논문 2011-48CI-5-12

GIS 벡터맵의 콘텐츠 기반 선택적 암호화 기술

(Contents Based Partial Encryption of GIS Vector Map)

장 봉 주*, 이 석 환**, 문 광 석***, 권 기 룡****

(Bong-Joo Jang, Suk-Hwan Lee, Kwang-Seok Moon, and Ki-Ryong Kwon)

요 약

최근 대용량의 지리정보시스템(geographic information system, GIS) DB 보안 중요성이 부각됨에 따라 GIS 네트워크 보안 및 데이터 암호화 기법에 대해 많은 연구가 진행되어 왔다. 그러나 이와 같은 기법들은 GIS 벡터맵 데이터에 대한 원천적인 불법 복제 및 유통에 취약하다. 본 논문에서는 GIS 벡터맵 데이터의 불법 복제 방지 및 권한제어를 위하여 GIS 벡터맵 압축 영역 상에서 레이어 단위의 선택적 암호화 기법을 제안한다. 제안한 기법에서는 벡터공간 상에서 벡터맵 압축 과정에서 생성되는 최소부호단위(minimum coding attribute, MCA)의 중점좌표와 방향 파라미터들에 대한 선택적 암호화를 각각 수행한다. 첫 번째 선택적 암호화에서는 MCA 레코드의 중점좌표 위치를 임의치환 함으로써 위치 암호화를 수행한다. 두 번째 선택적 암호화에서는 각 레코드 내의 좌표값들에 대한 방향 정보를 암호화함으로써 지형의 형태를 변화시키는 방향성 암호화를 수행한다. 실험 결과로부터 제안한 벡터맵 데이터 암호화 기법이 낮은 계산복잡도와 대용량 벡터맵 데이터를 효과적으로 암호화할 수 있음을 확인하였으며, 또한 제안 기법이 AES, DES 등의 일반적인 데이터 암호화 기법을 사용하는 콘텐츠 암호화 기술들에서 발생되는 압축효율의 저하를 최소화할 수 있음을 확인하였다.

Abstract

Recently, according as the importance of GIS(geography information system) database security is embossed, much researches had been achieved about GIS network security. But most such researches are weak against sourceful illegal reproductions and distributions of GIS vector data map. In this paper, we proposed an efficient layer unit contents based partial encryption technique in the vector map compression domain to prevent illegal distributions and unauthorized accesses. This method achieves a partial encryption about each central coordinate and directional parameters of a MCA(minimum coding attribute) that is created at the vector map compression processing in the vector space. First, the position encryption is applied as permutating randomly the center coordinate of each record that is minimum unit of vector map shape. And second, the direction encryption that changing shapes of vector map topography is applied as encrypting the direction of vertices's coordinates of each record. In experimental results, we confirmed that our proposed method can encipher the large volumed vector map data effectively in low computational complexity. Also, we could minimize the decline of compression efficiency that occurred by conventional contents based encryption schemes using AES or DES algorithms.

Keywords : 벡터맵(Vector Map), 선택적 암호화(Partial Encryption), GIS 보안(GIS security)

* 학생회원, **** 정회원-교신저자, 부경대학교 정보보호협동과정
(Interdisciplinary Program of Information Security, Pukyong National University)
** 정회원, 동명대학교 정보보호학과
(Department of Information Security, TongMyong University)
*** 정회원, 부경대학교 전자공학과
(Department of Electronic Engineering, Pukyong National University)
※ 이 논문은 2011년도 교육과학기술부의 재원으로 한국연구재단의 일반연구자지원사업 (2011-0010902) 및 한국산업기술진흥원의 지역혁신인력양성사업(1345-136-198) 의 지원을 받아 수행된 것임.
접수일자: 2011년 4월26일, 수정완료일: 2011년9월1일

Ⅰ. 서 론

GIS는 지리와 관련된 일괄의 정보를 수집 및 처리하여 관련 분야에서 사용할 수 있도록 하는 시스템을 일컫는 것으로서, 지리·공간적으로 참조가능한 모든 형태의 정보를 효과적으로 수집, 저장, 갱신, 조정, 분석 및 표현할 수 있도록 설계된 컴퓨터의 하드웨어와 소프트웨어 및 지리적 자료, 인적자원의 통합체를 의미한다. 이와 같은 GIS의 개념은 기존의 토지 관련 분야, 시설물 관리 분야, 교통 및 도시 계획/관리 분야뿐만 아니라, 첨단장비를 이용한 해양, 운송, 국방 등 대부분의 정보 산업에서 필수 요소가 되었을 만큼 그 중요성이 부각되었다. 이에 우리나라에서는 국가 GIS 구축 사업이 성공적으로 추진됨으로써 공공부문은 물론 민간 서비스 부문까지 공간정보의 활용을 크게 확산시켰다. 최근 내비게이션, 스마트폰, Wi-Fi 통신 기술 등의 모바일 시스템 기술이 획기적으로 발전됨에 따라 GIS 서비스는 인터넷 전자지도, 모바일 매쉬업 서비스, 소셜 커뮤니티 등을 통해 기존 Web-GIS 서비스와 Where 2.0이란 새로운 패러다임으로 급속히 팽창되고 있다. 이러한 GIS 서비스 상에서 가장 중요한 자료구조인 GIS DB의 데이터 구조는 그림 1에서와 같이 공간데이터 영역과 속성데이터 영역으로 구분된다. 여기서 공간데이터 영역은 벡터 데이터와 래스터 데이터로 다시 분류된다.

현재 민·관 차원의 GIS DB 구축 사업이 활발하게 이루어지면서 다양한 사회분야에 활용되면서, 구축된 GIS DB의 보안에 관련된 연구나 기술의 필요성이 제기되고 있다. GIS DB 보안은 공간정보 통합 과정에서 발생될 수 있는 DB 훼손 및 절취 등을 예방하기 위해 데이터를 암호화하거나 사용자 권한 설정을 통한 DB 접근을 제어한다. 실제로 국토지리정보원에서 구축한 GIS 데이터들을 일부 비양심적인 GIS 관련 업체들이나 2, 3차 소비자들이 불법 유통하는 사례가 증가되고 있다. 해양국토부는 2011년 현재 각 기관별로 다르게 구축된 GIS를 하나로 연동하기 위한 '국가공간정보 통합체계 구축사업'의 일환으로 전국의 모든 지자체 GIS DB의 안정적인 연동을 위한 지자체 개별적 GIS 보안 솔루션 구축에 많은 예산을 투자하고 있다.

현재까지 진행된 GIS DB 보안 기술을 살펴보면, GIS의 네트워크 전송을 보호하기 위한 네트워크 보안 기술이 주를 이루고 있으며, 일부 연구자들에 의하여 GIS DB 파일 혹은 표시영역에 대한 암호화 기반 접근 제어 기법들이 제시되고 있으며[1~4], 또한 GIS 데이터의 저작권자 인증을 위한 벡터맵 또는 래스터맵 데이터 워터마킹 기법들이 제시되고 있다[5~10].

그러나 기존의 접근제어 및 워터마킹 기반의 GIS DB 보안 기법들은 몇 가지 문제점을 가지고 있다. 첫째, GIS DB의 네트워크 보안의 경우 오프라인으로 데이터가 유출되거나, 네트워크 관리가 제대로 이루어지지 않을 경우 보안을 유지할 수 없는 문제가 발생한다. 둘째, GIS DB의 파일 암호화 및 표시영역 암호화의 경우, 일반적인 복잡한 암호화 기법을 사용하여야 하므로 계산복잡도가 증가된다. 그리고 GIS의 지도 표시영역에서 등고선, 주택, 도로, 하수관 등으로 표현되는 특정 속성들이 활성 및 비활성화가 자유롭게 이루어지며, 표시영역의 잦은 변경이 이벤트 형식으로 발생되는데, 이때마다 GIS DB의 암/복호화 과정이 수행되어야 하므로 시스템의 유연성이 부족하다. 특히, DBMS (database management system) 기반 보안 기술[3]은 DB 자료구조 변환에 취약하므로, 다양한 GIS 응용 기술에 적용하기 어렵다. 또한 GIS DB에서 특정 영역의 데이터만 추출하여 표시할 수 있게 하는 색인 기능이 필요하므로, 우선 암호화된 GIS DB를 복호해야 하는 단점을 가진다. 마지막으로 GIS 워터마킹의 경우, 비가시적인 정보를 GIS DB에 은닉함으로써 저작권을 보호하기 위한 후처리 과정으로 근본적인 GIS DB 보안책이 되기는 어렵다.

따라서 본 논문에서는 기존의 GIS DB 보안과는 달리 그림 1의 GIS DB의 데이터 중 가장 중요하고 방대한 정보를 가지고 있는 벡터맵 데이터의 원천적인 불법 복제 및 유통을 방지하고, 비인가자의 데이터 접근에 대한 권한제어를 위하여 벡터 데이터 압축영역 상에서 레이어 단위의 선택적 암호화 기법을 제안한다. 이 기

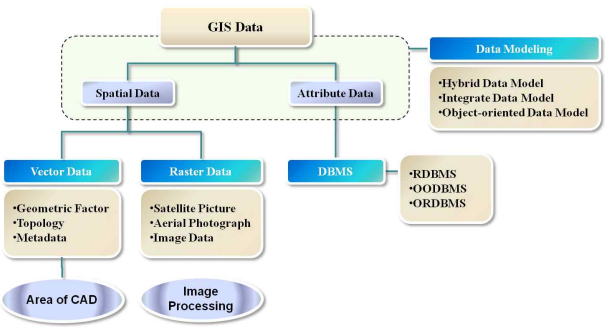


그림 1. 일반적인 GIS Database의 Data 구조
Fig. 1. A data structure of general GIS database.

법은 벡터맵 압축영역 상에서 위치 및 방향성을 결정하는 일부 파라미터들을 이용해 벡터맵 전체를 선택적 암호화하는 기법으로서, 낮은 계산복잡도로 지각적으로 높은 수준의 암호화 효율을 얻을 수 있으며, 다른 암호화 기법과는 달리 전체 벡터맵의 복호화 과정 없이 특정 영역에 대한 색인을 가능케 하는 장점이 있다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 기존의 GIS 보안 기술 및 관련 연구에 대하여 살펴보고, Ⅲ장에서는 제안한 선택적 암호화 기법에 대하여 자세히 살펴본다. 그리고 Ⅳ장에서는 제안 알고리즘을 구현하여 실험 및 고찰한 결과를 분석하며, 마지막 Ⅴ장에서는 본 논문의 결론을 맺는다.

Ⅱ. 관련 연구

GIS 수치지도는 대용량 DB의 구축을 전제로 제작되어야 하므로, 특별한 경우가 아니면 벡터 자료구조로 선택되는 것이 일반적이다. GIS 벡터맵은 철도, 하천, 도로, 건물 등 지형·지물의 특성과 데이터의 특성에 따라서 여러 개의 레이어들로 구성된다. 여기서 각 레이어는 점, 선, 면, 문자 등의 속성 집합들로 표현되며, 문자를 제외한 나머지 속성들은 하나 또는 그 이상의 꼭지점들로 표현된다. GIS 벡터맵은 제작 방식이나 제작자에 따라 주로 DXF(drawing exchange format)[11], SHP(shapefile shape format)[12]등의 포맷으로 저장되고 있으며, 국내에서는 국토지리정보원이 NGI(national geographic institute) 포맷으로 제작하여 배포하고 있다. 다양한 포맷으로 저장되더라도, 모든 벡터 데이터들은 2D 평면상에서 부동소수점을 갖는 좌표점들의 집합들로 표현된 속성들로 구성되며, 그 속성들의 집합에 의하여 지도상의 특정 레이어가 생성된다. GIS 벡터 데이터의 대표적인 속성인 폴리곤 및 폴리라인은 대부분의 지형 및 지물들을 표현하므로 벡터맵의 대부분을 차지한다. 따라서 본 논문에서는 다양한 GIS 벡터맵 데이터 포맷에 적용이 가능하기 위하여 주요 속성 성분인 폴리곤 및 폴리라인 기반의 선택적 암호화 기법을 제안한다. 본 절에서는 GIS 벡터맵에 대한 암호화 기법과 압축 기법에 대하여 살펴보기로 한다.

1. 벡터맵 기반 콘텐츠 암호화

앞서 언급한 바와 같이, 최근 GIS 보안 기술은 사회 전반에 걸쳐 GIS 기반 서비스가 증가함에 따라 그 중요성 또한 증가하고 있다. 반면, GIS DB의 핵심이라 할 수 있는 벡터맵 데이터의 보안을 위한 암호화 기술은 국 내·외적으로 그 연구가 미비하여 이에 대해서도 많은 연구가 필요하다. 기존 GIS 벡터맵 보호 기법들을 살펴보면, 온라인의 경우 네트워크 보안 모니터링 기술들이 많이 사용되어 왔으며, 오프라인의 경우 벡터맵 데이터 파일 자체를 AES, DES 등의 순수 암호화 기술들[15]을 이용하여 암호화하는 경우가 대부분이다.

Dakroury 등[2]은 워터마킹과 암호화 알고리즘을 동시에 적용한 온/오프라인 상의 벡터맵 저작권 보호 기법을 제안하였다. 이 기법에서는 256비트의 AES 블록 암호화 연산에 의하여 SHP 파일을 암호화하는 것으로 빠른 수행 속도를 실험결과로 제시하였다. 그러나 이 기법에서 사용된 SHP 파일의 벡터맵 데이터는 아프리카 및 이집트 경계선을 높은 축적비율로 나타낸 것으로 일반적인 GIS DB에서 사용되는 수치지도에 비하여 복잡도가 매우 낮으므로, 반복적인 AES 알고리즘을 적용하여도 데이터 처리량이 많지 않다. 특히 Web-GIS 또는 내비게이션 시스템에서 사용되는 벡터맵과 국방 및 관공서에서 사용되는 정밀수치지도는 대용량의 데이터들로 구성되므로, Dakroury의 기법은 정밀수치지도에 대한 계산복잡도가 매우 증가하게 된다. 또한, 이 기법은 SHP 파일 자체를 암호화함으로써 특정 영역 또는 특정 속성값을 추출하기 위하여 전체 지도의 복호화 과정을 거쳐야 하는 단점이 있다. 예를 들어 특정 지역의 도로 레이어를 표현하는 파일에서 일부 구간의 도로만을 화면에 표시하고자 할 때에도, 전체 파일을 복호화해야 하므로 시스템의 과중된 처리가 야기된다.

한편, Guangshi[3]는 오라클(Oracle) DBMS 상에서 R-Tree 공간색인 정보와 DES 기반으로 벡터공간 데이터를 암호화하는 기법을 제안하였다. 이 기법은 네트워크상에서 GIS 데이터를 클라이언트에 제공할 때 색인정보를 암호화하였고, 대칭키 및 비대칭 키 기반 암호화 키 관리를 구현하였다. 그러나 이 기법은 오라클이라는 특정 DBMS에 기반을 둔 것으로 네트워크상에서 전송되는 GIS데이터 암호화에는 유용하나, GIS DB 자체에 대한 보안이 불가능하다. 또한, 이 기법은 벡터맵 검색을 위한 색인정보를 암호화하는 것으로 벡터맵 데이터에 대한 보호가 이루어지지 않는 단점을 가진다.

이와 같은 기존의 벡터 데이터 암호화 기법들의 여러 문제점들을 해결하기 위하여 본 논문에서는 빠른 처리와 낮은 계산복잡도를 갖는 벡터맵 압축영역 상에서 생

성된 두 개의 파라미터를 이용하여 선택적 암호화 기법을 제안한다. 또한 온/오프라인 환경에 적용될 수 있고, 벡터맵 레코드들의 빠른 색인 검색이 가능하도록 레이어 단위의 암호화가 수행된다.

2. 벡터맵 압축

본 논문에서는 대용량과 높은 복잡도를 갖는 GIS 벡터맵 데이터의 실시간 처리를 위하여, 그림 2에서와 같이 다양한 정밀도 상의 바이너리 형식 벡터맵 압축 기법[13]을 이용하여 벡터맵 데이터들을 압축한다.

이 기법을 살펴보면, 하나의 벡터맵이 M개의 레이어 $\mathbf{L}=\{L_0,L_1,L_2,\cdots L_{M-1}\}$들로 구성되었을 때, 각 레이어 L_m에 포함된 N개의 폴리라인과 폴리곤 레코드 $P_{L_m}=\{p_0,p_1,p_2,\cdots p_{N-1}\}$들이 각각 독립적으로 압축된다. 여기서 하나의 속성 레코드 p_i는 $p_n=\{v_0,v_1,v_2,\cdots v_{I-1}\}$와 같이 I개의 꼭짓점들로 구성되며, p_i는 압축을 수행하기 위한 최소부호단위(minimum coding attribute, MCA)이다. 압축 과정에서는 MCA 단위의 꼭짓점들을 x, y 축 좌표의 64bit 부동소수점 값에 대한 정수부와 소수부를 분리하여 정렬한 후, 벡터 공간영역에서 2단계 에너지 집중(2-step spatial energy compaction, 2S-SEC)을 수행하여 계층적 부호화를 수행한다.

이 압축 기법은 최적의 압축효율을 위하여 그림 3의 예에서와 같이 특정 레이어의 최소 경계 영역(minimum boundary rectangle, MBR) B_l 상에서 각 레코드에 해당되는 MBR B_{p_n}의 중심좌표 m_{p_n}에 대한 꼭짓점들 v_i의 방향 부호 $s_{p_n i}$와 방향 크기 $f_{p_n i}$를 이용

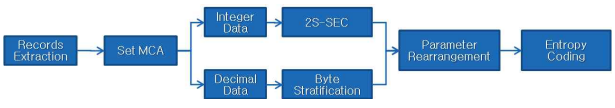


그림 2. Jang이 제안한 벡터맵 압축 알고리즘
Fig. 2. The proposed Jang's vector map compression algorithm.

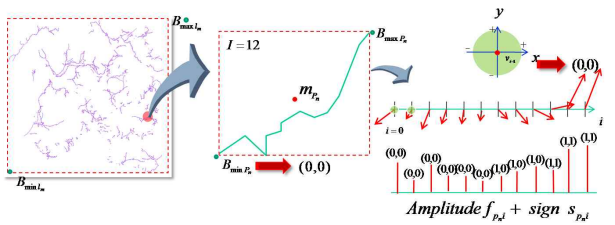


그림 3. Jang의 벡터맵 압축 시 에너지 집중 과정
Fig. 3. The energy compaction method on Jang's vector map compression algorithm.

하여 MCA내 좌표값들의 유사도를 높인다. 또한 이 기법은 각 레코드 별로 MCA를 구성하여 독립적으로 압축하므로, 압축된 상태에서도 지도상의 특정 영역에 대한 색인이 가능하다. 제안한 암호화 기법은 위의 2S-SEC 압축 과정에서 생성되는 중심좌표 m_{p_n}와 방향 부호 $s_{p_n i}$를 이용하여 대용량 벡터맵 데이터의 선택적 암호화를 수행한다.

Ⅲ. 벡터맵 데이터의 선택적 암호화 기법

앞서 언급한 바와 같이, 일반적으로 대용량 GIS DB에서 벡터맵 데이터를 압축 및 암호화하는 것은 높은 계산복잡도로 인해 많은 연산량과 수행시간을 요구한다. 따라서 본 논문에서는 벡터 공간영역에서의 높은 압축율과 낮은 계산복잡도를 가지면서, 압축영역 내에서도 빠른 속성 색인 검색이 가능한 선택적 암호화 기법을 제안한다. 여기서 제안한 기법에서는 위 절에서 설명된 2S-SEC 압축 기법에 의하여 생성된 중점좌표 m_{p_n} 및 방향 $s_{p_n i}$의 두 파라미터들을 암호화하며, 단일 파라미터만을 이용한 암호화 과정에서 발생될 수 있는 문제점들을 상호 보완하도록 두 암호화 과정을 수행한다. 제안한 2S-SEC 기반의 선택적 암호화 과정은 그림 4에서와 같이 중점좌표 m_{p_n}에 대한 위치 암호화와 각 꼭짓점의 방향 $s_{p_n i}$에 대한 방향 암호화로 나눠진다. 제안한 선택적 암호화 과정을 살펴보면, 먼저 벡터맵 레코드 압축과정 중, 2S-SEC 압축에서 생성된 중점좌표 m_{p_n}에 대해 암호화된 임의의 좌표로 치환함으로써 1차적인 위치 암호화가 수행된다. 그리고 중점좌표 m_{p_n}에 대한 각 꼭짓점의 방향 부호 $s_{p_n i}$들을 암호화함으로써 꼭짓점들의 방향을 임의로 변환하는 2차적 방향 암호화가 수행된다. 여기서 키 생성은 각 암호화 기법에 의해 결정된다.

1. 위치 암호화 기법

각 레코드의 중심좌표 m_{p_n}는 사용자정보로부터 해싱(hashing)된 J 길이를 갖는 위치 암호화 키 K_P를 기반으로 **Cipher** $C_P()$에 의하여

$$m^*_{p_n}=C_P(m_{p_n},K_P) \quad (1)$$

와 같이 암호화된다. 여기서 중심좌표 m_{p_n}는 압축을 위

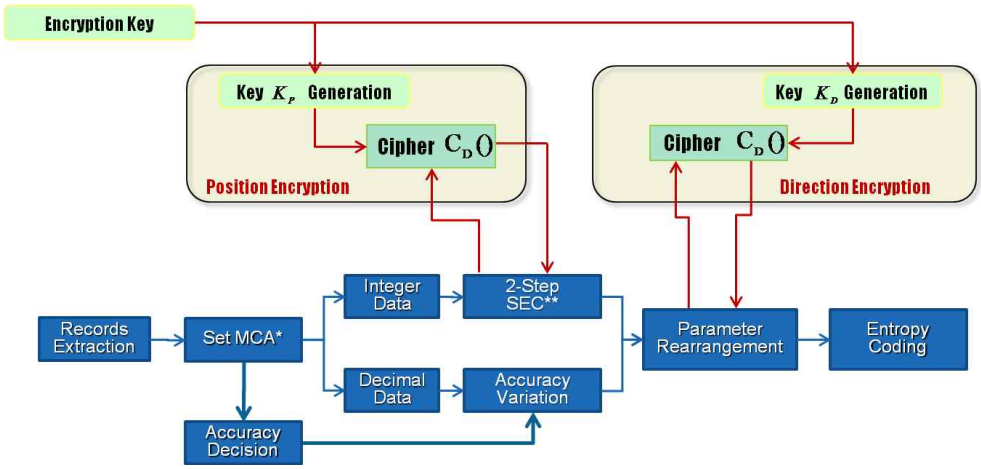


그림 4. 압축영역 상에서 제안한 벡터맵 암호화 알고리즘의 블록도
Fig. 4. A block diagram of the proposed vector map encryption algorithm on compression domain.

한 가상의 기준좌표를 나타내므로 $C_P()$에서는 x, y 좌표축을 동시에 고려하여야 한다. 따라서 위 식은 벡터 좌표계에 의하여 생성된 키 $K_P \rightarrow (k_{P_{row}}, k_{P_{col}})$를 기반으로 x, y 좌표값에 대하여

$$\begin{aligned} m^*_{p_n(x)} &= C_P(m_{p_n}(x), k_{P_{row}}), \\ m^*_{p_n(y)} &= C_P(m_{p_n}(y), k_{P_{col}}) \end{aligned} \tag{2}$$

와 같이 표현되어진다. 이 때, 암호화된 m_{p_n}의 좌표는 2차원 화소단위 영상이 갖는 정수 좌표값과는 달리 지리 공간적인 좌표값을 가지므로 좌표 임의치환을 위한 전처리과정이 필요하다.

제안한 기법에서는 암호화될 레이어 MBR과 암호화 키 길이를 이용하여 여러 개의 사각국부영역(rectangular local area, RLA)들로 나눈 후, 중심좌표 m_{p_n}가 포함된 국부 영역의 색인을 임의치환 함으로써 레코드의 위치 암호화를 수행한다. 제안한 위치 암호화 과정은 그림 5에서와 같다.

여기서 사각국부영역 RLA는 그림 5에서와 같이 레이어 L_m의 MBR B_{l_m}에 대한 J비트의 위치 암호화 키 K_P를 이용하여 수평 및 수직 크기 Δx 및 Δy에 의하여

$$\begin{aligned} \Delta x &= \frac{B_{\max l_m}(x) - B_{\min l_m}(x)}{2^{J/2}}, \\ \Delta y &= \frac{B_{\max l_m}(y) - B_{\min l_m}(y)}{2^{J/2}} \end{aligned} \tag{3}$$

와 같이 결정된다. 따라서 각 레이어 L_m는 $2^{J/2} \cdot 2^{J/2}$개의

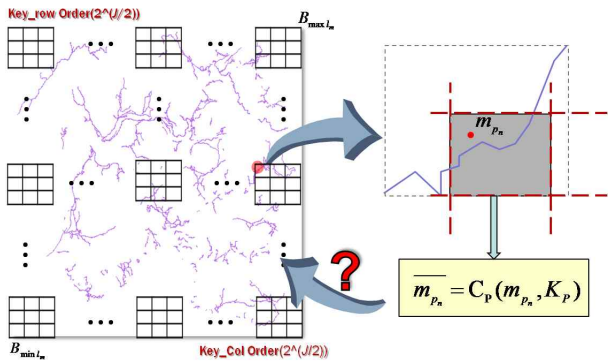


그림 5. 제안한 위치 암호화 기법의 예
Fig. 5. An example of the proposed position encryption algorithm.

$\Delta x \times \Delta y$ 크기를 갖는 RLA들로 나누어진다. 그리고 중점좌표 m_{p_n}를 갖는 RLA의 색인 r_{p_n}과 변위 d_{p_n}는

$$\begin{aligned} r_{p_n}(x) &= \lfloor m_{p_n}(x)/\Delta x \rfloor, \\ r_{p_n}(y) &= \lfloor m_{p_n}(y)/\Delta y \rfloor \end{aligned} \tag{4}$$

$$\begin{aligned} d_{p_n}(x) &= m_{p_n}(x) - (r_{p_n}(x) \cdot \Delta x), \\ d_{p_n}(y) &= m_{p_n}(y) - (r_{p_n}(y) \cdot \Delta y) \end{aligned} \tag{5}$$

와 같이 결정된다. 따라서 각 폴리곤 및 폴리라인 레코드 p_n에 대한 최종 위치 암호화된 중점좌표 m_{p_n}는 RLA의 색인 r_{p_n}과 변위 d_{p_n}에 의하여

$$\begin{aligned} m^*_{p_n}(x) &= E_P(r_{p_n}(x), k_{P_{row}}) \times \Delta x + d_{p_n}(x), \\ m^*_{p_n}(y) &= E_P(r_{p_n}(y), k_{P_{col}}) \times \Delta y + d_{p_n}(y) \end{aligned} \tag{6}$$

와 같이 구하여진다. 여기서, 암호화 함수 $E_P()$는 전형적

인 XOR, AES, 및 DES 등의 다양한 데이터 암호화 기법[15]들이 사용될 수 있다. 본 논문에서는 벡터맵의 지각적인 암호화 효율이 비슷한 수준에서 계산복잡도가 가장 낮은 XOR 암호화 기법을 이용하여 실험을 수행하였다. 이 때 암호화 키의 길이와 r_{p_n}의 길이가 동일하므로 XOR 연산에 곧바로 적용하였다.

한편, 임의의 RLA내에 여러 레코드가 존재할 경우, 동일한 암호화 키를 사용하면 RLA에 포함된 모든 레코드가 동일한 색인 값을 갖는 좌표로 치환된다. 이와 같은 중복성을 해결하기 위하여 제안한 기법에서는 위치 암호화 과정에서 증분 순서 n에 따라 암호화 키 K_P를 가변하며,

$$K_P(n) = \begin{cases} (K_P(n-1) \ll 1)+1, \text{if} < MSB\ of\ K_P(n-1)\ is\ 1 \\ K_P(n-1) \ll 1, \qquad otherwise \end{cases} \quad (7)$$

그림 6에서와 같이 K_P를 이용하여 두 좌표축에 대한 키 (k_{row},k_{col})를

$$\begin{aligned} k_{row} &= even\ bits\ of\ K_P(n) \\ k_{col} &= odd\ bits\ of\ K_P(n) \end{aligned}, \quad (8)$$

와 같이 생성한다.

그림 6은 제안된 벡터맵 데이터 암호화 과정에서 임의 RLA 내의 레코드 색인값 중복성을 최소화하기 위하여 사용한 키 생성 기법에 대하여 1바이트 길이를 갖는 짧은 비트 키를 예로서 나타낸 것이다. 그림 6의 예에 의해 1바이트 아스키 코드 'c'를 K_P에 의하여 (k_{row},k_{col})를 생성하는 과정을 간략히 나타내고 있다. 정밀 벡터맵의 동일 RLA내에 레코드 밀집도가 높지 않으므로 모든 레코드가 고유의 암호화 키를 가질 필요는 없다. 실제 본 논문의 실험에서는 해싱된 256-비트의 키를 사용한다. 이상과 같이, 제안한 방법에서는 암호화 키 K_P를 매 레코드마다 한 비트씩 순환함으로써 암호화 키의 중복성을 감소시키고, 보다 안전한 암호화를 수행할 수 있다.

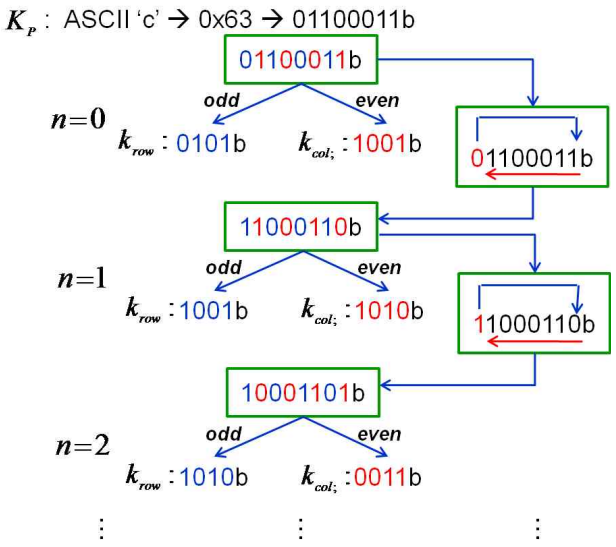


그림 6. 위치 암호화 키 생성 과정
Fig. 6. The position encryption key creation process.

2. 방향성 암호화 기법

각 레코드들이 위치 암호화에 의하여 임의 좌표로 이동되더라도 고유의 형태를 유지하고 있다. 따라서 레코드들의 고유 형태 분석을 통하여 암호화 키가 역추적될 수 있다. 따라서 제안한 방법에서는 강인한 벡터맵 암호화를 위하여 레코드 내 각 꼭짓점들의 벡터 방향성을 암호화한다.

2S-SEC에 의한 압축 과정에서 레코드 단위로 생성된 부호값 s_{p_n}은 각 꼭짓점의 벡터 방향성을 나타낸다. 제안한 방법에서는 부호값 s_{p_n}을 암호화 키 K_D 기반 **Cipher** $C_D()$에 의하여 방향성 암호화를

$$s^*_{p_n} = C_D(s_{p_n}, K_D) \quad (9)$$

와 같이 수행한다. 2S-SEC 기반의 방향성 암호화 과정은 그림 7에서와 같다. 여기서 암호화 기법은 위치 암호화에서와 같이 XOR 연산이 사용되었다. 또한 방향성 암호화 키 K_D는 중복성 방지를 위하여 K_P와 같이 증분 순서 n에 따라 순환되며, 레코드 p_n 내의 꼭지점 개수에 따라 키 길이가 결정된다.

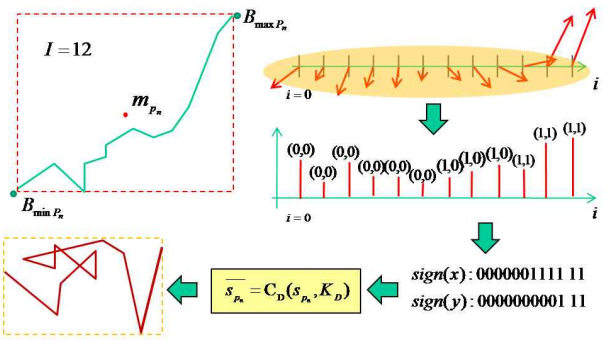


그림 7. 제안한 방향성 암호화 기법의 예
Fig. 7. An example of the proposed direction encryption algorithm.

Ⅳ. 실험 결과

본 실험에서는 제안한 벡터맵의 선택적 암호화 기법의 성능 평가를 위하여 그림 8의 1:1000 축적을 갖는 정밀 벡터맵 데이터에 대하여 위치 및 방향성 암호화를 수행하였다. 실험에 사용된 지도는 해발 100m의 등고선, 건물, 행정구역, 하천, 그리고 8개의 도로들의 레이어들로 구성되어 있다. 제안한 기법의 위치 및 방향성 암호화 과정은 벡터맵의 모든 레이어들에 대하여 수행하였으며, 그 중 지형의 주요 레이어 4개를 그림 8로부터 추출하여 이를 그림 9에 나타내었다.

기존 벡터맵 암호화 기술은 데이터 암호화 및 네트워크 암호화에 의존하지만, 제안한 기법에서는 벡터맵 지형 자체를 암호화한다. 따라서 기존의 암호화 기법과 제안한 기법과의 성능 평가 비교 기준이 모호하므로, 본 실험에서는 제안한 기법에 대한 자체 평가를 수행하였다.

위치 및 방향성 암호화된 주요 레이어들은 그림 10~13에서와 같다. 여기서 위치 암호화만 수행된 그림들을 살펴보면, 레이어 MBR 내에 각 레코드들의 위치가 임의 치환됨을 볼 수 있다. 그러나 암호화된 레코드들은 고유의 형태를 유지하므로, 암호화 키가 추정되거나 해당 벡터맵에 속한 특정 지역의 지리학적 특성이 예측될 수 있다. 또한 방향성 암호화만 수행될 경우, 각 레코드의 고유 형태가 변형되므로 벡터맵 내 세부

그림 8. 실험에 사용된 1:1000 축적 벡터맵 데이터
Fig. 8. 1:1000 scaled vector map data used in the proposed algorithm tests.

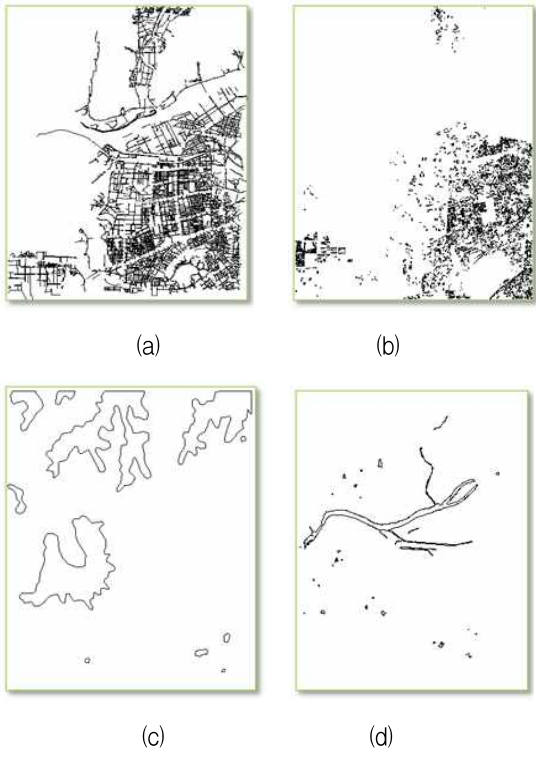


그림 9. 그림 8로부터 추출한 주요 레이어들,
(a) 일반도로(폴리라인), (b) 건물(폴리곤), (c) 해발 100m 등고선(폴리곤) 및 (d) 하천(폴리곤)
Fig. 9. Extracted several main layers from Fig.8,
(a) main street(polyline), (b) buildings(polygon),
(c) 100m contour line (polygon), and
(d) river(polygon).

형태는 쉽게 예측될 수 없다. 그러나 주거밀집지역과 같은 작은 단위의 레코드 집합일 경우 전체적인 레코드 분포를 이용하여 해당 레코드들의 지형 특성이 예측될 수 있다. 위치 및 방향성 암호화가 동시에 수행될 경우, 그림 10~13에서와 같이 해당 레코드들의 지형을 쉽게 예측할 수 없도록 치환됨을 볼 수 있다. 또한 일반적인 암호화 이론과 마찬가지로, 상대적으로 복잡하거나 많은 레코드 정보를 가진 레이어에 대해 암호화 요소가 더 많아지므로 단순한 레이어들에 비해 우수함을 알 수 있다.

실험 벡터맵 내에서 '고속도로', '지방도로' 및 '행정경계' 레이어들을 제외한 모든 레이어들이 암호화된 벡터맵과 원 벡터맵은 그림 14에서와 같다. 여기서 '고속도로', '지방도로' 및 '행정경계' 등의 레이어들도 제안한 암호화 기법에 의하여 암호화될 수 있으나, 본 실험에서는 원본 벡터맵과 암호화된 벡터맵을 쉽게 비교하기 위하여 암호화 대상에서 제외하였다. 그림 14(b)에서 확인할 수 있듯이 주요 도로 및 행정경계선을 기준으로

(a) (b) (c)

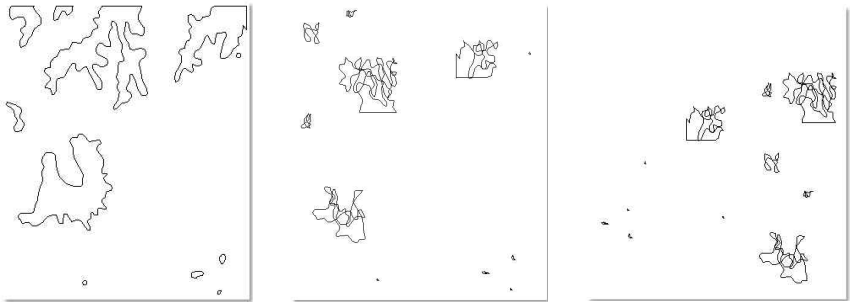
그림 10. 그림 9-(a)에 대한 (a) 암호화 전의 레이어, (b) 위치 암호화 결과 및 (c) 위치+방향성 암호화 결과

Fig. 10. Experimental results about Fig. 9-(a) (a) original polyline layer, (b) position encrypted layer, and (c) position + direction encrypted layer.

(a) (b) (c)

그림 11. 그림 9-(b)에 대한 (a) 암호화 전의 레이어, (b) 위치 암호화 결과 및 (c)위치+방향성 암호화 결과

Fig. 11. Experimental results about Fig. 9-(b) (a) original polylgon layer, (b) position encrypted layer, and (c) position + direction encrypted layer.



(a) (b) (c)

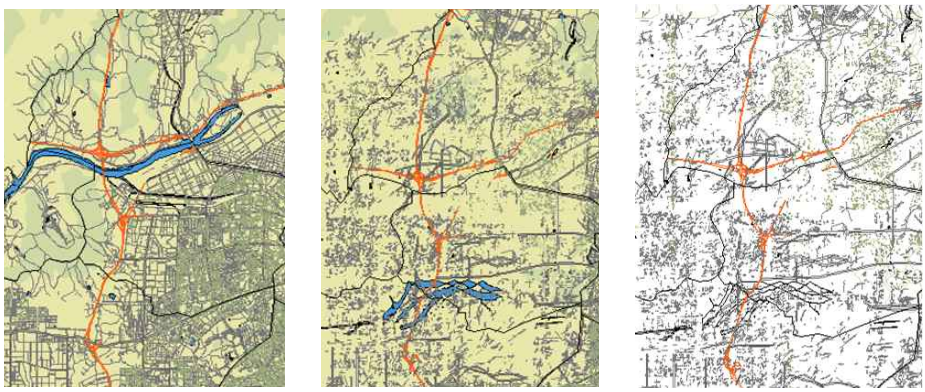
그림 12. 그림 9-(c)에 대한 (a) 암호화 전의 레이어, (b) 위치 암호화 결과 및 (c) 위치+방향성 암호화 결과

Fig. 12. Experimental results about Fig. 9-(c) (a) original polygon layer, (b) position encrypted layer, and (c) position + direction encrypted layer.

(a) (b) (c)

그림 13. 그림 9-(d)에 대한 (a) 암호화 전의 레이어, (b) 위치 암호화 결과 및 (c) 위치+방향성 암호화 결과

Fig. 13. Experimental results about Fig. 9-(d) (a) original polygon layer, (b) position encrypted layer, and (c) position + direction encrypted layer.



(a) (b) (c)

그림 14. 그림 8의 벡터맵을 제안한 기법으로 암호화한 결과
(a) 암호화 전의 벡터맵, (b) 암호화 후의 벡터맵 및 (c) 암호화 후 레이어 색상정보 임의치환
Fig. 14. The synthesis of encrypted layers.
(a) original vector map, (b) encrypted vector map, and (c) pseudo- colored map of (b).

표 1. 제안한 암호화 기법 적용 전, 후의 압축효율 비교
Table 1. Comparisons of compression efficiency among experimental results.

	original	Jang's compression(JC)	JC & position Encryption(PE)	JC & PE & Direction Encryptionm
그림 9-(a)	1,536,236	687,564	687,684	703,892
그림 9-(b)	1,134,340	511,307	511,533	524,469
그림 9-(c)	9,756	2,745	2,739	2,788
그림 9-(d)	49,420	12.038	12,032	12,244

벡터맵 암호화가 효과적으로 수행되었음을 볼 수 있다. 여기서 보다 높은 보안성을 위하여 그림 14(c)에서와 같이 암호화된 벡터맵에서 레이어별로 사용된 표현 색상을 제거하거나 의사 색상을 적용하게 되면 암호화에 의한 비가시성이 더욱 향상됨을 알 수 있었다. 전체 지도의 벡터맵이 암호화될 경우, 각 지리학적 영역을 암호화한 다음 각 영역들에 대하여 위치 암호화를 적용함으로써 지도 전체에 대하여 간단하고 빠른 암호화가 수행될 수 있다.

마지막으로 본 실험에서는 일반적인 콘텐츠 암호화에서 발생될 수 있는 압축효율에 대한 결과를 표 1에 나타내었다. 이 표를 살펴보면, 원본 벡터맵을 2S-SEC 방법으로 무손실 압축하였을 때 약 74%의 압축 효율(100%-압축데이터/원본데이터)이 발생하였다. 여기서 제안한 위치 암호화는 2S-SEC의 압축 기법만 사용하였을 경우에서와 거의 동일한 압축효율을 가진다. 이는 위치 암호화 기법이 MCA 기준 좌표만을 임의 치환함으로써 이루어지기 때문에 MCA단위로 수행되는 압축 과정에서 암호화로 인한 데이터 수정이 발생되지 않는 것을 의미한다. 반면, 방향성 암호화는 압축만 수행하였을 경우보다 평균 0.8%가 낮은 압축효율을 나타내었다. 이것은 2S-SEC 과정에서 집중된 방향성 부호들을 암호화함으로써 집중된 에너지가 분산됨에 의해 압축효율이 저하되는 결과를 야기한다. 하지만 분산된 에너지는 방향성부호값으로써 전체 압축 데이터 중 극히 일부를 차지하므로 시각적으로 높은 수준의 벡터맵 암호화를 위해 용인할 수 있는 수준이다. 실험 결과로부터 제안 고리즘이 벡터맵의 압축효율을 유지하면서 XOR 비트 연산만으로 이루어진 낮은 계산복잡도를 가지면서 시각적으로 높은 수준의 콘텐츠 암호화를 수행함을 확인하였다.

Ⅳ. 결 론

본 논문에서는 대용량 벡터맵 데이터의 낮은 계산복잡도를 갖고 암호화 영역에서 DB 색인이 가능한 벡터맵 콘텐츠 선택적 암호화 기법을 제안한다. 제안한 방법은 벡터맵을 구성하는 레이어별로 레코드 단위 압축 기법에서 생성된 위치 및 방향 정보를 가지는 두 파라미터들을 각각 암호화한다. 첫 번째 위치 암호화 과정

에서는 각 레코드의 중심좌표를 임의치환에 의하여 모든 꼭지점들을 임의치환 함으로써 벡터맵 내의 모든 지형물들의 위치를 암호화한다. 두 번째 방향 암호화 과정에서는 각 레코드의 내의 꼭지점 방향 정보들을 암호화함으로써 지형물의 형태를 변형시킨다. 여기서 암호화 과정에서는 대용량 벡터맵 데이터의 계산 복잡도를 최소화하기 위하여 XOR 연산에 의하여 암호화가 수행된다. 실험 결과로부터 제안한 벡터맵 선택적 암호화 기법이 낮은 계산 복잡도를 가지고, 방대한 벡터맵 데이터를 효과적으로 암호화 할 수 있음을 확인하였다. 그러나 XOR 연산만으로 암호화가 수행되기 때문에 순수 암호학적 관점에서 강인성을 평가한다면, AES 및 DES 보다 XOR 암호화가 보안성이 취약할 수 있다. 따라서 본 연구진들은 향후 암호학적 관점에서도 강인하고, 실시간성 및 압축효율을 보장할 수 있는 벡터맵 기반 선택적 암호화 기법을 연구하고자 한다.

본 논문에서 제안한 벡터맵 기반 선택적 암호화 기법은 다양한 종류 또는 표준 벡터맵에 적용할 수 있으며 온·오프라인 상의 GIS 서비스뿐만 아니라 모바일 기반의 위치기반 서비스에서 맵 DB 보안솔루션으로서 활용될 수 있다. 또한 제안한 방법이 CAD, 컴퓨터 그래픽스, 3D 콘텐츠 등 벡터 콘텐츠 기반 분야 등에서도 적용될 수 있을 것이다.

참 고 문 헌

[1] F. Wu, W. Cui, and H. Chen, “A Compound Chaos-Based Encryption Algorithm for Vector Geographic Data under Network Circumstance,” *Proc. of CISP*, Vol.1, pp.254-258, Sanya, Hainan, May 2008.

[2] Y. Dakroury, I. A. El-ghafar, and A Tammam, “Protecting GIS Data Using Cryptography and Digital Watermarking,” *IJCSNS*, Vol.10, No.1, pp.75-84, Jan. 2010.

[3] Giangshi Li “Research of Key Technologies on Encrypting Vector Spatial Data in Oracle Spatial,” *Proc. of ICIECS*, pp.1-4, Wuhan, China, Dec. 2010.

[4] 장봉주, 성택영, 문광석, 이석환, 권기룡, “GIS 벡터 맵 압축 영역에서 압축 파라미터와 XOR 연산을 이용한 선택적 암호화 기법,” *전자공학회 추계학술대회 논문집*, 468-469쪽, 2010년 11월

[5] 장혜정, 장봉주, 문광석, 이석환, 권기룡, “폴리곤 데이터의 무게중심을 이용한 지리정보시스템 워터마킹,” *제20회 영상처리 및 이해에 관한 워크샵*, 186쪽, 2008년 1월

[6] S. Khanna and F. Zaney, “Watermarking Maps: Hiding Information in Structured Data,” *Proc. of the Eleventh Annual ACM-SIAM symposium on Discrete Algorithms*, San Francisco, USA, pp.596-605, 2000.

[7] R. Ohbuchi, H. Ueda, and S. Endoh, “Watermarking 2D Vector Maps in the Mesh-spectral Domain,” *Shape Modeling International*, pp.216-228, Seoul, Korea, 2003.

[8] Anbo Li, Bingxian Lin, Ying Chen, and Guonian Lv, “Study on Copyright Authentication of GIS Vector Data Based on Zero-Watermarking,” *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, Vol. XXXVII Part B4, Beijing, July 2008.

[9] 이석환, 권기룡, “k-means++ 기반의 설계도면 워터마킹 기법,” *대한전자공학회 논문지*, 제46권, 제5호, 57-70쪽, 2009년 9월

[10] H. J. Chang, B. J. Jang, S. H. Lee, S. S. Park, and K. R. Kwon, “3D GIS Vector Map Watermarking Using Geometric Distribution,” *Proc. of ICME2009*, NewYork. USA, June 2009.

[11] Autodesk, *AutoCAD 2009: DXF Reference*, Autodesk, Jan. 2009.

[12] Environmental Systems Research Institute, *An ESRI White Paper: ESRI Shapefile Technical Description*, USA: ESRI, July 1998.

[13] B. J. Jang, S. H. Lee, K. S. Moon, and K. R. Kwon, “Effective Vector Map Compression Technique for Secure Encryption and Transmission,” *Pros. of FCV2010*, pp.299-303, Feb. 2010.

[14] Behrouz A. *Forouzan, Cryptography & Network Security*, McGraw-Hill inc., 2008.

[15] 류근호, 김상호, 안윤애, “시공간 GIS 및 시공간 데이터베이스 기술,” *대한전자공학회 전자공학회지*, 제29권, 12호, 31-42쪽, 2002년 12월

저 자 소 개

장 봉 주(학생회원)

2002년 부산외국어대학교 전자공학과 학사 졸업.
2004년 부산외국어대학교 전자컴퓨터공학과 석사 졸업.
2007년~현재 부경대학교 정보보호협동과정박사과정수료.

<주관심분야 : 영상압축, 멀티미디어 정보보호>

문 광 석(정회원)

1979년 경북대학교 전자공학과 학사 졸업.
1981년 경북대학교 전자공학과 석사 졸업.
1989년 경북대학교 전자공학과 박사 졸업.

1990년~현재 부경대학교 전자공학과 교수
<주관심분야 : 영상신호처리, 적응신호처리>

이 석 환(정회원)

1999년 경북대학교 전자공학과 학사 졸업.
2001년 경북대학교 전자공학과 석사 졸업.
2004년 경북대학교 전자공학과 박사 졸업.

2005년~현재 동명대학교 정보보호학과 조교수
<주관심분야 : 워터마킹, DRM, 영상신호처리>

권 기 룡(정회원)-교신저자

1986년 경북대학교 전자공학과 학사 졸업.
1990년 경북대학교 전자공학과 석사 졸업.
1994년 경북대학교 전자공학과 박사 졸업.

1996년~2006년 부산외국어대학교 디지털정보공학부 부교수
2006년~현재 부경대학교 IT융합응용공학과 교수
<주관심분야 : 멀티미디어 정보보호, 영상처리, 멀티미디어통신 및 신호처리>