Lossless Digital Watermarking Scheme for Image Maps

SUN Jianguo, ZHENG Chonghui, GAO Di

Research Center of Data Secrecy and Secrecy Technology, College of National Secrecy, Harbin Engineering University, Harbin 150001, Heilongjiang Province, P. R. China

Abstract: A lossless digital watermarking scheme, which was zero- perturbation on the content and graphics for the digital image maps, is proposed. During the simulation, the scheme has been utilized to model the copyright protection program as a commerce application. Compared to the traditional digital watermarking schemes, our scheme operates in redundancy areas of maps and is scalable to topology changes. Experimental results show that, with respect to the geometric attacks and image transformed, the performance of our scheme is better than the classical algorithms based space or frequency domain with much lower complexity.

Keywords: information hiding; digital watermarking; copyright protection; digital maps

I. INTRODUCTION

As the digital image map widely applied in the national economy important fields, users clearly propose the requirements that any unauthorized operation that changes geographic information content should be prohibited. On the other hand, when the information hiding technology based on spatial or frequency domain deal with regular operation, it also has weak robustness poor practicability and the embedded hidden information can easily be removed.

Therefore, the information hiding technology for digital image map must solve the security problem as follows:

(1) Lossless requirement for copyright protection technology in the process of image map application: to sure that technology itself doesn't produce data disturbance on accuracy and topology structure of the maps, such technologies are research value.

(2) Banning unauthorized copy operations: "defense before the event, blame after the event", the protection technology should achieve the goal that the digital maps cannot be copied and normally used in the unauthorized condition simultaneously.

(3) Tracking and identifying the leaking sources and directly responsible person: when the digital maps being illegally transmitted, in accordance with the copyright symbols, it should be further to determine the specific person, who seized the maps.

From the current development trend of the copyright protection technology in digital image map, above three factors are also the key problems that restrict and affect the further development of the geographic information, domestic and foreign scholars have researched nearly thirty years in the area of content security of digital maps, putting forward a variety of implementation plan and trying to solve the various problems, but those technologies still mainly focus on reducing or narrowing the changes to the content and discarding zero disturbance realizations. In addition, although some scholars have proposed the concept in line with standard lossless data, but still cannot balance the relationship among robustness, invisibility and hiding capacity, which is the main job of our research in this paper.

The rest of this paper is organized as follows. Section II outlines system model and expressions, followed by the lossless watermarking scheme in Section III. Section IV gives the experimental analysis procedure of our scheme. Finally, Section V concludes the paper.

II. SPATIAL CLUSTERING ANALYSIS

Processing area determined by the spatial clustering analysis method that is based on grid density, these areas would be used in embedding the watermarks.

(1) Remove all rendering layers of the digital image map *V*, filter out all additional attributes by the program assisted, such as, name, symbol, and color and so on, and only keep the position and the coordinate of the nodes.

(2) According to the amounts and the distribution of the nodes in the map, specify the step value and calculate to get the average density property threshold *Davg*.

$$Davg = \frac{n+l+c}{3} \times \frac{N}{M} \tag{2-1}$$

In the formula (2-1), *n, l, c* respectively represents the attribute entropy of isolated node, line node and polygon node. *N* is the numbers of the map, *M* is the numbers of the grid.

Under the constraints of *Davg*, we can get the initial classes of the image map, as shown in figure 1(b). Each class corresponds to a cluster.

(3) Appoint the node with minimum density difference value as the density center of the cluster. Density difference value *Mavg* is defined as follows.

$$Mavg = | A_i \times D_i - \sum_{j=1}^{k} (A_i \times D_j - Davg) / K \times S^2 | \tag{2-2}$$

In the formula (2-2), *Mavg* is the density difference value, D_i is the density entropy of the node *i*, A_i is the attribute entropy value, *K* is the total number of the nodes in the cluster and *S* represents the step length. As shown in figure 1(c), black dot is the only density center achieved by calculating.

We can get the initial transformation set, wipe out the topological relation among the nodes and achieve the discrete clustering results as *S*, as shown in figure 1(d).

Regarding to the size of *S*, make up the polynomial coefficient matrix based on two-dimensional space, the matrix elements specify 0 or 1 to the nodes of map.

For the copyright protection scheme with the blind detection, it can directly rely on security container for data recovery. The secret key randomly generate by the security container according to predefined rules in the process of transformation.

III. ZERO-BIT EMBEDDING SCHEME

Take code "110100" for example, the implementation of zero-bit dynamic expansion

In this paper, a lossless digital watermarking scheme is proposed to solve the security problems for digital image map.

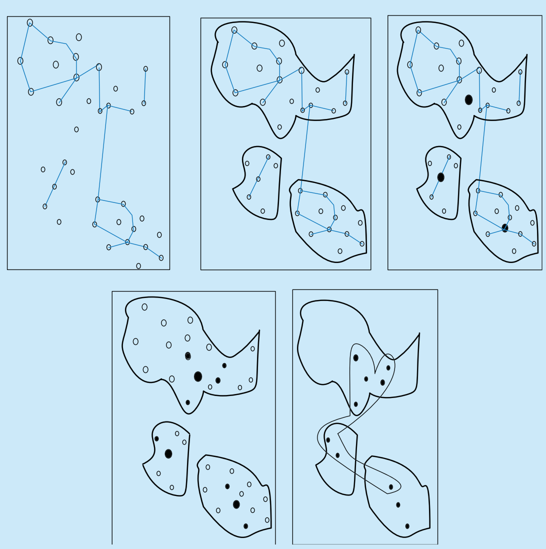

Fig.1 *The flowchart of spatial clustering scheme*
(a) Simplified space; (b) Class set; (c) Density center;(d) Target selection set; (e) Selected target set

scheme is as follows.

(1) Orderly read the same identical bits of the code, *via* "11", and it would be directly extended to the coordinates of node (x_i, y_i), operator "$\circ$" means hyphenation. Therefore, $y_i = y_i \circ 00$ means embedding bit value "1", it indicates the embedding value; $x_i = x_i \circ 00$ means embedding 2 bits in length, it indicates the embedding length. After embedding the code "11", the coordinates of node is $(x_i \circ 00, y_i \circ 00)$.

(2) Similarly, read the continuous sequence "0", $x_i = x_i \circ 0$, the length of the sequence is 1, and $y_i = y_i \circ 0$., means the value of embedding bit is 0. Extend the rest coding to the geographic coordinates of the node (x_k, y_k) and (x_m, y_m).

In order to improve the robustness of the zero-bit extension technology, the zero-bit extension focus on the free position of the coordinate definition block of the feature nodes, to solve the problem that the embedded watermarks have weak resistance on attacks, such as, precision reduction, coordinate adjustment. The specific implementation is as follows.

- According to the principle of zero-bit dynamic extension, embed the coding "110100" to the coordinates of the nodes (xi, yi), (xj, yj), (xk, yk), (xm, ym) in an selected image map,
- According to the file structure of the map, get the ID serial numbers corresponding to above four nodes in the TAB-file of the map.
- By mapping relation of the ID serial values of nodes in the space description MAP-file, get the block numbers and storage space of (xi, yi), (xj, yj), (xk, yk), (xm, ym).
- Read the contents of storage blocks, and find the terminator at the end of effective bits, record the position of terminator.
- Copyright watermarks would be respectively written to the corresponding coordinates block. Following up the terminator, there is enough space to embed several watermark bits for every selected feature nodes. The map editing software of the digital map would not read the content after terminator; we don't have to consider data disturbance and precision damage.
- The MAP-file is binary coding structure, the watermarking is also binary mode, and it makes the copyright information well hidden.
- Record all ID serial numbers of nodes in the map, which have been embedded the copyright information, and save as the secret key.
- In the extraction process, according to the secret key, can obtain copyright information Wt, synchronously extract copyright information duplicate from the coordinates definition block BWt.
- Copyright similarity is tested as the maximum similarity calculation between Wt (or BWt) and W0, W0 is the original.

Zero-bit techniques provide specific implementation strategy of nondestructive hiding scheme.

IV. Experimental Analysis

4.1 Experimental conditions

We use the VC.NET program framework based on MAPX plugins to test our proposed lossless scheme. Table 1 shows the contrast on the loss of precision between our algorithm and spatial algorithm, DFT algorithm, DCT algorithm and coordinate shift algorithm.

- Spatial algorithm: researchers suggest a digital watermarking algorithm based on the dual grid. This algorithm makes the watermark information hide into the least significant bits of the node coordinates dispersedly by double meshing.
- DFT algorithm: researchers correct and extend the MQUAD algorithm to embed watermark s into the transformed frequency coefficients by discrete fourier transform.
- DCT algorithm: extract the map's feature points to compose the feature image. The watermark information is embedded in the low-frequency coefficients by doing the discrete cosine transform for the feature image.

- Coordinate shift algorithm: researchers use drift coordinates to embed watermark information based on a particular two-dimensional vector map DXF files and take advantage of the characteristics of the Z-dimensional invalid coordinates.
- DWT algorithm: researchers choose the vector maps images' blue channel embedded watermark. According to the importance of the wavelet coefficients, the watermark is embedded using different embedding strength to embed the watermark.

Our experimental results show that watermarks are embedded into the superfluous positions of the node blocks in the properties file for an image map. At the meantime, zero-bit expansion scheme ensures that the coordinates just subjoins the 0 bits, no changes on the values, achieving accuracy lossless ultimately.

4.2 Anti-compression attacks

Data compression is used to sample nodes to describe the entire vector space and to ensure recovering the map in the error range. During data compression, each vector node is possible to be removed. Once the nodes carrying watermarks are removed, it easily lead to the copyright failure or failed in watermark extraction.

In order to test the performance of our algorithm on the anti-compression attack, we select two typical vector compression algorithms to compare.

The first compression algorithm: It converts map coordinates data type and does filter plugging point compression to the arc in vector map. This method's compression can be over eighty percent.

Another compression algorithm: Researcher uses the integer value to store coordinates, transforms coordinates storage structure and converts the coordinate offset. This method's compression can be over sixty percent.

Table 2 shows the bit error rate (error of bits / watermark total number of bits) under the two kinds of compression attack. In contrast Ref.[10] algorithm is more vulnerable. Ref.[5] algorithm also uses file as the embedded positions like ours, but it uses random strategy

Table I *Precision comparison after watermark being embedded*

Coordinate/X	Coordinate/X after watermark beding embedded					
	Our algorithm	Ref.[10]	Ref.[11]	Ref.[12]	Ref.[4]	Ref.[5]
112.293 833 40	112.293 833 400 0	112.301 345 600	112.293 846 80	112.293 839 20	112.293 836 80	112.293 833 00
86.256 325 40	86.256 325 400 0	86.134 596 030	86.256 335 10	86.256 324 03	86.256 328 60	86.256 322 30
89.135 532 69	89.135 532 690 0	89.160 039 200	89.135 531 73	89.135 531 06	89.135 531 94	89.135 532 39

Table II *Comparison of false negative rate between watermarking algorithms*

Compression Algorithm	Compression Ratio/%	Error Coding Ratio in watermark extracted after Compressed /%					
		Our algorithm	Ref.[10]	Ref.[11]	Ref.[12]	Ref.[4]	Ref.[5]
Ref.[13]Algorithm	5	2.17	18.83	10.86	13.15	11.34	8.13
Ref.[13]Algorithm	15	5.61	22.10	17.32	20.74	16.76	10.25
Ref.[14]Algorithm	10	3.20	17.58	8.89	13.87	14.70	12.58
Ref.[14]Algorithm	20	7.13	28.99	12.04	22.95	23.33	20.07

Table III *Comparison of false negative rate between same algorithms for attacks*

Geometric Attack		Error Coding Ratio /%					
		Our algorithm	Ref.[10]	Ref.[11]	Ref.[12]	Ref.[4]	Ref.[5]
Cropping	Crossing 1/2	0.61	3.9	3.1	3.64	3.1	3.04
	Upper Left 1/4	1.35	8.26	6.03	7.92	6.03	8.81
	Center 1/4	4.12	16.91	14.18	14.03	14.18	13.49
	Right 1/8	6.3	21.02	16.6	20.47	16.6	15.6
Distortion		0	27.48	19.82	23.39	17.18	0

to select the embed object so that the target object is easily removed by compression.

4.3 Robustness

The experiment selects geometric attacks such as the shearing and distortion. The test results are shown in Table 3 and the performance of our algorithm is better than other algorithms. Ref.[5] algorithm has higher bit error rate under the geometric attacks because it selects the embedded object without specific optimization guidance strategy. Our algorithm takes the embedding target group optimal selection strategy, therefore, it is lower probability that the nodes carrying watermarks would be removed.

V. Conclusions

We design a lossless digital watermarking scheme for image maps in MAPX formatted, which is approximately zero- perturbation on the content and graphics for maps. Because there are many formatted image maps, this algorithm cannot be universality. On comprehensive experiments, the performance of our scheme is superior to that of the proposed solutions on space and frequency algorithms. In addition, it is scalable to the topology changes to a certain extent.

It remains future work to investigate the layer features of the image maps and assignment method for watermarks with different formatted image maps.

Acknowledgements

The authors would like to thank the reviewers for their detailed reviews and constructive comments, which have helped improve the quality of this paper. This work was supported in part by National Science Fund for Distinguished Young Scholars under Grant No.61202455; Research Funds for the Central Universities under Grant No. HEUCF100612; Research Funds for the Doctoral Program of Higher Education of China under Grant No.20112304120025.

References

[1] Ohbuchi R, Ueda H, Endoh S. Robust watermarking of vector digital maps[A]. In: Proceedings of IEEE International Conference on Multimedia and Expo(ICME'02)[C], Lausanne, Switzerland, IEEE Press, 2002: 577 -580.

[2] Solachidis V, Nikolaidis N, Pitas I. Fourier descriptors watermarking of vector graphics images[C]//Proceedings of the International Conference of Image Proceessing, Vancouver, IEEE Society Press, 2000: 9–12.

[3] Nikolaidis N, Solachidis V. Fourier descriptors watermarking of vector graphics images[C]// Proceedings of the International Conference of Image Processing. Vancouver, IEEE Society Press, 2000: 10–13.

[4] LI Yuan-yuan, XU Lu-ping. Vector graphical objects watermarking scheme in wavelet domain[J]. Acta Photonica Sinica, 2004, 33(1): 97–100.

[5] MA Tao-lin, GU Zhong, ZHANG Liang-pei. Watermarking algorithm on 2D vector digital maps[J]. Geomatics and Information Science of Wunan University, 2006, 31(9): 792–794.

[6] XU De-he, ZHU Chang-qing, WANG Qi-sheng. A survey of the research on digital watermark for the vector digital map[J]. Geomantic World, 2007, 12(6): 42–48.

[7] NI Jin-sheng, WANG Yong-ming, QIAN Xiao-ming. Vector map technology practice course[M]. Beijing: Electronics Industry Press, 2008: 20–24, 35.

[8] Voigt M, Yang B, Busch C. Reversible watermarking of 2D-vector data[C]//Proceedings of the 2004 Multimedia and Security Workshop on Multimedia and Security. New York, IEEE Press, 2004: 160–165,

[9] QI Rui, QU Shao-lin. Development of geographic information system with MapX[M]. Beijing: Tsinghua University Press, 2003: 5–13.

[10] DENG Shu-jun, LU Liang, CHE Sen. Research on a digital watermarking algorithm suitable to vector map[C]//Proceedings of the IEEE International Conference on Automation and Logistics. Qingdao, 2007: 1236–1240, IEEE Society Press..

[11] ZHONG Shang-ping. Analysis and improvement of double embedded MQUAD watermarking algorithm[J]. Journal of Computer Research and Development, 2005, 42(S1): 142–149.

[12] LI Qing-yuan, LIU Xiao-dong, CAO Dai-yong. Discussion of vector data compression for Web GIS[J]. Chinese Journal of Image and Graphics, 2001, 6(12): 1225–1229.

[13] LI Qi, YANG Chao-wei, CHEN Ai-jun. Research of geographic database model[J]. Chinese Journal of Image and Graphics, 2000, 5(2): 119–123.

[14] Yang Bi-sheng, Li Qing-quan. Efficient compression of Vector data map based on clustering model[J]. Geomatics and Information Science of

Wuhan University, 2008, 33(3):265-268.

Biographies

SUN Jianguo, received her M.S. degree in computer science and technology in Harbin Institute of Technology and the Ph.D. degrees in computer science and technology at Harbin Engineering University, where he was an associate professor and the director of data security and secrecy technology research centre. He has been an IEEE member since 2008. His research interests include information hiding, data security, and mobile ad hoc networks. *The corresponding author. Email: sunjianguo@hrbeu.edu.cn

ZHENG Chonghui, received her M.S. degree, Ph.D. degree in materials science from Harbin Engineering University, Harbin, Heilongjiang, China. He is currently a professor in the College of National Secrecy, Harbin Engineering University. Her research interests include wireless networking, cognitive networks, integration of heterogeneous network, and mobile ad hoc networks.

GAO Di, received the M.S. degree in social sciences from Harbin Engineering University, Harbin, Heilongjiang, China, in 2005, respectively. She is currently a Ph.D. candidate at Harbin Engineering University, Harbin, Heilongjiang, China. Her research interests focus on wireless communications and human-computer interaction techniques.