

	(19) 대한민국특허청(KR) (12) 공개특허공보(A)	(11) 공개번호 10-2013-0025980 (43) 공개일자 2013년03월13일
(51) 국제특허분류(Int. Cl.) G06F 21/24 (2006.01) G06F 19/00 (2011.01) (21) 출원번호 10-2010-0129086 (22) 출원일자 2010년12월16일 심사청구일자 2010년12월16일		(71) 출원인 부경대학교 산학협력단 부산광역시 남구 신선로 365 (용당동, 부경대학교) (72) 발명자 권기룡 부산광역시 해운대구 센텀중앙로 142, 더샵센텀파 크 206동 403호 (재송동) 이석환 경상남도 김해시 삼계동 구지마을3단지푸르지오아 파트 2차 312동 501호 (뒷면에 계속) (74) 대리인 이수찬, 채종길, 박갑록

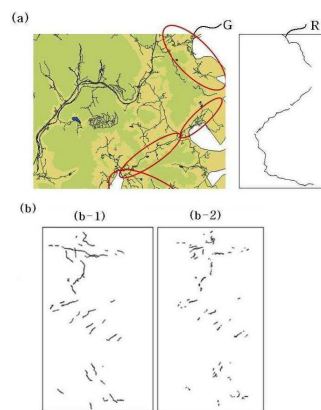
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 **지리정보관독장치 및 지리정보시스템의 벡터 맵 데이터 암호화 방법**

(57) 요약

(a) 지리정보관독장치의 서버에 접속된 데이터베이스에서 폴리라인 및 폴리곤 속성의 레이어로 구분된 지리정보를 로드하는 단계, (b) 상기 (a) 단계에서 추출된 상기 레이어에 최소 코딩 속성(MCA_ minimum Coding Attribute)을 설정하는 단계, (c) 상기 (b) 단계에서 상기 레이어의 정수부 좌표값 및 소수부 좌표값의 분리 및 압축하는 단계, (d) 상기 (c) 단계에서 추출된 상기 정수부 좌표값을 최소 경계 사각형(MBR) 레이어의 범위에 따라 위치성을 암호화하는 단계, (e) 상기 (d) 단계에서 암호화된 정수부 좌표값과 상기 (c) 추출된 상기 소수부의 좌표값 레이어의 매개변수를 재배열함과 동시에 상기 매개변수의 방향성을 암호화하는 단계 및 (f) 상기 (e) 단계의 매개변수를 엔트로피 코더에 의해 압축하는 단계를 포함하는 지리정보관독장치 및 지리정보시스템의 벡터 맵 데이터 암호화 방법이 개시된다. 상기와 같이 지리정보시스템에서 추출된 정보를 암호화하기 때문에 불법으로 지리정보가 복제되거나 유통되는 것을 방지하고 비인가자가 데이터에 접근하는 것을 제한할 수 있다.

대표도 - 도2



(72) 발명자

이춘옥

경상남도 창원시 마산합포구 월영동11길 57, 해오
름아파트 102동 302호 (해운동)

장봉주

부산광역시 수영구 연수로342번길 17-4, 201호 (광
안동, 금부드림빌)

성택영

부산광역시 연제구 금련로 48-11 (연산동)

이 발명을 지원한 국가연구개발사업

과제고유번호 M-03-2008-0702200520

부처명 지식경제부

연구사업명 지역혁신인력양성사업

연구과제명 GIS 콘텐츠의 불법유통 방지 및 사용자 접근제어를 위한 통합 GIS 보안 솔루션 개발

주관기관 부경대학교

연구기간 2008.08.01 ~ 2011.04.30

특허청구의 범위

청구항 1

- (a) 지리정보관독장치의 서버에 접속된 데이터베이스에서 폴리라인 및 폴리곤 속성의 레이어로 구분된 지리정보를 로드하는 단계,
- (b) 상기 (a) 단계에서 추출된 상기 레이어에 최소 코딩 속성(MCA_minimum Coding Attribute)을 설정하는 단계,
- (c) 상기 (b) 단계에서 설정된 상기 레이어의 정수부 좌표값 및 소수부 좌표값의 분리 및 압축하는 단계,
- (d) 상기 (c) 단계에서 추출된 상기 정수부 좌표값을 최소 경계 사각형(MBR) 레이어의 범위에 따라 위치성을 암호화하는 단계,
- (e) 상기 (d) 단계에서 암호화된 정수부 좌표값과 상기 (c) 추출된 상기 소수부의 좌표값 레이어의 매개변수를 재배열함과 동시에 상기 매개변수의 방향성을 암호화하는 단계 및
- (f) 상기 (e) 단계의 매개변수를 엔트로피 코더에 의해 압축하는 단계,
- 를 포함하는 지리정보시스템의 벡터 맵 데이터 암호화 방법.

청구항 2

제1항에 있어서,

상기 (d) 단계는,

- (i) 상기 최소 경계 사각형 좌표값을 암호화하는 제1 암호화키의 길이의 절반을 2의 승수로 사용하여 수평 및 수직 방향으로 블록을 생성하는 단계,
- (ii) 상기 블록 및 상기 (b) 단계 과정에서 생성된 상기 속성의 중심좌표가 속하는 좌표블록 레이블(DCp)을 생성하는 단계 및
- (iii) 상기 좌표블록 레이블을 암호화하며, 상기 좌표블록 레이블의 각 속성 위치를 상기 최소 경계 사각형 좌표값 범위 내에서 임의의 좌표값으로 변경하는 단계를 구비하는 것을 특징으로 하는 벡터 맵 데이터 암호화 방법.

청구항 3

제2항에 있어서,

상기 (i) 단계에서 생성된 상기 블록은 수직 및 수평 방향으로 0부터 $2^{Mz}-1$ 의 레이블(Lable)을 가지는 것을 특징으로 하는 벡터 맵 데이터 암호화 방법.

청구항 4

제2항에 있어서,

상기 (ii) 단계에서, 상기 좌표블록 레이블은 상기 중심좌표를 각 좌표값의 변화량으로 나눈 값으로 구해지는 것을 특징으로 하는 벡터 맵 데이터 암호화 방법.

청구항 5

제2항에 있어서,

상기 (iii) 단계에서, 상기 임의의 좌표값은, 상기 제1 암호화키의 길이의 비트열인 메시지k를 통해 상기 제1 암호화키의 길이가 증가함에 따라 홀수 비트열과 짝수 비트열로 분리된 값인 것을 특징으로 하는 벡터 맵 데이터 암호화 방법.

청구항 6

제5항에 있어서,

상기 메시지k는 상기 제1 암호화키의 길이가 증가함에 따라 한 비트씩 순환하는 것을 특징으로 하는 벡터 맵 데이터 암호화 방법.

청구항 7

제1항에 있어서,

상기 (e) 단계의 상기 매개변수는 방향성을 저장하는 부호집합으로 구성되며, 상기 부호집합은 x, y 좌표의 부호값이 나열된 이진 비트열인 것을 특징으로 하는 벡터 맵 데이터 암호화 방법.

청구항 8

제1항 내지 제7항 중 어느 한 항에 있어서,

상기 매개변수는, 상기 부호집합과 임의의 좌표값으로 구성되는 제2 암호화키로 암호화되는 것을 특징으로 하는 벡터 맵 데이터 암호화 방법.

청구항 9

제8항에 있어서,

상기 제2 암호화키는 상기 제1 암호화키에서 생성되는 것을 특징으로 하는 벡터 맵 데이터 암호화 방법.

청구항 10

지리정보시스템의 데이터 베이스에서 벡터 맵 데이터를 로드하는 맵로드부,

상기 맵로드부에서 로드된 벡터 맵 데이터를 폴리라인 및 폴리곤 속성의 레이어를 추출하는 추출부,

상기 레이어에 최소 코딩 속성을 설정하는 설정부,

상기 레이어의 정수부 좌표값 및 소수부 좌표값으로 분리하는 정수부 블록 및 소수부 블록 및 상기 정수부 좌표값의 위치성을 암호화 하는 제1 암호설정부를 구비하는 분리부, 및

상기 정수부 좌표값 및 소수부 좌표값의 매개변수의 방향성을 암호화하는 제2 암호설정부를 구비하며, 상기 매개변수를 재배열하는 정렬부를 포함하는 지리정보관독장치.

청구항 11

제10항에 있어서,

상기 정수부 블록 및 상기 소수부 블록은 상기 정수부 및 소수부 좌표값을 압축하는 압축설정부를 포함하는 것을 특징으로 하는 지리정보관독장치.

명세서

기술 분야

- [0001] 본 발명은 지리정보관독장치 및 지리정보시스템의 벡터 맵 데이터 암호화 방법에 관한 것으로, 보다 자세하게는 지리정보시스템(GIS_ Geographic Information System)에서 관독되는 GIS 벡터 맵 데이터를 압축하는 과정에서 GIS 벡터 맵 데이터를 암호화함으로써, 지리정보시스템을 사용하는 사용자 이외의 비인가자가 지리정보를 관독하거나 불법으로 유통되는 것을 방지하는 지리정보관독장치 및 지리정보시스템의 벡터 맵 데이터 암호화 방법에 관한 것이다.

배경 기술

- [0002] 최근, 네트워크, 휴대 인터넷, 개인용 멀티미디어 단말기 등의 발전과 함께 상기 기기들을 이용하여 지리정보시스템(GIS)의 사용이 증가하고 있다. 상기 지리정보시스템은 토지관련분야, 시설물관리분야, 교통분야 및 국방정보시스템 등의 여러 분야에서 시설 및 환경 등을 관리하기 위해 사용되며, 최근에 들어서는 실생활 공간을 모델링하고자 하는 요구에 따라 지리정보시스템의 중요성이 증가하고 있다.
- [0003] 하지만, 상기 지리정보시스템의 수요성에 비하여 실제 사용자는 필요한 지리정보를 단시간에 전송 및 저장하는데 불편함이 있었다. 예를 들어 지리정보시스템에서 관독된 지형의 위치나 거리 등은 벡터 맵으로 구성되어 있고, 이와 같이 구성된 정보는 그 양이 방대하기 때문에 이를 전송 받기 위한 시간이나 저장될 공간 등이 충분히 확보되어야 한다. 이와 같은 문제점을 위해 관독된 지리정보를 위치, 방향 등의 조건으로 분리하고, 분리된 정보를 압축하여 정보를 저장하기 위한 저장공간이나 전송 받는 시간을 줄여 사용자의 편의성을 향상시켰다.
- [0004] 그러나 상기와 같이 압축 저장된 지리정보시스템을 이용하여 악용하는 사례도 증가하고 있다. 즉, 지리정보시스템에서 관독된 정보를 비인가자가 임의로 저장하고, 저장된 정보를 불법으로 유통하기도 한다. 유통된 정보는 불법으로 복제되거나 또 다른 비인가자가 데이터에 접근하여 정보의 재산권이 노출된다. 더불어 유통된 정보가 국가기밀시설, 기밀지형 등의 정보인 경우, 유통된 정보에 의하여 국제적인 범죄로 확대될 수도 있다.
- [0005] 따라서, 대용량의 지리정보를 압축함과 동시에 지리정보의 불법다운 및 저장을 방지할 수 있는 지리정보의 암호화가 요구되고 있다.

발명의 내용

해결하려는 과제

- [0006] 본 발명의 실시예에 따르면, 지리정보 벡터 맵 데이터를 압축하는 과정에서 벡터 맵 데이터에 암호를 설정하여 지리정보의 불법적 유통을 방지하는 지리정보관독장치 및 지리정보시스템의 벡터 맵 데이터 암호화 방법이 제공된다.
- [0007] 또한, 본 발명의 실시예에 따르면, 지리정보 벡터 맵 데이터를 방향, 위치 등에 따라 선택적으로 암호화함으로써, 대용량의 지리정보 벡터 맵 데이터를 보다 간단하게 암호화할 수 있는 지리정보관독장치 및 지리정보시스템의 벡터 맵 데이터 암호화 방법이 제공된다.

과제의 해결 수단

- [0008] 본 발명의 실시예에 따른 지리정보관독장치 및 지리정보시스템의 벡터 맵 데이터 암호화 방법은 (a) 지리정보관독장치의 서버에 접속된 데이터베이스에서 폴리라인 및 폴리곤 속성의 레이어로 구분된 지리정보를 로드하는 단계, (b) 상기 (a) 단계에서 추출된 상기 레이어에 최소 코딩 속성(MCA_ minimum Coding Attribute)을 설정하는 단계, (c) 상기 (b) 단계에서 상기 레이어의 정수부 좌표값 및 소수부 좌표값의 분리 및 압축하는 단계, (d) 상기 (c) 단계에서 추출된 상기 정수부 좌표값을 최소 경계 사각형(MBR) 레이어의 범위에 따라 위치성을 암호화하는 단계, (e) 상기 (d) 단계에서 암호화된 정수부 좌표값과 상기 (c) 추출된 상기 소수부의 좌표값 레이어의 매개변수를 재배열함과 동시에 상기 매개변수의 방향성을 암호화하는 단계 및 (f) 상기 (e) 단계의 매개변수를 엔

트로피 코더에 의해 압축하는 단계를 포함한다.

- [0009] 상기와 같이 지리정보시스템에서 추출된 정보를 암호화하기 때문에 불법으로 지리정보가 복제되거나 유통되는 것을 방지하고 비인가자가 데이터에 접근하는 것을 제한할 수 있다.
- [0010] 이때, 상기 (d) 단계는, (i) 상기 최소 경계 사각형 좌표값을 암호화하는 제1 암호화키의 길이의 절반을 2의 승수로 사용하여 수평 및 수직 방향으로 블록을 생성하는 단계, (ii) 상기 블록 및 상기 (b) 단계 과정에서 생성된 상기 속성의 중심좌표가 속하는 좌표블록 레이블(DCp)을 생성하는 단계 및 (iii) 상기 좌표블록 레이블을 암호화하며, 상기 좌표블록의 레이블의 각 속성 위치를 상기 최소 경계 사각형 좌표값 범위 내에서 임의의 좌표값으로 변경하는 단계를 구비한다.
- [0011] 상기와 같이 정수부 좌표값 레이어를 블록화하고, 블록을 형성하는 최소 경계 사각형 좌표값 내에서 좌표블록 레이블을 암호화함으로써, 필요한 정보를 선택적으로 암호화할 수 있다. 또한, 최소 경계 사각형 좌표값 범위 내에서 좌표값을 변경하기 때문에 지도 내 속성들의 구성을 변경시켜 보다 안전한 암호화가 이뤄질 수 있다.
- [0012] 한편, 상기 (i) 단계에서 생성된 블록은 수직 및 수평 방향으로 0부터 $2^{N/2}-1$ 의 레이블(Lable)을 가진다. 상기 레이블은 데이터베이스에서 로드된 위치 정보를 데이터 관리자의 암호화 과정이 보다 용이하도록 임의로 구획되는 영역이라고 할 수 있다. 상기와 같이 로드된 위치정보를 구획함에 따라 필요한 레이블을 선택하여 암호화할 수 있으며, 데이터 관리자는 암호화 영역을 블록화하기 때문에 영역의 혼돈을 최소화하여 암호화 과정을 수행할 수 있다.
- [0013] 또한, 상기 (ii) 단계의 좌표블록 레이블은 중심 좌표를 각 좌표값의 변화량으로 나눈 값으로 구해질 수 있다. 이때, 각 좌표값의 변화량은 최소 경계 사각형 좌표값의 최대 길이 및 최소 길의 차이에서 제1 암호화키의 길이의 절반을 2의 승수로 나눈 값으로 구해지며, 최소 경계 사각형 좌표값의 범위에 따라 변경될 수 있기 때문에 각 위치 정보에서 서로 다른 좌표블록 레이블이 구현되기 때문에 데이터 관리자 이외의 비인가의 데이터 접근에 권한제어가 강화될 수 있다.
- [0014] 더불어, (iii) 단계에서, 임의의 좌표값은, 제1 암호화키의 길이의 비트열인 메시지k를 통해 제1 암호화키의 길이가 증가함에 따라 홀수 비트열과 짝수 비트열로 분리된 값이라고 할 수 있다. 이와 같이 좌표블록 레이블을 좌표화하고, 이를 홀수 비트열과 짝수 비트열로 분리된 값을 사용함으로써, 좌표블록 레이블의 암호를 중복됨 없이 사용할 수 있게 하며, 이를 통해 암호의 안전성을 향상시킬 수 있다.
- [0015] 상기와 같은 단계를 통해 정수부 좌표값을 선택적으로 암호화할 수 있으며, 정수부 좌표값을 암호화함으로써, 지도 내 속성들의 위치를 암호화할 수 있게 된다.
- [0016] 상기 메시지k는 제1 암호화키의 길이가 증가함에 따라 한 비트씩 순환할 수 있다. 이와 같이 메시지k를 한 비트씩 순환함에 따라 제1 암호화키의 중복성을 최소화시켜 보다 안전한 암호화를 수행할 수 있다.
- [0017] 한편, 상기 (e) 단계의 소수부의 좌표값 레이어는 방향성을 저장하는 부호집합으로 구성되며, 부호집합은 x, y 좌표의 부호값이 나열된 이진 비트열이 될 수 있다.
- [0018] 상기와 같이 구성된 소수부 좌표값 레이어는, 부호집합과 임의의 좌표값으로 구성되는 제2 암호화키로 암호화될 수 있다. 이때, 제2 암호화키는 제1 암호화키에서 생성되지만, 암호화하는 방법에 의하여 절삭되거나 반복됨으로써 길이가 제2 암호화키의 길이가 달라질 수 있다.
- [0019] 한편, 본 발명의 실시예에 따른 지리정보관독장치는 지리정보시스템의 데이터 베이스에서 벡터 맵 데이터를 로드하는 맵로드부, 상기 맵로드부에서 로드된 벡터 맵 데이터를 폴리라인 및 폴리곤 속성의 레이어를 추출하며, 추출된 레이어를 선택 추출하는 추출부, 상기 레이어에 최소 코딩 속성을 설정하는 설정부, 상기 레이어의 정수부 좌표값 및 소수부 좌표값으로 분리하는 정수부 블록 및 소수부 블록 및 상기 정수부 좌표값의 위치성을 암호화 하는 제1 암호설정부를 구비하는 분리부, 및 상기 정수부 좌표값 및 소수부 좌표값의 매개변수의 방향성을 암호화하는 제2 암호설정부를 구비하며, 상기 매개변수를 재배열하는 정렬부를 포함한다.
- [0020] 상기와 같은 구성에 의하여 지리정보관독장치에서 로드된 지리정보를 선택적으로 암호화할 수 있으며, 그로 인하여 데이터관리자 이외의 비인가자가 데이터를 불법으로 열람하거나 다운 및 저장하는 권한을 제어하여 정보의 안전성이 향상될 수 있다.
- [0021] 한편, 상기 정수부 블록 및 소수부 블록은 정수 및 소수부 좌표값을 압축하는 압축설정부를 포함하여 지리정보의 용량을 줄여 데이터 관리자의 정보관리를 보다 용이하게 할 수 있다.

발명의 효과

- [0022] 본 발명에 따르면, 대용량의 지리정보 벡터 맵 데이터를 압축하는 과정에서 벡터 맵 데이터 중 위치 정보와 방향 정보를 암호화하여 비인가자가 판독된 지리정보를 판독하거나 저장하는 것을 방지한다.
- [0023] 또한, 본 발명에 따르면, 지리정보시스템에서 판독된 지리정보 벡터 맵 데이터 중 선택된 정보만을 암호화함에 따라 대용량의 지리정보를 암호화하는 번거로움을 줄이고, 보다 간단하게 벡터 맵 데이터를 암호화한다.
- [0024] 더불어, 본 발명에 따르면, 지리정보시스템에서 판독된 지리정보 벡터 맵 데이터의 홀수, 짝수 비트열이 다르게 구성되고, 구성된 비트열이 순환하며 암호화되기 때문에 지리정보 벡터 맵 데이터가 중복되어 암호화되는 것을 방지하고, 지리정보 벡터 맵 데이터 암호화의 안정성이 향상될 수 있다.

도면의 간단한 설명

- [0025] 도 1은 본 발명의 실시예에 따른 블록도이다.
- 도 2는 본 발명의 실시예에 따른 실험 실시예를 도시한 도면이다.
- 도 3은 본 발명의 실시예에 따른 순서도이다.
- 도 4는 본 발명의 암호화기에 따른 위치 및 기호 암호화를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0026] 이하, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있을 정도로 상세히 설명하기 위하여, 본 발명의 가장 바람직한 실시예를 첨부한 도면을 참조하여 상세하게 설명한다. 또한, 본 발명을 설명하는데 있어서 동일 부분은 동일 부호를 붙이고, 그 반복 설명은 생략한다.
- [0027] 도 1은 본 발명의 실시예에 따른 블록도이고, 도 2는 본 발명의 실시예에 따른 실험 실시예를 도시한 도면이다.
- [0028] 도면을 설명하기에 앞서, 본 발명의 지리정보판독장치(GIS)는 철도, 하천 도로, 지형 등의 지형지물의 특성을 판독하는 장치라고 할 수 있다. 상기 지리정보판독장치는 각 지형지물의 특성을 데이터로 전송 받고, 전송 받은 데이터의 특성에 따라 여러 개의 레이어(layer)들로 구성되며, 각 레이어는 점, 선, 면, 문자의 4 가지 특성으로 표현되는 예를 들어 설명하기로 하지만 예시되는 지리정보판독장치에 의하여 본 발명이 제한되는 것은 아니다.
- [0029] 상기 지리정보판독장치(10)를 보다 자세하게 살펴보면, 지리정보판독장치(10)는 맵로드부(120), 추출부(130), 설정부(140), 분리부(150) 및 정렬부(180)를 포함한다.
- [0030] 상기 맵로드부(120)는 지리정보판독장치(10)의 데이터베이스에 저장된 지리정보 벡터 맵 데이터를 판독하고, 추출부(130)은 판독된 지리정보 벡터 맵 데이터 중에서 레이어를 선택 및 추출한다.
- [0031] 이때, 맵로드부(120)에서 판독하는 지리정보 벡터 맵 데이터는 속성(attribute)에 따라 여러 레이어로 구분된 파일이며, 상기 속성은, 라인(line), 폴리라인(polyline), 폴리곤(polygon), 문자 등으로 구분된다.
- [0032] 또한, 추출부(130)는 상기 라인, 폴리라인, 폴리곤, 문자 중 적어도 어느 하나의 속성을 선택하고 추출할 수 있으며, 이하 본 발명의 실시예는 설명의 편의상, 폴리라인과 폴리곤의 속성을 가지는 레이어의 압축, 암호화된 정보를 선택 추출하는 예를 들어 설명하기로 한다.
- [0033] 상기 추출부(130)에서 레이어를 추출 및 선택하면, 설정부(140)는 추출된 레이어에 최소 코딩 속성(MCA_Minimum Coding Attribute)을 설정한다. 즉, 각 레이어에 포함된 속성의 수만큼 최소 코딩 속성이 생성되고, 설정된 최소 코딩 속성은 레이어를 압축할 수 있는 압축 단위가 될 수 있다.
- [0034] 한편, 분리부(150)는 최소 코딩 속성이 설정된 레이어의 정수부 좌표값 및 소수부 좌표값을 분리한다. 분리된 정수부 좌표값 및 소수부 좌표값은 정수부블록(160) 및 소수부블록(170)을 통해 분리되고, 분리된 정수부 좌표값의 위치성은 제1 암호설정부(165)를 통해 암호화될 수 있다.
- [0035] 상기 제1 암호설정부(165)는 폴리라인 또는 폴리곤 속성 중에서 정수부 좌표값의 위치성을 암호화한다. 이와 같

이 정수부 좌표값의 위치성을 암호화함에 따라 데이터 관리자 이외의 비인가자가 추출된 데이터의 위치를 파악하는 것을 방지할 수 있다.

[0036] 한편, 정수부블록(160)과 소수부블록(170)은 정수부 및 소수부 좌표값을 압축할 수 있다. 이와 같이 정수부 및 소수부 좌표값을 압축함으로써, 방대한 용량의 지리정보를 간략화하고, 이를 통해 데이터를 저장하기 위한 저장 공간과, 데이터를 전송 받는 전송 시간 등의 관리가 보다 용이해질 수 있다. 이때, 정수부 및 소수부 좌표값을 나누어 압축하면, 각 좌표 데이터가 나타내는 값의 엔트로피가 최대화되어 압축의 효율이 향상될 수 있다.

[0037] 한편, 분리된 정수부 좌표값은 공간영역에서의 에너지 집중(SEC_ Spatial Energy Compaction)이 수행되고, 특히 2-스텝(step)에서 SHP 형식의 에너지 집중이 수행될 수 있다.

[0038] 상기 SHP 형식의 레이어 파일은 x 좌표와 y 좌표를 축으로 하는 레이어의 MBR(minimum bounding rectangle) 좌표와, 각 레이어 내의 속성이 갖는 MBR 좌표를 포함한다. 상기 MBR 은 최소 경계 사각형을 의미하며, MBR은 가장 작은 값을 갖는 x, y 축의 좌표값과 가장 큰 값을 갖는 x, y축의 좌표값으로 이루어진다.

[0039] 상기와 같이 레이어가 정수부 및 소수부 좌표값으로 분리되고, 상기 정수부 좌표값의 위치성을 암호화하면, 정렬부(180)에서 정수부와 소수부 좌표값의 매개변수를 재배열한다. 이때, 정렬부(180)는 제2 암호설정부(185)를 통하여 매개변수를 암호화할 수 있다. 이와 같이 매개변수를 암호화함에 따라 관독된 지리정보의 암호성을 향상시켜 외부로의 유출을 방지한다.

[0040] 제2 암호설정부(185)에 대해 보다 자세하게 살펴보면, 제2 암호설정부(185)는 재배열된 매개변수의 방향성을 암호화할 수 있다. 여기서, 제2 암호설정부(185)는 정수부와 소수부 좌표값의 매개변수인 실제 벡터 맵 데이터의 방향성에 암호를 설정하여 비인가자가 데이터를 저장하거나 다운, 불법 유출하는 것을 방지할 수 있다.

[0041] 한편, 본 발명의 제1 및 제2 암호설정부(185)에서 정수부 좌표값과 매개변수를 암호화하는 암호화 함수는 간단한 비트간 XOR연산, AES, DES 및 ARIA 등 여러 스트림 및 블록기반 암호화 기법을 호환하여 사용할 수 있으며, 암호화 기법에 따라 본 발명이 제한되는 것은 아니다.

[0042] 데이터의 방향성을 암호화하면 매개변수의 엔트로피를 코딩하여, 관리자의 저장매체에 저장될 수 있다.

[0043] 상기의 지리정보관독장치(10)를 이용하여 관독된 지형과 지형에서 추출된 레이어는 도 2의 (a)에 표시되어 있으며, 관독된 지형이 암호화된 레이어는 도 2의 (b)에 표시되어 있다.

[0044] 우선, 지리정보관독장치(10)에서 관독된 지형(G)은 레이어(R)로 추출된다. 추출된 레이어는 주로 등고선, 하천, 강, 도로 등이 될 수 있으며, 본 발명에서는 선으로 표현된 예를 들기로 한다.

[0045] 레이어가 추출되면, 레이어의 방향성과 위치성을 암호화할 수 있다. 레이어의 방향성을 암호화한 것은 (b-1)에 도시되어 있고, 방향성을 암호화한 것은 (b-2)에 도시되어 있다.

[0046] 상기와 같이 추출된 레이어의 위치성과 방향성을 암호화함으로써, 원본 레이어를 관독할 수 없도록 하여 지도정보 데이터 관리자 이외의 비인가자가 전송 받거나 저장하는 것을 방지하여 지리정보 데이터의 안정성을 향상시킨다.

[0047] 이하 도면을 참조하여 벡터 맵 데이터의 암호화 과정에 대해 보다 자세하게 살펴보기로 한다.

[0048] 도 3은 본 발명의 실시예에 따른 순서도이고, 도 4는 본 발명의 암호화기에 따른 위치 및 기호 암호화에 따른 도면이다.

[0049] 도면을 참고하면, 지리정보관독장치(10)의 서버에 접속된 데이터베이스에서 폴리라인 및 폴리곤 속성의 레이어로 구분된 지리정보를 관독할 수 있다(S210).

[0050] 상기 지리정보는 지리정보관독장치(10)에서 관독하는 속성에 따라 여러 레이어로 구분된 파일이라고 할 수 있으며, 속성은 일 예로, 라인(line), 폴리라인(polyline), 폴리곤(polygon), 문자 등이라고 할 수 있다. 이러한 지리정보 중에서 폴리라인 및 폴리곤 속성을 갖는 M개의 레이어 $L = \{l_0, l_1, l_2, \dots, l_{M-1}\}$ 가 선택될 수 있다.

[0051] 한편, 선택된 레이어는 최소 코딩 속성(MCA_ Minimum Coding Attribute)이 설정될 수 있다(S220). 이때, 각 레이어에는 포함된 속성 $l_m = \{P_0, P_1, P_2, \dots, P_{N-1}\}$ 의 수 N만큼의 MCA가 설정되고, 생성된 각각의 속성

$P_n = \{V_0, V_1, V_2, \dots, V_{I-1}\}$ 에 대해서는 추후에 독립적으로 코딩이 수행된다.

[0052] 상기 레이어에 최소 코딩 속성이 설정되면, 레이어는 정수부 좌표값 및 소수부 좌표값으로 분리된다(S230). 이때, 하기 (식 1)에 의해 레이어를 64비트 부동소수점으로 표현된 각각의 속성을 구성하는 모든 좌표값을 정수부(integer portion) $P_{Zn} = \{Z_0, Z_1, Z_2, \dots, Z_{I-1}\}$ 및 소수부(decimal portion) $P_{Rn} = \{R_0, R_1, R_2, \dots, R_{I-1}\}$ 로 분리하게 된다.

[0053]
$$Z_i = \text{floor}(V_i)$$

$$R_i = (V_i - Z_i) \cdot 10^c, (0 < i \leq I-1) \quad (\text{식 1})$$

[0054] (식 1)에서, c는 소수점 밑수 정밀도이며, (식 1)의 첫 번째 수학적식은 벡터 좌표 집합에서 정수부를 분리하기 위한 것이고, 두 번째 수학적식은 소수부를 정수화하기 위한 것이다.

[0055] 만약, 64비트의 부동소수점으로 표현된 좌표 데이터가 나타내는 값이 정수부와 소수부 좌표값으로 분리하지 않고 바로 압축되면, 각각의 좌표 데이터가 나타내는 값의 엔트로피를 최소화하는 것이 곤란하여 압축 효율이 저하된다. 따라서, 본 발명의 실시예에서는 압축 효율을 향상시키기 위하여 좌표 데이터는 정수부와 실수부 좌표값으로 분리되고, 정수부 좌표값에 대해서는 공간영역에서의 에너지 집중(SEC: Spatial Energy Compaction)이 수행되고, 소수부 좌표값에 대해서는 다양한 정밀도로 계층적 압축이 수행된다.

[0056] 레이어를 정수부 및 소수부 좌표값으로 분리하면, 추출된 정수부 좌표값을 암호화한다(S240). 이때, 정수부 좌표값의 속성은 벡터 맵 데이터의 위치성을 구성하고 있으며, 상기 정수 좌표값을 암호화함으로써, 지리정보 벡터 맵 데이터 내 속성을 변경시켜 지리정보의 안정성이 향상된다.

[0057] 한편, 정수부 좌표값을 암호화하기 위하여, 정수부 좌표값의 최소 경계 사각형(MBR: minimum bounding rectangle)을 설정하고, 설정된 최소 경계 사각형 좌표값을 암호화하기 위하여 제1 암호화키의 길이의 절반을 2의 승수로 사용하여 수평 및 수직 방향으로 블록을 생성할 수 있다(S242). 상기 최소 경계 사각형은 x 좌표와 y 좌표를 축으로 표현되는 레이어의 최소 경계 사각형 좌표를 의미한다.

[0058] 보다 자세하게 살펴보면, 상기 블록(160, 170)은 수직 및 수평 방향으로 0부터 $2^{M/2}-1$ (식 2)의 레이블(Label)로 구성된다. 즉, 도 3와 (식 2)를 참고하면, 최소 경계 사각형을 설정하기 위하여 제1 암호화키를 1바이트인 8비트로 사용하였고, 상기 8비트는 제1 암호화키의 길이이며, (식 2)의 N값에 대응된다. 설정된 제1 암호화키로 인하여 블록은 $2^{8/2} = 16$ 이 될 수 있기 때문에 가로 16블록, 세로 16 블록의 구간으로 최소 경계 사각형의 전체 구간을 나눌 수 있다.

[0059] 상기과 같이 블록(160, 170)이 생성되면, 좌표블록 레이블(DCp)를 생성한다(S244). 상기 좌표블록 레이블은 압축된 정수부 및 소수부 좌표값의 중심좌표라고 할 수 있다. 이때, 좌표블록 레이블은 하기의 (식 3)에 도시된 바와 같이 좌표값이 될 수 있으며, 좌표값은 중심좌표를 각 좌표값의 변화량(Δ_{row} , Δ_{col})으로 나눈값으로 구해질 수 있다.

[0060]
$$DC_{P_n}(x) = \lfloor m_{P_n}(x) / \Delta_{row} \rfloor$$

$$DC_{P_n}(y) = \lfloor m_{P_n}(y) / \Delta_{col} \rfloor \quad (\text{식 3})$$

[0061] 이때, 각 좌표값의 변화량은 다음의 (식 4)을 통해 구해질 수 있다. 보다 자세히 살펴보면, B_{max} 은 블록의 최대 길이가 될 수 있으며, B_{min} 은 블록의 최소 길이라고 할 수 있다. 블록의 최대 길이와 최소 길이가 구해지면, 최소 경계 사각형 좌표값의 최대 길이 및 최소 길의 차이에서 제1 암호화키의 길이의 절반을 2의 승수로 나눈 값으로 좌표값의 변화량을 구한다. 여기서, 좌표값의 변화량은 최소 경계 사각형 좌표값의 범위에 따라 변경될 수 있고, 범위에 따라 서로 다른 좌표블록 레이블이 구현될 수 있다.

[0062]
$$\Delta_{row} = \frac{B_{max}(x) - B_{min}(x)}{2^{M/2}}$$

$$\Delta_{col} = \frac{B_{max}(y) - B_{min}(y)}{2^{M/2}} \quad (\text{식 4})$$

[0063] 상기과 같이 좌표블록 레이블을 생성하면, 생성된 좌표블록 레이블을 암호화하고, 좌표블록 레이블의 각 속성 위치를 최소 경계 사각형 좌표값 범위 내에서 임의의 좌표값으로 변경한다(S246). 임의의 좌표값

$(\overline{DC_{P_n}(x)}, \overline{DC_{P_n}(y)})$)은 하기 (식 5)를 통해 변경될 수 있다.

$$\begin{aligned} \overline{DC_{P_n}(x)} &= C_A(DC_{P_n}(x), k_{row}) \\ \overline{DC_{P_n}(y)} &= C_A(DC_{P_n}(y), k_{column}) \end{aligned} \quad (\text{식 5})$$

상기 (식 5)를 살펴보면, 메시지 $k(k_{row}, k_{column})$ 는 제1 암호화키의 길이가 증가함에 따라 홀수 비트열과 짝수 비트열로 분리되는 값이다. 보다 자세하게, k_{col} 과 k_{row} 는 최소 경계 사각형 좌표값을 암호화하는 제1 암호화키의 길이(n)의 홀수 비트열과 짝수 비트열을 의미하고, 홀수 비트열과 짝수 비트열은 다음과 같다.

$$k(n) = \begin{cases} k(n-1) \ll 1+1, & \text{if } < MSB \text{ of } k(n-1) \text{ is } 1 \\ k(n-1) \ll 1, & \text{otherwise} \end{cases} \quad (\text{식 6})$$

상기 (식 6)에 의해 메시지 k 는 제1 암호화키에 의해 홀수 비트열과 짝수 비트열로 분리되고, 한 비트씩 순환될 수 있다. 메시지 k 가 홀수 비트열과 짝수 비트열로 분리되고, 한 비트씩 순환함에 따라 중복성을 최소화하며 제1 암호화키를 암호화할 수 있다. 이로 인하여 보다 안정적으로 정수부 좌표값의 암호화가 수행된다.

상기와 같이 정수부 좌표값의 위치성을 암호화하면, 암호화된 정수부 좌표값과 정수부 좌표값과 분리된 소수부 좌표값 레이어의 매개변수를 재배열함과 동시에 매개변수의 방향성을 암호화할 수 있다(S250).

상기 매개변수는 방향성을 저장하는 부호집합이라고 할 수 있으며, 부호집합은 x, y 좌표의 부호값이 나열된 이진 비트열이 될 수 있다. 즉, 도 3의 (b)에 도시된 바와 같이 최소 경계 사각형의 매개변수의 각 속성들은 x 또는 y좌표의 부호값과 방향성을 포함한다.

이러한 매개변수의 방향성을 암호화하기 위하여 매개변수를 좌표값으로 분리하고, 재배열한다. (식 7)을 참고하면, 배열된 매개변수 좌표값($\overline{S_{P_n}}$)은, 부호집합(S_{P_n})과 제2 암호화키($k_s(n)$)가 배열되어 구현된다. 여기서, 제2 암호화키는 정수부 좌표값을 암호화한 제1 암호화키에 의해 생성되며, 암호화 과정 중에 절삭되거나 반복됨으로써 길이가 달라질 수 있기 때문에 제1 암호화키와 구별된다.

$$\overline{S_{P_n}} = C_B(S_{P_n}, k_s(n)) \quad (\text{식 7})$$

상기와 같이 지리정보의 벡터 맵 데이터의 방향성 및 위치성을 암호화하여 지리정보 데이터를 관리하는 관리자와의 비인가자가 지리정보 데이터를 불법으로 전송받거나 저장하는 것을 방지한다. 또한, 지리정보 데이터가 암호화됨에 따라 불법으로 유통되는 것을 방지할 수 있다.

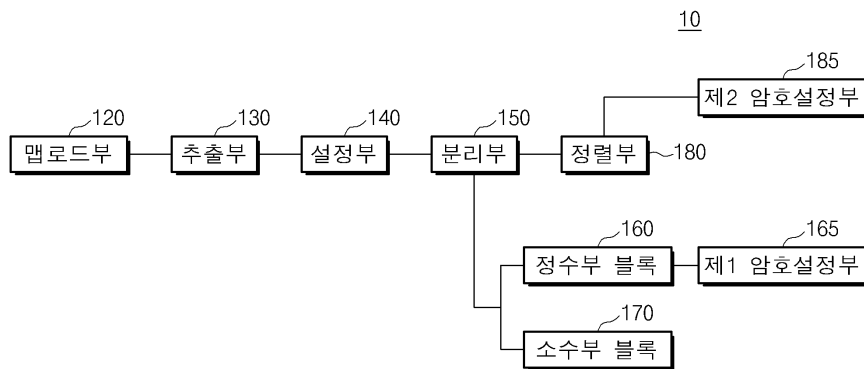
이상, 본 발명자에 의해서 이루어진 발명을 상기 실시예에 따라 구체적으로 설명하였지만, 본 발명은 상기 실시예에 한정되는 것은 아니고, 그 요지를 이탈하지 않는 범위에서 여러 가지로 변경 가능한 것은 물론이다.

부호의 설명

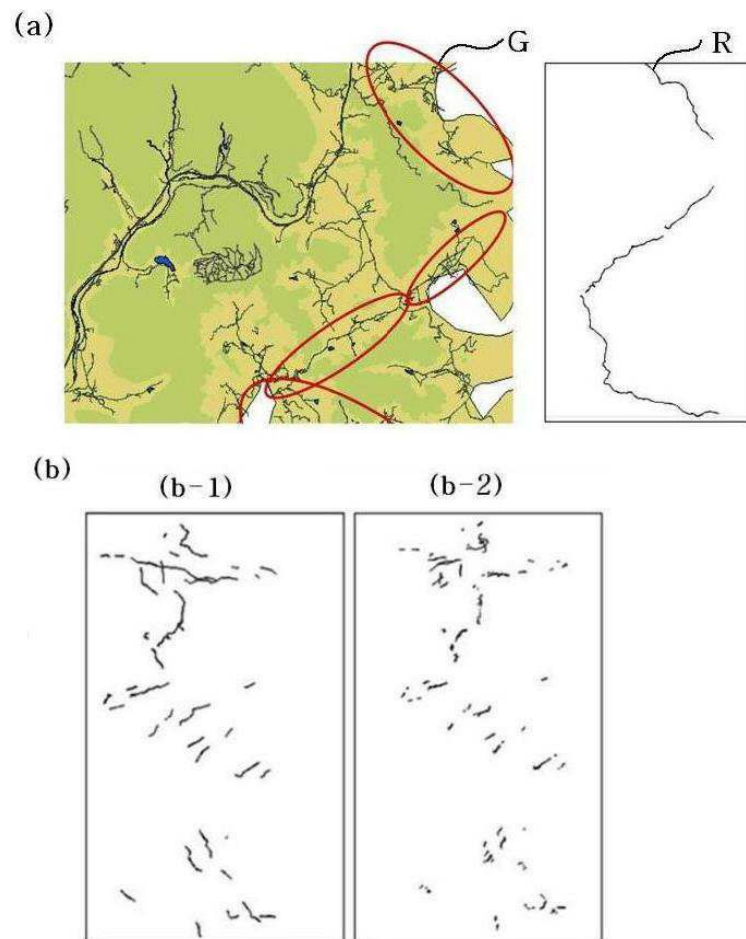
10: 지리정보관독장치	120: 맵로드부
130: 추출부	140: 설정부
150: 분리부	160: 정수부블록
135: 제1 암호설정부	170: 소수부블록
180: 정렬부	185: 제2 암호설정부

도면

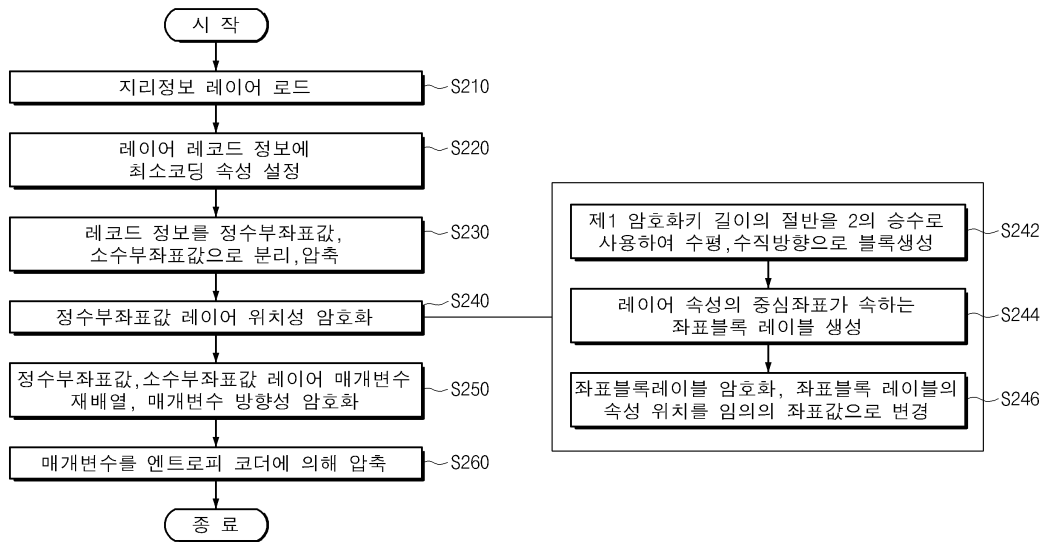
도면1



도면2



도면3



도면4

