Journal of Korea Multimedia Society Vol. 13, No. 5, May 2010(pp. 710-721)

# GIS 웹 맵 서비스 구현을 위한 스마트 폰에서의 정보은닉 기법

김진호[†], 서용수[††], 권기룡[†††]


## 요 약

최근, 모바일 임베디드 기술의 발달로 인하여 일반 사용자가 멀티미디어콘텐츠를 손쉽게 제작하고 이를 GIS(geographic information system) 웹 맵과 연동하여 다양하게 응용 하는 매쉬업 서비스가 웹 2.0 인터넷환경에서 활발히 서비스되고 있다. 그러나 매쉬업 서비스에서 다뤄지는 콘텐츠는 웹 맵과 연동되어 GPS 좌표정보와 같은 사용자의 공간상 이동 경로를 포함하는 새로운 형태의 콘텐츠인데 반해 해당 콘텐츠에 대한 지적 재산 및 사생활 보호를 위한 방법이 아직까지 존재하지 않는다. 본 논문에서는 GIS 웹 맵 매쉬업 서비스에서 사용자 사생활 보호와 불법 촬영자 추적을 위하여 모바일 카메라 폰을 통해 촬영된 이미지 내에 위치정보와 사용자 정보를 은닉하는 기법을 제안하고 이를 스마트 폰에 구현하였다. 위치정보에 대하여 좌표값의 오차 범위를 최소화하기 위해 비트 가중치를 고려하여 색차신호에 은닉하였으며, 부정 촬영자를 추적하기 위해 장비 고유번호, 전화번호, 촬영날짜 정보를 휘도신호에 대해 주파수도메인 상에 은닉하였다. 실험결과 위치정보 삽입에서 다양한 영상처리에 대해서 신뢰할 수 있는 오차범위를 가짐을 확인할 수 있었고, 포맷변환 시에도 위치정보를 정확히 추출하였다. 휘도신호의 정보은닉 실험 결과 공격에 의해 훼손된 영상에 대하여 유사도 패턴 매칭을 통하여 삽입한 정보를 모두 검출 하였다.


# Information Hiding Technique in Smart Phone for the Implementation of GIS Web-Map Service

Jin-Ho Kim[†], Yong-Su Seo[††], Ki-Ryong Kwon[†††]


## ABSTRACT

Recently, for the advancement of embedded technology about mobile device, a new kind of service, mash-up is appeared. It is service or application combining multimedia content making tool or device and web-GIS(geographic information system) service in the mobile environment. This service can be ease to use for casual user and can apply in various ways. So, It is served in web 2.0 environment actively. But, in the mashup service, because generated multimedia contents linked with web map are new type of multimedia contents which include user's migration routes in the space such as GPS coordinates. Thus, there are no protection ways for intellectual property created by GIS web-map service users and user's privacy. In this paper, we proposed a location and user information hiding scheme for GIS web-map service. This scheme embeds location and user information into a picture that is taken by camera module on the mobile phone. It is not only protecting way for user's privacy but is also tracing way against illegal photographer who is peeping person through hidden camera. And than, we also realized proposed scheme on the mobile smart phone. For minimizing margin of error about location coordinate value against contents manipulating attacks, GPS information is embedded into chrominance


※ 교신저자(Corresponding Author) : 권기룡, 주소 : 부산광역시 남구 대연3동 599-1, 전화 : 051)629-6257, FAX : 051)629-6210, E-mail : krkwon@pknu.ac.kr
접수일 : 2010년 4월 29일, 수정일 : 2010년 5월 20일
완료일 : 2010년 5월 30일
[†] 준회원, 전자부품연구원 SoC플랫폼연구센터 SW개발팀
(E-mail : jino17@lycos.co.kr )
[††] 정회원, 동서대학교 정보시스템공학부 부교수
(E-mail : seoyong@gdsu.dongseo.ac.kr)
[†††] 종신회원, 부경대학교 IT융합응용공학과 교수
※ 이 논문은 한국산업기술진흥원의 지역혁신인력양성사업 및 중소기업청 산학협력실지원사업으로 수행된 연구결과임.

signal of contents considering weight of each digit about binary type of GPS coordinate value. And for tracing illegal photographer, user information such as serial number of mobile phone, phone number and photographing date is embedded into frequency spectrum of contents luminance signal. In the experimental results, we confirmed that the error of extracted information against various image processing attacks is within reliable tolerance. And after file format translation attack, we extracted embedded information from the attacked contents without no damage. Using similarity between extracted one and original templete, we also extracted whole information from damaged chrominance signal of contents by various image processing attacks.

**Key words:** Geotagging(지오태깅), Information hiding(정보은닉), GIS mashup(GIS 매쉬업), Web-Map service(웹맵 서비스)

## 1. 서 론

웹 2.0(web 2.0)이라는 용어로 대변되는 최근의 웹 어플리케이션과 웹 사이트 환경에서는, 사용자는 포털 인터넷 사이트의 운영자가 제공하는 서비스의 수동적인 수용자에 그치는 것이 아니라 포털 사이트에서 제공되는 서비스를 이용해서 콘텐츠를 생산하고 다시 이를 소비하는 능동적인 주체로 변화하였다. 즉, 웹 2.0은 사용자들의 참여와 개방성을 통해 사용자들이 일방적으로 정보를 제공받지 않고 블로그, 검색 등을 활용해 스스로 정보 및 네트워크를 창조하고 공유하는 것을 가능하게 한다. 대표적인 예로, 사용자 참여 중심의 인터넷 환경에서 사용자가 포털 인터넷 사이트에서 제공하는 홈페이지 또는 블로그 등에 자신이 직접 제작한 멀티미디어콘텐츠(UCC, user created contents)를 업로드하고 커뮤니티 내에 많은 사람들과 쉽게 공유하여 자신의 생각을 표현하는 행위를 들 수 있다[1].

웹 2.0과 더불어 새롭게 주목되고 있는 서비스 중 하나로 매쉬업(mashup) 서비스를 들 수 있다. 이것은 웹 2.0과 더불어 웹 서비스의 새로운 패러다임으로 서로 상관관계가 적었던 상호 독립적인 기술 및 콘텐츠(contents)를 하나로 융합하여 새로운 형태의 사용자 지향 서비스 및 어플리케이션들을 제공하는 기술을 일컫는다. 최초의 매쉬업은 폴 래드마셔(Paul Rademacher)가 구글 맵스를 해킹해 자신이 가지고 있는 부동산 정보와 지도를 조합시켜 하우징맵스닷컴을 운영하면서 주목받았다. 구글은 폴 래드마셔를 고소하지 않고 채용하였으며, 구글 맵스의 API (application programming interface)를 공개하면서 수많은 이들이 이를 활용하도록 했다. 그 이후 지도 서비스를 이용하여 사용자가 가까운 곳에서 직거래를 하는 서비스, 물품 배송 시 제품이 주문되고 있는 상황을 지도상에 실시간으로 보여주는 서비스 등이 나타났다[2].

그 중에서 사진 매쉬업(photo mashup)은 국내외로 가장 활발히 이용되고 있는 매쉬업 분야로써, 이는 자신이 촬영한 사진에 태깅(tagging)한 위치정보를 이용하여 웹 맵 위에 나타내어 내가 언제, 어디서, 무엇을 했는지에 대한 정보를 공유한다. 뿐만 아니라 위치정보와 콘텐츠 정보를 이용하여 맛집 소개, 관광지 소개, 부동산 중계, 관공서에서의 위험물신고 등의 다양한 위치기반서비스(LBS, location based service)를 제공할 수 있다.

이와 함께 멀티미디어콘텐츠 제작에 있어 모바일 임베디드 장비의 급속한 발전으로 전문가가 아닌 일반 사용자들도 간단한 조작만으로 고화질의 디지털 카메라 또는 모바일 카메라 폰을 이용한 멀티미디어 콘텐츠 제작이 손쉬워졌다. 또한 GPS 수신기를 장착한 단말기가 최근 출시되고 있으며, GPS 수신기를 이용한 다양한 활용이 가능함으로 대부분의 모바일 장비에 장착될 것으로 예상된다. 이에 사용자가 직접 제작한 멀티미디어 지오콘텐츠를 이용한 매쉬업 서비스의 이용은 더욱 더 활성화 될 것이라 생각된다.

매쉬업 서비스는 다양하고 재미있는 서비스를 손쉽게 만들 수 있고 서비스를 구축하는데 들어가는 비용이 매우 작다는 장점이 있지만, 최근 이슈화 되고 있는 문제점으로 지적 재산의 보호와 사용자의 사생활 침해에 대한 보호방법이 없다는 문제점이 있다. 예를 들면, 사람과 장소를 불문하고 허가 없이 사진을 촬영하고 이후 인터넷을 통하여 불법 유포함으로써 심각한 개인 사생활 침해와 도덕적 문제를 발생시킨 경우가 많이 보고되어 왔으며, 국가 기밀을 요하는 문서나 기업의 중요 핵심 기술에 대한 비문이나 장비 등을 불법 촬영함으로써 국가나 기업에게 큰 경제적 손실을 입히는 경우가 종종 언론을 통해

알려졌다. 또한, 태깅된 위치정보는 개인의 중요한 정보로서, 개인의 행적이 노출되어 개인의 사생활이 침해될 가능성이 크고, 파일 헤더에 태깅된 위치정보는 타인에 의해 쉽게 훼손, 수정될 수 있어 범죄 현장의 알리바이(alibi) 조작과 같이 악의적으로 사용될 가능성이 있기 때문에 위험성이 다분히 있다.

따라서 본 논문에서는 상기와 같은 문제점을 방지하기 위하여 콘텐츠 보호 방법으로 사용되어지는 정보은닉 기법을 이용하여 사용자의 개인정보, 위치정보 등을 워터마크로 사용하여 정보를 은닉함으로써 이러한 문제점들을 해결하고자 한다. 본 논문에서는 불법 촬영자를 추적하고 사용자의 사생활을 보호 할 수 있는 안전한 웹 맵 매쉬업 서비스 구현을 위하여 GPS의 위치정보와 사용자 정보를 사진에 은닉하는 기법을 제안하고 GPS가 탑재된 모바일 카메라 폰 상에 그 기법을 구현 한다. 카메라 폰에서 촬영된 사진과 이에 은닉된 정보를 웹 맵에 전송하는 데이터 전송 클라이언트 툴을 고안하고, 전송된 위치정보와 사용자 정보, 사진 데이터를 이용하여 GIS 웹 맵과 연동하여 매쉬업 서비스를 구현한다.

본 논문의 구성으로 2장에서는 GIS 웹 맵 매쉬업 서비스에서 사용되는 지오태깅 방법과 문제점에 대해 상세히 알아보고, 3장은 본 논문에서 제안하는 지오태깅 방법 및 정보은닉 기법에 대해 서술 하였으며, 4장은 제안한 방법의 비가시성과 강인성에 대한 실험결과 및 고찰을 하고 구현한 GIS 웹 맵 서비스에 대해 설명한다. 마지막으로 5장의 결론으로 제안한 방법에 대해 평가하고자 한다.

## 2. 관련 연구

본 절에서는 GIS 웹 맵 매쉬업 서비스에서 사용되어지는 기존의 기술로써 지오태깅 기법에 대해 설명하고, 그 문제점에 대해 자세히 설명한다. 그리고 문제점을 해결하기 위해 적용되는 기술로써 정보은닉 기법에 대해 살펴본다.

### 2.1 지오태깅 방법

지오태깅은 위치 데이터(위도/경도 좌표)를 사진(JPEG), 웹사이트(HTML 페이지) 또는 RSS(really simple syndication) Feeds 내에 추가하는 방법으로 위치 정보를 이용한 다양한 기술에 응용되고 있으며, 특히 카메라를 통해 촬영된 영상 내에 촬영당시의 GPS 정보를 결합하여 개인 블로그에서 해당 지역의 사진을 블로그 방문자들과 함께 공유하는 등 영상 위치정보 검색에 많이 이용되고 있다[3,4].

JPEG(joint photographic experts group) 포맷 지오태깅 기술에서는 위치 데이터를 EXIF(exchangeable image file format) 내에 삽입하는 것이다. EXIF 메타데이터는 JPEG 헤더 정보 중 APP1(application marker segment 1)에 속하며, APP1 Length 값의 크기의 정보를 가진다. APP1의 정보는 두 개의 IFD (image file directory)로 나누어지며, 첫 번째 '0th-IFD'는 사진 자체의 정보로써 사진크기, 카메라 정보 및 촬영 시 셔터 스피드 등이 위치하고 있다. 두 번째 '1th-IFD'에는 원본 영상을 축소한 썸네일(thumbnail)영상이 위치한다. 여기서 GPS 정보는 '0th-IFD' 내에 'GPS-IFD'에 위치하며, 표 1은 10진수 단위로 구성된 위도 및 경도 좌표가 GPS sub-IFD 내에 일련의 유리수로 표현되어짐을 볼 수 있다[5,6].

EXIF 헤더 정보에 위치정보를 삽입하는 방법은 태깅 후 영상 편집 및 파일 포맷 변경이 불가능하며, 편집 및 포맷 변경 시 EXIF 메타데이터 삭제될 수 있다. 또한 지오태깅된 콘텐츠는 저작권보호, 인증 및 포렌식(forensic) 등 콘텐츠 보호 기법의 적용이 불가능하다.

따라서 본 논문에서는 다양한 영상 편집 및 파일 포맷에 강인하고, 위도/경도의 위치 정보의 특성을 고려한 가중치 기반 정보은닉 기술을 적용하여, 지오콘텐츠의 인증, 포렌식, 저작권보호 기능을 가지는 정보은닉 기법을 제안하고 그것을 스마트 폰에 구현한다.

본 논문에서는 기존의 저작권 보호를 위한 워터마킹 기술[7-9]이 아닌 새로운 사용자 정의형 양방향 웹-GIS 서비스 제공과 더불어 모바일 지오콘텐츠에 대한 인증 기능이 포함된 정보은닉 기술을 개발하고자 한다. 또한 기존의 정보은닉 기법과는 달리 위치정보를 워터마크로 삽입하므로, 이는 정확한 위치 검출을 수행하여야 한다. 따라서 각종 공격에 강인한 계층적 정보은닉 기법에 의한 정확한 위치 검출 기법을 개발한다.

## 3. 제안한 정보은닉 기법

기존 정보은닉 기법들의 경우, 여러 가지 공격들에 대한 은닉정보의 강인성 보장을 위해 콘텐츠 내

표 1. GPS IFD 태그 내용 및 형식

| 순 서 | 태그 명칭 | 내 용 | Dump[hex] | 형 식 |
|---|---|---|---|---|
| 1 | GPSVersionID | 2 2 0 0 | 02 02 00 00 | 4 bytes, int8u[4] |
| 2 | GPSLatitudeRef | N | 4e 00 | 2 byte. string[2] |
| 3 | GPSLatitude | 57 (57/1)<br>38 (38/1)<br>56.83 (5683/100) | 00 00 00 39<br>00 00 00 01<br>00 00 00 26<br>00 00 00 01<br>00 00 16 33<br>00 00 00 64 | 24 bytes, rational64u[3] |
| 4 | GPSLongitudeRef | W | 57 00 | 2byte. string[2] |
| 5 | GPSLongitude | 10 (10/1)<br>24 (24/1)<br>26.79 (2679/100) | 00 00 00 0a<br>00 00 00 01<br>00 00 00 18<br>00 00 00 01<br>00 00 0a 77<br>00 00 00 64 | 24 bytes, rational64u[3] |

은닉정보 삽입 영역 및 삽입 방법, 은닉정보 자체에 대한 오류내성 보장 기법들을 다양하게 연구하여 은닉정보 검출율을 높이고자 하였다. 그러나 모든 공격에 강인한 정보은닉 기법은 아직까지 존재하지 않으며 공격을 통해 변경된 은닉정보는 다양한 자리 값에서 무작위로 변경이 된다. 이때 은닉정보가 사용자의 위치정보인 GPS 좌표 값일 경우, 기존 정보은닉 기법으로는 매우 큰 공간적 의미를 지니는 GPS 좌표 값 중 상위 자리 값들의 오류 없는 검출을 보장 할 수 없다. 이러한 문제점 때문에 기존의 정보은닉 기법들은 지리정보 태깅을 위한 지오태깅 기법으로 대체하기가 어렵다. 따라서 본 논문에서는 기존 지오태깅 및 정보은닉 기법들이 가지는 약점들을 극복하고자 삽입되는 은닉정보의 자리 값들 중 의미가 큰 상위 자리 값들에 대해 가중치를 부여하여 각종 공격에 의해 은닉정보가 변경되더라도 허용 오차 범위 이내에서 값들이 변경되는 새로운 정보은닉 기법을 제안한다.

제안하는 기법은 휘도(luminance)성분과 색차(chrominance)성분의 고유 특성에 따라 두 가지 정보은닉 기법으로 나누어 수행 된다. 고주파 성분이 많은 휘도성분은 DWT변환을 이용하여 주파수 성분으로 변환한 후, 사용자 정보를 워터마크 패턴의 비트열로 영상에 적응적으로 저주파 영역에 삽입하며, 색차성분에 대하여 JPEG 인코딩 과정에서 8×8 블록 단위로 분할하여 DCT(discrete cosine transform) 변환 후 양자화된 Cb, Cr의 DC계수 값의 차이를 이용하여 위치정보에 가중치를 적용하여 은닉한다. 본 논문에서 제안하는 정보은닉을 위한 워터마킹 기법의 전체 수행 과정을 아래 그림 1에 나타내었다.

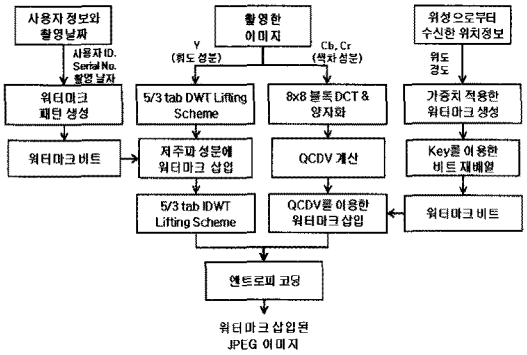



그림 1. 스마트폰 내 정보은닉 기법의 전체 과정도

### 3.1 사용자 정보 이용한 휘도성분에 대한 정보은닉 기법

제안한 휘도성분에 대한 정보은닉 알고리즘에서는 불법 촬영자를 추적 및 색출하기 위해, 그림 2와 같이 사진이 촬영된 모바일 폰 사용자의 전화번호, 장비의 고유번호, 촬영날짜 정보를 가지는 이진 이미지 패턴을 생성하여 워터마크로 사용한다.

각각의 아스키 문자를 나타내는 36개(0~9, A~Z)의 10×20 크기의 이진 영상 집합을 모바일 장비의 메모리에 미리 저장해 두고, 사진 촬영 시 36개 이진 영상 중 24개 이진영상을 선택해서 조합한 후, 그림 2-(a)와 같이 80×60 크기의 사용자 정보를 담은 이진

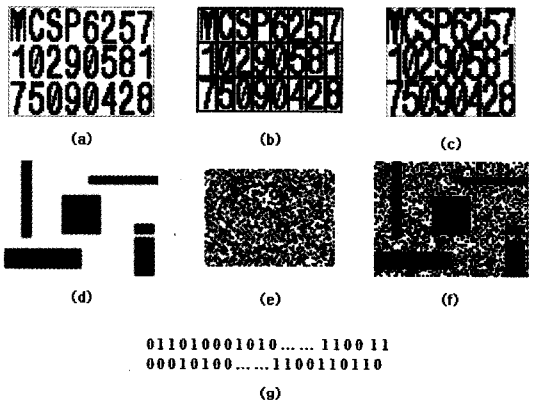



그림 2. 사용자 정보를 이용한 워터마크 생성 (a)사용자 시스템 정보 생성, (b)경계선과 삽입정보 분리, (c)분리된 사용자정보, (d)워터마크 패턴, (e)암호화한 사용자 정보, (f)워터마크 정보생성, (g)워터마크 이진 비트열

영상을 생성한다. 여기서 생성된 조합 영상에서 각각의 문자 사이의 중요하지 않은 테두리 정보 화소들을 이용하여 그림 2-(d)와 같이 패턴영상을 만들고, 그림 2-(c)의 사용자 정보는 2-(e)와 같이 암호화 키를 이용하여 암호화 하여 그림 2-(d)와 합하여 그림 2-(f)와 같은 워터마크 영상을 생성한다. 이는 워터마크 추출 시 회전, 절삭, 스케일링 등의 영상처리를 하더라도 워터마크 패턴을 찾아내 원본 워터마크를 복원 할 수 있다. 최종적으로 워터마크는 이진 비트열로 변환 후 휘도 신호에 대해 DWT변환 후 주파수 영역에서 은닉하게 된다. 계산 복잡도와 연산량을 감소시키며, 메모리 사용을 최소화하기 위해 JPEG 표준으로 채택된 Le Gall의 5/3 Tab 정수 DWT와 Lifting Scheme을 이용하였다[10]. 그림 3와 같이 주파수 변환 후, 3-레벨 DWT 변환계수의 LL3영역에

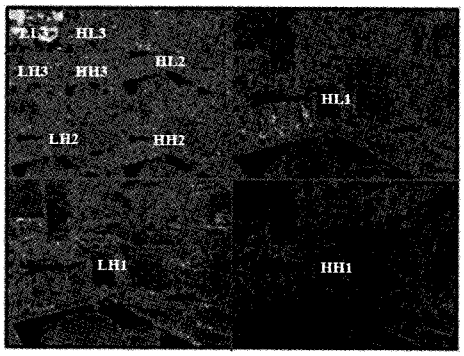



그림 3. Le Gall의 5/3tab 정수 DWT변환 후 영상

은닉하게 된다.

워터마크를 삽입강도를 각 영역별로 적응적으로 워터마크를 삽입강도를 각 영역별로 적응적으로 조절하기 위해 식 (1)과 같이 DWT 3-레벨의 고주파 특성을 이용하여 LH3, HL3 그리고 HH3 영역의 고주파 계수 $C_{LH3(m,n)}$, $C_{HL3(m,n)}$, $C_{HH3(m,n)}$들에 대한 합의 평균으로 $Th$을 결정되며, 이를 이용하여 LL3 영역에 은닉되는 워터마크의 강도를 결정한다.

$$Th = \frac{\sum_{m=0}^{M}\sum_{n=0}^{N}(|C_{LH3(m,n)}|+|C_{HL3(m,n)}|+|C_{HH3(m,n)}|)}{(M\times N\times 3)} \quad (1)$$

여기서 $M$과 $N$은 DWT변환 영역에서 레벨 3의 주파수 영역의 수직, 수평 크기를 나타낸다.

워터마크는 모든 LL3의 계수에 1비트씩 은닉되며, LL3의 해당 위치 계수 값 $C_{LL3(m,n)}$에 대한 주파수 특성 값 $g_{(m,n)}$을 식 (2)과 같이 결정한 후, 식 (1)에서 결정된 $Th$을 이용하여 워터마크 삽입강도 $mag_{(m,n)}$을 식 (3)과 같이 결정한다.

$$g_{(m,n)} = (|C_{LH3(m,n)}|+|C_{HL3(m,n)}|+|C_{HH3(m,n)}|)/3 \quad (2)$$

$$mag_{(m,n)} = \begin{cases} 3, & \text{if}(g_{(m,n)} > Th) \\ 1, & otherwise \end{cases} \quad (3)$$

따라서 워터마크는 식 (4)와 같이 정수 기반 DWT 변환 영역의 LL3 계수들의 비트 플레인(bit plane) 상에 은닉된다.

$$C^{*}_{LL3(m,n)} = \begin{cases} C_{LL3(m,n)} \,|\, (1 \ll mag_{(m,n)}) & ,\text{if}(w=1) \\ C_{LL3(m,n)} \,\&\, inv(1 \ll mag_{(m,n)}) & ,otherwise \end{cases} \quad (4)$$

이때, |, &, ≪, $inv()$는 비트 연산자로서 | 는 OR 연산자, &는 AND 연산자, ≪는 ≪가호 좌측편의 데이터를 기호 우측편의 비트수만큼 왼쪽으로 쉬프트 연산하는 쉬프트 연산자이다. 또, $inv()$는 해당 비트 값을 반전하는 토글 연산자이다.

### 3.2 휘도성분 정보은닉 추출 알고리즘

휘도성분에서의 정보은닉 추출은 삽입의 역 순으로 이루어진다. 워터마크가 삽입된 영상의 휘도성분을 Le Gall의 5/3tab 정수 DWT변환 후, 식 (1)에서 3-레벨의 모든 고주파 영역의 평균 값 $Th$을 구하고, LL3의 해당 위치 계수 값 $C^{*}_{LL3(m,n)}$에 대한 주파수 특성 값을 식 (2)에 의해 구하고, 두 값을 비교하여 식 (5), (6)와 같이 워터마크를 판별한다.

if $g_{(m,n)} \geq Th$

$$\widehat{w_i} = \begin{cases} 1, & \text{if}(C^*_{LL3(m,n)} \& (0x01 \ll 3)) = 8 \\ 0, & otherwise \end{cases} \quad (5)$$

else if $g_{(m,n)} < Th$

$$\widehat{w_i} = \begin{cases} 1, & \text{if}(C^*_{LL3(m,n)} \& (0x01 \ll 1)) = 2 \\ 0, & otherwise \end{cases} \quad (6)$$

불법 촬영자에 의해 유포된 불법 촬영 영상은 인터넷 환경에서 제 3의 또 다른 사용자가 불법 복제 할 수 있으며, 이러한 과정에서 필터링, 모자이크, 재압축 등과 같 은 공격으로 간주되는 영상처리가 수행될 수 있다. 이렇게 훼손된 영상에서 삽입한 최초 촬영자의 정보를 검출하기 위해서 워터마크 추출 후 36개의 원본 패턴과 비교하여 유사도를 이용한 정보 검출을 수행한다. 그림 4는 유사도 매칭을 통한 정보 검출 과정을 그림으로 나타내었다. 먼저 훼손된 워터마크 삽입 영상에서 식 (5), (6)을 이용해 워터마크를 추출하고, 삽입 시 사용하였던 재배열 키 값을 이용해 재배열 과정을 거친다. 이후 10×20 크기의 24개 패턴을 추출하고 각각의 패턴에 대해 36개의 원본 패턴과 비교하여 유사도 값을 구한다. 여기서 유사도는 영상의 화질 열화를 정량적으로 측정할 때 쓰이는 PSNR(peak signal to noise ratio) 값을 사용하였다. 유사도 측정 후 가장 높은 값을 가지는 패턴을 삽입 정보라 결정한다.

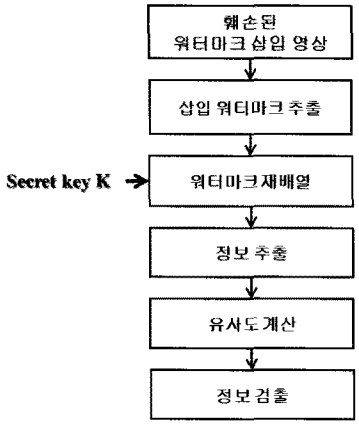



그림 4. 유사도 매칭을 이용한 정보 검출

### 3.3 위치정보 이용한 색차성분에 대한 정보은닉

GPS수신기에서 수신된 위도, 경도 값을 그림 5의 위치정보 수신부와 같이 획득한다. 먼저 GPS수신기

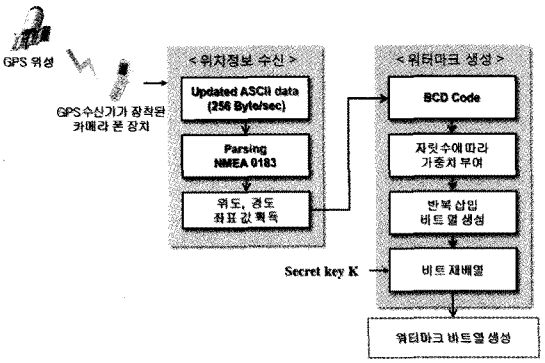



그림 5. 위치정보를 이용한 워터마크 생성

는 위성으로 부터 일정한 NMEA-0183 (national marine electronics association) 규약을 가지고 전송되는 ASCII 형태의 데이터를 초당 256바이트를 수신한다[11]. 이후, 임베디드 장치의 임시 메모리에 저장된 ASCII 데이터를 규약의 속성 정보에 따라 분석하고 위도, 경도 좌표 값을 획득한다.

이후 수신된 위치 좌표 값은 그림 5의 워터마크 생성부와 같이 정밀도를 높이기 위하여 상위 자릿수에 가중치를 두어 많은 양의 비트를 생성한다. 그리고 비밀 키를 이용하여 비트를 재배열 하여 워터마크 비트열을 생성한다.

생성된 워터마크 비트열은 색차 신호에 대하여 JPEG 인코딩 과정에서 아래와 같은 단계를 거쳐 수행된다[5].

[단계 1] Cb, Cr성분 영상을 8×8 블록으로 겹치지 않게 나눈다.

[단계 2] Cb, Cr성분 영상을 블록 단위로 DCT 변환한다.

[단계 3] 식 (7)과 같이 변환된 주파수 계수 중 DC 계수 값을 이용하여 Cb, Cr의 차이 값(QCDV)을 구한다.

$$QCDV_k = \left\lfloor \frac{b_{dc,k}}{q_{0,0}} \right\rfloor - \left\lfloor \frac{r_{dc,k}}{q_{0,0}} \right\rfloor \quad (7)$$

여기서, $b_{dc,k}$는 Cb 성분 영상의 $k$번째 블록 내 DC 계수를 뜻하며 $r_{dc,k}$는 Cr 성분 영상의 $k$번째 블록 내 DC 계수를 뜻한다. 또, $q_{0,0}$는 양자화 테이블 내 (0,0) 좌표에 위치하는 원소를 의미하는데 해당 원소로 Cb, Cr 성분 영상의 블록 내 DC성분을 양자화 한다.

[단계 4] 나머지연산을 이용하여 QCDV를 제수 값

$m$으로 나눈 나머지 값을 구한다.

[단계 5] 삽입되는 워터마크의 비트 값에 따라 Cb, Cr의 양자화된 DC계수 값을 나머지 값이 식 (8), (9)과 같이 이동한 만큼 변경하여 삽입한다.

$$\text{if } \mathrm{mod}(QCDV_k, m) \geq 0$$

$$\mathrm{mod}(QCDV_k^*, m) = \begin{cases} \frac{m}{4}, & \text{if } w=0 \\ \frac{3m}{4}, & otherwise \end{cases} \quad (8)$$

$$\text{else if } \mathrm{mod}(QCDV_k, m) < 0$$

$$\mathrm{mod}(QCDV_k^*, m) = \begin{cases} -\frac{m}{4}, & \text{if } w=1 \\ -\frac{3m}{4}, & otherwise \end{cases} \quad (9)$$

예를 들면, $\frac{m}{2} \leq \mathrm{mod}(QCDV_k, m) < m$ 일 때, 워터마크의 삽입 비트에 따라 $\mathrm{mod}(QCDV_k^*, m)$ 값은 그림 6과 같이 이동한다.

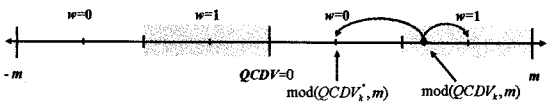



그림 6. 워터마크 삽입 방법

$w=0$일 때, 식 (10)과 같이 Cb, Cr 크기 값을 변경하여 $\mathrm{mod}(QCDV_k^*, m)$ 값을 그림 8의 $w=0$ 범위의 가운데에 위치하게 왼쪽으로 이동하여 워터마크를 삽입하고, $w=1$일 때, 식 (11)과 같이 Cb, Cr 크기 값을 변경하여 $\mathrm{mod}(QCDV_k^*, m)$ 값을 그림 8의 $w=1$범위의 가운데에 위치하게 오른쪽으로 이동하여 워터마크를 삽입한다.

$$\text{if } w=0$$

$$Cb = Cb - \frac{m}{4} \quad (10)$$

$$Cr = Cr - \mathrm{mod}(QCDV, \frac{m}{2})$$

$$\text{if } w=1$$

$$Cr = Cr - (\frac{3}{4}m - QCDV) \quad (11)$$

### 3.4 색차 성분 정보은닉 추출 알고리즘

색차성분에 대한 정보은닉 추출은 삽입의 역 순으로 수행된다. 워터마크가 삽입된 영상의 Cb, Cr 데이터는 JPEG 인코딩 과정 중 단계 1, 2 ,3을 수행한 후 식 (7)에 의해 $QCDV_k^*$를 구한다. 그리고 식 (12), (13)과 같이 워터마크를 판별한다.

$$\text{if } QCDV \geq 0$$

$$\widehat{w_k} = \begin{cases} 1, & \text{if } \frac{m}{2} < \mathrm{mod}(QCDV_k^*, m) < m \\ 0, & else \text{ if } 0 < \mathrm{mod}(QCDV_k^*, m) < \frac{m}{2} \end{cases} \quad (12)$$

$$\text{else if } QCDV < 0$$

$$\widehat{w_k} = \begin{cases} 1, & \text{if } -\frac{m}{2} < \mathrm{mod}(QCDV_k^*, m) < 0 \\ 0, & else \text{ if } -m < \mathrm{mod}(QCDV_k^*, m) < -\frac{m}{2} \end{cases} \quad (13)$$

### 3.5 시스템 설계 및 구현

제안한 정보은닉 기법을 모바일 카메라 폰에 구현하기 위하여 스마트폰 SCH-M490을 사용하였다. 이 장비는 마이크로소프트사(MS, Microsoft)의 Windows Mobile 6.1 professional 운영체제(OS, operating system)를 사용하며, 480×800 LCD display, 5M Pixel CMOS 카메라, A-GPS를 내부에 장착하고 있다. 그리고 MS 홈페이지에서 에뮬레이터 프로그램을 비롯하여, 다양한 API를 오픈 소스로 제공하고 있어 본 시스템을 구현하고 개발 하는데 최적의 장비이다. 세부 구성과 개발환경은 아래 표 2와 같다.

Windows Mobile 6 SDK(software develope kit)의 SHCameraCapture, ImageFactory, Mobile GPS API함수를 사용하여 이미지를 캡처(capture)하고 내부 GPS 수신기에서 수신된 위도, 경도 값을 획득하였다[12].

본 논문에서 제안한 정보은닉 기법을 이용하여 안전한 GIS 웹 맵 서비스를 구현하는 방법과 과정을 그림 7-(a)에 나타내었다. 모바일 카메라 폰을 이용해 촬영된 영상은 웹 맵에 업로드하기 위해서 PC에 다운로드하고 GIS 웹 맵 서버와 데이터를 전송하고

표 2. 스마트폰 SCH-M490 구성 및 개발환경

| 구 분 | 내 용 |
|---|---|
| OS | Microsoft Windows Mobile 6.1 |
| CPU | Marvel Monahans PXA 312 806Mhz |
| Display | 480×800 WVGA |
| GPS | Samsung GPS Card Ver.1 |
| Camera | 5M Pixel |
| 개발 툴 | Visual Studio 2008 Professional |

받을 수 있는 전용 툴을 이용하여 업로드 한다. 전용 클라이언트 툴은 먼저 사용자 인증 과정을 거쳐 서버에 로그인 한 후 사진 파일을 드래그앤드롭(drag and drop)하여 영상을 서버 창으로 옮기면, 먼저 영상에서 위치정보의 정보은닉 유무를 확인하고, 위치정보를 추출한다. 영상은 FTP 서버를 통해 전송되고 위치정보는 사용자 정보, 촬영일시, 사용 권한 등의 내용과 함께 DB서버로 전송한다.

전송된 위치정보와 영상을 이용하여 GIS 웹 맵 매쉬업 서비스를 그림 7-(b)와 같이 구현하였다. Google Maps의 오픈 GIS 위성데이터를 이용하였으며, 세부 기능으로 앨범, 블로그 연동, 지역 관련 뉴스 등을 연계하여 서비스 할 수 있으며 그 밖에도 다양한 매쉬업 서비스 응용이 가능하다.

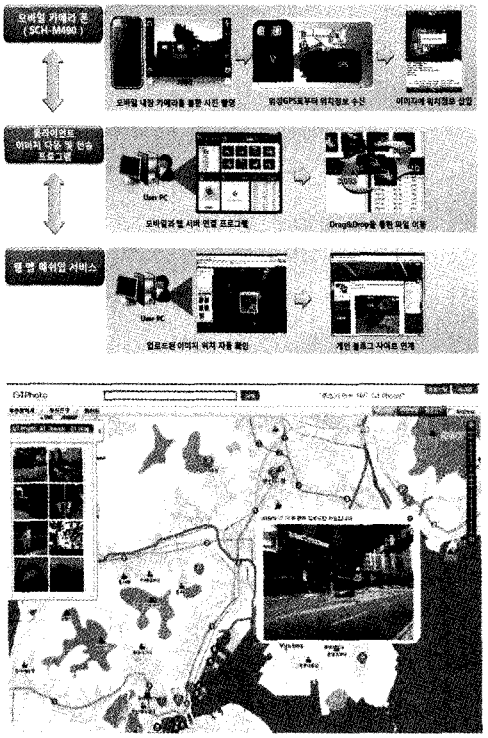


그림 7. (a) 지오콘텐츠 생성과 GIS 웹 맵 구현, (b)구현한 GIS 웹 맵 매쉬업 서비스

## 4. 실험 결과 및 고찰

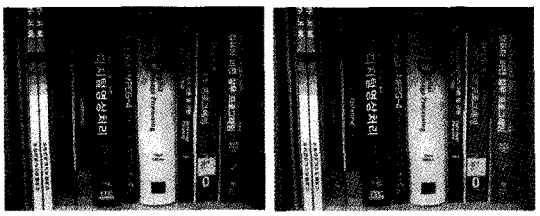
본 절에서는 안전한 GIS 웹 맵 매쉬업 서비스를 구현하기 위하여 지오콘텐츠(geo-contents)를 생성하는 모바일 카메라 폰과 생성된 지오콘텐츠를 웹 맵에 전송하기 위한 클라이언트 툴, 그리고 지오콘텐츠를 이용하여 서비스 되는 GIS 웹 맵 서비스에 대하여 설명하고, 제안한 정보은닉 기법의 성능을 평가하기 위하여 비가시성 및 다양한 공격에 대한 강인성 실험을 하고 그 결과를 분석하였다.

실험에 사용된 영상 데이터는 모바일 카메라 폰(SCH-M490)의 5M Pixel CMOS 카메라를 이용해 촬영된 정지영상이다. 영상은 640×480 8비트 RGB 데이터이며, 사용자 카메라 폰의 시스템 정보로서 장비번호: MCSP6257, 전화번호: 1029058175, 촬영날짜: 090428으로 이루어진 총 24개 문자를 사용하였으며, 위치정보는 위도 좌표 값: 3508.0671, 경도 좌표 값: 12906.1766을 사용하였다. 정보은닉에 사용되는 파라미터 값으로 색차신호 워터마킹에서 나머지 연산에 사용되는 제수 값 $m$은 비가시성과 강인성을 고려하여 실험적으로 $m=12$로 하였다.

제안한 정보은닉 알고리즘에 대한 평가를 위해 워터마크를 삽입한 후 비가시성에 대한 정량적인 평가를 위해 식 (14)의 PSNR을 측정하였으다. 이때, $M$, $N$은 영상의 너비와 높이 크기이며 $x(i,j)$와 $\hat{x}(i,j)$는 각각 원영상과 워터마크가 삽입된 영상의 $(i,j)$좌표 픽셀값이다. 공격에 대한 강인성 실험을 위하여 Stirmark Ver 3.1 [13]을 이용하여 JPEG 압축, 미디언 필터링, 샤프닝 필터링, 스케일링 공격을 실험하였다. 영상에서 추출한 워터마크를 원 워터마크에 대해 BER(bit error ratio), ND(numeric difference), 실제 오차거리를 각각 측정하였다.

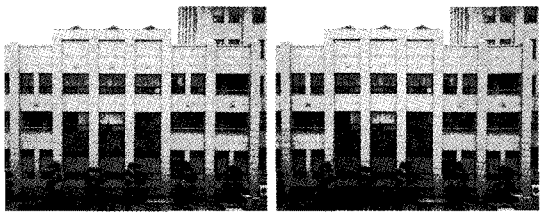
$$PSNR[dB] = 10\log\frac{255^2}{\frac{1}{M\times N}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}|x(i,j)-\hat{x}(i,j)|^2} \quad (14)$$

실험결과 영상으로 아래 그림 8, 9 및 10에 나타내었다. 시각적으로 두 영상은 큰 차이를 느낄 수 없음을 알 수 있었다.



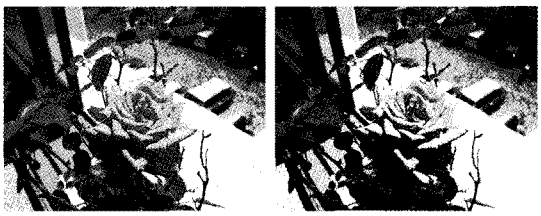
(a) (b)

그림 8. book 영상 (a)원본영상, (b)정보은닉을 수행한 영상



(a) (b)

그림 9. building 영상 (a)원본영상, (b)정보은닉을 수행한 영상



(a) (b)

그림 10. flower 영상 (a)원본영상, (b)정보은닉을 수행한 영상

원본 영상에 대해 정보은닉을 수행 전과 수행 후 두 영상의 PSNR을 측정한 결과 표 3과 같이 나왔다. 결과 수치로 제안한 정보은닉 방법이 충분히 비가시성을 만족함을 알 수 있었다.

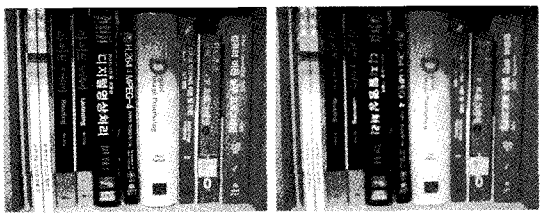
인터넷 환경에서 수행 될 수 있는 다양한 영상처리 공격에 대한 강인성 실험을 위해 그림 11와 같이 JPEG압축, 고주파/저주파 필터링, 스케일링 공격을 실행하고 워터마크 검출을 하였다.

휘도성분에 삽입한 24개 문자의 정보은닉 패턴 검출은 그림 12와 같이 수행되어져 결정된다. JPEG 압축 부호화에 의해 훼손된 영상에 대하여 워터마크 비트를 검출하고, 삽입 시 사용했던 워터마크 키 값을 이용하여 그림 12-(c)와 같이 비트열을 재배열한다. 그 후 테두리 정보에 의해 나누어진 각각의 문자 패턴에 대하여 36개 원본 패턴과 비교하여 유사도 값을 표 5와 같이 계산하였으며, 가장 높은 수치의 문자를 삽입 정보로 결정하게 된다.

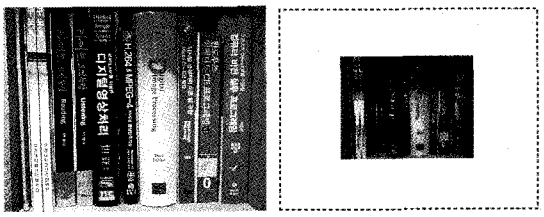
표 4는 워터마크가 삽입된 JPEG 영상에 대해 공격 실험한 결과를 나타내었다. JPEG압축 공격에 대

표 3. 원본 영상과 정보은닉을 수행한 영상의 PSNR(dB)

| Compression rate | book 영상 | building 영상 | flower 영상 |
|---|---|---|---|
| 1/9 | 39.21 | 39.24 | 43.32 |



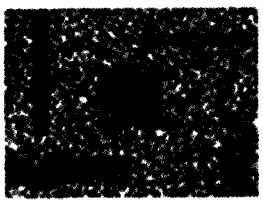
(a) (b)



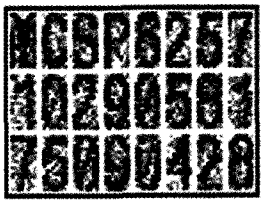
(c) (d)

그림 11. Stirmark 3.1 을 이용한 공격실험 (a) JPEG 압축, (b) Median 공격, (c) Sharpening 공격, (d) Scaling 공격

(a)



(b)




(c)

```
>>1st M-11.29, 2nd Y-7.33, 3rd I-6.47
>>1st C-10.58, 2nd O-8.78, 3rd 0-8.39
>>1st S-10.15, 2nd J-8.19, 3rd 8-8.05
>>1st P-9.89, 2nd R-8.39, 3rd F-8.24
>>1st 6-11.74, 2nd 5-9.51, 3rd 8-9.14
>>1st 2-11.03, 2nd Z-8.65, 3rd 3-7.12
>>1st 5-11.04, 2nd 6-9.17, 3rd S-8.65
>>1st 7-10.53, 2nd Z-8.59, 3rd I-8.13
>>1st 1-10.60, 2nd 4-8.64, 3rd 4-6.04
>>1st 0-10.69, 2nd O-9.02, 3rd U-8.60
```

(d)

```
# Serial Number : MCSP6257
# Phone  Number : 1029058175
# Snap   Date   : 090428
```

(e)

그림 12. 휘도성분 정보검출 결과 (a)JPEG 압축에 의한 화질열화, (b)추출한 워터마크, (c)키 값을 이용한 워터마크 재배열, (d)원본 패턴과 유사도 결과, (e) 최종 검출 정보

표 4. JPEG 압축과 필터링 공격에 대한 위치정보 오차

| Attack | | bit error(%) | 추출한 위도/경도 | 차이 값 (실거리 오차M) |
|---|---|---|---|---|
| JPEG Quality (%) | 90 | 7.54 | 3508.0671/12906.1766 | - |
| | 80 | 11.35 | 3508.0671/12906.1766 | - |
| | 70 | 16.79 | 3508.0671/12906.1766 | - |
| | 60 | 21.88 | 3508.0671/12906.1766 | - |
| | 50 | 27.19 | 3508.0671/12906.1766 | - |
| | 40 | 35.31 | 3508.0664/12906.1766 | 0.0007(1M) |
| | 35 | 38.42 | 3508.0694/12906.1782 | 0.0039(5M) |
| Median (mask) | 3 | 3.88 | 3508.0671/12906.1766 | - |
| | 5 | 7.96 | 3508.0671/12906.1766 | - |
| | 7 | 16.81 | 3508.0671/12906.1766 | - |
| | 9 | 24.06 | 3508.0671/12906.1766 | - |
| Sharpening (alpha) | 0.8 | 25.83 | 3508.0671/12906.1766 | - |
| | 0.6 | 26.31 | 3508.0671/12906.1766 | - |
| | 0.2 | 26.92 | 3508.0671/12906.1766 | - |
| | 0 | 27.75 | 3508.0671/12906.1766 | - |
| Scaling (rate) | 0.5 | 1.56 | 3508.0671/12906.1766 | - |
| | 1.5 | 11.13 | 3508.0671/12906.1766 | - |

하여 quality 50%까지 ND가 0이었으며 quality 40%에서 ND가 0.0026이었다. 그 외 median, sharpening, scaling 공격에 대해 모두 BER이 발생하였지만 ND 오차는 발생하지 않았다. JPEG 압축 quality 40%에서 실제 삽입 경도 값은 3508.0658 이지만 추출된 값은 3508.0632로 소수점 이하 셋째, 넷째자리에서 오류가 나타났다. 이 값의 ND 수치는 실제 도면상에서 경위도좌표계로 변경 시 4M로 10M 이내의 작은 오차 범위로서 추출된 위치 좌표 정보의 신뢰성을 보장하였다.

## 5. 결 론

최근 웹 2.0의 사용자 참여 중심의 인터넷 웹서비스 환경에서 타 이종 기술 간의 통합 기술로써 사용자 편의를 위한 매쉬업 서비스가 속속 등장하고 있다. 여기서 사용되는 중요 기술로써 지오태깅 방법이 있으며, 이를 2장 관련 연구에서 자세히 살펴보았다. 이러한 최근 인터넷 환경과 함께 모바일 임베디드 기술의 발달은 멀티미디어콘텐츠의 제작이 특정 전문가만이 할 수 있는 것이 아니라 일반 사용자가 GUI 환경에서 손쉽게 제작 및 편집이 가능하게 되었고, 따라서 사용자가 직접 만드는 멀티미디어콘텐츠의 생산은 급속하게 증가되고 있다. 이에 따른 문제점으로 멀티미디어콘텐츠의 지적 재산의 보호와 사용자의 사생활 침해에 대한 보호 방법이 없다는 것이다.

본 논문에서는 GIS 웹 맵 매쉬업 서비스에서 사용자 사생활 보호와 불법 촬영자 추적을 위하여 GPS의 위치 정보와 사용자 정보를 은닉하는 기법을 제안하였다. 제안한 기법은 위치정보에 대하여 좌표 값의 오차 범위를 최소화하기 위해 비트 가중치를 고려한 양자화 변조를 이용하여 색차신호에 은닉하였으며, 부정 촬영자를 추적하여 색출하기 위해 장비 고유번호, 전화번호, 촬영 날짜 정보를 워터마크로 하여 휘도 신호에 대해 정수기반 5/3 Tab DWT 도메인 상에 은닉하였다.

실험 결과 위치정보 삽입에서 다양한 영상처리에 대해서 신뢰할 수 있는 오차범위를 가짐을 확인할 수 있었고, 포맷변환 시에도 위치정보를 정확히 추출함으로써 파일 헤더에 정보를 삽입하여 헤더정보가 삭제되는 기존의 지오태깅 기법의 한계를 극복할 수 있었다. 휘도신호에 삽입하는 최초 불법 촬영자 정보 은닉 실험 결과 다양한 공격에 의해 훼손된 영상에 대하여 유사도 패턴 매칭을 통하여 삽입한 정보를

표 8. JPEG 압축에 의해 훼손된 영상에 대한 패턴의 유사도 계산 결과와 사용자 정보 검출 결과

| 순서 | 1st | | 2nd | | 3st | |
|---|---|---|---|---|---|---|
| | 문자 | 유사도[dB] | 문자 | 유사도[dB] | 문자 | 유사도[dB] |
| 1 | M | 11.99 | Y | 8.84 | 5 | 8.78 |
| 2 | C | 12.87 | O | 10.51 | D | 7.83 |
| 3 | S | 13.38 | O | 10.80 | G | 8.19 |
| 4 | P | 12.93 | R | 11.95 | F | 8.08 |
| 5 | 6 | 13.30 | 5 | 8.81 | 8 | 8.50 |
| 6 | 2 | 12.74 | P | 8.83 | Q | 6.64 |
| 7 | 5 | 12.56 | 6 | 8.57 | C | 7.37 |
| 8 | 7 | 11.83 | I | 9.91 | T | 9.48 |
| 9 | 1 | 12.46 | 4 | 9.56 | R | 8.82 |
| 10 | 0 | 12.37 | 9 | 10.05 | O | 9.45 |
| 11 | 2 | 12.52 | P | 9.92 | F | 9.15 |
| 12 | 9 | 13.11 | D | 8.49 | 8 | 6.47 |
| 13 | 0 | 12.87 | 5 | 8.33 | 7 | 7.17 |
| 14 | 5 | 12.92 | 3 | 10.69 | Z | 9.52 |
| 15 | 8 | 12.87 | C | 9.69 | 6 | 8.92 |
| 16 | 1 | 13.74 | 4 | 8.31 | A | 6.44 |
| 17 | 7 | 11.86 | T | 8.39 | I | 8.25 |
| 18 | 5 | 12.38 | 8 | 9.74 | E | 8.30 |
| 19 | 0 | 11.77 | 0 | 9.96 | 8 | 9.69 |
| 20 | 9 | 13.11 | 4 | 10.30 | 1 | 10.14 |
| 21 | 0 | 12.22 | 8 | 8.46 | 0 | 7.37 |
| 22 | 4 | 12.72 | 9 | 10.45 | 1 | 9.59 |
| 23 | 2 | 13.30 | 0 | 8.45 | Z | 8.20 |
| 24 | 8 | 12.64 | B | 8.74 | 9 | 8.39 |

모두 검출 할 수 있었다. 또한, 본 논문에서 제안한 정보은닉 기법을 모바일 카메라 폰에 구현하였으며, 안전한 GIS 웹 맵 서비스를 시현하기 위하여 상용 오픈소스 GIS 웹 맵을 이용하여 웹 서비스를 구축하였다. 이때 사진을 PC에 다운로드 하고 위치정보와 사진을 웹 서버에 전송하는 클라이언트 툴을 개발하였다.

본 논문의 연구 결과로써 웹 맵 서비스를 사용하는 사용자의 사생활 침해를 방지하고 최초 불법 촬영자를 추적하여 적발 할 수 있는 안전한 웹 맵 서비스 방법을 제시하였으며, 본 논문의 연구 결과가 사용자 참여 중심의 웹 2.0에서 안전하게 웹 맵 매쉬업 서비스를 사용 할 수 있는 보다 다양한 연구가 활발히 이루어지는 계기가 될 것으로 예상된다.

## 참 고 문 헌

[1] Tim O'Reilly, "What is Web 2.0," http://oreilly.com/web2/archive/what-is-web-20.html, 2005.

[2] http://en.wikipedia.org/wiki/Mashup_(web_application_hybrid)

[3] Anick Jesdanun, "GPS adds dimension to online photos, fans of 'geotagging' says practice is headed for the mainstream," http://www.msnbc.msn.com/id/22732770/, Jan. 20, 2008.

[4] Thota Chandrasekhar, "Geo-coding Images," *United States(US) Patent*, US-0258642, Nov.

2007.

[5] JEITA CP-3451, "Exchangeable image file format for digital still cameras: Exif Version 2.2," *Japan Electronics and Information Technology Industries Association*, April 2002.

[6] ISO/ISE 10918-1/ITU-T Recommendation T.81, "Digital Compression and Coding of Continuous-tonestill image," 1992.

[7] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Robust data hiding for images," Proc of the IEEE Digital Signal Processing Workshop, pp.37-40, 1996.

[8] E.J. Delp, "Multimedia security: the 22nd century approach," *Multimedia Systems*, Vol. 11(2), pp. 95-97, 2005.

[9] C. I. Podilchuk and W. Xent, "Image adaptive watermarking using visual models," *IEEE Journal on Selected Area in communications*, vol.16, no.4, pp.525-539, May 1997.

[10] D. L. Gall and A Tabatabai, "Subband coding of digital images using symmetric short kemel filters and arithmetic coding techniques," Processing of IEEE International Conference Acoustics, Speech, and Signal Processing, Vol. 2, pp. 761-764, New York, April 1988.

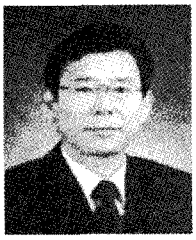
[11] http://en.wikipedia.org/wiki/NMEA_0183

[12] http://msdn.microsoft.com/en-us/library/bb158486.aspx

[13] StirMark Bechmark, http://www.petitcolas.net/fabien/watermarking/stirmark

**김 진 호**

2008년 동서대학교 전자공학과 (학사)
2010년 부경대학교 대학원 컴퓨터공학과(석사)
~현재 전자부품연구원 SoC플랫폼연구센터 SW개발팀
관심분야 : 임베디드시스템SW, 멀티미디어 정보처리



**서 용 수**

1975년 2월 경북대학교 전자공학과 졸업(공학사)
1982년 2월 동아대학교 대학원전자공학과 졸업(공학석사)
1992년 2월 경북대학교 대학원 전자공학과 졸업(공학박사)
1994년 3월~현재 동서대학교 정보시스템공학부 부교수.
관심분야 : 영상처리, 패턴인식, Remote Sensing 등임.

**권 기 룡**

1986년 경북대학교 전자공학과 학사 졸업(공학사)
1990년 경북대학교 전자공학과 석사 졸업(공학석사)
1994년 경북대학교 전자공학과 박사 졸업(공학박사)
2000년~2001년 Univ. of Minnesota, Post-Doc.
1996년~2005년 부산외국어대학교 디지털정보공학부 부교수
2006년~현재 부경대학교 IT융합응용공학과 교수
2009년~현재 한국멀티미디어학회 이사
관심분야 : 멀티미디어 정보보호, 영상처리, 웨이블릿 변환