http://dx.doi.org/10.3745/KIPSTB.2011.18B.6.355

차이값 히스토그램 기반 가역 워터마킹을 이용한 블록 단위 영상 인증 알고리즘

여 동 규[†] · 이 해 연[††]

요 약

위변조되지 않은 고신뢰성의 영상이 요구되는 서비스에서 무결성을 인증하기위하여 가역 워터마킹 기법이 유용하게 적용될 수 있다. 콘텐츠의 인증을 위한 기존의 연구들은 워터마크의 제거후에 원본 복원이 불가능한 것이 많다. 가역 워터마킹 기법은 디지털 콘텐츠에 지각적 투명성을 유지하며 워터마크를 삽입한 후, 이를 아무런 손상없이 원본 상태로 복원할 수 있는 메시지 은닉 수단으로서 높은 품질과 높은 삽입용량이 요구되는 분야에서 다양하게 이용되어질 수 있다. 본 논문에서는 차이값 히스토그램 기반의 가역 워터마킹을 이용하여 영상의 위변조된 영역을 탐지하는 블록단위 인증 알고리즘을 제안한다. 먼저, 영상의 각 블록에 대하여 DCT 계수에 기반하여 영상의 특징값을 추출하고, 사용자의 정보와 결합하여 영상 인증 코드를 생성한다. 생성된 인증코드는 가역 워터마킹을 통하여 콘텐츠 자체에 직접 삽입한다. 이와 같은 영상의 인증을 위해서는 추출된 인증코드와 새로 생성된 인증코드의 비교를 수행한다. 다양한 영상들에 대하여 비교 분석한 실험 결과에 따르면 제안한 알고리즘은 완전한 가역성과 함께 낮은 왜곡을 유지하면서도 97% 이상의 높은 인증률을 얻을 수 있었다.

키워드 : 영상 인증, 가역 워터마킹, 차이값 히스토그램

Block-based Image Authentication Algorithm using Differential Histogram-based Reversible Watermarking

Dong-Gyu Yeo[†] · Hae-Yeoun Lee[††]

ABSTRACT

In most applications requiring high-confidential images, reversible watermarking is an effective way to ensure the integrity of images. Many watermarking researches which have been adapted to authenticate contents cannot recover the original image after authentication. However, reversible watermarking inserts the watermark signal into digital contents in such a way that the original contents can be restored without any quality loss while preserving visual quality. To detect malicious tampering, this paper presents a new block-based image authentication algorithm using differential histogram-based reversible watermarking. To generate an authentication code, the DCT-based authentication feature from each image block is extracted and combined with user-specific code. Then, the authentication code is embedded into image itself with reversible watermarking. The image can be authenticated by comparing the extracted code and the newly generated code and restored into the original image. Through experiments using multiple images, we prove that the presented algorithm has achieved over 97% authentication rate with high visual quality and complete reversibility.

Keywords : Image Authentication, Reversible Watermarking, Differential Histogram

1. 서 론

하드웨어 및 소프트웨어의 정보처리 능력과 통신 기술의 비약적인 발달로 인하여 음악, 영상, 동영상, 전자문서, 교육자료, 애니메이션과 같은 디지털 콘텐츠를 이용한 많은 서비스가 개발되어지고 보편적인 일상이 되어왔다. 그러나 쉽게 복사되어지고 수정후 재생산이 매우 쉽다는 디지털 데이터의 특성으로 인하여, 콘텐츠의 불법적인 유통과 위조로 인한 많은 문제점이 대두되었다. 특히 영상 데이터를 이용하는 많은 서비스들, 예를 들어 환자의 의료영상을 다루는 의료서비스 분야 및 감시카메라 영상데이터의 관리, 군사 및 위성 영상, 예술작품, 격오지 원격측정 분야등은 반드시 위변조되지 않은 고신뢰성의 영상이 필요하다. 만일 이들 서비스에서 위변조된 영상이 사용된다면 많은 인적 및 물적

※ 본 연구는 문화체육관광부 및 한국저작권위원회의 2011년도 저작권 기술개발사업의 연구결과로 수행되었음.
† 정 회 원 : 국립금오공과대학교 모바일연구소 박사후연구원
†† 정 회 원 : 국립금오공과대학교 컴퓨터공학부 교수(교신저자)
논문접수 : 2011년 5월 6일
수 정 일 : 1차 2011년 7월 28일
심사완료 : 2011년 8월 17일

피해를 가져올 수도 있으며 법률적 증거로서의 기능을 상실할 수도 있다. 따라서 위변조된 콘텐츠의 유통을 방지하기 위한 다양한 보안 기술의 요구도 증가하게 되었다.

영상 자료의 무결성을 인증하기 위해서는 수신된 영상이 위변조되지 않았다는 것을 증명할 수 있어야만 하며, 인증의 처리과정은 거대한 분량의 멀티미디어 흐름에 지장이 없도록 실시간에 가깝게 처리되어져야만 한다. 또한 공격자가 쉽게 유추하거나 복제할 수 없도록 보안성 조건도 만족하여야만 한다. 초창기의 인증 기술은 암호화 기법을 이용하여 정당한 수신자만이 영상을 볼 수 있도록 하는 방법이었다. 그러나 암호화 기술은 콘텐츠 배포과정에서의 보호만 보장할 뿐이며, 한 번 복호화된 콘텐츠는 더 이상 보호될 수 없기 때문에 콘텐츠의 무결성을 입증하기 위한 충분한 수단을 제공하기에는 부족하다.

원본 콘텐츠에 대한 사후 보안 기술로서의 디지털 워터마킹 기술은 디지털 콘텐츠에 기밀 정보를 비가시적으로 삽입하는 기술로서, 소유권 증명, 저작권 보호, 방송 모니터링, 콘텐츠 인증 등의 다양한 목적으로 활용되고 있다. 특히 디지털 워터마킹 기술은 응용에 따라 다양한 삽입용량과 지각적 투명성, 강인성, 기밀성, 계산 복잡도 등의 요구조건을 만족시킬 수 있기 때문에, 배포된 이후에 콘텐츠를 보호할 수 있는 수단으로 이용되기에 좋은 수단이 될 수 있다[1].

디지털 워터마킹은 원본 콘텐츠에 대한 메타데이터 혹은 무결성 검증을 위한 인증코드 및 저작권 정보 등의 워터마크 정보를 비가시적으로 콘텐츠에 삽입할 수 있으며, 응용관점에 따라 강인성(Robust) 워터마킹과 연성(Fragile) 워터마킹으로 분류된다. 강인성 워터마킹은 콘텐츠의 시각적 품질을 유지하면서 모든 가능한 왜곡 시도로부터 워터마크의 내용이 보호될 수 있도록 설계된다. 반면 연성 워터마킹은 아주 작은 변형만으로도 쉽게 워터마크가 손상되기 때문에 콘텐츠의 위조 및 변조에 대한 무결성 입증이나 인증에 유용하게 적용될 수 있다.

콘텐츠의 무결성 입증 및 위변조 인증을 하기 위하여 콘텐츠에 데이터를 은닉하려면 필연적으로 원본 콘텐츠의 수정이 불가피한데, 의료 영상이나 군사적 영상, 법률적 증거, 원격 측정값, 예술작품 등의 응용분야에서는 어떠한 손상도 없는 원본 영상이 필요하다. 변경의 정도가 극히 미미하고 인간의 지각능력으로는 전혀 알아볼 수 없을지라도 올바른 결정에 영향을 미칠 수 있으며 법률적 문제가 될 수 있기 때문이다.

콘텐츠의 인증을 위한 기존의 연구들은 삽입한 워터마크의 강인성에 초점을 맞추었기 때문에 워터마크의 제거후에 원본 복원이 불가능한 것이 많고, 위변조에 대한 정확도 또한 높지 않았다. 연성 워터마킹에 속하는 가역(Reversible) 워터마킹은 워터마킹된 콘텐츠에서 메시지를 제거한 후 원본 콘텐츠로 완전한 복원이 가능하기 때문에 콘텐츠의 무결성 인증뿐만 아니라 위변조 조작에 대한 증명, 저작권 보호를 위한 훌륭한 용도로 이용되어질 수 있다[2].

콘텐츠의 무결성 인증을 할 때, 전체 콘텐츠에 대하여 위변조 여부를 판별하기보다는 어느 영역이 위변조 되었는지 탐지하는 것이 실제 응용에서 더 유용할 수 있다. 본 논문에서는 영상 콘텐츠의 무결성을 인증하고 위조 영역을 탐지하기 위한 가역 워터마킹 기반의 영상 콘텐츠 인증 기법을 제안한다. 제안한 기법은 영상을 작은 크기의 블록으로 나누고 각 블록 단위로 워터마크를 삽입하여 무결성 인증을 수행한다.

본 논문은 다음과 같이 구성되어 있다. 2장에서 영상 인증 분야의 기존 주요 연구들을 통하여 무결성을 검증하는 알고리즘적인 차이에 대하여 논한다. 또한 영상인증을 위한 인증코드에 대하여 설명한다. 3장에서는 본 논문에서 제안하는 블록단위 영상 인증 가역 워터마킹 알고리즘에 대하여 설명한다. 실험 및 성능 분석은 4장에서 제시하며, 5장에서 결론을 맺는다.

2. 관련 연구

디지털 영상 콘텐츠의 인증과 무결성 검증을 위한 여러 데이터 은닉 기술들이 제안되어졌는데, 강인성 워터마킹보다는 주로 연성 워터마킹 기술들이 제안되었다. 연성 워터마킹으로 삽입된 은닉 데이터는 작은 조작에도 손상되기 쉬우므로 위변조 여부 판별에 쉽게 응용 가능하기 때문이다.

2.1 영상 인증 알고리즘

Zhou et al. [3]은 유방조영술 영상의 원본 검증을 위한 전자봉투 데이터를 LSB에 삽입하는 방법을 제안하였다. Rajendra et al. [4] 또한 의료 영상에 환자 정보를 삽입하기 위한 LSB 기반의 알고리즘을 제안하였다. LSB 기반 알고리즘의 주요 단점은, 만일 삽입하려는 데이터가 원본 영상 자체에 의존적이 아니라면 보안성이 쉽게 무너질 가능성이 있다는 것이다. 영상의 LSB를 삽입할 데이터로 치환하는 단순한 기법인 경우, 인증된 영상의 LSB 데이터를 위조된 다른 영상에 복사하기만 하면 쉽게 위변조가 가능하다. Yu et al. [5] 은 LSB를 수정하는 대신 웨이블릿 영역에서 평균 양자화 기법을 이용하여 데이터를 삽입하였다. 이들 방법들[3-5]은 영상의 영역별 인증이 아닌 전체 영상에 대하여 한 번의 위변조 여부를 판단하는 방식이기 때문에 활용도가 높지 않다. [6-8]의 연구에서는 영상을 일정한 영역으로 분할하여 인증코드를 삽입함으로써 위변조 판별을 지역화 하였다. Lin et al. [9]과 Lee et al. [10]은 영상의 위변조 탐지 및 복구를 위한 계층적 데이터 은닉 기법을 제안하였는데, 인접한 4x4 블록간의 평균 밝기값을 비교하고 패리티를 체크하는 방법을 사용하였다.

그러나 [3-10]의 방법들은 삽입된 인증 데이터를 제거한 후 원본 영상으로 완전한 복구가 불가능한 비가역적(Irreversible) 워터마킹 방법들이기 때문에 영상의 품질이 중요한 분야에서는 적용하기 어렵다. 콘텐츠에 대한 인증을 마친 후 원본 영상으로의 완전한 복원을 위해서는 가역 워터마킹 알고리즘이 이용되어진다. 가역 워터마킹 연구들은

지각적 투명성 및 완전한 가역성을 제공하기 위하여 각기 다른 영상의 특징을 이용하여 메시지를 삽입한다. Celik et al.[11]은 무손실 압축기법을 이용하여 비트 평면을 압축한 후 빈 공간에 메시지를 삽입하였으며, Lee et al.[12]은 주파수 영역에서의 변환계수에 삽입하였다. 또한 Tian[13] 과 Thodi et al.[14]은 원본 영상의 특성값을 확장하여 삽입하는 차이값 확장 방법을 사용하였다. 최근에는 계산 복잡도가 높지 않으며 높은 삽입용량을 얻을 수 있는 히스토그램 기반 방법들[15-21]에 관한 연구가 활발히 진행중인데 알고리즘에 따라 영상의 밝기값에 대한 히스토그램을 이용하거나 차이값에 대한 히스토그램을 이용한다. 밝기값 히스토그램 수정 기법을 이용하는 가역 워터마킹 알고리즘들[15-16]은 데이터를 삽입하려는 최대점 주위의 빈(Bin)을 쉬프팅하여 공간을 확보하고, 삽입하려는 메시지의 비트에 따라 최대점을 좌우로 쉬프팅시킴으로써 데이터를 삽입한다. 차이값 히스토그램을 이용하는 알고리즘들[17-21]은 인접한 픽셀과의 밝기값 차이를 이용하여 계산한다. 차이값 히스토그램을 이용하면 하나의 최대점만 사용하더라도 밝기값 히스토그램 사용 방법보다 더 높은 삽입용량을 얻을 수 있기 때문에 최근의 가역 워터마킹 연구들은 차이값 히스토그램을 이용하는 추세이다.

2.2 영상 인증 코드

블록 단위의 영상 인증에 관한 기존 연구들은 영상 블록에 대한 특징값을 유일하게 구분하기 위하여 여러 종류의 인증코드를 생성하여 사용하였는데, 일반적으로 평균값, 패리티값, 체크섬, 해시값 등을 사용하여왔다. 그러나 이러한 값들은 그 크기가 작기 때문에 오탐지의 가능성이 존재한다. 예를 들어 평균값을 인증코드로 사용할 경우 일반적인 영상에서 8 비트의 크기를 가지므로, 인증코드의 경우의 수는 2^8 가지(256)이다. 이것이 의미하는 것은 1/256의 확률로 우연에 의한 오탐지의 가능성이 존재한다는 것이다. 만일 공격자의 위변조 행위가 원영상과 매우 유사하도록 유지하며 미미하게 이루어질 경우에는 오탐지의 확률이 더욱 높아진다. 따라서 인증코드는 오탐지 확률을 최소화할 수 있을 정도의 길이를 가져야만 한다. 그러나 지나치게 큰 길이의 인증코드는 워터마킹 기법으로 메시지를 삽입하고자 할 때, 삽입가능한 최대 용량을 초과할 수 있으므로 워터마킹 알고리즘에 따라 알맞은 크기를 가져야 한다. 기존 연구들에서의 인증코드들은 길이가 작다는 단점 뿐만 아니라, 인증코드가 인증을 위한 목적으로밖에 사용되어지지 않는다는 것이다. 인증코드가 인증을 위한 단순한 목적뿐 아니라 추가적인 용도를 가진다면 더욱 활용성이 높아질 것이다. 본 논문에서는 영상 블록에 대한 DCT 계수들을 인증코드로 사용하는데, 이는 인증을 위한 충분한 길이의 유일한 특징값을 만들어 오탐지의 확률을 현저히 낮출 뿐만 아니라 향후의 연구에서 손상 영역을 복원하기 위한 기술로 확장할 수 있기 때문이다.

영상 압축기술에서 비롯된 DCT 방법은 시간축의 화상신호를 주파수축으로 변환하는 방법으로서 이산적 코사인 함수를 사용하는 직교 변환 부호화 방식이다. DCT를 통한 고효율의 다운사이징 및 복원특징으로 인하여 현재 정지영상 및 동영상을 위한 대표적인 부호화 및 압축기술로 사용되어지고 있다. DCT를 통한 영상 압축알고리즘은 영상 블록에 대하여 화소값들을 주파수 영역으로 분해하여 변환한 후, 저주파수 영역에 집중된 DCT 계수들을 양자화하여 원영상보다 적은 비트로 표현함으로써 압축하는 방식이다. 이때 DCT 계수들을 얼마나 많이 선택하여 저장하느냐에 따라 압축효율 및 복원된 영상의 품질이 결정된다. 영상블록의 평균값이나 체크섬같이 작은 길이의 특징값이 아니라 여러 개의 상위 DCT 계수를 인증코드로 선택함으로써 적절한 길이를 보장할 뿐만 아니라 손상된 블록에 대하여 비교적 원본과 유사하게 복원하는데 사용할 수도 있다.

3. 가역 워터마킹을 통한 블록 기반 인증 알고리즘

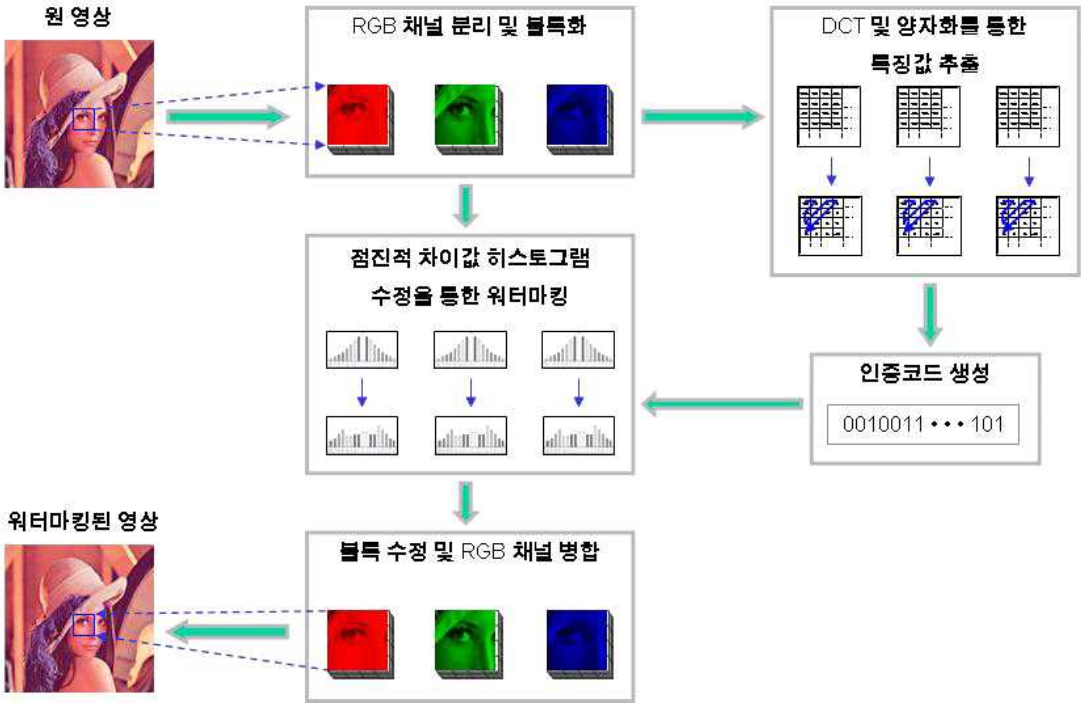
본 논문에서는 영상에 대한 블록단위의 인증을 수행하기 위하여, 각 블록에 대한 특징값을 추출하여 점진적 차이값 히스토그램 기반의 워터마킹 기법으로 특징값을 삽입한 후 인증을 수행하는 방법을 제안한다. 각 블록에 대한 인증코드는 상위 DCT 계수 8 Bytes를 사용한다.

3.1 영상 블록 단위 인증 알고리즘

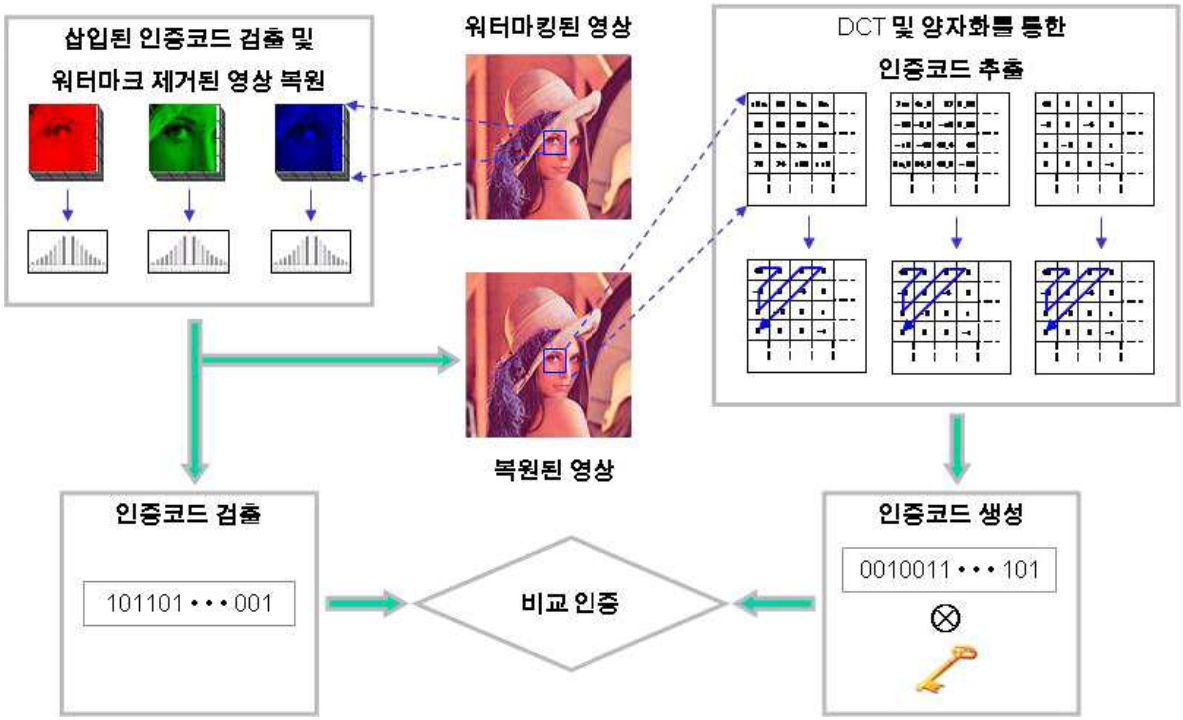
본 논문에서는 전체 영상을 16x16 크기의 블록으로 나누고, 각 블록에 인증코드를 삽입한다. 3.3절에서 설명하는 단일 블록에 대한 삽입 및 검출 알고리즘을 모든 블록에 적용하여 전체 인증코드 삽입 및 검출을 통한 인증을 수행한다.

삽입과정에서는 영상의 위변조에 대한 블록 단위의 인증을 수행하기 위하여 각 블록에 인증코드를 워터마킹 기법으로 삽입하여야 한다. (그림 1)에 도시한 것처럼 우선 원영상을 RGB 색상 채널로 분리한다. 분리된 채널을 16x16 크기의 블록 단위로 분할하고, 각각의 블록에 대하여 DCT 및 양자화 과정을 통하여 추출된 특징값을 비밀키와 XOR 연산하여 인증코드를 생성한다. 인증코드를 삽입하기 위하여 본 논문에서는 점진적 차이값 히스토그램 방법을 사용한다. 따라서 블록에 대한 점진적 차이값 히스토그램을 구성하고, 이를 수정하여 인증코드를 삽입한다. 수정된 히스토그램을 이용하여 블록의 픽셀값을 갱신한다. 이 과정을 각 채널별로 수행한 후 RGB 채널을 다시 병합하면 워터마크가 삽입된 영상을 얻을 수 있다.

검출과정에서는 워터마크 기법으로 인증코드가 삽입된 영상이 배포된 후, 공격자 및 외부적인 요인에 의한 손상 여부를 판단하기 위하여 인증과정이 필요하다. 워터마킹된 영상을 RGB 채널로 분리하여 16x16 크기의 블록 단위로 분할한다. 분할된 각 블록마다 점진적 차이값 히스토그램을 구성하게 되며, 이를 통해 삽입되었던 인증코드를 검출해 낼 수 있다. 인증코드를 검출한 뒤 원영상을 복원하기 위하여 차이값 히스토그램을 수정하여 워터마크를 제거한다. 히스토그램이 복원되었으므로 이를 이용하여 원영상 블록을 복원하게 되

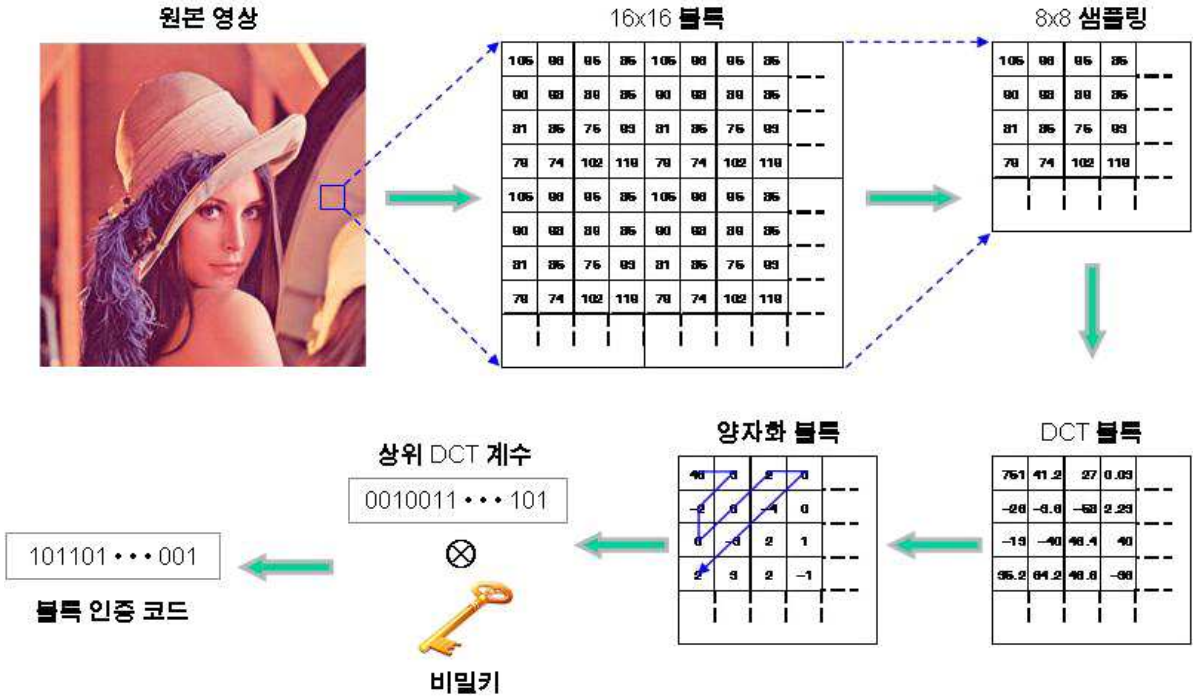


(그림 1) 전체 인증코드 삽입 절차



(그림 2) 전체 인증코드 검출 및 인증 절차

고, 각 채널마다 같은 과정을 반복하여 병합시키면 전체 원영상이 복원된다. 최초 인증코드는 원영상에 대하여 추출된 특징값이므로 복원된 원영상에 대하여 같은 DCT 및 양자화 과정을 거쳐서 특징값을 추출하고 비밀키와 XOR 연산을 수행한다. 이제 검출된 인증코드와 추출한 인증코드를 블록단위로 비교함으로써 손상에 대한 인증을 수행하게 된다. 만일 손상된 블록이 있다면 인증코드가 일치하지 않게되어 위변조라 판단할 수 있다. 전체 과정을 (그림 2)에 도시하였다.



(그림 3) 인증코드 생성 알고리즘

3.2 인증코드 생성 알고리즘

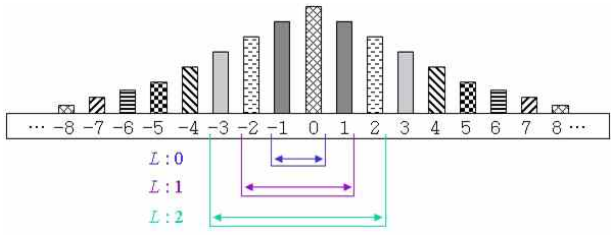
고성능의 인증률을 달성하기 위해서는 오탐지의 확률을 최소화하기 위한 충분한 길이의 인증코드를 사용하여야 하므로 각 블록에 대한 DCT 상위 계수들을 선택하여 인증을 위한 특징값으로 사용한다. 실험적으로 얻은 최적의 인증코드 길이는 8 Bytes로서 이것의 우연에 의한 오탐지 확률은 1/(2^64)가지 즉, 1/(1.84467E+19) = 5.42101E-20의 확률이므로 그 가능성은 거의 없다고 할 수 있을 것이다. 삽입해야 할 블록별 인증코드의 길이는 64 비트이므로 블록의 삽입가능 용량이 충분한지 확인하여야 한다. 8x8 블록으로 영상을 분할할 경우에는 삽입공간이 많이 부족하여 적절하지 않다는 것을 실험을 통하여 알아내었다. 따라서 본 논문에서는 (그림 3)과 같이 원영상을 16x16 크기의 블록으로 분할하고, 각 블록을 다시 8x8 크기로 평균값 샘플링을 한 뒤 DCT 및 양자화 과정을 수행하여 상위 8 Bytes의 계수를 선택하여 인증코드를 생성한다. 이 때, 만일 공격자가 영상의 색상정보를 일부 변화시키는 것이 아니라 블록보다 큰 크기의 영역을 완전히 잘라내기 공격을 하였을 때는 3.1절에서 설명한 알고리즘으로 인증을 수행하였을 때 해당 블록에서 검출한 인증코드와 계산된 인증코드가 0으로 같아지게 되어 올바른 인증을 수행할 수 없게 된다. 이 문제를 방지하기 위하여, 선택된 DCT 인증코드를 영상의 수신측과 공유된 비밀키와 XOR 연산을 수행하여 최종적인 인증코드를 생성한다. 비밀키는 인증기관을 통하여 발행된 키를 사용할 수도 있으며 또는 사용자 정보(user-specific code), 즉 사용자에 특화된 고유ID/비밀번호/기관코드/영상생성장치ID/타임코드 등을 응용목적에 따라 유연하게 사용할 수 있다.

3.3 단일 블록 인증코드 삽입 및 검출 알고리즘

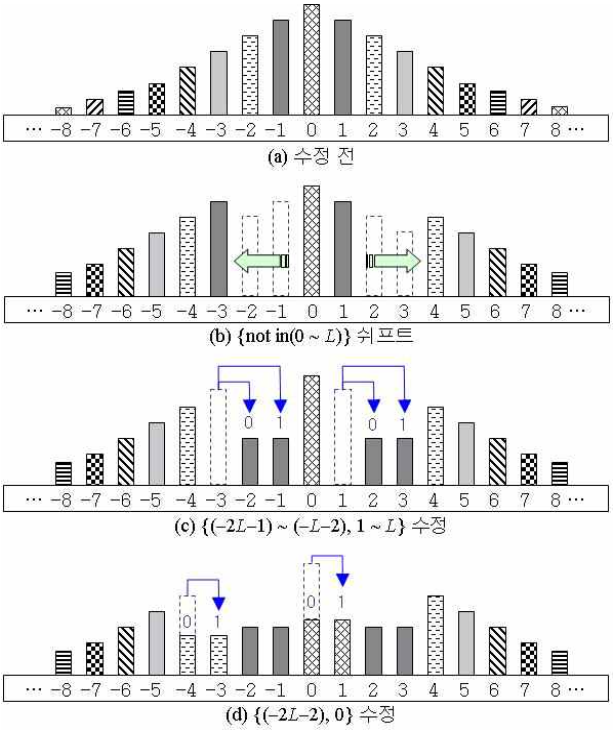
본 논문에서는 3.2절의 기법으로 생성된 인증코드를 각 블록에 삽입하고 검출하기 위하여 본 논문의 저자가 연구한 점진적 차이값 히스토그램 쉬프팅을 이용한 가역 워터마킹 알고리즘[21]을 변형하여 사용하였다. [21]의 연구는 영상에 기밀정보를 비가시적으로 삽입한 후 검출과정에서 원본으로의 완전한 복원이 가능한 가역 워터마킹 알고리즘으로서, 본 논문에서는 이를 응용하여 블록단위로 인증정보를 삽입하는데 이용하였다. 3.3.1절과 3.3.2절에서 각각 단일 블록에 대한 인증코드 삽입 알고리즘 및 검출 알고리즘을 설명한다.

3.3.1 단일 블록 인증코드 삽입 알고리즘

삽입되는 메시지의 용량 및 워터마크 영상의 품질은 응용분야의 요구에 따라 삽입레벨 L 로 조절한다. 0부터 시작되는 L의 값에 따라 차이값 히스토그램에서 메시지 삽입에 이용되는 빈은 0번 빈 주위인 {($-L$-1)~($+L$)}까지로서 (그림 4)에 나타내었다.



(그림 4) 메시지 삽입에 이용되는 히스토그램 빈



(그림 5) 인증코드 삽입과정에서의 히스토그램 수정 절차
(삽입레벨 L=1의 경우)

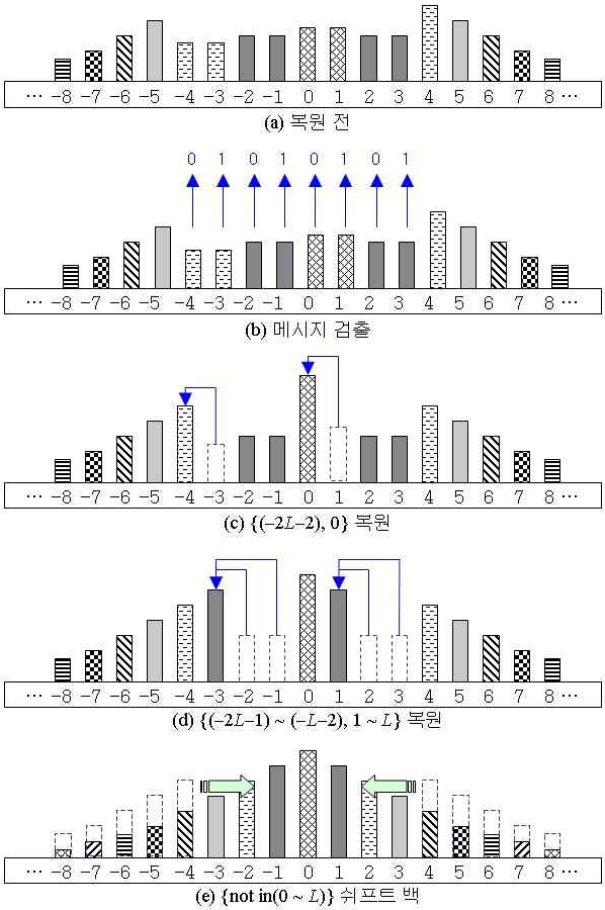
삽입레벨 L이 1인 경우 메시지가 삽입되는 과정에서 히스토그램이 수정되는 절차를 (그림 5)에 나타내었다. 먼저 원영상에 대하여 점진적으로 차이값 히스토그램을 구성한 후, 삽입공간을 확보하기 위하여 삽입에 이용되지 않는 빈들을 쉬프트한다. 다음으로 삽입할 메시지의 비트에 따라 히스토그램을 수정하고, 수정된 히스토그램을 반영한 은닉영상을 만들어 낸다.

3.3.2 단일 블록 인증코드 검출 알고리즘

삽입레벨 L이 1인 경우 메시지를 검출하고 원본영상을 복원하는 과정에서 히스토그램이 수정되는 절차를 (그림 6)에 나타내었다. 먼저 은닉영상에 대하여 점진적으로 차이값 히스토그램을 구성한 후, 메시지 삽입공간을 스캔하여 삽입된 메시지를 검출한다. 다음으로 메시지를 삽입하기 위하여 수정되었던 히스토그램을 복원하고, 공간확보를 위하여 쉬프트되었던 빈들을 복원한다. 마지막으로 복원된 히스토그램을 이용하여 원영상을 복원하게 된다.

4. 실험 및 성능 평가

본 논문에서 실험에 사용된 영상은 USC-SIPI(University of Southern California-Signal & Image Processing Institute) 이미지 데이터베이스의 8-Bits 컬러 512x512 영상 8 개 이며 (그림 7)에 나타내었다. 영상의 품질은 다음 수식 (1)과 수식 (2)를 통하여 계산된 PSNR(dB)로 측정하였다.



(그림 6) 메시지 검출 및 복원과정에서의 히스토그램 수정 절차
(삽입레벨 L=1의 경우)

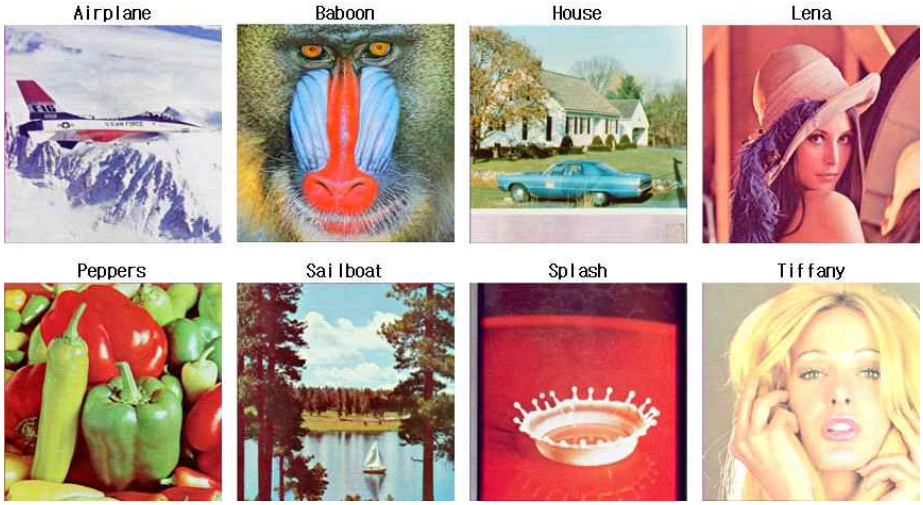
$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(p_{(i,j)} - p'_{(i,j)})^2 \qquad (1)$$

$$PSNR_{dB} = 10\log_{10}\frac{(2^n-1)^2}{MSE} \qquad (2)$$

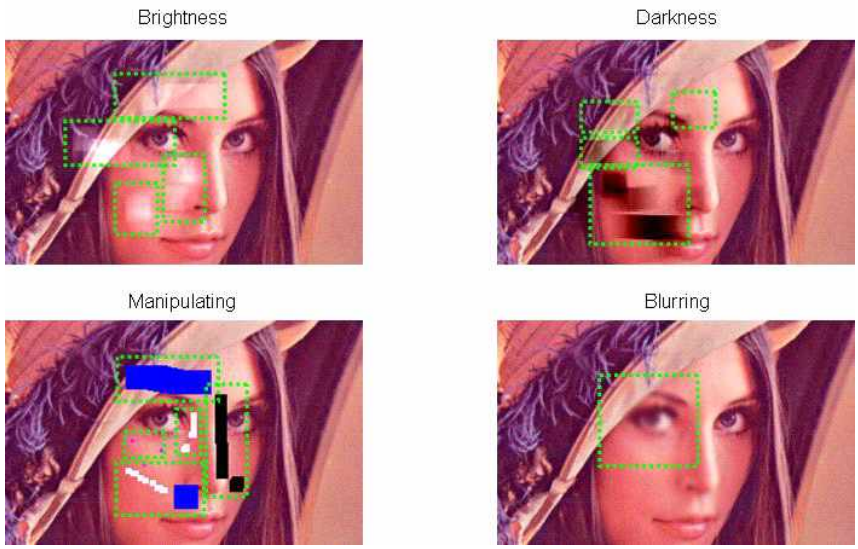
M 과 N 은 각각 영상의 가로 및 세로 크기이며, $p_{(i,j)}$ 는 원본 영상의 픽셀값, $p'_{(i,j)}$ 은 마크가 삽입된 영상의 픽셀값이고, n 은 한 픽셀을 표현할 때 필요한 비트의 수(Bit Depth)이다.

성능평가를 위하여 (그림 8)의 대표적인 공격방법인 “Brightness”, “Darkness”, “Manipulating”, “Blurring” 과 “Copy&Paste”에 대하여 실험하였다. 인텔 i5-450M 마이크로 프로세서와 MS Windows 7 개인용 컴퓨터 환경에서 Visual Studio C++ 6.0을 이용하여 성능을 측정하였다.

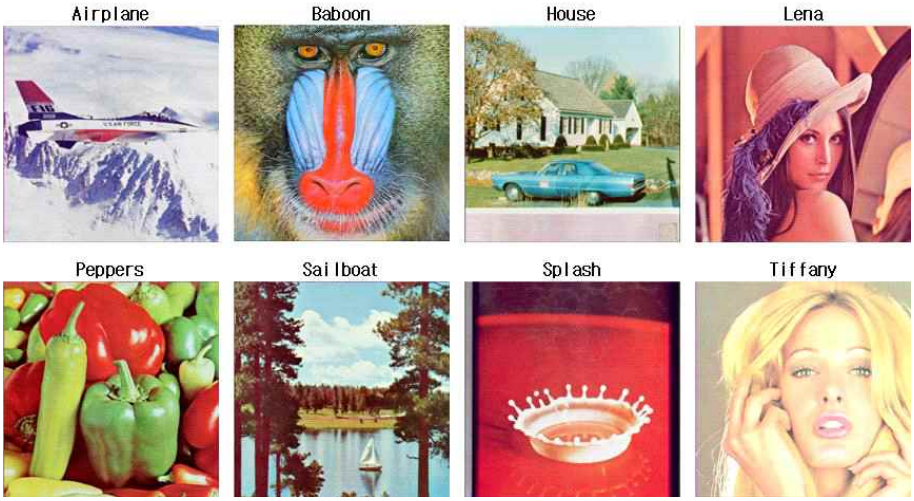
전체 인증코드를 삽입한 영상을 나타낸 (그림 9)를 통해 알 수 있듯이 영상의 변화를 인간의 시각적 능력으로 감지할 수 없다. 실험영상에 대하여 인증코드를 워터마킹한 결과를 <표 1>에 나타내었다. 시각적 품질인 PSNR은 평균



(그림 7) 실험 영상

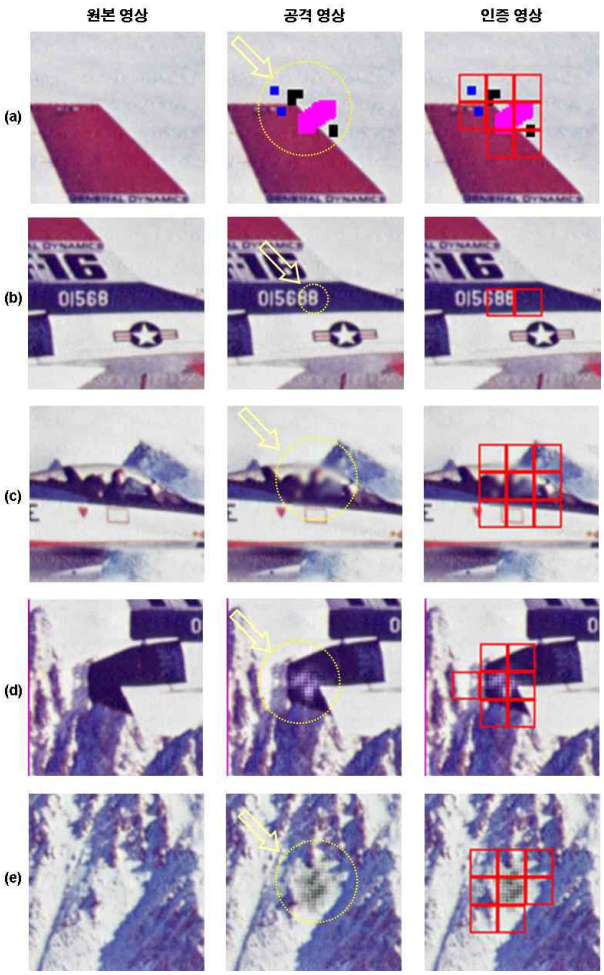


(그림 8) 공격의 종류



(그림 9) 인증코드 삽입된 영상

(그림 10) House 영상 인증 실험



(그림 11) Airplane 영상 인증 실험 확대: (a) Manipulating, (b) Copy&Paste, (c) Blurring, (d) Brightness, (e) Darkness

36 dB로 양호한 상태이다. 이 결과를 통해 알 수 있듯이, 제안한 영상 인증 가역 워터마킹 알고리즘의 성능은 영상 특성에 따라 조금씩 달라진다. 예를 들면, Splash처럼 저주파 성분을 더 많이 포함하고 있는 영상이 품질을 좋게 유지하면서도 높은 삽입용량을 얻을 수 있지만 Baboon처럼 고주파 성분이 많은 영상은 상대적으로 품질이 낮아진다는 것을 알 수 있다. 16x16 블록에 8 Bytes 씩 RGB 채널 각각에 삽입되었으므로 삽입용량은 0.75 bpp로 동일하다. 단일 채널에 대한 삽입용량은 0.25 bpp가 된다. 삽입과정에 걸린 시간은 평균 0.69초이며, 검출 및 인증에 걸린 시간은 평균 0.64초이다. 인증률은 97.7%로서 대부분의 손상 블록을 탐지할 수 있었다. (그림 10)은 House 영상에 대하여 실제 공격을 하였을 때 위변조를 탐지한 실험 결과 영상이며, (그림 11)은 Airplane 영상에 대한 인증결과를 확대한 것이다.

〈표 1〉 인증코드 워터마킹 성능평가 결과

영상	PSNR (dB)	Payload (bpp)	삽입 수행시간 (초)	인증 수행시간 (초)	인증률 (%)
Airplane	38.08	0.75	0.671	0.640	97.38
Baboon	28.56	0.75	0.733	0.640	98.68
House	34.80	0.75	0.686	0.639	96.04
Lena	35.45	0.75	0.687	0.656	97.89
Peppers	36.19	0.75	0.682	0.655	98.12
Sailboat	34.17	0.75	0.686	0.640	97.60
Splash	42.71	0.75	0.655	0.640	97.84
Tiffany	37.04	0.75	0.686	0.640	98.07
평균	35.88	0.75	0.69	0.64	97.70

5. 결 론

본 논문에서는 영상 콘텐츠의 무결성을 검증하기 위한 알고리즘으로서, 원본 영상을 16x16 크기의 블록단위로 분할하여 각 블록에 DCT 계수를 통한 인증코드를 삽입함으로써 공격자에 의한 손상여부를 인증할 수 있는 기법을 제안하였다. 인증코드를 삽입하는 알고리즘은 점진적 차이값 히스토

그램을 수정하는 방법을 이용하였다. 컬러영상의 RGB 색상 채널에 대하여 각각 인증함으로써 인증의 정확도를 높였다. 대표영상들을 이용하여 실험한 결과 시각적 품질을 유지하면서도 고속으로 인증코드를 삽입 및 검출/인증할 수 있음을 확인하였다.

본 논문에서 인증코드로 사용하는 16x16 블록단위의 DCT 계수를 통한 특징값 사용 방법은 오탐지 확률을 현저히 저하시킬 뿐만 아니라, 향후의 기능 추가를 위한 확장성이 좋다는 추가적 장점을 갖는다. DCT 계수를 통하여 손상 블록에 대하여 최대한 원본에 가깝도록 복원할 수 있다는 것과 함께, 동영상 압축에 대표적으로 사용되고 있는 16x16 크기의 매크로 블록과 동일한 블록 크기를 사용함으로써 동영상 인증기술로도 확장되어 질 수 있다.

기존의 많은 연구에서와 마찬가지로 영상에 대한 위변조 공격행위가 매우 미미할 경우, 예를 들어 블록내의 한 개의 픽셀만 밝기값을 1 만큼 조정할 경우 DCT 값의 변화가 없기 때문에 위변조를 탐지하지 못한다는 단점은 향후 지속적인 연구를 통하여 해결해야할 과제이다.

참 고 문 헌

[1] I. J. Cox, M. Miller, J. A. Bloom, J. Fridrich and T. Kalker, “Digital Watermarking and Steganography,” Morgan Kaufmann Publishers Inc., San Francisco, CA, 2007.

[2] M. Awrangjeb, “An Overview of Reversible Data Hiding,” Proc. of the Sixth International Conference on Computer and Information Technology, Jahangirnagar University, Bangladesh, pp.75-79, 2003.

[3] X. Q. Zhou, H. K. Huang, S. L. Lou, “Authenticity and integrity of digital mammography images,” IEEE Trans. Medical Imaging, Vol.20, No.8, pp.784-791, Aug., 2001.

[4] A. U. Rajendra, D. Anand, B. P. Subbanna, U. C. Niranjan, “Compact storage of medical images with patient information,” IEEE Trans. Information Technology in Biomedicine, Vol.5, No.4, pp.320-323, Dec., 2001.

[5] G.-J. Yu, C.-S. Lu, H.-Y. M. Liao, “Mean-quantization-based fragile watermarking for image authentication,” Optical Engineering, Vol.40, No.7, pp.1396-1408, Jul., 2001.

[6] K.-F. Li, T.-S. Chen, S.-C. Wu, “Image tamper detection and recovery system based on discrete wavelet transform,” IEEE Pacific Rim Conf. on Communications, Computers and Signal Processing, Vol.1, pp.164 - 167, Aug., 2001.

[7] P.-L. Lin, P.-W. Huang, A.-W. Peng, “A fragile watermarking scheme for image authentication with localization and recovery,” IEEE Sixth International Symposium on Multimedia Software Engineering, pp.146 - 153, Dec., 2004.

[8] C.-L. Wang, R.-H. Hwang, T.-S. Chen, H.-Y. Lee, “Detecting and restoring system of tampered image based on discrete wavelet transformation and block truncation coding,” 19th International Conference on Advanced Information Networking and Applications, 2005.

[9] P. L. Lin, C. K. Hsieh, P. W. Huang, “A hierarchical digital watermarking method for image tamper detection and recovery,” Pattern Recognition, Vol.38, No.12, pp.2519-2529, Dec., 2005.

[10] T.-Y. Lee, S. D. Lin, “Dual watermark for image tamper detection and recovery,” Pattern Recognition, Vol.41, No.11, pp.3497-3506, Nov., 2008.

[11] M.U. Celik, G. Sharma, A.M. Tekalp and E. Saber, “Lossless generalized-LSB data embedding,” IEEE Trans. on Image Processing, Vol.14, No.2, pp.253-266, 2005.

[12] S. Lee, C.D. Yoo and T. Kalker, “Reversible image watermarking based on integer-to-integer wavelet transform,” IEEE Trans. on Information Forensics and Security, Vol.2, No.3, pp.321-330, 2007.

[13] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. on Circuits and Systems for Video Technology, Vol.13, No.8, pp.890-896, 2003.

[14] D.M. Thodi and J.J. Rodriguez, “Expansion embedding techniques for reversible watermarking,” IEEE Trans. on Image Processing, Vol.16, No.3, pp.721-730, 2007.

[15] Z. Ni, Y.-Q. Shi, N. Ansari and W. Su, “Reversible data hiding,” IEEE Trans. on Circuits and Systems for Video Technology, Vol.16, No.3, pp.354-362, Mar., 2006.

[16] W.-C. Kuo, D.-J. Jiang and Y.-C. Huang, “Reversible data hiding based on histogram,” International Conference on Intelligent Computing, Lecture Notes in Artificial Intelligence, Vol.4682, Springer-Verlag, Qing Dao, China, pp.1152-1161, 2007.

[17] S.-K. Lee, Y.-H. Suh and Y.-S. Ho, “Lossless data hiding based on histogram modification of difference images,” Pacific Rim Conference on Multimedia, Lecture Notes in Computer Science, Vol.3333, Springer-Verlag, Tokyo, Japan, pp.340-347, 2005.

[18] P. Tsai, Y.-C. Hu and H.-L. Yeh, “Reversible image hiding scheme using predictive coding and histogram shifting,” Signal Processing, Vol.89, No.6, pp.1129-1143, 2009.

[19] K.-S. Kim, M.-J. Lee, H.-Y. Lee and H.-K. Lee, “Reversible data hiding exploiting spatial correlation between sub-sampled images,” Pattern Recognition, Vol.42, No.11, pp.3083-3096, 2009.

[20] D.-G. Yeo, H.-Y. Lee, B. M. Kim, K.-S. Kim, “Reversible Image Watermarking with Differential Histogram Shifting and Error Prediction Compensation,” Journal of KIISE : Software and Applications, Vol.37, No.6, pp.417-429, 2010.

[21] D.-G. Yeo, H.-Y. Lee, and B. M. Kim, “High Capacity Reversible Watermarking using Differential Histogram Shifting and Predicted Error Compensation,” Journal of Electronic Imaging, SPIE, Vol.20, No.1, 2011.

여 동 규

e-mail : sylot@kumoh.ac.kr

1999년 국립금오공과대학교 컴퓨터공학과 (학사)

2001년 국립금오공과대학교 컴퓨터공학과 (공학석사)

2010년 국립금오공과대학교 컴퓨터공학과 (공학박사)

2010년~현 재 국립금오공과대학교 모바일연구소 박사후연구원

관심분야 : 정보보호, 디지털워터마킹, 디지털포렌식 등

이 해 연

e-mail : haeyeoun.lee@kumoh.ac.kr

1997년 성균관대학교 정보공학과(학사)

1999년 한국과학기술원 전산학과(공학석사)

2006년 한국과학기술원 전자전산학과 전산학전공(공학박사)

2001년~2006년 (주)쎄트렉아이 선임연구원

2006년~2007년 코넬대학교 박사후연구원

2008년~현 재 국립금오공과대학교 컴퓨터공학부 교수

관심분야 : 멀티미디어, 영상처리, 콘텐츠보안, 디지털워터마킹 등