Journal of Korea Spatial Information Society Vol.21, No.3 : 31-43, June 2013
http://dx.doi.org/10.12672/ksis.2013.21.3.031
ISSN 2287-9242(Print)
ISSN 2287-9250(Online)

# 강인성 향상을 위한 벡터 맵 워터마킹 알고리즘의 적용과 평가

# Application and Evaluation of Vector Map Watermarking Algorithm for Robustness Enhancement

원 성 민* 박 수 홍**
Sung Min Won Soo Hong Park

**요 약** 벡터 맵 데이터는 다른 멀티미디어에 비하여 높은 가치를 지님에도 불구하고 데이터의 불법 복제와 저작권에 대한 인식과 연구는 미비한 실정이다. 본 연구에서는 벡터 맵 데이터의 저장 구조를 고려하여 다양한 공격에 대하여 강인한 워터마킹 기법을 제안하고자 한다. 워터마킹 알고리즘의 설계를 위하여 여섯 가지 접근 방법을 고안하였다(포인트 기반의 접근, 최소 둘레 삼각형 구성, 길이 비율에 대한 워터마크 삽입, 워터마크 이미지의 위치를 참조, 그룹화, 일방함수의 사용). 제안 방법은 입력 효과성, 오검출률, 충실도의 특성을 만족하고 강인성 측면에서 노이즈 첨가를 제외한 모든 공격에서 강인함을 보였다. 또한 제안 방법은 원본 데이터가 필요 없는 Blind 방식이며, 데이터 의존적이지 않은 장점을 갖는다. 추가로 단순화 공격에 대하여 단순화 정도가 심해짐에 따라 강인성이 저하되는 선행 연구의 문제점을 해결할 수 있었다.

**키워드** : 디지털 워터마킹, 벡터 맵, 최소 둘레 삼각형, 일방 함수

**Abstract** Although the vector map data possesses much higher values than other types of multimedia, the data copyright and the protection against illegal duplication are still far away from the attention. This paper proposes a novel watermarking technique which is both robust to diverse attacks and optimized to a vector map structure. Six approaches are proposed for the design of the watermarking algorithm: point-based approach, building a minimum perimeter triangle, watermark embedding in the length ratio, referencing to the pixel position of the watermark image, grouping, and using the one-way function. Our method preserves the characteristics of watermarking such as embedding effectiveness, fidelity, and false positive rate, while maintaining robustness to all types of attack except a noise attack. Furthermore, our method is a blind scheme in which robustness is independent of the map data. Finally, our method provides a solution to the challenging issue of degraded robustness under severe simplification attacks.

**Keywords** : digital watermarking, vector map data, minimum perimeter triangles, one-way function

## 1. 서 론

과거 종이지도 형태로 보급·유통되던 지리정보는 컴퓨터 기술의 비약적인 발전으로 디지털 지도의 형태로 제작되어 다양한 분야에 사용되고 있다. 특히 지리정보시스템의 발전으로 수치지도의 사용이 국가차원의 시설물 관리와 같은 공공분야 뿐만 아니라 민간 분야로 확산되고 있는 실정이다. 디지털 지도를 구성하는 주요 데이터인 벡터 맵 데이터는 생성과 유지에 많은 노력과 높은 비용을 필요로 한다. 측량을 위한 고정밀 측량 장비와 많은 양의 업무 자원이 필요하고 측량 데이터의 디지털화, 벡터화와 같은 복잡한 작업이 필요하다[15].

위와 같이 벡터 맵 데이터는 다른 멀티미디어에 비하여 높은 가치를 지님에도 불구하고 데이터의 불법복제와 소유권에 대한 인식과 연구는 미비한

* 인하대학교 지리정보공학과 석사 kurt18n@gmail.com
** 인하대학교 지리정보공학과 교수 shpark@inha.ac.kr

실정이다. 디지털 데이터의 보호를 위하여 주로 사용되는 방법으로 전자 서명(Digital Signature), 메시지 인증 코드(Message Authentication Code) 등의 암호화 기술이 있다. 이러한 방법들은 매우 신뢰성 있고 광범위하게 사용되지만 암호가 해독된 후에 얼마든지 복제가 가능하다는 문제점이 존재한다. 이에 대한 대안으로 디지털 워터마킹 기술이 디지털 데이터의 불법 복제를 방지하기 위한 방법으로 사용되고 있다[1].

디지털 워터마킹은 디지털 데이터에 부가정보를 은닉하여 함께 저장하는 기법이다[21]. 디지털 워터마킹에서 인증정보는 데이터에 내재되어 저장되기 때문에 암호가 해독된 이후의 복제된 데이터에서도 소유권을 입증할 수 있는 부가정보를 추출할 수 있다. 1990년대 이후로 이미지, 비디오, 오디오 등의 멀티미디어에 대한 워터마킹 연구가 활발히 진행되어왔으나 벡터 맵 데이터의 워터마킹에 대한 연구는 미비한 실정이다[8]. 벡터 맵은 다른 미디어 타입과는 달리 포인트, 라인, 폴리곤으로 구성된 특별한 저장구조를 갖으며 데이터의 공격 유형 또한 다른 미디어 타입과는 달리 기하 공격, 버텍스 공격, 재배열 공격, 노이즈 공격 등으로 구성된다[15]. 따라서 널리 사용되던 전통적인 워터마킹 방법을 그대로 적용할 수 없다[2].

또한 현재까지 연구된 벡터 맵 워터마킹 기법들은 몇 가지 문제점들 때문에 일반적인 방법으로 사용되기 어렵다. 일반적으로 디지털 워터마킹은 입력 효과성, 충실도, 오검출률, 강인성 등의 특징을 갖으며[5], 선행 연구들은 강인성 측면에서 특정 공격에 대하여 취약한 연구가 대부분이다. 강인성 측면의 문제점뿐만 아니라 데이터의 양과 종류에 따라서 검출률이 변하는 데이터 의존적인 문제가 발생하는 연구도 존재한다.

이러한 선행 연구들의 문제점을 해결하기 위하여 벡터 맵 데이터의 저장구조와 공격 유형을 고려한 새로운 접근 방법과 워터마킹 기법의 연구가 필요하다. 본 연구에서는 워터마킹의 주요 특성인 입력 효과성, 오검출률, 충실도의 특성을 만족하고 데이터 의존성이 없는 강인한 워터마킹 기법을 제안하고자 한다. 이를 위하여 국내외 관련 연구를 살펴보고 한계점을 분석하였다. 그리고 워터마킹 기법의 설계를 위하여 여섯 가지 접근 방법을 고안하였으며, 이를 사용하여 워터마킹 알고리즘을 설계하고 구현하였다. 제안된 방법을 평가하기 위하여 폴리곤 타입의 수치지도에 워터마크를 삽입하고 워터마킹의 주요 특성을 만족하는지 여부를 실험하였다.

## 2. 관련 연구

벡터 맵 데이터의 디지털 워터마킹에 관한 연구는 1990년대 후반부터 시작되어 공간 영역, 변환 영역의 방법 모두에서 다양한 연구가 진행되었으며, 그 중 비교적 잘 알려진 연구들에 대하여 분석하였다. 먼저 공간 영역의 방법은 데이터의 값을 직접적으로 수정하여 워터마크를 삽입하는 방법이다.

Ohbuchi 외[16]는 Grid, Quadtree 등의 방법을 사용하여 공간을 분할하고 분할된 직사각형내의 좌표에 PRNS(Pseudo Random Number Sequence)를 이용하여 워터마크를 삽입하였다. 이 방법은 대부분의 공격에 대하여 강인한 방법이다. 그러나 검출 시에 원본 데이터가 필요하며, 원본 데이터와 워터마크가 삽입된 데이터를 매칭하는 과정이 어렵다는 단점이 있다. 또한 데이터 의존적인 문제도 존재한다. 직사각형 내부의 좌표개수를 늘리면 강인성이 향상되는 대신에 워터마크 정보의 적재량이 적어지고, 좌표 개수를 줄이면 적재량이 많아지는 대신에 강인성이 저하된다.

Voigt과 Busch[23]는 직사각형의 패치를 맵에 씌우고 패치를 더 작은 서브패치로 나누며 떨어져 있는 두 패치의 통계적인 접근을 통하여 워터마크를 삽입하였다. 이 방법은 패치를 씌울 때 특정 기준좌표를 기반으로 하고 있다. 따라서 이동, 회전, 축척 변환 등의 기하 공격이 발생하면 기준좌표가 변하기 때문에 검출이 불가능하다. 또한 패치 내부의 좌표 개수가 적어질수록 강인성이 저하되는 문제도 존재한다.

Schulz와 Voigt[20]은 공간을 정사각형의 패치로 분할시키고 워터마크 비트에 따라 좌표를 패치 내부의 4개 교차점 중 하나로 이동시키는 방법으로 워터마크를 삽입하였다. 이 방법은 회전, 축척 변환이 발생 할 경우 패치를 적용 할 수 없기 때문에 기하 공격에 대하여 취약하다는 단점이 있다. 또한 패치 내부의 포인트 개수가 적어질수록 에러율이 높아지기 때문에 데이터 의존성의 문제도 존재한다.

Marques 외[13]는 이미지 형태의 워터마크를 삽입하기 위하여 벡터 맵의 모든 좌표를 정방행렬로

구성하고 이미지의 픽셀 값을 이용하여 각 좌표에 워터마크를 삽입하고 있다. 이미지 형태의 워터마크를 삽입하기 때문에 소유권을 명확히 파악할 수 있다는 장점이 있다. 그러나 원본 데이터가 필요한 Non-blind 방법이고 기하 공격이 발생하였을 때 원본 데이터와의 매칭이 어려워 검출이 불가능하다.

김정엽·박수홍[9]은 모든 좌표의 최근점 쌍을 이용하고 최근점 쌍 간의 길이에 워터마크를 삽입하는 방법을 제안하였다. 두 좌표 간의 길이는 이동, 회전 공격에 대하여 변하지 않지만 축척 변환이 일어났을 때 변하는 성질을 지니므로 축척 변환에 대하여 검출이 불가능 하다. 또한 단순화 공격과 무작위 노이즈 첨가에 대하여 취약하다.

위에서 살펴본 공간 영역의 워터마킹 연구 외에 변환 영역의 워터마킹 연구에는 Kitamura 외, Li와 Xu, Ohbuchi 외[11, 12, 17] 등이 있다. 이러한 방법은 각각 DFT, DWT 등의 주파수 변환과 Mesh spectrum 영역을 이용하여 변환 계수에 워터마크를 삽입한다. 주파수 변환을 이용한 방법은 특정 공격에 대하여 강인한 대신에 다른 공격의 강인성은 저하된다는 문제점이 있다. 그리고 Ohbuchi 외[17]의 방법은 [16]에서 나타난 Non-blind 방법, 데이터 의존성 등의 단점을 그대로 갖고 있다.

관련 연구들을 종합하여 볼 때, 모든 연구에서 충실도를 만족함을 확인할 수 있다. 그러나 특정 공격에 대하여 강인성이 취약한 연구가 대부분 이었으며 강인성을 만족하더라도 Non-blind 방식이거나 데이터 의존적이라는 문제점들이 존재하였다. 따라서 본 연구에서는 관련연구에서 나타난 문제점들을 보완할 수 있는 강인한 워터마킹 기법을 제안하고자 한다.

## 3. 접근 방법

본 절에서는 워터마킹 기법의 설계를 위한 여섯 가지 접근 방법을 소개하고 각 접근 방법들이 강인성 향상과 보안성 강화에 어떻게 기여하는지 살펴본다.

### 3.1 포인트 기반의 접근

벡터 맵의 모든 버텍스를 중복을 고려하지 않고 워터마킹의 삽입에 사용한다면 삽입 후에 위상관계가 변하는 문제가 발생할 수 있다. 이러한 경우는 두 개의 객체가 동일한 위치의 버텍스를 포함하고, 동일 위치의 두 버텍스에 대하여 서로 다른 계산이 적용 되었을 때 발생한다. 두 개의 라인 객체가 서로 연결되어있는 경우, 두 개의 폴리곤 객체가 서로 인접하여 있는 경우 등이 그 예이다. 이러한 현상은 워터마크를 삽입하기 전에 모든 버텍스 데이터를 포인트 집합으로 구성하고 구성된 포인트들이 서로 중복되지 않도록 중복을 제거하여 해결할 수 있다. 이를 통하여 동일한 위치의 두 버텍스에 대하여 동일한 연산이 적용되므로 위상관계의 변화를 피할 수 있다. 또한 이러한 접근은 포인트, 라인, 폴리곤 등의 모든 벡터 데이터 타입에 대하여 워터마크 삽입이 가능하다는 장점을 갖는다.

### 3.2 최소 둘레 삼각형 구성

최소 둘레 삼각형은 주어진 포인트 집합에서 둘레가 최소가 되는 삼각형을 말한다. 주어진 포인트 집합에서 최소 둘레 삼각형을 구하고, 구해진 세 점을 제외하고 다시 최소 둘레 삼각형을 구하는 것을 반복하여 모든 포인트들에 대하여 삼각형 집합을 구할 수 있다. 최소 둘레 삼각형은 이동, 회전, 축척 변환이 발생하여도 변하지 않고 유지되기 때문에 기하 공격에 대하여 강인한 이점을 제공한다. 또한 좌표가 삽입되거나 삭제되는 버텍스 공격이 발생하여도 발생 지점 주변을 제외한 지역의 삼각형은 변하지 않는다. 즉, 버텍스 공격이 발생하지 않은 지역의 워터마크는 깨지지 않고 살아남을 수 있다. 마지막으로 객체 또는 버텍스의 저장 순서가 변하는 재배열 공격이 발생하여도 최소 둘레 삼각형은 포인트 간의 길이를 이용하여 구성되기 때문에 이와 무관하게 일정하게 유지된다. 따라서 최소 둘레 삼각형을 벡터 맵 워터마킹에 이용함으로써 기하 공격, 버텍스 공격, 재배열 공격에 대한 강인성을 만족할 수 있다. 최소 둘레 삼각형을 구하는 문제는 최근점 쌍을 구하는 문제[3]와 유사하며 이를 변형시킨 방법[14]으로 해결할 수 있다.

### 3.3 길이 비율에 대한 워터마크 삽입

워터마크를 삽입할 수 있는 기하학적 대상으로는 좌표, 길이, 면적, 각도, 길이 비율, 면적 비율 등이 있다. 이러한 기하적인 요소들에 워터마크를 삽입하면 버텍스 공격, 재배열 공격에 대하여 강인성을 만족 할 수 있다. 이것은 버텍스 공격이 일어나지 않은 지역의 기하적인 요소가 변하지 않고, 재배열 공

격이 발생하여도 기하적인 요소에는 영향을 미치지 않기 때문이다. 하지만 몇몇 기하 요소들은 기본적인 기하 공격에 대한 강인성을 만족하지 못한다. 각 요소의 기하 공격에 대한 강인성은 Table 1과 같이 정리할 수 있다.

Table 1. Geometrical features' robustness against geometrical attacks (o: robust, x: fragile)

| | Translation | Rotation | Scaling | RST Transformation |
|---|---|---|---|---|
| Coordinate | x | x | x | x |
| Length | o | o | x | x |
| Area | o | o | x | x |
| Angle | o | o | o | o |
| Ratio of the length | o | o | o | o |
| Ratio of the area | o | o | o | o |

모든 기하 공격에 대하여 강인한 요소는 각도, 길이비율, 면적비율 등이다. 먼저 각도는 세 가지 기하 공격에 대하여 강인성을 모두 만족하지만 각도를 수정하게 되면 실제 좌표에 반영되는 위치의 오차가 커질 우려가 있고 오차를 예측하고 조정하기 어렵다. 또한 본 연구에서는 최소둘레 삼각형을 이용하고자 하므로 면적 비율을 구하여 적용하기가 어렵다. 따라서 본 연구에서는 길이 비율을 워터마크의 삽입 대상으로 선정하였다.

### 3.4 워터마크 이미지의 픽셀 위치를 참조

선행 연구들에서는 순차적인 이진 배열 또는 이미지 형태의 워터마크를 삽입하기 위하여 워터마크의 삽입 순서를 결정하게 된다. 만약에 워터마크의 삽입순서를 단순히 데이터가 저장된 순서대로 한다면 재배열과 같이 저장순서가 바뀌는 공격에 대하여 강인성이 취약해진다. 또한 버텍스 공격으로 인하여 정보량이 변하면 저장 순서 또한 달라지므로 워터마크의 검출이 어려워진다. 이러한 단점을 극복하기 위하여 본 연구에서는 삽입하고자 하는 배열 또는 이미지의 위치를 워터마크에 함께 삽입하고자 한다. 이러한 방법을 사용하면 워터마크를 검출 할 때, 삽입하는 순서와 무관하게 워터마크 이미지를 복원할 수 있다. 결국 검출되는 순서를 고려할 필요가 없으므로 버텍스 공격, 재배열 공격에도 강인해진다.

### 3.5 그룹화

단순화는 라인 또는 폴리곤 데이터에서 객체의 형태를 유지하며 잉여점을 제거하는 과정이다. 단순화를 거치면 정보의 손실이 발생하므로 단순화에 대한 강인성을 만족시키는 것은 어려우며 대부분의 선행 연구에서 단순화 공격에 대한 강인성이 취약한 것을 확인할 수 있다. 가능한 해결 방법으로는 단순화 과정을 거쳐도 삭제되지 않는 기준점에 워터마크를 삽입하는 것이다[15].

폴리곤 데이터에서 각 객체의 시작점은 단순화 과정을 거쳐도 삭제되지 않는 기준점이 될 수 있다. 라인 데이터의 경우에는 객체의 시작점과 끝점이 기준점이 될 수 있다. 이는 Douglas와 Peucker[6], Reumann과 Witkam[19], Opheim[18] 등의 단순화 알고리즘이 단순화 대상의 시작점과 끝점은 삭제하지 않기 때문이다. 또한 의도적으로 폴리곤의 시작점을 변경하지 않는 이상 일반적인 조작에 의하여 시작점이 변경되는 경우는 없다. 따라서 객체의 시작점과 시작점이 아닌 포인트를 따로 분리하여 워터마크를 삽입한다면 단순화 공격에 대하여 강인한 방법이 될 수 있다.

### 3.6 일방함수의 사용

특정 워터마킹 알고리즘이 알려질 경우 해커가 워터마크의 존재 여부를 확인해 보거나 이를 무력화하려는 시도가 있을 수 있다[4]. 이러한 시도를 방지하기 위하여 삽입된 워터마크를 역으로 추적하는 것이 어렵도록 일방함수를 사용하여 워터마킹 기법에 활용할 수 있다[7]. 일방함수란 함수 값의 계산은 가능하지만 역으로 계산할 수 없는 함수를 말한다. 주어진 값을 자연수로 나눈 나머지를 구하는 모듈러 연산의 경우 일방함수의 특성을 지닌다[22]. 본 연구에서는 모듈러 연산을 워터마크 삽입에 사용하여 워터마킹 알고리즘이 알려질 경우에 해커의 역추적을 방지하고자 한다.

## 4. 워터마킹 알고리즘

본 절에서는 워터마크의 삽입, 검출 알고리즘에

대하여 설명한다. 삽입, 검출 알고리즘은 각각 Figure 1, Figure 2의 흐름도로 전체적인 과정을 표현할 수 있으며 상세한 내용은 다음과 같다.

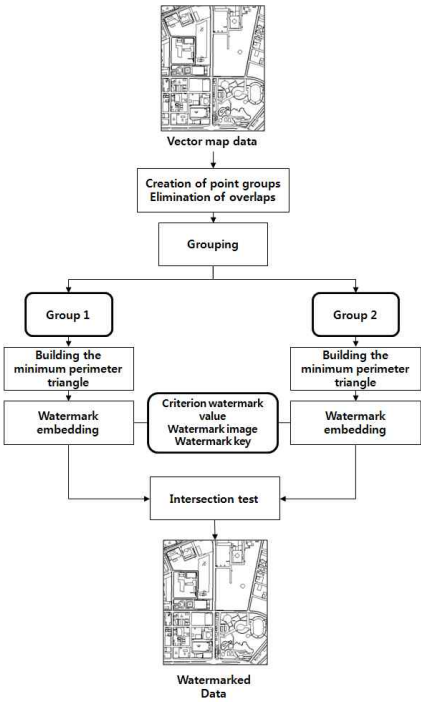



Figure 1. Watermark Embedding Process

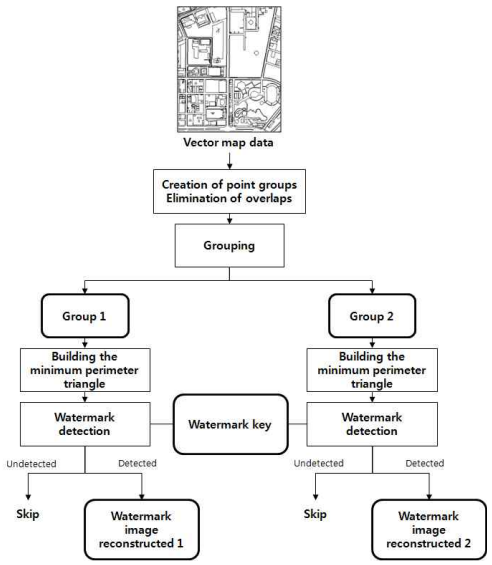



Figure 2. Watermark Detection Process

### 4.1 워터마크 삽입 알고리즘

#### 4.1.1 Step1, 포인트 집합의 생성과 중복 제거

워터마크 삽입의 첫 번째 절차는 벡터 데이터의 모든 버텍스를 포인트 집합으로 구성하는 것이다. 또한 구성된 포인트들의 좌표가 서로 중복되지 않도록 중복 제거를 한다.

#### 4.1.2 Step2, 그룹화

주어진 포인트 집합을 두 그룹으로 나누며 각 그룹은 다음과 같다

① 그룹1 : 폴리곤 데이터의 경우 객체의 시작점들의 포인트 집합, 라인 데이터의 경우 객체의 시작점과 끝점들의 포인트 집합

② 그룹2 : 전체 포인트 집합에서 그룹1을 제외한 포인트 집합

#### 4.1.3 Step3, 최소 둘레 삼각형 구성

두 그룹에 대하여 각각 최소둘레 삼각형 집합을 구성한다. 이 과정은 주어진 포인트 집합에서 최소둘레 삼각형을 구하고 해당 세 점을 제외하고 다시 최소둘레 삼각형을 구하는 방식으로 반복된다.

#### 4.1.4 Step4, 워터마크 값, 이미지, 키 생성

워터마크 삽입에 필요한 기준 워터마크 값, 워터마크 이미지, 워터마크 키를 생성한다. 기준 워터마크 값은 3자리의 자연수로 워터마크가 삽입되었는지 아닌지를 판별하는데 사용된다. 따라서 차후 검출 시에 기준 워터마크 값이 정상적으로 검출된 것들만 워터마크 이미지 복원에 사용한다. 만약 기준 워터마크 값이 2자리 이하의 자연수이면 워터마크가 삽입되지 않았는데 우연히 검출될 확률이 높아진다. 따라서 기준 워터마크 값을 3자리의 자연수로 제한하였다.

워터마크 이미지는 0 또는 1로 이루어진 이진 영상이며 워터마크 값의 길이가 너무 길어지는 것을 방지하기 위하여 행과 열의 크기를 각각 100 미만으로 제한한다. 행과 열의 곱은 (그룹1의 포인트 개수)/3 보다 작도록 제한한다. 제안하는 방법에서는 하나의 삼각형에 하나의 워터마크 비트를 삽입하므로 워터마크 이미지가 그룹1에 완전히 삽입되도록 하기 위하여 워터마크 이미지의 크기가 제한된다.

워터마크 이미지의 행 개수, 열 개수, 기준 워터마크 값을 워터마크 키로 저장한다. 워터마크 키는 파일로 저장되어 추후 워터마크 검출에 사용된다.

#### 4.1.5 Step5, 워터마크 삽입

그룹1, 그룹2에 대하여 각 최소둘레 삼각형 집합에서 둘레가 가장 작은 삼각형부터 순차적으로 워터마크를 삽입한다. 또한 삽입되는 워터마크 이미지

의 픽셀은 좌상단부터 우하단의 순서로 삽입되며 이미지의 모든 픽셀의 삽입이 끝나면 다시 좌상단부터 반복한다. 워터마크의 삽입 대상은 최소둘레 삼각형의 가장 긴 변을 제외한 두 변의 길이 비율이다. 길이 비율의 소수점 둘째자리 이하를 최종 워터마크 값으로 바꾸어 워터마크를 삽입하게 된다. 그 이유는 워터마킹의 충실도와 강인성을 모두 만족시키기 위함이다. 만약 더 낮은 자리에 워터마크를 삽입하면 강인성이 저하되고 더 높은 자리에 삽입하면 충실도가 저하된다.

최종 삽입되는 워터마크 값을 만들기 위하여 먼저 기준 워터마크 값 $wm1$에 대하여 모듈러 연산을 적용한다. 삼각형의 장변을 제외한 두 변 중 단변의 길이를 $d1$, 장변의 길이를 $d2$, 소수점 이하 버림 함수를 $floor()$, 나머지를 구하는 모듈러 연산을 $\mathrm{mod}$, 모듈러 연산이 적용된 새로운 기준 워터마크 값을 $wm1'$이라 하면 $wm1'$을 구하는 과정은 다음과 같다.

$$R = d2/d1 \tag{1}$$

$$x = floor(R * 10) \tag{2}$$

$$Y = f(x) \tag{3}$$

$$wm1' = Y \bmod (wm1) \tag{4}$$

워터마크의 삽입을 $R$의 소수점 둘째 자리 이하에 하기 때문에 $x$는 워터마크가 삽입되어도 변하지 않는 값이다. 따라서 검출 시에 동일한 $wm1'$을 구할 수 있다.

최종적으로 삽입되는 워터마크 값은 $wm1'$과 페이지 번호, 워터마크 이미지의 비트, 워터마크 비트의 열 위치, 행 위치를 연속적으로 붙인 값이다. 이 때, 페이지 번호는 현재 삽입하는 워터마크 이미지가 몇 번째 반복되어 삽입하는지를 의미한다. 최종적인 워터마크 값은 자리수를 고려하여 다음과 같이 표현될 수 있다.

$$Watermark = WWWPBCCRR \tag{5}$$

(WWW= $wm1'$, P= 페이지, B= 비트, CC= 열 위치, RR= 행 위치)

이제 앞서 구한 최종 워터마크 값을 길이 비율 $R$에 삽입한다. $R$의 소수점 둘째 자리 이하를 최종 워터마크 값으로 교체하여 새로운 길이 비율 $R'$을 구한다. 두 변 중 단변의 길이 $d1$을 고정하고 $d2$를 변화시키면 워터마크 삽입 후의 장변의 길이 $d2'$은 다음과 같이 구할 수 있다.

$$d2' = R' * d1 \tag{6}$$

위의 워터마크 삽입 과정은 Figure 3으로 표현할 수 있다.

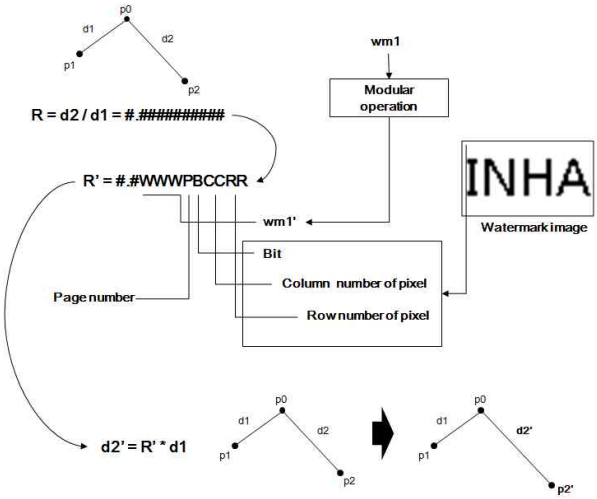



Figure 3. Watermark embedding in the length ratio

워터마크를 삽입 한 후에 장변의 길이 $d2$는 $d2'$으로 변하며 이에 따라 포인트 $p2$는 $p2'$으로 좌표가 변한다. $p2'$의 좌표는 삼각함수를 이용하여 다음과 같이 구할 수 있다.

$$p2'.x = p0.x + d2' * \cos\theta \tag{7}$$

$$p2'.y = p0.y + d2' * \sin\theta \tag{8}$$

4.1.6 Step6, 교차 테스트

워터마크의 삽입이 모두 끝난 후, 위상 관계가 변하였는지 여부를 살펴보기 위하여 교차 테스트를 실시한다. 워터마킹 기법에서 위상관계의 훼손 여부를 살펴보기 위한 교차 테스트는 [7, 10]에서 제안되었다. 이 방법은 벡터 데이터의 모든 선분을 비교하여 교차함, 교차하지 않음, 포함의 세 가지 경우를 구하고 원본 데이터와 워터마크가 삽입된 데이터의 교차 테스트 결과를 비교한다. 본 연구에서는

위의 방법을 사용하여 교차테스트를 수행하며 원본 데이터와 워터마크가 삽입된 데이터의 교차테스트 결과를 비교하여 다르다면 워터마크 삽입을 취소한다.

### 4.2 워터마크 검출 알고리즘

워터마크의 검출 과정은 삽입 과정과 유사하다. 워터마크가 삽입된 벡터 맵에 대하여 삽입 과정의 Step 1, 2, 3의 과정을 동일하게 수행한다. 그 다음 각 삼각형들에 대하여 워터마크를 검출한다. 삽입 과정과 마찬가지로 모듈러 연산을 적용하며, 이때 $wm1$은 키 파일에 저장된 기준 워터마크 값을 사용한다. 각 삼각형의 길이 비율 $R$과 $wm1$으로 식 1~4의 모듈러 연산을 적용하여 $wm1'$을 얻을 수 있다.

다음으로 길이 비율 $R$로부터 워터마크 값을 추출한다.

$$R = \#.\#WWWPBCCRR \tag{9}$$

$$Watermark = WWWPBCCRR \tag{10}$$

(WWW= $wm1^{\circ}$, P= 페이지, B= 비트, CC= 열, RR= 행)

$wm1'$과 $wm1^{\circ}$을 비교하여 다음과 같이 워터마크 이미지를 복원한다.

① ($wm1'$ == $wm1^{\circ}$) 인 경우,
워터마크가 검출됨
페이지, 비트, 열, 행을 이용하여 워터마크 이미지 복원
② ($wm1'$ != $wm1^{\circ}$) 인 경우,
워터마크가 검출되지 않음
건너뜀

### 4.3 검출률

본 연구에서 검출 과정의 결과는 기준 워터마크 값의 검출 여부와 복원된 워터마크 이미지이다. 먼저 검출 여부는 기준 워터마크 값이 검출 되는지에 따라 다음과 같이 검출률을 계산할 수 있다.

$$\text{검출률} = \frac{\text{기준 워터마크 값이 검출된 개수}}{\text{삽입한 워터마크의 개수}} \times 100 \tag{11}$$

복원된 워터마크 이미지는 삽입에서 사용한 원본 워터마크 이미지와 비교할 수 있다. 두 이미지는 이진 영상이므로 비트 에러율(Bit Error Rate)을 계산하여 에러가 발생한 정도를 확인할 수 있다.

$$BER = \frac{\text{발생한 에러 비트의 개수}}{\text{삽입한 워터마크 비트의 개수}} \times 100 \tag{12}$$

## 5. 실험 및 분석

### 5.1 실험 개요

제안된 방법을 검증하기 위하여 1:5000 수치지도를 실험 데이터로 선정하고 입력 효과성, 충실도, 오검출률, 강인성 등에 대하여 평가하였다. 광주 지역의 1:5000 수치지도에서 건물에 해당하는 폴리곤 레이어를 추출하여 실험에 사용하였다. 실험에 사용한 폴리곤 데이터는 객체의 개수가 4859개 이고, TM 중부원점 좌표계를 사용한다. 또한 워터마크 삽입에 사용한 기준 워터마크 값 은 247, 워터마크 이미지는 53*30의 영문 이니셜을 사용하였다. 실험 데이터와 워터마크 이미지는 Figure 4와 같다.

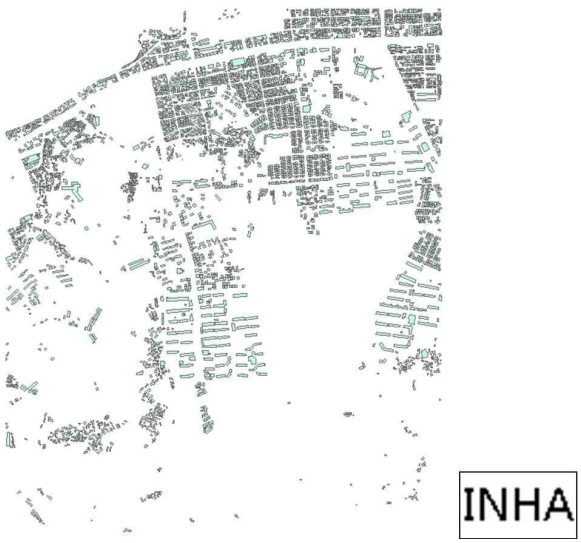



Figure 4. Digital map and watermark image

실험 항목과 내용은 입력 효과성, 충실도, 오검출률, 강인성 등의 워터마크 특성에 의거하여 Table 2와 같이 구성하였다.

### 5.2 실험 결과 및 분석

제안된 방법의 충실도를 살펴보기 위하여 원본 데이터와 워터마크가 삽입된 데이터 사이의 RMSE

Table 2. Experimental conditions

| Characteristics of watermarking | | Experimental conditions |
|---|---|---|
| Embedding effectiveness | | Detect watermark after embedding |
| Fidelity | Error of coordinate | After embedding, Analyze the RMSE between original and watermarked data |
| | Topology | Analyze the result of intersection test |
| False positive rate | | Detecting watermark from the original data |
| Robustness (geometrical attacks) | Translation | Detect watermark after translation in the X-axis direction (1 to 1000m) |
| | Rotation | Detect watermark after rotation (1° to 315°) |
| | Scaling | Detect watermark after scaling (scale factor: 0.8~10) |
| | RST | Detect watermark after translation (10,10), rotation 12°, Scaling 0.9 |
| Robustness (vertex attacks) | Vertex Add/Del | Detect watermark after adding and deleting objects randomly |
| | Cropping | Detect watermark after cropping (remaining data: 85%, 50%, 35%) |
| | Simplification | Detect watermark after simplification using Douglas-Peucker (threshold: 1~5m) |
| Robustness (reordering attacks) | Object reordering | Detect watermark after reordering the objects randomly |
| | Vertex reordering | Detect watermark after reordering the vertices reversely |
| Robustness (noise attacks) | Format-dxf | Detect watermark after shp-to-dxf-to-shp conversion |
| | Format-Geodatabase | Detect watermark after shp-to-ESRI geodatabase-to-shp conversion |
| | Noise | Detect watermark after adding random noise |

(Root Mean Square Error)를 구하여 삽입 후 어느 정도의 거리 오차가 발생하였는지 살펴보았다 (Table 3). 그 결과 RMSE = 0.1253m로 나타났고, 1:5000 수치지도의 허용오차인 3.50m(국립지리원, 1988) 보다 작은 것을 확인하였다. 또한 오차 거리의 최대값도 0.8740m로 허용오차 보다 작았다. 따라서 제안하는 방법은 위치 오차 측면에서 충실도를 만족한다.

다음으로 위상 측면의 충실도를 살펴보면, 교차테스트를 수행한 후에 위상관계가 변하는 경우가 발생하지 않아 워터마크의 삽입에도 위상관계가 그대로 유지됨을 확인하였다. 만약 위상관계가 변하는 경우가 발생한다면 해당 부분의 워터마크 삽입이 취소될 것이다.

Table 3. Error of coordinate after watermark embedding

| Error of coordinate (Fidelity) | Value(m) |
|---|---|
| RMSE X-axis | 0.0906 |
| RMSE Y-axis | 0.0866 |
| RMSE | 0.1253 |
| Maximum distance error | 0.8740 |

제안된 방법의 입력 효과성, 오검출률, 강인성에 대한 실험 결과는 Table 4와 같다.

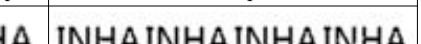
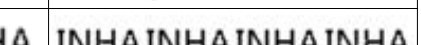
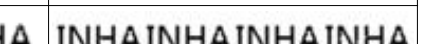
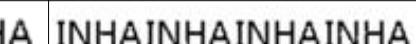
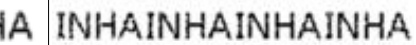
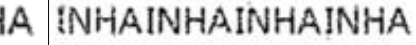
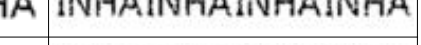
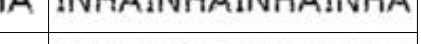
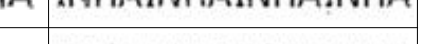
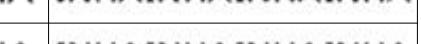
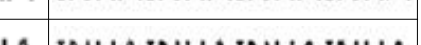
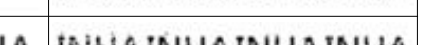
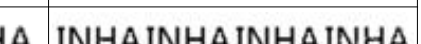
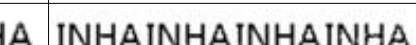
입력 효과성 실험에서 그룹1의 검출률과 그룹2의 검출률이 각각 97.16%, 98.72%로 높은 검출률을 보인다. 삽입한 워터마크가 100% 검출되지 않는 이유는 워터마크 삽입 후 좌표의 변화로 인해 검출 시에 구성되는 최소둘레 삼각형 들이 변하기 때문이다. 그러나 97% 이상의 데이터는 최소둘레 삼각형이 유지되므로 워터마크가 정상적으로 검출되었다고 볼 수 있다. BER 또한 0.31%, 0.12%로 매우 낮게 나왔으며 복원된 워터마크 이미지도 육안으로 식별하는데 문제가 없다. 따라서 제안하는 방법은 입력 효과성을 만족한다.

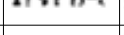
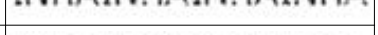
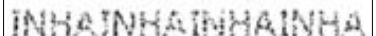
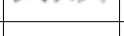
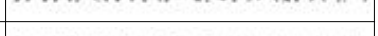
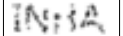
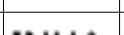
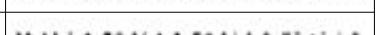
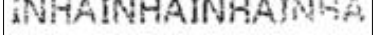
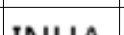
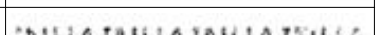
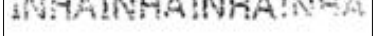
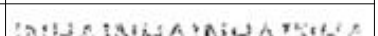
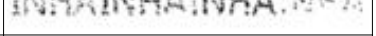
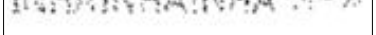
오검출률의 실험에서 검출률이 0.2% 이내로 나타났고 BER이 16%이상으로 나타났다. 검출률이 매우 낮으므로 원본 데이터에서 워터마크가 정상적으로 검출되었다고 보기 어렵다. 또한 기준 워터마크 값이 검출되지 않으면 해당 픽셀의 워터마크 이미지를 복원하지 않으므로 워터마크 이미지의 대부분의 픽셀이 0의 값을 갖는다. 위의 결과로 볼 때, 연구된 방법은 오검출률을 만족한다.

기하 공격에 대한 강인성 실험에서 검출률은 그룹1, 그룹2 모두 97% 이상으로 높게 나왔다. BER의 경우 회전 공격에 대하여 2%가 넘어가기도 하는데 복원된 이미지를 육안으로 식별하는데 무리는 없다. 제안하는 방법은 기하 공격에 대하여 강인함을 보였다.

버텍스 공격에 대한 강인성 실험에서 객체의 추가/삭제 공격에 대하여 90% 이상의 높은 검출률을 보인다. 객체가 더 많이 추가/삭제 될수록 검출률은

Table 4. Experimental results on embedding effectiveness, false positive rate, and robustness

| | | Detection rate(%) | | BER(%) | | Watermark image reconstructed | |
|---|---|---|---|---|---|---|---|
| | | Group1 | Group2 | Group1 | Group2 | Group1 | Group2 |
| Embedding effectiveness | | 97.16 | 98.72 | 0.31 | 0.12 |  |  |
| False positive rate | | 0.18 | 0.20 | 16.44 | 17.73 | | |
| Robustness – geometrical attacks | Translation 1m | 97.16 | 98.72 | 0.31 | 0.12 |  |  |
| | Translation 10m | 97.16 | 98.72 | 0.31 | 0.12 |  |  |
| | Translation 100m | 97.16 | 98.72 | 0.31 | 0.12 |  |  |
| | Translation 1000m | 97.16 | 98.72 | 0.31 | 0.12 |  |  |
| | Rotation 1° | 97.10 | 98.77 | 1.24 | 1.75 |  |  |
| | Rotation 15° | 97.16 | 98.77 | 1.67 | 2.45 |  |  |
| | Rotation 90° | 97.16 | 98.65 | 0.31 | 0.13 |  |  |
| | Rotation 120° | 97.16 | 98.78 | 1.42 | 2.37 |  |  |
| | Rotation 180° | 97.16 | 98.72 | 0.31 | 0.12 |  |  |
| | Rotation 240° | 97.16 | 98.72 | 1.48 | 2.18 |  |  |
| | Rotation 315° | 97.16 | 98.78 | 1.24 | 2.07 |  |  |
| | Scaling 0.8 | 96.85 | 98.67 | 1.24 | 1.80 |  |  |
| | Scaling 1.1 | 97.16 | 98.75 | 0.74 | 1.13 |  |  |
| | Scaling 2 | 97.16 | 98.78 | 0.31 | 0.12 |  |  |
| | Scaling 10 | 97.16 | 98.78 | 1.05 | 1.18 |  |  |
| | RST | 97.16 | 98.47 | 1.55 | 2.68 |  |  |
| Robustness – vertex attacks | Vertex Adding 10 | 96.72 | 98.53 | 0.31 | 0.17 |  |  |
| | Vertex Adding 50 | 96.92 | 98.15 | 0.37 | 0.27 |  |  |
| | Vertex Adding 100 | 95.43 | 98.13 | 0.37 | 0.33 |  |  |
| | Vertex Deleting 10 | 96.11 | 98.10 | 0.43 | 0.20 |  |  |
| | Vertex Deleting 50 | 94.81 | 96.85 | 0.56 | 0.40 |  |  |
| | Vertex Deleting 100 | 91.97 | 95.03 | 0.80 | 0.82 |  |  |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Robustness – vertex attacks | Cropping 85% | 80.96 | 83.70 | 1.92 | 2.75 |  |  |
| | Cropping 50% | 45.80 | 49.60 | 7.29 | 9.00 |  |  |
| | Cropping 35% | 32.63 | 35.53 | 9.70 | 11.32 |  |  |
| | Simplification 1m | 97.46 | 86.55 | 0.31 | 2.25 |  |  |
| | Simplification 2m | 97.16 | 62.23 | 0.31 | 6.67 |  |  |
| | Simplification 3m | 97.16 | 49.97 | 0.31 | 8.58 |  |  |
| | Simplification 4m | 97.16 | 40.10 | 0.31 | 10.52 |  |  |
| | Simplification 5m | 97.16 | 29.17 | 0.31 | 12.45 |  |  |
| Robustness – reordering attacks | Object reordering | 97.16 | 98.72 | 0.31 | 0.12 |  |  |
| | Vertex reordering | 97.16 | 98.72 | 0.31 | 0.12 |  |  |
| Robustness – noise attacks | Format - dxf | 97.16 | 98.47 | 3.83 | 6.20 |  |  |
| | Format - Geodatabase | 97.16 | 98.47 | 1.98 | 3.35 |  |  |
| | Noise (-1, 1) | 0.12 | 0.22 | 16.44 | 17.80 | | |
| | Noise (-0.1, 0.1) | 0.56 | 0.12 | 16.50 | 17.77 | | |
| | Noise (-0.01, 0.01) | 2.35 | 1.08 | 16.63 | 17.92 | |  |
| | Noise (-0.001, 0.001) | 18.79 | 10.27 | 16.81 | 18.57 |  |  |
| | Noise (-0.0001, 0.0001) | 76.58 | 58.72 | 20.09 | 23.28 |  |  |

낮아지겠지만, 추가/삭제가 일어나지 않은 부분의 최소둘레 삼각형은 동일하게 유지되기 때문에 정상적으로 검출이 된다.

잘라내기 공격에 대해서는 전체 데이터양의 85%, 50%, 35% 가 남아있을 때, 그룹2의 검출률이 각각 83%, 49%, 35%로 나타났다. 즉, 워터마크가 삽입된 데이터양에 비례하여 비슷한 검출률이 나타나고 있다. 복원된 이미지를 살펴보면 전체 데이터양의 35%가 남아있을 때까지는 어느 정도 육안으로 식별이 가능하다.

단순화 공격은 임계치를 크게 둘수록 단순화의 정도가 심해지고 좌표의 삭제가 많이 발생한다. 실험결과에서는 임계치가 커질수록 그룹2의 검출률이 낮아지고 BER은 높아진다. 그러나 그룹1의 검출률은 변함없이 90%이상으로 높게 유지되고 BER 또한 0.31로 낮게 유지된다. 따라서 단순화 공격에 대하여 그룹1의 검출률과 BER은 영향을 받지 않는다.

직접적인 데이터의 손실이 발생하는 버텍스 공격에 대하여 제안하는 방법은 대체로 강인함을 보인다. 데이터의 양이 절반 이상 줄어드는 경우에도 남아있는 데이터에 대해서는 모두 검출이 되고 복원된 이미지도 육안으로 식별이 가능하다. 특히 단순화 공격에 대하여 데이터의 손실이 발생하여도 그룹1의 검출률을 높게 유지시킨다.

재배열 공격에 대하여 객체 재배열, 버텍스 재배열 모두 높은 검출률을 보이고 BER 또한 낮은 것으로 나타났다. 따라서 제안된 방법은 재배열 공격에 대하여 강인함을 보인다.

파일 포맷 변환에 대하여 dxf 포맷, ESRI의

Geodatabase 모두 높은 검출률을 보이고 BER 또한 낮은 것으로 나타났다. 따라서 제안된 방법은 파일 포맷 변환에 대하여 강인함을 보인다. 무작위 노이즈가 첨가된 경우 검출률이 낮게 나타났다. 그러나 노이즈의 진폭이 감소함에 따라 검출률이 높아지고 있으며 진폭이 (-0.0001~0.0001) 인 경우에 그룹1과 그룹2의 검출률이 76%, 58%로 나타났다. BER을 살펴보면 기준 워터마크 값의 검출과 상관없이 복원이 불가능한 것으로 나타났다. 노이즈 공격에 대하여 이미지가 복원되려면 더욱 낮은 진폭의 노이즈가 첨가되어야 할 것이다.

### 5.3 방법론 평가

실험 결과를 토대로 본 연구의 방법론을 워터마킹의 특성에 의거하여 평가하고 관련 연구들과 비교하였다(Table 6).

제안된 방법론은 원본 데이터가 필요 없는 Blind 방식이며 충실도 측면에서 맵의 허용오차를 만족하고 위상관계가 고려되었다. 또한 노이즈 공격을 제외한 모든 공격에 대하여 강인성을 만족한다. 데이터 의존성 측면에서도 데이터양에 무관하게 높은 검출률을 보인다는 장점을 가진다.

제안된 방법론을 관련 연구들과 비교하여 보면, 관련 연구들 중에는 원본 사용여부, 강인성, 충실도,

Table 5. Primary characteristics and relative importance of vector map watermarking

| relative importance | Characteristics | Details |
|---|---|---|
| 1 | Fidelity | Error of coordinate<br>Shape and topology |
| 2 | Robustness | RST Transformation<br>Adding and deleting object<br>Simplification<br>File format conversion |
| 3 | Embedding effectiveness | |
| 4 | False positive rate | |

Table 6. Comparison of our methodology with related research

| Domain | Research | Blind/Non-blind | Robustness | | | | | | | | | | Fidelity | | Data dependency |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Geometrical attacks | | | Vertex attacks | | | Reordering attacks | | Noise attacks | | | | |
| | | | Translation | Rotation | Scaling | Add/Del Object | Cropping | Simplification | Object reordering | Vertex reordering | Format conversion | Random noise | Error of coordinate | Topology | |
| Spatial | Ohbuchi, R. 2002 [16] | N | o | o | o | o | o | o | o | o | o | o | o | x | √ |
| | Voigt, M. 2003 [23] | B | x | x | x | o | o | o | o | o | o | o | o | x | √ |
| | Schulz, G. 2004 [20] | B | o | x | x | - | o | o | o | o | o | o | o | x | √ |
| | Marques, D. A. 2007 [13] | N | x | x | x | o | o | x | o | o | o | o | o | x | |
| | Kim, J. Y. 2009 [9] | B | o | o | x | o | o | x | o | o | o | x | o | o | |
| Transform | Kitamura, I. 2001 [11] | N | x | x | x | o | x | x | o | o | o | o | o | x | |
| | Li, Y. 2003 [12] | B | o | o | o | x | x | x | x | x | o | o | o | x | |
| | Ohbuchi, R. 2003 [17] | N | o | o | o | o | o | o | o | o | o | o | o | x | √ |
| Spatial | Proposed method | B | o | o | o | o | o | o | o | o | o | x | o | o | |

* Blind/Non-blind (B/N), Robustness (o: robust, x: fragile, -: not mentioned), Fidelity (o: satisfy, x: not satisfy), Data dependency (√: dependent)

데이터 의존성에 대하여 모두 뛰어난 방법이 존재하지 않는 반면에, 제안된 방법에서 이를 만족하고 있다. 물론 무작위 노이즈 첨가에 대하여 취약하지만 노이즈 첨가는 다른 공격에 비하여 상대적으로 중요도가 낮다고 할 수 있다. 즉, 제안된 방법론은 상대적으로 중요도가 낮은 노이즈 첨가에 취약하지만 이를 제외한 중요한 특성들에 대하여 강인하다. 벡터 맵 워터마킹에서 중요도가 높은 조작들은 RST 변환, 객체의 추가/삭제, 단순화, 파일 포맷 변환 등이며(Table 5) 이러한 공격들은 실제로 빈번하게 발생되기 때문에 이 중에 하나라도 강인성이 취약하면 일반적인 방법으로 사용하기 어렵다. 제안된 방법은 이에 대해 모두 강인성을 만족한다.

관련 연구들과의 또 다른 차이점은 제안된 방법론은 단순화 공격에 대하여 높은 검출률을 유지한다는 점이다. 단순화 공격에 대하여 강인성을 만족하는 관련 연구들도 단순화의 정도가 심해질 경우에는 강인성이 저하되는 단점을 갖는다. 특히 도로 데이터와 같이 곡선부가 많은 데이터에서는 단순화 과정을 거치면 많은 양의 데이터가 삭제된다. 그러나 제안된 방법에서는 객체의 시작점을 따로 그룹으로 구성하여 워터마크를 삽입하기 때문에 강인성을 유지할 수 있다.

## 6. 결 론

본 연구에서는 워터마킹 기법의 설계를 위하여 여섯 가지 접근 방법을 고안하였으며, 이를 사용하여 강인한 워터마킹 기법을 설계하였다. 본 연구의 방법론은 충실도, 입력 효과성, 오검출률 등의 특성을 만족하고 강인성 측면에서 노이즈 첨가를 제외한 모든 공격에서 강인함을 보였다. 관련 연구들은 RST 변환, 객체의 추가/삭제, 단순화 등의 중요하고 빈번하게 발생하는 조작에 대하여 강인성이 취약한 반면 제안된 방법은 이에 대해 모두 강인성이 뛰어남을 보였다. 또한 제안 방법론은 원본 데이터가 필요 없는 Blind 방식이며 데이터 의존적이지 않은 장점을 갖는다. 마지막으로 본 연구에서는 단순화 공격에 대하여 단순화 정도가 심해짐에 따라 강인성이 저하되는 선행 연구의 문제점을 해결하였다.

제안 방법은 무작위 노이즈 첨가에는 취약한 것으로 나타났다. 그러나 해커가 고의적으로 무작위 노이즈를 첨가하면 맵의 유효성이 저하되므로 실제로 발생되기 어렵다[15]. 또한 무작위 노이즈에 강인한 기법이 되려면 다른 공격에 대한 강인성이 저하되거나 데이터 의존적인 문제가 발생하기 때문에 모든 공격에 대하여 강인한 방법은 아직 존재하지 않는다.

본 연구에서는 이미지 형태의 워터마크를 삽입하여 검출 시에 소유권을 더욱 명확히 확인 할 수 있도록 하였다. 대부분의 관련 연구에서는 비트 배열 또는 정수 형태의 워터마크를 삽입하며 이러한 방법은 워터마크를 명확히 판단하고 소유권을 인정하기 어렵다. 본 연구의 방법은 검출 시에 이미지 형태의 워터마크를 복원하여 소유권을 명확히 판단할 수 있게 한다.

본 연구의 방법론은 실험에서 사용한 수치지도뿐만 아니라 포인트, 라인, 폴리곤 형태로 이루어진 모든 벡터 데이터의 소유권 보호를 위해 사용 될 수 있으며 이를 통하여 벡터 맵 데이터의 불법 복제를 방지할 수 있는 주요한 방법이 될 것으로 기대된다.

## References

[1] Burdescu, D. D; Stanescu, L; Mihaescu, M. C. 2010, Two Spatial Watermarking Techniques for Digital Images, Advanced Techniques in Multimedia Watermarking : Image, Video and Audio Applications, p. 1-20, IGI Global.

[2] Chang, H. H; Chen, T; Kan K. S. 2003, Watermarking 2D/3D Graphics for Copyright Protection, Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing, 4:720-723.

[3] Cormen T. H; Leiserson C. E; Rivest, R. L; Stein, C. 2001, Introduction to Algorithms, Second Edition, p. 957-961, MIT Press and McGraw-Hill.

[4] Cox, I. J; Miller, M. L; Bloom, J. A. 2000, Watermarking applications and their properties, Proc. of International Conference on Information Technology: Coding and Computing, 6-10.

[5] Cox. I. J; Miller, M. L; Bloom, J. A; Fridrich, J; Kalker, T. 2008, Digital Watermarking and Steganography, Morgan Kaufmann.

[6] Douglas D; Peucker T. 1973, Algorithms for the reduction of the number of points required to represent a digitized line or its caricature, Cartographica: The International Journal for Geographic Information and Geovisualization, 10(2):112-122.

[7] Kim, J. Y. 2008, Digital Watermarking for 2D Vector Map Data in Spatial Domain, Doctor's thesis, Inha University.

[8] Kim, J. Y; Park, S. H. 2007, Vector Map Data Watermarking Method using Binary Notation, The Journal of GIS Association of Korea, 15(4):385-395.

[9] Kim, J. Y; Park, S. H. 2009, A Blind Vector Digital Watermarking for GIS using the Closest Pair of Points, KISE: Information Network, 36(6):536-544.

[10] Kim, J. Y; Park, S. H. 2009, Digital Watermarking of 2D Vector Map Data for the Accuracy and Topology of the Data, The Journal of GIS Association of Korea, 17(1):51-66.

[11] Kitamura, I; Kanai, S; Kishinami, T. 2001, Copyright Protection of Vector Map using Digital Watermarking Method based on Discrete Fourier Transform, Proc. of IEEE 2001 International Symposium on Geoscience and Remote Sensing, 3:9-13.

[12] Li, Y; Xu, L. 2003, A Blind Watermarking of Vector Graphics Images, Proc. of International Conference on Computational Intelligence and Multimedia Applications, 27-30.

[13] Marques, D. A; Magalhaes, K. M; Dahab, R. 2007, RAWVec-A Method for Watermarking Vector Maps, in SBSeg 2007: Symposium on Information and Computer Systems Security.

[14] Negruseri, C. 2009, Google Code Jam 2009 World Finals Problem B. Min Perimeter, Accessed February 28. http://code.google.com/codejam/contest/dashboard?c=311101#s=a&a=1

[15] Niu, X. M; Shao, C; Wang, X. 2006, A Survey of digital vector map watermarking, International Journal of Innovative Computing, Information and Control, 2(6):1301-1316.

[16] Ohbuchi R; Ueda, H; Endoh, S. 2002, Robust watermarking of vector digiral maps, Proc. of the International Conference on Multimedia and Expo, 1:577-580.

[17] Ohbuchi R; Ueda, H; Endoh, S. 2003, Watermarking 2D Vector Maps in the Mesh-Spectral Domain, Proc. of the Shape Modeling International 2003, 216-228.

[18] Opheim, H. 1982, Fast Data Reduction of a Digitized Curve, Geo-Processing, 2:33-40.

[19] Reumann, K; Witkam, A. P. M. 1974, Optimizing curve segmentation in computer graphics, Proc. of International Computing Symposium, North-Holland Publishing Company, 467-472.

[20] Schulz, G; Voigt, M. 2004, A high capacity watermarking system for digital maps, Proc. of the 2004 workshop on Multimedia and Security, 180-186.

[21] Sequeira, A; Kundur, D. 2001, Communications and information theory in watermarking: A survey, Proc. of SPIE Multimedia Systems and Application IV, 4518:216-227.

[22] Singh, S. 2009, The Code Book, p. 250-255, Younglim Cardinal.

[23] Voigt, M; Busch, C. 2003, Feature based watermarking of 2D-Vector Data, Proc. of SPIE Security and Watermarking of Multimedia Content, 5020:359-366.

논문접수 : 2012.11.15
수 정 일 : 1차 2013.03.04 / 2차 2013.05.14
심사완료 : 2013.06.10