韓國地形空間情報學會誌 第18卷 第3號 2010年 9月 pp. 57-65

연구논문

Development of Digital Watermarking Technology to Protect Cadastral Map Information

Kim, Jung Yeop* · Lee, Hyun Joon · Hong, Sung Eon*****

要 旨

본 연구에서는 디지털워터마킹 방법을 이용하여 디지털 지적도면의 불법유통과 불법복제 등을 방지할 수 있는 대책을 마련하여 보고자 하였다. 이를 위해 기존 연구의 워터마킹 방법을 토대로 지적도면의 특성에 적합하도록 디지털 워터마킹 방법을 개발하고, 이에 대한 성능을 평가하여 보았다. 연구결과, 기존 연구성과를 토대로 워터마크 키와 일방함수를 이용하여 알고리즘을 보완함으로써 워터마킹의 보안성을 강화하였다. 또한 충실도, 강인성, 긍정적 오류율을 모두 만족시키는 동시에 위상 관계 역시 변화가 없는 것으로 나타났다. 본 연구에서 제시하는 방법은 지적도면 뿐만 아니라 GIS, 네비게이션 데이터와 같은 벡터데이터에도 이용 가능하도록 개선하였기 때문에 향후 방법론에 대한 추가적인 보완을 통한다면 보다 광범위하게 이용될 수 있을 것으로 기대한다.

핵심용어 : 디지털워터마킹, 디지털 지적도면, 워커마크 키, 일방함수, 보안성, 벡터데이터

Abstract

This research aimed to prevent illegal distribution and reproduction of digital cadastral map information using digital watermarking. To this end, a digital watermarking was developed in consideration of the properties of cadastral maps and based on watermarking methods, after which its performance was evaluated. A watermark key and a one-way function was used to compensate for the algorithm and, therefore, watermarking security, based on the existing research results. In these ways, the present method meets the requirements for fidelity, robustness, false positive rate and the maintenance of consistent topology. The advanced techniques suggested in this paper were devised so as to be suitable for vector data such as GIS and navigation data as well as cadastral maps. Moreover, if the existing methodology is further improved, it could be expected to be used even more widely.

Keywords : Digital watermarking, Digital cadastral map, Watermark key, One-way function, security, Vector data.

1. Introduction

With the rapid introduction and enhancement of the Internet and computer networking around the world, more and more people have been able to easily gain access to digital data. The wide propagation of multimedia data, moreover, has made it possible for many people to acquire and manipulate a wide range of data. Along with these advances, however, the risk of illegal data copying and reproduction has grown[1]. Thus, many people have looked to data embedding methods identifying digital data owners in order to protect copyright[2].

Digital watermarking is the method of embedding information for, among other purposes, proving copyright in cases of dispute[3]-[11]. Digital watermarking technologies have been a topic of interest since the middle of the 1990s, from which time they have been combined with various multimedia data. Digital watermarking can be used for various purposes, such as owner identification, transaction tracking and content authentication[12]. Correspondingly, this technology has been widely applied.

Cadastral information management is a nation's

2010년 7월 30일 접수, 2010년 8월 26일 채택

* Post Doctor, University of Missouri Columbia at Columbia(jyfloo@gmail.com)

** Professor, Dept. of Real Estate & Cadastrology, Kyungil University(hjlee@kiu.ac.kr)

*** Corresponding Author, Member · Professor, Dept. of Land Management, Cheongju University(hongsu2005@cju.ac.kr)

most important land-related data management, akin to the protection of public land ownership and the management of national land. Each country has its own unique cadastral system, and most countries such as Germany, France, Switzerland, Japan, Korea and Taiwan manage cadastral large-scale maps. Moreover, most countries digitalize analog maps and operate a cadastral system with digital cadastral maps.

The importance of an interest in cadastral maps and conversion to digitalized map-management systems has increased with concerns for data spillage and illegal distribution of cadastral maps. Recently, the application of digital watermarking technology to the protection of land ownership claims and the copyrighting of GIS-related vector spatial data has been studied. However, considering the importance of cadastral maps to countries, watermarking technology to protect land ownership and copyright must rapidly adopt cadastral map data rather than GIS data or navigation data.

Research on digital watermarking has focused mainly on multimedia data, the research on vector data remaining relatively insufficient. Thus far, research on digital watermarking regarding vector data has been concerned mainly with the frequency domain method[13]-[16], which provides robustness against attacks, and the spatial domain method[17]-[20] which easily controls distortion.

In the previous research on watermarking technology, the watermark has not been extracted for various data operations including insert/erase, and neither have topological changes made after embedding of the watermark been considered[13]-[20].

Since cadastral map data is directly relevant to protecting public land ownership, it is managed using the most large-scale and accurate methods available. Indeed, in order to effectively protect cadastral map data with watermarking technology, accuracy in embedding and extracting watermarks is one of the most essential aspects. Additionally, there must be no distortion when cadastral map data is compared with the original.

This study aimed to devise watermarking technology that compensates for the limitations of the watermarking methods found in the previous research. It also intended to develop a method optimized for cadastral maps targeting parcel and to suggest an advanced watermarking technology to protect cadastral map data accurately and safely.

Chapter II deals with the basic principles of digital watermarking and the considerations involved in applying watermarking to cadastral maps, which is, with the properties of cadastral maps compared with general vector data. Chapter III describes proposed watermarking scheme considering properties of cadastral maps. Chapter IV compares the performance of advanced digital watermarking with the methods described in the previous research. Finally, Chapter V discusses the present research results.

2. Considerations in applying digital watermarking and cadastral maps

2.1 Digital watermarking

The most essential purpose of digital watermarking is to identify ownership. That is why special information must be inserted to identify ownership accurately. Generally, this special information must have no problem in using data and maintain consistent information after frequent data operation. That is, a watermark-embedding algorithm must be used to insert additional information necessary to prove the ownership of the original data. Thereby, accurately watermarked data can be created. Further, it must be possible to prove ownership by extracting the created watermarked data again through a watermark-extraction algorithm. Figure 1 illustrates the basic principles of embedding and extracting watermarks.

Digital watermarking techniques can be classified based on many criteria including the data type and robustness of the embedded watermarks. More than anything else, classification based on watermark- embedding methods is very common. Watermarks can be embedded in the frequency domain or the spatial domain. The former is strong against many attacks but has difficulty controlling distortion[11]. The latter, whereas not poor at responding to many attacks, can control distortion easily compared with the frequency domain. Since both methods have advantages

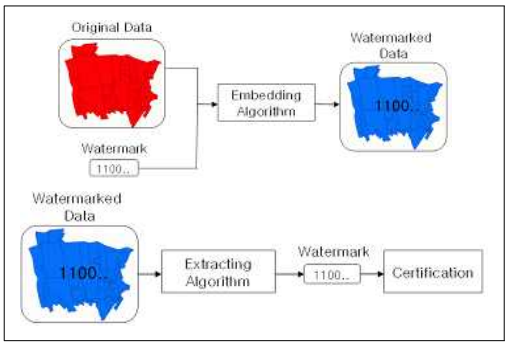


Fig 1. Embedding and extracting watermarks

and disadvantages, it is best to select the watermarking method according to the properties of the pertinent data.

The criteria by which digital watermarking performance is evaluated are as follows: 1) embedding effectiveness, which is the ability to extract watermarks after embedding them; 2) fidelity, reflecting whether the original data is normal after the embedding of watermarks; 3) robustness, which is the ability to extract watermarks after applying various processes to them, and 4) the false positive rate at which watermarks are extracted from data with no watermarks embedded[2]. Watermarking methods must be ideal in meeting all of the evaluation criteria[1],[21]. In particular, fidelity and robustness are a trade-off. Therefore, important evaluation criteria must be selected and applied to satisfy purpose for using watermarking and data property, and for other criteria, attenuation effect must be made.

2.2 Cadastral maps

The properties of cadastral maps must be accurately reflected in the application of digital watermarking to protect cadastral map data. In other words, the unique characteristics of cadastral maps as differentiated from those of general GIS vector data must be considered.

Cadastral maps are essential to the large-scale and effective management of national land resources. Borders, registered with maps, are the foundation of land ownership protection. Therefore, unlike general GIS vector data, cadastral map data must ensure accuracy. Digital topographic maps are mainly created/managed in small scales by each country, but cadastral maps are managed in large scale with high positional accuracy. Therefore, cadastral maps must ensure high positional accuracy after watermarks are embedded in them. That is, it is important to maintain, to the extent possible, the raw data.

In addition, in order to update cadastral maps to reflect changes in land description items, attacks against various operations must be prevented. In particular, to protect the integrity of partition subdivisions of lot divisions, annexation consolidations, registration conversions, file format conversions and map matchings, which frequently occur with changes in land description items, attacks against various operations must be prevented. That is, in order to apply watermarking technology to cadastral maps, the requirements of fidelity, robustness and false positive rate must be satisfied.

Moreover, cadastral map data is a kind of spatial data. Therefore, when employing watermarking, topology must be maintained as for GIS data.

3. The proposed watermarking scheme

As discussed above, when applying watermarking to cadastral map data, the most important consideration is to minimize any damage to the original data. That is, when watermarks are embedded, they must be the same as the original. Therefore, the present research devised a watermarking method to satisfy watermarking fidelity. Besides, if the topology is damaged when watermarks are embedded, the watermarking method must consider not damaging the topology. In this case, the advantage of the watermarking method in the spatial domain is fully utilized. The digital watermarking method presented in this paper can be classified into two parts: watermark embedding and watermark extraction.

3.1 Watermark embedding

Watermark embedding starts with raising the coordinates in the data to the second power. Since it is the principle followed in this research to embed watermarks into all coordinates in the data, all coordinates have to be raised to the second power, re-

spectively for the x, y data coordinates. Only values in constant digits must be raised to the second power. For example, multiplying the constant digits of the 204177.66 coordinates, 41688247329 are generated.

The method suggested in this research is to embed watermarks into a position lower than the decimal point, so that only constant digit values have to be raised to the second power in order to extract the watermarks later. After the constant digits are so raised, each digit is added.

In the present case, the watermark key, one of the watermarking features, was used. Rather than adding all of the digits, the data owner adds digits within a certain range. For example, it is possible to add all digits ranging from 4 (a first digit) to 9 (the last digit). Using the watermark key, it is also possible to add values within a certain range. The added values use remainders with quotients of 15. When 41688247329 are added together, the result is 4+1+6+8+8+2+4+7+3+2+9 = 54. When 54 are divided by 15, the remainder is 9. 15 were designated considering the floating point representation of IEEE754 and the data coordinates used in this research. The floating point representation of IEEE754 makes it possible to calculate the number of bits expressing values less than the decimal point.

For watermark embedding, 15 were selected for use with the methods suggested in this research.

With the value obtained from the remainder, the position at which to embed the watermark is selected. After expressing the coordinates with IEEE754, the position is moved to the position as many as the remainder less than a decimal point and then convert the value remaining from the movement position into

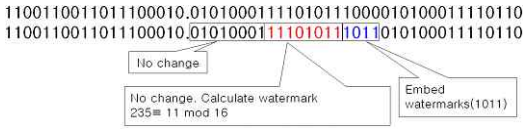


Fig 2. Example of watermark embedding suggested in this research

decimal value. For example, if 1100110011011000110011001111010010011 is saved as the coordinates, move the value less than decimal point into the position as many as the underline and then the position is moved to the underline, after which the value is converted into a decimal number.

1100110011011000110011001111010010011 => 001100111(2) = 102. Convert the remainder generated when the converted value is divided by 16 into a binary number. The converted value is the watermark to be embedded, and the 4 digits after the underlined bits are converted to watermarks. For example, 1100110011011000110011001111011 0010011 are the final coordinates indicating where the watermark is inserted. Figure 2 shows an example of the watermark embedding suggested in this research.

Watermark embedding is performed as follows, and the pseudo code is shown in Figure 3.

Step 1. Raise the constant value of the original x, y data coordinates to the second power
Step 2. Add values within a certain range with the watermark key
Step 3. Determine the position at which to embed the watermark using the remainder
Step 4. Calculate the watermark using the re-

```
Insert_Watermark()
    while( number of coordinates)
        temp      ← (coordinates)^2
        watermark ← sum(temp) % 15
        intersection_point<x,y>   ← calculate_intersection_points
        watermark_point<x,y>      ← intersection_point<x,y>
    End while
End
```

Fig 3. Watermark-embedding pseudo code

```
Detect_Watermark()
        while(number of coordinates)
                temp ← (coordinates)^2
                watermark ← sum(temp) % 15
                if reflect watermark in watermark_point<x,y> then
                        extraction success
                else
                        extraction fail
        End while
End
```

Fig 4. Watermark-extraction pseudo code

mainder

Step 5. Embed the watermark

3.2 Watermark extraction

The watermark-extraction process is similar to the watermark-embedding process. First of all, before extracting watermarks, preprocess is performed on the watermarked data on the same state of the original. When data operations such as rotation and translation are performed, the data is converted to its original data state. After completing the preprocess, the watermark key is used for embedding the watermark and performing the same process as watermark embedding. When calculating the watermark to be finally embedded, check if the position at which to embed the calculated watermark is correct. Watermark extraction is performed as follows, and the pseudo code is shown in Figure 4.

Step 1. Raise the constant value of the original x, y data coordinates to the second power

Step 2. Add values within a certain range with the watermark key

Step 3. Determine the position at which to embed the watermark using the remainder

Step 4. Calculate the watermark using the remainder

Step 5. Check if the calculated watermark is identical to the embedded watermark

Step 6. Detect the watermark

In order to evaluate the extraction ratio of the watermark, the CR (Correspondence Ratio) was used in this research. The relevant formula is as follows.

$$CR = \frac{\text{The number of extracted watermark coordinates}}{\text{The number of data coordinates used for extraction}}$$

4. Experimental results and analysis

4.1 Experimental Data

In order to test the watermarking, a cadastral map of Gangnam-gu, Seoul, was utilized. The target map was of 1:1,200 scale and 38cm of position accuracy. 1:1,200 scale maps are the most common type managed in Korea and the most widely used in cadastral work(Figure 5). The map was created in shp and dxf formats. Therefore, in this research, changes in the watermarking were analyzed by converting the file format between the two sets of data along with experiment in shp file format. .shp file of ESRI complies with the floating point representation of IEEE754.

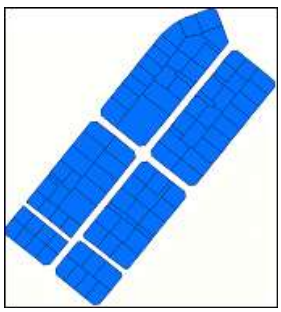


Fig 5. Experimental cadastral map(scale 1:1,200)

4.2 Experimental Results

In this research, many experiments with cadastral maps were conducted to evaluate the performance, including robustness, of the watermarking against many operations crucial to cadastral work. Major tasks currently performed in cadastral work using cadastral maps include partition subdivisions of lot divisions, annexation consolidations, registration conversions, file format conversions, serial map mapping and editing. These operations are the same as in GIS-based map mating (partition subdivisions of lot divisions and/serial map mapping), adding objects (registration conversion), deleting objects (annexation consolidation), file format conversion and clipping/generalization (editing). Finally, it is important to check if there are any topological changes in cadastral maps in the form of spatial data.

Attacks or operations against data were conducted in ArcMAP 9.1. The watermark embedding and extracting systems are embodied using Visual C++6.0 of Visual studio 6.0.

In the experiment, the watermark keys 1 and 11 were used with the selected data, and attacks against watermark-embedded data were conducted in adding/erasing objects, map matching, clipping and generalization.

First of all, the extraction ratio was evaluated for object addition. In the experiment, objects not embedded with the watermark were randomly added to the watermark-embedded data (Figure 6, left). By analyzing the extraction ratio through experimentation, the CR value was determined to be 93.3%, because watermarks were not embedded in the added data and watermarks were extracted from other objects except for the corresponding objects. Therefore, the extraction ratio was considered to be remarkably high, showing robustness against data addition.

Next, attacks by deleting objects were experimented on. In the experiments, the CR value was determined to be 93.4%, because, as the watermark-embedded objects disappeared and objects were integrated (annexation), new coordinates were generated. This result also showed a high CR value, proving that the suggested method ensures robustness against object deletion(Figure 6, right).

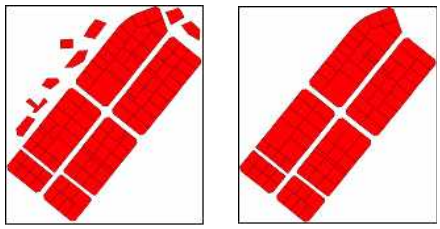


Fig 6. Object addition (left) and deletion (right) test

Map matching was evaluated by dividing the raw data already used in experimentation into two and embedding watermarks into each of them using the same watermark key (Figure 7). By merging much data together, map matching was conducted, which is the same process as embedding watermarks into each cadastral map and connecting those maps (creating cadastral maps). The experimental result was a CR value of 100%, because the watermarks embedded into each data did not disappear or maintain their original coordinates. Therefore, this research proves that there are no significant problems with map matching.

The clipping operation next was evaluated. The raw data was clipped into three parts, and the extraction ratio was analyzed (Figure 8). The extraction ratio of the three parts was over 90%, proving that clipping presents no problem for the suggested method. In a data generalization evaluation, many operations were conducted using ArcMap 9.1 of ESRI. The generalization of ArcMap 9.1 was based on the Douglas-Peuker algorithm. Thresholds of 1m, 3m, and 5m were respectively applied to the algorithm. According to the experimental result, the CR value was a full 100% for all of the parts (Figure 9), because new coordinates were not added to the watermarks even though the coordinates where the watermarks were embedded were deleted during generalization. Therefore, the suggested method was proved to be robust against generalization.

Considering that cadastral maps are managed in shp and dxf file formats, robustness against file format conversion was tested. To this end, the .shp format used in the present research was converted into the .dxf format and then converted back into the .shp format again. The test proved that there are no problems associated with watermark extraction, because

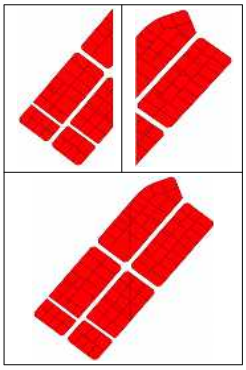
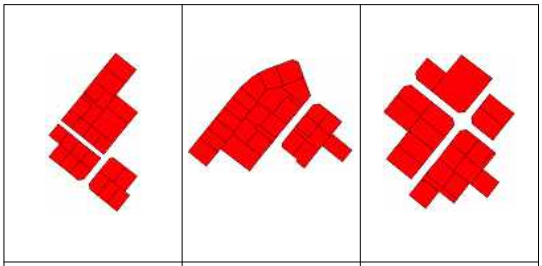
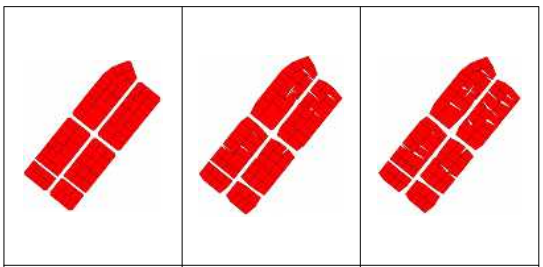


Fig 7. Data map matching test



No. 1 extraction ratio 99.0%	No. 2 extraction ratio 100%	No. 3 extraction ratio 100%

Fig 8. Data clipping test



threshold 1m	threshold 3m	threshold 5m

Fig 9. Data generalization test

the method suggested in this research is based on floating point representation of IEEE754, and the .dxf file format was shown also to comply with IEEE754.

The robustness of the suggested method was evaluated using the CR values in various attacks. All of the experimental results showed a high CR value, proving that the method can prevent illegal distribution and reproduction of cadastral maps. However, since coordinates and positional information are very important in map data, a watermarking method that is strong against many attacks is important, though a method that satisfies fidelity is also crucial. In this research, a watermark was embedded and a comparison to the raw material was analyzed, as shown in Table 1. In addition, in order to check for topological changes after the watermark was embedded, the raw data was compared with the data embedded with the watermark. According to the comparison analysis, when the allowable error of the 1:1,200 cadastral map is 0.38m, the result is within the allowable error, satisfying fidelity.

Finally, the false positive rate of detection of watermarks from data not embedded with watermarks was evaluated. For the experiment, a watermark was extracted from a general vector map data not embedded with any watermark. According to the experimental result, the CR value was 6.8%. This value is much lower than the normal value, proving that the suggested method has an allowable false positive rate.

The present research comprehensively analyzed each digital watermarking feature. Much of the statistical data and examination of topological changes showed that the suggested method satisfies fidelity. Given the possibility to extract embedded watermarks against various attacks, the suggested method certainly satisfies robustness. The low false positive

Table 1. Comparison experiment for fidelity

Comparison Experiment	Result(m)
RMSE	0.03
Maximum difference of distance	0.19
Minimum difference of distance	0.00
Average difference of distance	0.01
Change of topology	N

Table 2. Satisfaction examination according to watermarking performance evaluation criteria

Watermarking performance evaluation criteria	Fidelity	Robustness	False Positive Rate	Change of topology
Experimental result	Satisfied	Satisfied	Satisfied	No

rate, moreover, proves that the suggested method satisfies that requirement as well.

5. Conclusion and future work

In this research, the suggested digital watermarking method was designed to satisfy the requirements of fidelity, robustness, false positive rate and topology considering the characteristics of cadastral maps. In other words, the method's watermark key and one-way function were used to strengthen algorithm security.

In particular, unlike previous watermarking studies that did not consider topological changes, the present research focused on detecting topological changes by comparing the time after the watermark is embedded and the time before the watermark is embedded, ultimately improving fidelity. In a forthcoming study, positional accuracy, one of the essential attributes of cadastral maps, will be considered.

The watermark-extraction ratio is high not only in extracting embedded watermarks but also in adding and deleting objects, map matching and generalization. Experiments targeting various attacks also proved that the suggested method satisfies robustness. Along with meeting fidelity and robustness, the suggested method maintains a constant topology and compensates for the previous vector map digital watermarking methods.

However, the suggested method requires preprocessing for watermark extraction. This challenge must be solved to improve the simplicity of the watermarking process.

Also, the suggested method will be improved to be available for vector data such as GIS and navigation data as well as for cadastral maps, making it still more widely applicable.

References

1. Y.H. Ko, 2002, "Object-Oriented Watermarking Method based on PSADT and Two-Layer Watermarking Method", PhD Thesis, Korea Advanced Institute of Science and Technology.
2. H.S. Kim, 2005, Digital Watermarking, Green Publishing.
3. J. Zhao, E. Koch, 1998, "A Generic Digital Watermarking Model", *Computer & Graphics*, 22(4):397-403.
4. H.C. Wu, C.C. Chang, 2005, "A Novel Digital Image Watermarking Scheme based on the Vector Quantization Technique", *Computers & Security*, 24(6):460-471.
5. T.V. Nguyen, J.C. Patra, 2008, "A Simple ICA-based Digital Image Watermarking Scheme", *Digital Signal Processing*, 18(5):762-776.
6. C. Jin, 2006, "Affine Invariant Watermarking Algorithm using Feature Matching", *Digital Signal Processing*, 16(3):247-254.
7. A.A. Mohammad, A.A, Sameer, 2008, "An Improved SVD-based Watermarking Scheme for Protecting Rightful Ownership", *Signal Processing*, 88(9):2158-2180.
8. G. Voyatzis, I. Pitas, 1998, "Digital Image Watermarking using Mixing Systems", *Computers & Graphics*, 22(4):405-416.
9. K.S. Jonathan, H.Frank and G.Bernd, 1998, "Digital Watermarking of Text, Image, and Video Documents", *Computers & Graphics*, 22(6):687-695.
10. M.C. Hu, D.C. Lou, M.C. Chang, 2007, "Dual-wrapped Digital Watermarking Scheme for Image Copyright Protection", *Computers & Security*, 26(4):319-330.
11. S.H Joo, Y.H. Suh, J.H. Shin, and Hisakazu Kikuchi, 2002, "A New Robust Watermark Embedding into Wavelet DC Components", *ETRI Journal*, 24(5):401-404,.
12. J.Y. Kim, S.H. Park, 2008, "Vector Map Data Watermarking Method using Binary Notation", *The Journal of Geographic Information System Association of Korea*, 14(4):385-395.
13. V.Solachidis, N.Nikolaidis, and I.Pitas, 2000, "Fourier descriptors watermarking of vector graphics images", *Proceedings of the International Conference on Image Processing*, Vancouver, Canada.
14. I.Kitamura, S.Kanai, and T.Kishinami, 2001, "Copyright Protection of Vector map using Digital Watermarking Method based on Discrete Fourier Transform", *Proceedings of the IEEE 2001*

International Symposium on Geoscience and Remote Sensing Symposium, Sydney, Australia.

15. Y.Y.Li, and L.P.Xu, 2003, "A Blind Watermarking of Vector Graphics Images", *Proceedings of the Fifth International Conference on Computational Intelligence and Multimedia Applications*, Xi'an, China.
16. M.Voigt, B.Yang, and C.Busch, 2004, "Reversible Watermarking of 2D-Vector Data", *Proceedings of the 2004 Multimedia and Security Workshop on Multimedia and security*, Magdeburg, Germany, 2004.
17. R.Ohbuchi, H.Ueda, and S.Endoh, 2002, "Robust Watermarking of Vector Digital Maps", *Proceedings of IEEE International Conference on Multimedia and Expo*, Lausanne, Switzerland.
18. H.I. Kang, K.I. Kim, and J.U. Choi, 2001, "A vector watermarking using the generalized square mask", *Proceedings of International Conference on Information Technology: Coding and Computing*, Las Vegas, Nevada, USA.
19. M.Voigt, and C.Busch, 2003, "Feature-based Watermarking of 2D Vector Data", *Proceedings of the SPIE-Security and Watermarking of Multimedia Content*, Santa Clara, CA, USA.
20. C.Y.Shao, H.L.Wang, X.M.Niu, and X.T.Wang, 2006, "A Shape-preserving Method for Watermarking 2D Vector Maps based on Statistic Detection", *Proceedings of IEICE-Transactions on Information and Systems*, vol.E89-D, no.3, pp.1290-1293.
21. H.H. Song, 2004, "Robust Image Watermarking Algorithm using DWT and Fuzzy Inference", PhD Thesis, Mokwon Unviersity.