JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 20, No. 9 : 1723~1729 Sep. 2016

강인성과 비지각성 향상을 위한 다중 바코드 워터마킹 기법

서정희[1] · 박흥복[2*]

Multiple Barcode Watermarking Technique for Improve Robustness and Imperceptibility

Jung-Hee Seo[1]· Hung-Bog Park[2*]

[1]Department of Computer Engineering, Tongmyong University, Busan 48520 Korea
[2*]Department of Computer Engineering, Pukyong National University, Busan 48513, Korea

요 약

디지털 워터마킹은 강인성과 투명성, 용량에 대한 세 개의 서로 직교하는 성능 특성으로 간주되는 최적의 균형 값을 찾기 위해 시도된다. 따라서 본 논문은 다양한 공격에 강인하고 비지각적인 워터마크 내장을 위해서 여러 주파수 대역에 다중-바코드를 내장하는 워터마크 기법을 제안한다. 그리고 다양한 주파수 대역에 중복된 바코드 워터마크 내장 기법은 다양한 공격에 영상의 내장된 워터마크가 남아있을 가능성이 높아 강인성을 만족할 수 있으나 많은 양의 중복된 바코드 데이터의 내장은 비지각성에서 문제가 발생할 수 있다. 따라서 워터마크의 요구 조건인 강인성과 비시각성의 서로 상반되는 특징을 만족시키기 위해서 주파수 대역별 바코드 데이터의 값을 변경하여 영상에 포함시킨다. 실험 결과, 본 논문에서 제안된 기법의 소유권 인증은 특별한 하드웨어 장치를 요구하지 않고 추출된 워터마크를 모바일 앱의 바코드 스캐너를 통해서 손쉽게 인증하여 낮은 복잡도와 저비용, 빠른 검증을 지원한다.

ABSTRACT

Digital watermarking is tried to get an optimum tradeoffs between its performance characteristics, robustness, transparency and capacity. This paper is, therefore, suggesting a watermarking technique that builds multiple barcodes in various frequency bands to implement embedded watermarks that is imperceptible and robust against various attacks. Even though a watermark technique with duplicated barcode watermarks embedded in various frequency bands can satisfy robustness as there is high possibility that watermarks embedded in an image remains after various attacks, the duplicated barcode data can weaken imperceptibility. Thus, to satisfy the conflicting characteristic requirements of watermarks, robustness and imperceptibility, different barcode data is embedded in each frequency band. The test shows that ownership authentication with the technique suggested in this thesis does not require specialized hardware, and extracted watermarks can be easily identified through a mobile barcode scanner app, which allows low complexity, low cost and swift identification.

키워드 : 바코드 워터마킹, 강인성, 비지각성, 소유권 인증

Key word : Barcode Watermarking, Robustness, Imperceptibility, Ownership Authentication

Received 28 April 2016, **Revised** 29 April 2016, **Accepted** 16 May 2016

* **Corresponding Author** Hung-Bog Park(E-mail:git@pknu.ac.kr, Tel:+82-51-629-6246)
Department of Computer Engineering, Pukyong National University, Busan 48513, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2016.20.9.1723 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

최근 몇 년 동안, 카메라가 장착된 모바일폰과 디지털 카메라의 확산으로 이들 기기들을 통해서 개인의 일상을 캡쳐하고 웹상에 영상들을 업로드하고 있다.

캡처된 디지털 미디어를 공유하는 것이 일반적인 관행이 되었고, 인터넷과 저장기기를 통해 전달될 수 있다. 그러나, 디지털 미디어는 통신하는 동안 쉽게 복사, 위조 및 불법 복제될 수 있다. 이러한 미디어의 불법 조작을 금지하기 위해 디지털 워터마킹은 소유권과 디지털 멀티미디어의 무결성을 보호하기 위한 기술의 집합을 의미한다[1].

또한 소셜 미디어 및 온라인 스토리지 웹 사이트의 급속한 발전으로 디지털 이미지에 대한 개인 정보는 그 어느 때보다 쉽게 접근할 수 있다. 법률이나 보험에서 법정 증거로 디지털 이미징의 중요한 상황에서, 소규모의 불명확성의 판단을 변경할 수 있다. 따라서, 디지털 이미지의 무결성을 보호하는 것이 중요해지고 있다. 디지털 이미지의 신뢰성은 워터마크 기술을 사용하는 변조 검출 알고리즘(tamper detection algorithm)을 이용하여 확보할 수 있다[2].

강인성과 비지각성은 워터마크의 주요 논점의 대상이 된다.

기존의 워터마크 시스템들은 강인성(Robustness)과 비지각성(Imperceptibility)의 관점에서 워터마크 내장 및 인증 알고리즘을 개발하고 있다. 디지털 워터마크의 필수 요건 중에서 강인성은 비소유권자의 불법적인 영상의 변형에서도 내장된 소유권 정보를 추출할 수 있어야 하고, 비지각성은 워터마크가 삽입된 영상과 원영상과는 감각적으로 구별되어서는 안된다[3].

응용 프로그램의 종류를 고려하더라고 강인성은 워터 마킹 시스템의 실용성에 영향을 미치는 중요한 문제이다. 데이터 숨기기에서, 강인성은 파괴하거나 숨겨진 워터마크를 제거하는데 사용되는 공격에 저항하는 능력을 의미한다[4].

비지각성은 시각적 또는 청각적으로 워터마크가 내장된 정보를 인식하지 못하기 때문에 멀티미디어 데이터의 상업적 가치를 극대화할 수 있다.

논문 [5]는 컬러 영상에 대해 워터마크의 견고성과 비시각성에 중점을 두고 주파수 영역에서 다중 레벨의 워터마크를 내장하고 추출하는 기법을 제안하고 JPEG 압축과 같은 신호 공격에 강인하고 다중 레벨에 대한 워터마크의 비시각성을 보장한다.

그리고 워터마크 방식은 비시각성과 강인성의 충돌을 피할 수가 없다. 따라서 논문 [6]에서는 이 문제를 해결하기 위해서 다음과 같이 새로운 방식을 제안하였다. (1) 서브 이미지는 혼돈 순서에 의해 추출된다. 서브 이미지의 로컬 DWT는 워터마크에 대한 로컬 공격을 저항할 수 있다. (2) 워터마크는 혼란 순서와 모듈 연산을 사용하여 암호화된다. (3) 제안된 구성은 웨이블릿 패킷 계수의 관계를 이용하여 블라인드 추출을 실현한다.

워터마크는 시각적이거나 비시각적이다. 비시각적 디지털 워터마킹은 이미지, 오디오 또는 비디오 데이터와 같은 멀티미디어 데이터 객체로 감지할 수 없는 신호의 삽입을 포함한다. 워터마크는 객체의 기원을 추적하기 때문에 검출할 (또는 그 이후의 추출)수 있고 소유권에 대한 주장을 할 수 있다[7].

비시각적인 메커니즘은 표시된 미디어의 품질과 가독성을 보존할 수 있다. 안정성, 품질 및 안전의 요점을 만족시키기 위해, 비시각적인 워터마킹 알고리즘은 일반적으로 계산 복잡도 중 하나이며, 시각적인 워터마킹 접근 방법에 비해, 추가의 장비를 필요로 한다. 시각적 및 비시각적 워터마킹 방법은 자신의 본질에 따라 서로 다른 애플리케이션을 위해 설계되었다. 그럼에도 불구하고, 이러한 개발 방법은 기존의 응용 프로그램에 더 많은 관심을 지불하였으나 모바일 장치를 위한 애플리케이션에 부족하다[1].

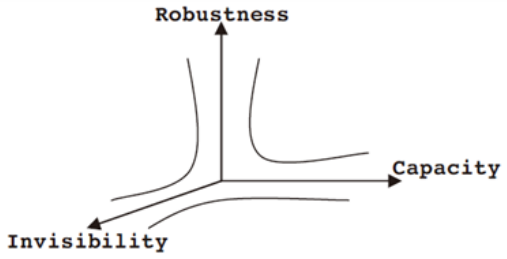


Fig. 1 Tradeoffs between robustness, invisibility and capacity

논문 [8]의 그림 1은 워터마킹 문제의 견고성과 투명성, 용량에 대한 세 개의 서로 직교하는 성능 특성으로 간주되는 최적의 균형 값을 찾기 위해 시도된다.

따라서 본 논문은 다양한 공격에 강인하고 비지각적

인 워터마크 내장을 위해서 여러 주파수 대역에 다중-바코드를 내장하는 워터마크 기법을 제안한다.

추가적인 장비가 필요 없이 바코드 워터마크를 시각적으로 추출하여 모바일폰의 바코드 스캐너 앱에 의해서 쉽게 소유권을 인증할 수 있다.

본 논문의 구성은 다음과 같다. 2절에서는 기존의 디지털 워터마크 기법에 대해 기술하고, 3장은 강인성과 비지각성 향상을 위한 다중-바코드 워터마킹 알고리즘을 제안하고, 4장은 구현 결과 및 분석, 5장은 결론, 참고문헌 순으로 기술한다.

Ⅱ. 관련 연구

Pei-Yu Lin 외 등 [1]은 모바일 기기로 촬영한 매체에 눈에 보이지 않지만 인식할 수 있는 워터마크를 은폐할 수 있는 디지털 미디어에 대한 패턴 전시(Pattern Exhibition)의 새로운 방법을 설명한다. 인간의 지각으로, 표시 매체를 감지할 수 없는 워터마크는 이미지 콘텐츠의 충실도 및 가독성을 유지할 수 있다. 설계된 윈도우 기반 히스토그램 조작에 의해, 표시 매체의 매립 패턴이 나타나 시각적으로 인식할 수 있다. 즉, 설계 메커니즘은 모바일 애플리케이션을 위한 의미있는 패턴 공유 및 식별을 촉진하기 위해 시각적과 비시각적 워터마킹 기술 모두의 필수 요소를 만족시킬 수 있다. 시뮬레이션은 마크된 이미지의 PSNR이 기존의 워터마킹 알고리즘 보다 많은 (50~70dB 정도)로 우수한 것을 보여준다. 프로세스는, 낮은 복잡도로 효율적인 내측 히스토그램 조작을 통한 모바일 장치를 통해 실제 적용될 수 있다.

Sajjad Dadkhah 외 등 [2]는 특이 값 분해 (Singular Value Decomposition:SVD)에 기초하여 유효(effective) 탬퍼(tamper) 검출과 자체 복구 알고리즘을 제안하였다. 이 방법은 이미지 블록의 특이 값 분해에 기초하여 두 개의 다른 변조 검색 키를 생성한다. 생성된 각 탬퍼 검출과 자체 복구 키는 각 이미지 블록에 대해 고유하며, 비밀 키를 이용하여 암호화된다. 이 논문에서는 액티브 워터마크를 사용하여 효과적인, SVD 기반의 탬퍼 감지 및 자동 복구 알고리즘을 제안하고 있다. 제안된 방식은 4 × 4 및 2 × 2 크기의 블록마다 탬퍼 검출키 별개의 두 세트를 생성하고, 회수된 이미지 탬퍼 지역화 및 품질을 개선하는 효율적인 탬퍼 검출 방식을 생성하는 랜덤 블록 매핑 알고리즘을 채택하였다.

Chun-Shien Lu외 등 [4]는 워터마크 추정 공격 (watermark-estimation attack: WEA)에 대처하기 위해, 미디어 해시와 내장된 신호의 하이브리드로 새로운 콘텐트-의존 워터마크를 제안하였다. 일부 연구에서 적어도 하나의 워터마크가 존재하는 등의 견고성이 유지될 수 있다는 희망으로 영상에 다중 중복 워터마크가 삽입된다. 이런 독특한 특성을 살려, 논문은 비디오 프레임과 같은 이미지에서 각 영상 단위로 처리하였다.

Cong Jin 외 등 [6]은 Chaotic 암호화를 사용하는 웨이블릿 패킷 기반의 강력한 블라인드 워터마크 기법을 제안하였다. 이진 워터마크 정보는 모듈 연산에 의해 하나의 차원 순서로 변경된다. 암호화된 워터마크 순서는 나중에 얻는 순서와 변조된 후 이진 Chaotic 시퀀스와 XOR 연산을 수행할 수 있다. 워터마크의 내장은 8 × 8 블록으로 원영상을 분할한 다음 웨이블릿 패킷 분해가 적용되는 또 다른 서열 Chaotic에 의해 총 원래 이미지 블록의 1/4에 대해 서브 영상을 추출한다. 웨이블릿 패킷 계수의 관계를 이용하여 워터마크를 삽입한다. 추출하는 워터마크는 원본 이미지를 필요로 하지 않는 블라인드 워터마크를 실현한다. 제안된 기법의 실험 결과는 JPEG 압축, 가우시안 잡음, 자르기 및 크기 조정 등 다양한 공격에 대한 매우 강력한 것을 보여 주었다.

Shi Liu 외 등 [7]은 광학적 더블 임의의 위상 인코딩 (Double Random Phase Encoding : DRPE)의 수치 시뮬레이션을 기반으로 디지털 비시각적 이미지 워터마킹 기술을 제안하였다.

Pillai Praveen Thulasidharan 외 등 [8]은 공격 검출 기능과 QR 코드 기반의 블라인드 디지털 이미지 워터마킹 기술은 여기에서 설명된다. 이 기술은 워터마크 데이터로서 이미지, 서버 포트 주소 또는 웹 사이트 주소를 포함하는 키 기반 구조를 설명한다; 이는 매립된 데이터의 확장성과 검증 애플리케이션의 적응성을 증가시킨다. 워터마킹 문제는 소스 인코딩, 채널 인코딩 및 감쇠 검출 문제와 같은 워터마크 데이터 표현, 워터마크 내장과 공격 추출과 같은 신호 통신 문제로 공식화된다.

각각의 신호 처리 문제의 수학적 측면에서 충분한 배경 지원으로 디지털 이미지 워터마킹에 확장된다. QR 코드의 사용은 확장된 유용성을 보장하는 반면 특정 워

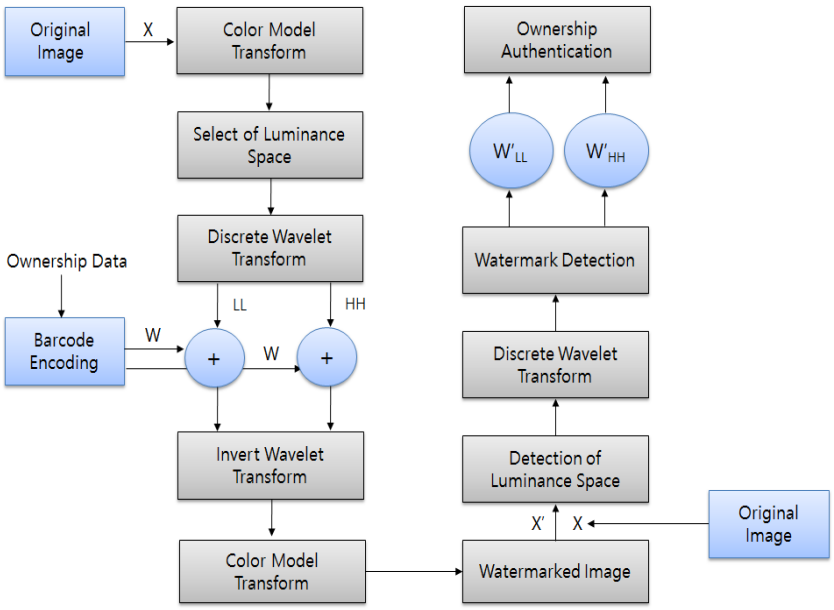


Fig. 2 Procedure of Watermark Embedding, Detection and Authentication

터마크 데이터 애플리케이션은 검증 애플리케이션의 적응성을 달성한다. QR 코드는 커버 화상의 DWT 도메인의 1-번째 레벨의 공격 내성(Attack Resistant)으로 HH 성분에 포함되고, 공격자에 의해 악의적인 간섭을 검출하기 위해 상기 stego-영상의 고주파 구성 요소에서 발생하는 고유 이미지 레지스트리 코드가 사용된다. 키 기반의 접근 및 공격 방지를 포함하는 도메인은 시각적인 불변 공격에 대해 이 방법이 강력하다. 테스트 결과는 제안된 모든 양상들에 있어서의 준수함을 나타낸다.

Teoh Chin Yew 외 등 [9]는 하드 카피 형태의 문서는 여전히 토지 제목, 신청서, 계약 및 티켓 등 특히 중요한 문서를 사용하는 것을 부정할 수 없다. 그러나 수년간 위조 사건이 보고되고 이와 같이, 하드 카피 문서의 무결성을 검증하는 메커니즘을 가지는 것은 필수적이다. 이 연구는 하드 카피 위조의 작용을 감소키는데 도움을 주기 위해 데이터를 저장하는 능력을 갖는 2 차원 바코드의 사용을 제안하였다. 이 연구는 압축 소프트웨어 GZIP 및 BZIP2과 2 차원 바코드 QR 코드 또는 데이터 매트릭스 디스플레이의 효율적인 공간 사용을 표시하고 하드 카피 문서 시스템의 무결성 검증의 응용 프로그램에 적합하다.

Ⅲ. 다중-바코드 워터마킹 기법

본 논문에서 제안하는 다양한 주파수 대역에 중복된 바코드 워터마크 내장 기법은 다양한 공격에 영상의 내장된 워터마크가 남아있는 가능성이 높아 강인성을 만족할 수 있으나 많은 양의 중복된 바코드 데이터의 내장은 비시각성에서 문제가 발생할 수 있다. 따라서 워터마크의 요구 조건인 강인성과 비시각성의 서로 상반되는 특징을 만족시키기 위해서 영상의 주파수 대역에 따라 서로 다른 바코드 데이터 값을 포함시킨다.

그림 2는 다중-바코드의 워터마크 내장 및 추출, 인증 절차를 나타낸다.

3.1. 워터마크 내장

본 논문은 소유권을 인식하기 위해서 문자열 형태의 소유권 데이터를 포함한 2D 바코드를 생성한다. 즉, 바코드 인코딩은 바코드 생성 함수에 의해 문자로 구성된다. 즉, 0~255의 값으로 구성된 2차원 매트릭스의 코드를 생성한다. 이 바코드를 영상의 DWT(Discrete Wavelet Transform) 영역의 저주파수(LL)와 고주파수(HH) 대역에 중복 내장한다.

저주파수(LL) 대역의 워터마크 내장은 압축과 같은

손실에서 워터마크의 추출이 강인하지만 Brightness, Contrast, Gamma와 같은 신호 공격에는 워터마크의 추출이 어렵다. 따라서 다양한 신호 공격에 저항하기 위해 LL 대역과 HH 대역에 바코드를 중복 내장한다. 그러나 서로 다른 주파수 대역에 같은 값의 바코드를 내장하면 비지각성의 문제를 야기시킨다.

따라서 영상의 선택된 주파수 대역에 바코드의 픽셀 값을 변경하여 포함한다.

영상의 소유권 인증을 위한 바코드의 내장은 에러 정정 기능과 각각의 비트에 많은 정보를 표현할 수 있는 장점이 있다. 워터마크 내장 절차는 다음과 같다. 먼저 원영상의 컬러 모델을 RGB에 HSL로 변경한 후 휘도 영상을 추출한다. 추출된 휘도 영상은 이산 웨이브릿 변환(Discrete Wavelet Transform)을 수행하여 서로 다른 주파수 대역으로 분해한다.

소유권 데이터가 포함된 바코드는 LL 대역과 HH 대역에 워터마크로 내장된다.

바코드가 내장된 주파수 영역을 웨이브릿 역변환을 수행하여 휘도 영상으로 변환하고, 이 영상을 다시 RGB 컬러 모델로 변경하면 워터마크가 내장된 영상이 생성된다.

3.2. 워터마크 추출 및 인증

워터마크 추출 절차는 워터마크가 내장된 영상에서 Luminance 공간을 추출한다. 그리고 이산 웨이브릿 변환을 수행하여 주파수 영역으로 변환하고 워터마크가 내장된 LL과 HH 대역을 선택하여 저주파수 대역의 워터마크(W'LL)와 고주파수 대역의 워터마크(W'HH)를 추출한다.

워터마크 인증 과정은 바코드 형태의 W'LL과 W'HH를 모바일 카메라로 캡쳐하고 바코드 스캐너 앱을 이용해서 인증 여부를 평가한다.

기존의 연구에서는 디지털 워터마크 검출 또는 인간 시각 시스템에 의해 추출되거나 인식할 수 없고, 오직 전문 장치에 의해 추출될 수 있었으나, 본 논문은 전문적인 장비가 필요 없이 워터마크를 추출한다. 따라서 본 논문에서 제안된 기법의 소유권 인증 과정은 특별한 하드웨어 장치를 요구하지 않고 추출된 워터마크를 모바일 앱을 통해서 손쉽게 인증하고 낮은 복잡도와 저비용, 빠른 검증을 지원한다.

Ⅳ. 구현 결과 및 분석

바코드는 QR 코드로서 크기는 256×256 그레이 스케일, Error Correcting Level은 L를 사용하였다.

본 논문은 워터마크가 내장된 영상에서 웨이브릿 변환을 수행하여 주파수 대역으로 변환하고 주파수 대역별 워터마크를 추출한 후 바코드 스캐너 앱을 통해서 소유권 데이터의 인식 여부를 검증하였다.

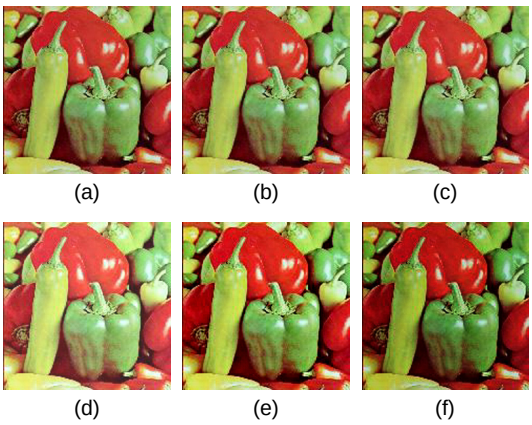


Fig. 3 Original Image, Watermarked Image and various signal attacked Images (a) Original (b) Watermarked (c) JPEG (d) Brightness (e) Contrast (f) Gamma

그림 3은 원영상(a)과 워터마크가 내장된 영상(b)을 나타낸다. 그리고 (c)~(f)는 워터마크가 내장된 영상(b)에서 JPEG 압축, Brightness, Contrast, Gamma와 같이 신호 처리 공격을 수행한 결과를 나타낸다.

그림 4는 원본 바코드와 워터마크가 내장된 영상에서 바코드를 추출한 영상을 나타낸다.

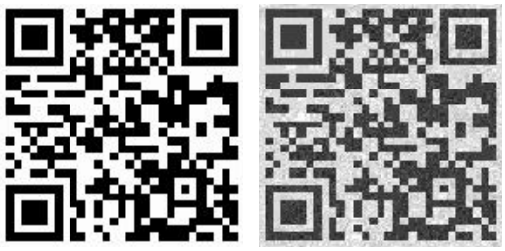
표 1은 다양한 신호 처리 공격에 대한 PSNR을 비교한 결과를 나타낸다. 워터마크된 영상(Watermarked Image)과 같이 중복 바코드의 많은 량의 정보를 내장하였음에도 불구하고 PSNR의 결과도 좋게 나타났다.

영상의 화질 평가를 위해 원영상과 워터마크가 내장된 변형이 가해진 영상에 PSNR(Peak Signal to Noise Ratio : 식 (1))와 MSE(Mean Square Error : 식 (2))을 사용하였다.

$$PSNR = 10 \cdot \log_{10} \frac{255^2}{MSE} \quad (1)$$

$$MSE = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}(X(i,j) - X'(i,j))^2 \quad (2)$$

여기서 i, j는 영상의 Resolution을 나타내고, X(i, j)는 좌표 (i, j)의 원영상의 휘도 요소의 픽셀값, X'(i, j)는 워터마크가 내장된 영상의 휘도 요소를 나타낸다.



(a) (b)

Fig. 4 Barcode Images (a) Original Barcode (b) Detected Barcode

Table. 1 A Comparative Analysis of PSNR(dB) for common signal processing attacks

Images / Attacks	PSNR(dB)			
	Lena	Baboon	Paper	House
Watermarked Image	40.36	40.42	40.35	40.34
JPEG (80%)	38.62	38.70	39.28	38.94
Brightness (α=160)	17.93	17.92	17.81	17.81
Contrast (α=50)	29.46	29.76	29.11	28.41
Gamma (α=1.5)	18.95	18.19	19.46	18.37

표 2는 다양한 신호 처리 공격에 대한 소유권 인증을 위한 바코드 인식률을 나타낸다. Lena 영상에서 Contrast 신호 공격은 소유권 데이터가 인식되지 않았고, Gamma 신호 공격에서는 소유권 데이터를 잘못 인식되는 결과를 제외하고는 모든 영상에서 바코드에 내장한 소유권 데이터를 바코드 스캐너에 의해서 인증되었다. 제안된 방법의 워터마크 내장 용량은 기존의 방법에 비해 더 많은 용량을 추가했음에도 불구하고 비시각성을 만족시키고, PSNR의 평가도 기존 방법보다 우수하다.

영상에 보이지 않는 소유권 데이터인 바코드는 인증 또는 소유권의 증명을 보여주기 위해 내장하였고, 바코드 스캐너 앱에 의해서 쉽게 소유권을 인증할 수 있다. 따라서 인터넷을 통해 이미지의 무단 복제 및 배포를 자제하는데 기여할 수 있다.

Table. 2 A Comparative Analysis of Barcode Authentication for common signal processing attacks

Images / Attacks	Barcode Authentication			
	Lena	Baboon	Paper	House
Watermarked Image	○	○	○	○
JPEG (80%)	○	○	○	○
Brightness (α=160)	○	○	○	○
Contrast (α=50)	×	○	○	○
Gamma (α=1.5)	△	○	○	○

Ⅴ. 결 론

본 논문은 다양한 공격에 강인하고 비지각적인 워터마크 내장을 위해서 여러 주파수 대역에 바코드를 중복 내장하는 워터마크 기법을 제안하였다.

실험 결과, 영상의 서로 다른 주파수 대역에 소유권 데이터가 포함된 바코드를 내장한 결과, 강인성과 비지각성을 확인할 수 있었다. 영상의 서로 다른 주파수 대역을 고려하여 바코드의 값을 변형한 후 LL과 HH 대역에 내장함으로써 각 대역의 특징에 고려하여 강인성과 비지각성을 높일 수 있다.

워터마크 인증 과정에서 추가적인 장비가 필요 없이 바코드 워터마크를 시각적으로 추출하여 바코드 스캐너 앱에 의해서 쉽게 소유권을 인증할 수 있다.

따라서 기존의 워터마크와 비교하여 다중-바코드 워터마킹은 비지각성 및 강인성, 데이터 삽입률을 높여 소유권 인증에 효과적이고 영상의 화질에 손상 없이 보다 쉽게 처리할 수 있었다.

REFERENCES

[1] P. Y. Lin, W. F. Hsieh, “Media pattern exhibition mechanism via mobile devices,” *J. Vis. Commun. Image R.*, vol. 25, no. 8, pp. 1856-1864, Nov. 2014.

[2] S. Dadkhah, A. A. Manaf, Y. Hori, A. E. Hassanien, S. Sadeghi, “An effective SVD-based image tampering detection and self-recovery using active watermarking,” *Signal Processing: Image Communication*, vol. 29, no. 10, pp. 1197-1210, Nov. 2014.

[3] J. H. Seo, H. B. Park, “Digital Watermarking for Multi-Level Data Hiding to Color Image,” *The KIPS Transactions : Part B*, vol. 14-B, no. 5, pp.337-342, Oct. 2007.

[4] C. S. Lu, and C. Y. Hsu, “Near-Optimal Watermark Estimation and Its Countermeasure: Antidisclosure Watermark for Multiple Watermark Embedding,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 17, no. 4, pp. 454-467, Apr. 2007.

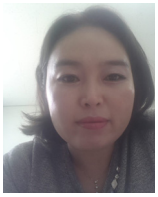
[5] H. B. Park, J. H. Seo, “Multi-Level digital Watermarking for Color Image of Multimedia Contents,” *The Journal of The Korean Institute of Maritime Information & Communication Sciences*, vol. 10, no. 11, pp. 1946-1953, Nov. 2006.

[6] C. Jin, S. W. Jin, “Wavelet Packets-based Robust Blind Digital Watermark Scheme,” *Proceedings of the 2008 International Conference on Wavelet Analysis and Pattern Recognition*, Hong Kong, vol. 2, pp. 724-728, Aug. 2008.

[7] S. Liu, B. M. Hennelly, J. T. Sheridan, “Digital image watermarking spread-space spread-spectrum technique based on Double Random Phase Encoding,” *Optics Communications*, vol. 300, pp. 162-177, July 2013.

[8] P. P. Thulasidharan, M. S. Nair, “QR code based blind digital image watermarking with attackdetection code,” *Int. J. Electron. Commun. (AEÜU)*, vol. 69, no. 7, pp. 1074-1084, July 2015.

[9] T. C. Yew, M. Salleh, S. Ibrahim, “Spatial Resource Analysis of Two Dimensional Barcodes,” *Innovations in Information Technology*, pp. 421-425, Dec. 2008.



서정희(Jung-Hee Seo)

1994년 신라대학교 자연과학대학 전자계산학과(이학사)
1997년 경성대학교 대학원 전산통계학과(이학석사)
2006년 부경대학교 대학원 전자상거래 시스템전공(공학박사)
현재 동명대학교 컴퓨터공학과 조교수
※관심분야 : 모바일, 멀티미디어 응용, 정보 보호, 원격 교육

박흥복(Hung-Bog Park)

1982년 경북대학교 공과대학 컴퓨터공학과(공학사)
1984년 경북대학교 대학원 컴퓨터공학과(공학석사)
1995년 인하대학교 대학원 전자계산학전공(이학박사)
1984년~1995년 동명대학 전자계산과 부교수
2001.2~2002.2 The University of Arizona 객원교수
1996년~현재 부경대학교 컴퓨터공학과 교수
※관심분야 : 모바일 시스템, 멀티미디어 응용, 컴파일러, 원격 교육