitas, A. Giannoula, Watermarking of sets of polygonal lines using fusion techniques. Proc IEEE International Conference on Multimedia and Expo. Lauzanne, Switzerland, 549-552, 2002

[8] R. Ohbuchi, H. Ueda, S. Endoh, Watermarking 2D vector maps in the mesh-spectral domain. 2003 International Conference on Shape Modeling and Applications, Seoul, Korea. IEEE Computer Society, pp.12-16 May 2003

[9] R. Ohbuchi, A. Mukaiyama, S. Takahashi, A frequency-domain approach to watermarking 3D shapes, Computer Graphics Forum 21 (3), pp.1-10, 2002

[10] VOIGT M, YANG B , BUSCH C. Reversible watermarking of 2D-vector data, In Proc of the 2004 Multimedia and Security Workshop on Multimedia and Security. Germany , Magdeburg, 2004 : 160-165

[11] Han-ling Zhang, Ming-ming Gao. A Semi-fragile Digital Watermarking Algorithm for 2D Vector Graphics Tamper Localization, Proceedings of the 2009 International Conference on Multimedia Information Networking and Security, Volume 01: 549-552

[12] Parag Agarwal, Balakrishnan Prabhakaran, Robust blind watermarking mechanism for point sampled geometry, Proceedings of the 9th workshop on Multimedia & security, September 20-21, 2007, Dallas, Texas, USA, 2007 : 175 – 186

[13] B. Vallet and B. Lévy. Spectral geometry processing with manifold harmonics. In Proceedings of Eurographics, volume 27, pages 251-260, 2008

[14] Wen Q, Sun T F, Wang S X. Concept and application of zero watermark. ACT A Electronica Sinica, 2003, 31 (2): 214-216

[15] Anbo Li, Bingxian Lin, Ying Chen, Guonian Lü. Study on copyright authentication of GIS vector data based on zero-watermarking. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. Vol. XXXVII. Part B4. Beijing 2008

[16] ZHANG Zuo-li, SUN Shu-sen, WANG Ya-ming, ZHENG Ke-biao. Zero-watermarking algorithm for 2D vector map. Computer Engineering and Design, Volume 30 (6), pages 1473-1475, 2009

[17] CAO Liujuan, MEN Chaoguang, SUN Jianguo. A double zero-watermarking algorithm for 2D vector maps. Journal of Harbin Engineering University, 2011, 32 (3): 340-344

[18] ZHANG Xiao-peng, TONG Xiao-hua, LIU Miao-long. A New Zero-watermark Algorithm Based on Chaotic

Sequences and Wavelet Transform. Geomatics & Spatial Information Technology, 2010, 33 (1): 156-160
[19] MIN Lian-quan , LI Qiang , YANG Yu-bin , YU Qi-hong. A Survey of Watermarking Techniques for Vector Map Data. Journal of Geomatics Science and Technology, 2009, 26 (2): 96-102
[20] Cyril Bazin, Jean-Marie Le Bars, Jacques Madelaine. A blind, fast and robust method for geographical data watermarking. In: Proceedings of the 2nd ACM symposium on information, computer and communications security, ASIASCCS'07, pp 265–272
[21] DING Wei, YAN Wei-Qi, QIDong-Xu. Digital Image Scrambling Technology Based on Arnold Transformation. Journal of Computer-Aided Design & Computer Graphics, Vol 3, No. 4: pages 338-341, 2001
[22] Sun W. The periodicity of Arnold transformation. Journal of North China University of Technology, 1999, 11 (1): 29-32.
[23] Qi D X, Zou J C, Han X Y.A new scramble transformation and its application to image hiding. Science in China: Series E, 2000, 30 (5): 440-447.
[24] Zou J C, Tie X Y.Arnold transformation of digital image with two dimensions and its periodicity. Journal of North China University of Technology, 2000, 12 (1): 10-14.
[25] Zhao H. Arnold transformation of n dimensions and its periodicity. Journal of North China University of Technology, 2002, 14 (1): 21-25.
[26] Rongbo Zhu, "Intelligent Collaborative Event Query Algorithm in Wireless Sensor Networks," International Journal of Distributed Sensor Networks, vol. 2012, Article ID 728521, pp.1-11, 2012.
[27] Rongbo Zhu, Yingying Qin and Jiangqing Wang, "Energy-aware distributed intelligent date gathering algorithm in wireless sensor networks," International Journal of Distributed Sensor Networks, vol. 2011, Article ID 235724, pp. 1-13, 2011.

Wang Xun received the Doctor's degree in department of computer science from Zhejiang University. He is a professor in the department of computer and electronic engineering of Zhejiang Gongshang University. His research interests are in multimedia information retrieval, pattern recognition, mobile networks, and statistical machine learning.

Huang Ding Jun is working towards his MS degree in the theory of software from the department of computer and electronic engineering of Zhejiang Gongshang University. His research interests are in information retrieval, pattern recognition, and statistical machine learning.

Zhang Zhi Yong received the master's degree in department of Mechanical and Energy Engineering from Zhejiang University, Hangzhou, P.R. China in 2001. In 2005, He received the Doctor's degree in department of computer science from Zhejiang University. Now, He is an associate professor in the department of computer and electronic engineering of Zhejiang Gongshang University. His research interests are in information retrieval, pattern recognition, and statistical machine learning.