ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
*Published By:* **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
September 2013,
Vol. 6, No. (3):
Pgs. 333-339

# Digital Vector Map Watermarking: Applications, Techniques and Attacks

**TAWFIQ A. ABBAS* and MAJID J. JAWAD[1]**

*Dean of Information Technology, College - Babylon University, Iraq.
[1]College of Science, Computer, Science dep.- Babylon University, Iraq.

(Received: August 16, 2013; Accepted: August 30, 2013)

## ABSTRACT

This paper surveys of digital vector map watermarking. Some information will be presented, such as the features of digital vector map, some digital vector map watermarking algorithms, possible attacks on embedded watermark. Also, challenges in field of digital vector map watermarking will be presented.

**Key words*:*** Digital Watermarking; Vector Map; GIS;Topology

## INTRODUCTION

In general, digital watermarking means digitally adding a small amount of data(referred to as watermark) in a digital object (host). The information encoded in the watermark can be used to identify the copyright owner of the object or to detect any tampering performed onto the object[1]. It can be used in several applications, such as copyright protection, Copy Protection, Content Authentication...etc.[2]. Watermarking can be applied in several media, such as image, movie, audio, etc.[4-6]. In the recent years, this technology is focused on the digital vector map. Recently, Geo-spatial data is increasingly used in many applications like navigation systems, location based services offered by cell phones with Global Positioning System (GPS), Web based map services, and developing geographic information system (GIS) for city planning and disaster management[7].

The acquisition of digital vector map is expensive and time consuming process as it requires lots of labor and information resources to acquire geospatial data. Because the digital vector map is stored in digital form, it can be copied and redistributed illegally. To avoid illegal duplication and distribution, one of the remarkable methods used for copyright protection is digital watermarking.The rest of the paper is organized as follows. In section [2], the characteristics of digital vector map is presented. In section[3], the requirements of digital vector map watermarking will be presented.In Section 4, survey on digital vector map will be presented. In Section 5, some attacks on digital vector map watermarking will be presented. The conclusions will be listed section 6.

### Characteristics of digital vector map

Vector map data is normally composed of spatial data, attribution data, and some additional data used as indices or extra descriptions. Spatial data describes the geographical locations of the map objects which represent the geographical objects in the real world and always take the form of three basic geometrical elements, i.e. points, polylines and polygons. All these map objects are formed by many organized vertices.

Spatial data is actually a sequence of coordinates of these vertices based on a certain geographical coordinate system. Attribution data describes the properties of map objects such as their names, categories and some other information.

It is obvious that the information recorded by attribution data is very important and cannot be modified arbitrarily, so does the other additional data mentioned above.

In all proposed watermarking algorithms, the space for embedding watermark is provided by the spatial data, i.e. the coordinates of vertices[8].

### Requirements of Digital vector map watermarking

This section will introduce the important requirements of watermarking systems from the perspective of digital vector map. These requirements can be listed as the following:-

### Fidelity, Transparency, or Imperceptibility

Fidelity, transparency, or imperceptibility means the relative similarity between the un-watermarked vector map and the one after the watermarking operation. A good watermarking technique will produce a high fidelity, i.e., it introduces very little distortion to the host object. Transparency refers to the invisibility of the watermark to human observers. In other word, it refers to the perceptual quality level between the original and watermarked data[9].

### The Robustness

Which is the resilience of the inserted watermark data to any processes (attacks) aimed at either removing or distorting it. A robust watermarking technique should produce watermarks that are able to withstand different types of attacks and its watermark extraction process should be able to retrieve the watermark from the attacked host with little difficulty[10.]

### The Watermark Payload

This is the amount of information that the watermark signal carries. The ideal size of a watermarking technique depends on the application in which the technique is used. Some applications such as copyright protection requires very small payload whereas watermarking for broadcast monitoring requires high payload.

### The Security

The security of a watermarking technique is defined as the level of difficulty in identifying what algorithms used to perform the watermarking process. A highly secure watermarking process would produce output that does not contain any specific signatures that can be used to identify the algorithm[11].

### The Reversibility

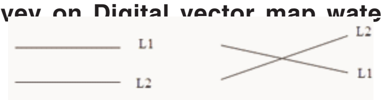
This requirement determines whether the reverse of the watermarking technique can be applied to reconstruct the un-watermarked data from its watermarked counterpart. Reversible watermarking is suitable for hiding data in vector maps because the distortions induced by data embedding can be removed after extracting the hidden bits. For some specific applications of vector map, any disturbance to data accuracy during watermark embedding and extracting is undesirable[12].

### False Positive

This is the detection of watermarks in data that does not contain any watermarks. When we talk of the false positive rate, we refer to the number of false positives we expect to occur in a given number of runs of the detector. In most applications, it is necessary to distinguish between data that contains watermarks and data that doesn't. The false positive rate of a watermark detection system is the probability that it will identify an un-watermarked piece of data as containing a watermark. The seriousness of such an error depends on the application[13].

### Preserving the Map Topology

This requirement is only applicable to vector map watermarking in which the topology of vector map can be changed after a watermarking operation in a high degree and makes the watermarked map invalid to use. Any vector map has to maintain the topology during embedding methods, since the position accuracy and topology are very important to GIS vector map unlike in general multimedia data. When embedding watermark information in a collection of geometric primitives not only perception constraints have to be met but also geometrical properties must be preserved: For example, if there is parallel rivers ina geographic map, after embedding operation, these rivers must not intersected with each other, also, some rivers may overlap with streets after watermarking operation. Fig.1 shows the possible problem after embedding operation. Most of proposed digital vector map watermarking schemes, don't taken into account this situation[14].



(a) L1 and L2 before embedding operation (In parallel situation)

(b) L1 and L2 before embedding operation (In intersection situation)

**Fig. 1: Possible problem, after embedding operation**

### Survey on Digital vector map watermarking algorithms

The watermarking algorithms can be done in two domains, spatial domain and transform domain. In spatial domain the watermark is embedded directly by modifying the coordinate values of vertices, by using several procedures, such as using the locational relationship of vertices, the statistical features of coordinates, etc, While in watermarking a vector map in transform domain, the watermark data is embedded not by directly modifying the coordinates of the vertices, but their transform coefficients instead. The main transforms considered DFT, DWT, and DCT.

In [15], a blind watermarking scheme for vector map is proposed based on Minimum Encasing Rectangle (MER) of the map. MER is the rectangle of minimum area which completely covers all the vertices in the map. MER is employed to keep synchronization when watermarks are embedded and detected due to its geometry invariance property. After gridding the map into cells based on MER and constructing grid weight array, spatial data is converted into frequency domain with DCT. Watermarks are embedded in DCT coefficients with middle-frequency.

By slightly modifying the distribution of vertices, a watermarked map is generated. Experiments show that our watermarking algorithm is robust against rotation, scaling, translation attacks. Furthermore, the robustness of the algorithm against geometry attacks stays invariant with the different magnitude of the translation offset, rotation angle and scaling factor.

In [16], a blind watermarking scheme for copyright protection of GIS vector map is proposed based on ESRI shapefile. The watermarking scheme mainly uses polyline length or perimeter distribution. The watermark is embedded to the local mean length/perimeter of a suitable group of polyline/polygon data by changing all coordinates of vertices according to the constraints of the robustness and the invisibility. All the details of the above procedures are found in the above paper. Experimental results verified that the proposed scheme has robustness against various geometric attacks.

In[17], a blind watermarking scheme based on the DFT (Discrete Fourier Transform) is proposed. This scheme is applied in several steps. First, the vertex sequence that extracted from vector map is carried on DFT transform. Second, divide the phase of DFT according to the quantization step size. Finally, we a new watermarking scheme is introduced to embed the watermark into the phase of DFT through quantification, which provides robustness for watermark attacking. All the details of the above procedures are found in the above paper. Extensive experiments are conducted to validate the availability, invisibility and the robustness of the scheme.

In [18], watermarking scheme proposed based on polygon type of ESRI by using k-means clustering algorithm. This watermarking scheme use k-means clustering algorithm to make all polygons into some clusters. If we want to embed k number of watermark bit, we should divide the polygons into k clusters according to the distribution of centers of polygon using k-means clustering. Then the watermark bit is embedded to the mean distance length of each polygon in a cluster by using odd-even coding. Finally, the coordinates of vertices is be changed according to the new mean distance length of polygon which has been embedded watermark. From experimental results, we verify that the proposed scheme has outstanding invisibility and good robustness against various geometric attacks.Odd-even coding is illustrated in details in above paper.

In[19], a reversible watermarking strategy for 2D-vector maps is proposed based on iterative embedding. It begins with vertex grouping of each polyline. Then only the highly correlated data sets are selected as the cover data for iterative embedding. Finally, the iterative embedding is carried out by reversibly modifying the median vertex coordinates of each selected embedding unit. The original vector data can be strictly recovered with accurate watermark extraction. Meanwhile, both higher payload capacity and better invisibility are proved through both theoretical analysis and comprehensive experimental validations. Experimental results show that the proposed reversible watermarking method is very suitable for 2D-vector map copyright protection and secret communication.

In[20], a non-blind watermarking scheme is proposed for copyright protection of vector map. In this algorithm, watermark is embedded in low frequency coefficients of wavelet transform. In this scheme, the robustness of watermark depends on the embedding strength *p*. If the embedding strength increases, the robustness of watermark increases, but the visual degradation increases and vice versa. Experimental results show that the proposed algorithm is robust against noise, data compression, format exchanging, and vertex addition/deletion.

In[21], a reversible fragile watermarking is proposed for vector map. In this paper, a calculating watermark for each spatial feature group, embedding the watermark in a reversible manner and marking the original location of each feature using interpolated vertices. While the mark of each feature ensures superior accuracy of tamper localization, the reversible data-hiding method provides exact recovery of the original content. Moreover, this paper discusses selecting appropriate embedding parameters to achieve good performance in terms of the tamper localization ability, invisibility, authentication power and security. Experimental results show that the proposed scheme could detect and locate malicious attacks such as vertex/feature modification, vertex addition/deletion, and feature addition/deletion.There are two main drawbacks in our scheme. First, it cannot be applied to Point features. Second, it can locate tampered feature groups but not tampered regions.

In [22], a new blind watermarking scheme for vector map is proposed. The proposed scheme is based on angle and random table. Angles in vector map are not changed easily. The embedding procedure of the watermark is done by; firstly, calculating the angle using three points (coordinates), secondly by using random table, the integer number of calculated angle is changed by using the random table.

Finally, the changed angle is reflected to the points (coordinates) which are used in calculated angle. In the other words the coordinate is changed according to the value of a new changed angle. The extracting procedure of the watermark is approximately same as embedding procedure. In this scheme, the topology of the vector map is preserved after embedding the watermark. Experimental results show that the proposed scheme is robust against several attacks, such as translation, scaling, and vertex attacks. However, this scheme has a weak point that we cannot extract watermarks if the angle is changed.Table 1 shows a summary of the survey that is mentioned in this section

From the above survey, we found several challenges. These challenges are listed as the following

**Table 1: Summary of the survey**

| No | Paper | Domain | Blindness | Reversibility | Topology | Fidelity | Similarity |
|---|---|---|---|---|---|---|---|
| 1 | 15 | DCT | “ | x | x | x | x |
| 2 | 16 | Spatial | “ | x | x | x | x |
| 3 | 17 | DFT | “ | x | x | x | “ |
| 4 | 18 | Spatial | “ | x | x | x | x |
| 5 | 19 | Spatial | “ | “ | x | “ | x |
| 6 | 20 | DWT | x | x | x | x | “ |
| 7 | 21 | Spatial | “ | “ | x | x | x |
| 8 | 22 | Spatial | “ | x | “ | “ | “ |

### Distortion Control

After embedding operation some distortions can be occurred such as distortion of the shape or the topology within a map. In this case, the watermarking techniques are good but the distortion of the shape or the topology makes the vector map invalid. From the above survey, most algorithms don’t take into account these distortions.

### Evaluating the Vector Map’s Fidelity

After applying watermarking schemes, the embedding of hidden messages should not degrade the validity of the cover data. From the above survey, most proposed schemes don’t use appropriate measures for evaluating the fidelity of the watermarked vector maps.

### Evaluating the Watermark’s Similarity

After applying watermark extracting procedure the robustness is measured. This measure is be done by evaluate the similarity between the original watermark and the extracted watermark. From the above survey, most proposed schemes don’t use appropriate measures for evaluating the similarity.

### Reversibility

Reversible watermarking is very desirable watermarking technique in digital vector watermark. In some applications, any changing in the map is undesirable. For example, in military applications this situation is very crucial.From above survey, most of proposed schemes don’t take into account the reversibility.

## Some attacks on digital vector map watermarking

A successful attack means that the watermark can be removed whereas the validity of the cover data can be preserved. The spatial data of vector maps is virtually a floating point data sequence with a certain precision. Consequently, the manners and the features of the possible attacks to vector map watermarking are also different from the general multimedia watermarking. In this section, some attacks will be listed.

### Geometrical Attacks

Some geometrical transforms such as translation, rotation, and scaling are the main forms of geometrical attacks. For vector maps, the above mentioned attacks are virtually coordinate transformations where almost no information would be lost[23].

### Vertex Attacking

Vertex attacking means the attacks in vertex level, e.g. adding new vertices into the map (interpolation) or removing vertices from the map (simplification or cropping). Such attacks, especially the map simplification and cropping, are very serious to vector map watermarking. On the other hand, map simplification is also a common operation in applications to enhance the speed of handling the map data. As a result, the ability of surviving the map simplification is very important to a robust watermarking scheme [24].

### Object Reordering

This is an attack in object level. The spatial data of a vector map is composed of many coordinates of arranged vertices representing map objects.

All objects are stored in the map file in a certain order. Either reordering the objects in the map, or reordering the vertices within an object can produce a new map file without degrading data's precision. To some watermarking scheme which is dependent on the objects' order, this operation will be a fatal attack[25].

### Noise Distortion

There are mainly two sources which could introduce noise into vector maps. The first one is some kind of daily works. For example, there are several popular file formats in GIS world. The transformation among those formats could make the data slightly distorted. The other one is a malicious attack. Attackers attempt to destroy the watermark by adding noise into data sets. Noise distortion is a serious attack but it is generally not a good choice for an attacker because the imposition of noise could possibly degrade the map's validity [26].

## CONCLUSIONS

In this paper some information related to digital vector map watermarking are represented such as , requirements of digital vector map, attacks on digital vector map watermarking. Also, some recommendations about challenges related to applying digital vector map are represented in this paper.

## REFERENCES

1. T. A. Abbas and M. J. Jawad, "Proposed New Watermarking Approach for Vector Image*,"Oriental Journal of Computer Science and Technology*; vol (6), no (2), pp. 99-103, 2013
2. E. Muharemagic and Borko Furht,"Survey Of Watermarking Techniques And Applications," *Department of Computer Science and Engineering Florida Atlantic University, 777 Glades Road Boca Raton*, FL 33431-0991, U.S.A.
3. I. HADI and SAAD TALEB HASSON**, "**Graph Construction based on Database of Movie objects**,"** *Oriental Journal of Computer Science and Technology*, **6**(2): 61-65 (2013).
4. B. P.Chaudhari and A.K.Gulve , "Approaches of Digital Image Watermarking Using ICA," *Computer Science and Engineering Department*, G.E.C.A, B.A.M.University, Aurangabad.
5. M. A. T. ALSALAMI and Marwan M. AL-AKAIDI," Digital Audio Watermarking: Survey," *Computer Science Dept*. – Zarka Private University, Jordan.
6. M. D.Swanson,"Multimedia Data-Embedding and Watermarking Technologies," *proceedings of the ieee*, **86**(6): (1998).
7. Sangita Zope- Chaudhari and P. Venkatachalam, " Robust Watermarking for Protection of Geospatial Data," *IACSIT Hong Kong Conferences*, IPCSIT 29 (2012).
8. X. Niu, ChengYong Shao and XiaoTong Wang,"a survey of digital vector map watermarking", *International Journal of Innovative, Computing, Information and Control*, 2(6): (2006).
9. L. Huang, W. Zhou, R. Jiang and A. Li, "Data Quality Inspection of Watermarked GIS Vector Map," *18th International Conference on Geoinformatics,* **1- 5**: 18-20 (2010).
10. F. Cheng, H. Yin,X. Zhang and D. Zhang, "A Digital Watermarking Algorithm for Vector Map*," International Conference on Challenges in Environmental Science and Computer Engineering (CESCE),*pp. 101 -

103*,* 6-7 March 2010.

11. B. Lin, A. Li, "Study on Benchmark System for Copyright Marking Algorithms of GIS Vector Data," *18th International Conference on Geoinformatics*, 18-20 June 2010.

12. S. Zhong, B. Liao and G. Chen, "A reversible watermarking scheme for two-dimensional CAD engineering graphics based on improved difference expansion*," International Journal of Advancements in Computing Technology,* vol. 3, no. 3 (2011).

13. B. Lin and A. Li," Study on Benchmark System for Copyright Marking Algorithms of GIS Vector Data*,"18th International Conference on Geoinformatics,* pp. 1 - 5, (2010).

14. S. Huber, R. Kwitt, P. Meerwald, Martin Held and Andreas Uhl, "Watermarking of 2d Vector Graphics with Distortion Constraint*,"IEEE International Conference on Multimedia and Expo (ICME),* pp. 480 - 485 (2010).

15. C. Wang, L. Zhang, B. Liang, H. Z., W. Du and Y. Peng, "Watermarking Vector Maps Based on Minimum Encasing Rectangle,"*International Conference on Intelligent Computation Technology and Automation (ICICTA),* 28-29 (2011).

16. X. Huo, T. Seung, B. Jang, K. Kwon and S. Lee, "A Watermarking Scheme Using Polyline and Polygon Characteristic of Shapefile,"*3rd nternational Conference on Intelligent Networks and Intelligent Systems (ICINIS)*, 1-3 (2010).

17. S. Tao, X. Dehe, L. Chengming and S. Jianguo, "Watermarking Gis Data For Digital Map Copyright Protection," *In Proceedings of 24th International Cartographic Conference*, pp.1-9, Santiago, Chile, (2009).

18. X. Huo, K. Moon, S. Lee, T. Seung and K. Kwon, "Protecting GIS Vector Map using the k-means Clustering Algorithm and Odd - even Coding," *17th Korea-Japan Joint Workshop on Frontiers of Computer Vision (FCV),* pp*1 - 5.* , 9-11 (2011).

19. L. Cao, C. Men and X. Li,"Iterative Embedding-Based Reversible watermarking for 2d-Vector Maps," *17th IEEE International Conference on Image Processing (ICIP) ,* pp. 3685 - 3688, 26-29 (2010).

20. S. Zope- Chaudhari and P. Venkatachalam, "Robust Watermarking for Protection of Geospatial Data," In *Proceedings of International Conference on Security Science and Technology (IACSIT),* pp. 34-38 (2012).

21. N. Wang and C. Men, "Reversible Watermarking for 2-D Vector Map Authentication with Localization," *Computer Aided Design Journal*, pp.230-330 (2012).

22. Jungyeop Kim, "Robust Vector Digital Watermarking Using Angles and a Random Table,"*Advances in Information Sciences and Service Sciences*, 2(4): (2010).

23. C. Men, L. Cao, X. Li and N. Wang, "*Global Characteristic-based Lossless Watermarking for 2D-Vector Maps," International conference on Mechatronics and Automation (ICMA)*, pp. 276 – 281, 4-7 Aug. 2010.

24. C. Wang, W. Wang, B. Wu and Q. QIN, "*A Watermarking Algorithm for Vector Data Based on Spatial Domain,"1st International Conference on Information Science and Engineering (ICISE)*, pp. 1959 - 1962 (2009).

25. X. Niu, C. Shao and X. Wang, "A Survey of Digital Vector Map Watermarking," International Journal of Innovative Computing, Information and Control (ICIC), vol. 2, no. 6, pp. 1301—1316, ISSN 1349-4198 (2006).

26. W. Baiyan, W. Wei and M. Dandan,"*2D Vector Map Watermarking based on the Spatial Relations,"International Conference on Earth Observation Data Processing and Analysis (ICEODPA),*Vol. 7285 (2008).