

# 가역 워터마킹 기술을 통한 JPEG 압축 영상의 무결성 인증 알고리즘

조 현 우<sup>†</sup> · 여 동 규<sup>††</sup> · 이 해 연<sup>†††</sup>

## 요 약

멀티미디어 콘텐츠는 디지털 데이터의 특성상 수정과 복제가 쉽고, 이에 따라 불법 유통과 위·변조 등의 문제가 발생할 수 있다. 최근 여러 분야에서 멀티미디어 콘텐츠 보안의 중요성이 높아지고 있고, 이러한 기술적 요구에 맞추어 다양한 멀티미디어 콘텐츠 보안 기술이 연구되고 있다. 본 논문에서는 JPEG 압축 표준에서 사용할 수 있는 가역 워터마킹 및 콘텐츠 인증 알고리즘을 제안한다. 영상의 샘플 블록을 이용하여 특징적인 인증 코드를 생성하고, JPEG 압축 과정 중 비손실 과정에서 보존되는 데이터를 이용해 히스토그램 쉬프팅 기법을 이용하여 인증 코드를 삽입한다. 디코딩 과정에서 영상 인증과 동시에 품질을 복원한다. 제안 알고리즘의 성능 평가를 위해 다양한 영상을 대상으로 품질과 압축률을 평가하였다. 삽입된 영상의 PSNR과 압축률은 각각 33.13dB과 90.65%로, 표준 인코딩 영상 대비 2.44dB의 PSNR 차이와 1.63%의 압축률 차이를 보였다.

키워드 : 무결성 인증, 가역 워터마킹, JPEG, 히스토그램 쉬프팅

## Integrity Authentication Algorithm of JPEG Compressed Images through Reversible Watermarking

Hyun-Wu Jo<sup>†</sup> · Dong-Gyu Yeo<sup>††</sup> · Hae-Yeoun Lee<sup>†††</sup>

## ABSTRACT

Multimedia contents can be copied and manipulated without quality degradation. Therefore, they are vulnerable to digital forgery and illegal distribution. In these days, with increasing the importance of multimedia security, various multimedia security techniques are studied. In this paper, we propose a content authentication algorithm based on reversible watermarking which supports JPEG compression commonly used for multimedia contents. After splitting image blocks, a specific authentication code for each block is extracted and embedded into the quantized coefficients on JPEG compression which are preserved against lossy processing. At a decoding process, the watermarked JPEG image is authenticated by extracting the embedded code and restored to have the original image quality. To evaluate the performance of the proposed algorithm, we analyzed image quality and compression ratio on various test images. The average PSNR value and compression ratio of the watermarked JPEG image were 33.13dB and 90.65%, respectively, whose difference with the standard JPEG compression were 2.44dB and 1.63%.

Keywords : Integrity Authentication, Reversible Watermarking, JPEG, Histogram Shifting

## 1. 서 론

하드웨어 및 소프트웨어의 발달로 인해 동영상, 사진, 음악, 출판문서 등의 멀티미디어 콘텐츠 생산과 보급이 확대

되었고, 관계된 서비스가 등장하면서 매년 그 시장 규모가 커지고 있다. 멀티미디어 콘텐츠는 전자적으로 저장, 유통되는 디지털 데이터의 특성상 콘텐츠의 복제와 변형이 쉽고, 따라서 위·변조와 불법적인 유통 문제가 발생하기 쉽다. 콘텐츠 시장의 규모가 커지고, 멀티미디어 데이터를 조작할 수 있는 고성능 하드웨어의 보급이 가속화 되면서 멀티미디어 콘텐츠에 적용 가능한 보안 기술의 중요도는 날이 갈수록 높아지고 있다.

의료, 군사, 예술 등 많은 분야에서 멀티미디어 데이터의 신뢰성과 보안성 등이 중요한 기준으로 요구된다. 감시카메

※ 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(2011-0005129).  
† 정 회 원: (주)에이티아이 연구원  
†† 준 회 원: 국립금오공과대학교 모바일연구소 박사후연구원  
††† 정 회 원: 국립금오공과대학교 컴퓨터소프트웨어공학과 교수(교신저자)  
논문접수: 2011년 10월 10일  
수정일: 1차 2011년 11월 22일  
심사완료: 2012년 1월 3일

라 영상이나 차량의 블랙박스 영상의 경우 조작으로 인해 인적, 물적 피해를 유발하거나 법적 증거자료로서의 기능을 잃을 수 있다. 의료용 영상의 경우 환자의 건강이나 생명과 직결될 수 있는 분야이므로 이러한 영상 데이터들은 높은 신뢰성이 요구된다[1].

디지털 워터마킹 알고리즘은 크게 강인성 워터마킹(Robust Watermarking) 알고리즘과 연성 워터마킹(Fragile Watermarking) 알고리즘의 두 종류로 분류된다. 강인성 워터마킹 알고리즘의 대부분은 영상 변형이나 왜곡 등으로 인해 영상이 공격을 받더라도 최대한으로 워터마크를 보호할 수 있는 방향으로 설계되었기 때문에 데이터의 은닉이나 보존을 위한 워터마킹 분야에 적절하다. 영상 인증을 위해 사용되는 워터마킹 알고리즘은 연성 워터마킹 알고리즘이 적합하다. 연성 워터마킹 알고리즘은 공격에 의해 쉽게 워터마크가 손상되어 영상의 원본 여부 인증에 유용하기 때문이다. 가역 워터마킹은 연성 워터마킹 기술의 하나로, 영상에 삽입한 워터마크를 제거하여 원본 영상을 일부 복원 또는 완전 복원이 가능하다. 기존의 영상 인증을 위하여 연구된 가역 워터마킹 기술들은 주로 압축이 적용되지 않은 영상에 대해 워터마크를 삽입하고 검출하는 방식이었는데, 이러한 방식은 영상의 압축 과정에서 워터마크가 쉽게 손상되는 단점이 있어 영상을 압축하여 저장하는 영상 포맷에 대해서는 적용하기 어려워 실용성이 떨어지는 문제가 있었다[2].

본 논문에서는 JPEG 영상 압축 표준에 적용할 수 있는 실용적인 영상 콘텐츠 무결성 보장을 위한 가역 워터마킹 기술을 제안한다. 영상 압축 저장 포맷에 적용 가능한 워터마킹 알고리즘을 적용하여 영상 콘텐츠의 신뢰성과 실용성을 동시에 보존할 수 있다.

이와 관련하여 2장에서는 현재까지 개발된 워터마킹 알고리즘과 영상 인증 기술에 대해 분석하고 JPEG 압축 표준에 대해 간단히 설명한다. 3장에서 JPEG 압축 프로세스 상에서 적용할 수 있는 워터마크 삽입 기술과 영상 인증 방법에 대해서 기술한다. 4장에서 알고리즘에 대한 실험 데이터를 제시하고 5장에서 결론을 내린다.

## 2. 관련 연구

### 2.1 영상 인증 기술

디지털 영상에서 데이터의 은닉과 보안성 유지를 위해 여러 가지 워터마킹 기술이 제안되었는데, 데이터의 은닉과 손실 영상 복원 등에 사용되는 워터마킹 알고리즘은 영상의 변형이나 공격에 강한 강인 워터마킹 알고리즘이 주로 사용되고, 인증 및 무결성 보장에는 작은 조작이나 공격에 쉽게 손상되는 연성 워터마킹 알고리즘이 사용된다.

Wong et al. 은 영상의 DCT 변환 영역에서 AC 성분들을 추출하여 워터마크 Host 벡터를 만들고, Logical XOR을 통해 이진 데이터로 구성된 워터마크를 삽입하는 기술을 제안하였다[3]. 블록 간에 고르지 않은 삽입용량 문제를 해결하기 위해 인접한 DCT 블록 데이터들 간의 AC 성분을 서

플링하여 삽입 용량을 평균화하였다. 하지만 이 방식은 압축률이 낮아질수록 저장 공간을 확보하기 어렵고, 워터마크 삽입용량에 비해 화질 저하가 많이 발생하며 가역성을 보장하지 못한다.

Shi et al. 에서는 JPEG 압축에서 영상 인증을 위한 기술로 특정한 비밀키를 이용하여 이진 랜덤 시퀀스로 구성된 워터마크를 생성하고 DCT 블록 데이터에 삽입하는 알고리즘을 제안하였다[4]. 하지만 하나의 DCT 블록에 대해 4비트의 워터마크를 삽입함으로써 워터마크의 중복성이 우려되어 알고리즘의 신뢰성이 낮고, DCT 계수의 LSB를 워터마크로 치환하여 워터마킹 기술의 가역성이 부족하다.

Zhou et al. 과 Rajendra et al. 에서는 의료용 영상에서 원본 여부를 검증하기 위한 인증 데이터나 환자 정보를 기록하기 위한 방법으로 LSB에 데이터를 삽입하는 방법을 제안하였다[5-6]. LSB 기반 워터마킹 알고리즘의 단점으로는 보안이 취약하다는 점이다. 픽셀 데이터의 LSB값을 단순히 워터마크 데이터로 치환하는 경우 LSB 데이터를 위조된 다른 영상에 복사하는 것만으로 쉽게 위변조가 가능하다.

Kang et al. 은 디지털 영상에서의 인증과 변형 검출 및 저작권 보호를 목적으로 하는 DWT기반 다중 워터마킹 기술을 제안하였다[7]. 영상의 변형 위치 검출을 위해 저주파 영역인 LL밴드의 LSB에 워터마크 정보를 삽입하고, 저작권 보호를 위해 고주파 부분의 웨이블릿 계수를 교환하여 워터마크 정보를 삽입하였다. Lin et al. 은 영상의 위변조 탐지 및 복구를 위한 계층적 데이터 은닉 기법을 제안하였다[8]. 하지만 이들 방법들은 워터마크를 삽입한 후 원본을 복구할 수 없는 비가역적 워터마킹 알고리즘이기 때문에 영상의 품질이 중요한 분야에서는 그 활용도가 떨어진다.

Kim et al. 은 영상의 히스토그램 보정을 이용하여 DCT 변환 영역 중 고주파 영역의 계수 조정을 통해 워터마크를 삽입하는 방식을 제안하였는데, 삽입 과정에서 명도 히스토그램에 대한 조정 과정을 거쳐 영상 전체에 대한 손실이 일어나고, 삽입한 워터마크를 삭제하고 원본을 복원하기 어려워 워터마킹 알고리즘의 가역성이 떨어지는 단점이 있다[9].

Emmanuel et al. 은 JPEG-2000 포맷에서 적용 가능한 가역 워터마킹 알고리즘을 제안하였다[10]. DWT 변환 영역 중 LL 영역의 2차원 서브밴드 계수에 대해 래스터 스캐닝을 통해 1차원 서브밴드 계수를 얻어내고, 이를 서브밴드 계수의 평균값과 가까운 랜덤값으로 임계치화하여 N 비트 길이의 상태를 생성한다. 상태 비트들에 대하여 특정한 상태 그룹 테이블(State group table)과 비교하여 두 그룹으로 나누고, 분류에 따라 워터마크 패턴을 결정한다. 이 방식은 가역 워터마킹으로 영상의 품질 복원은 가능하나, 비대칭 워터마킹 알고리즘으로 설계되어 삽입 워터마크와 추출 워터마크가 달라 삽입 워터마크의 보존이 필요한 분야에 적용하기에는 어려움이 따른다.

Zain et al. 은 그레이 채널 초음파 영상에 대해 영상 인증을 목적으로 하는 워터마킹 알고리즘을 제안하였다[11]. 이 방법은 워터마킹 영상이 JPEG 압축 과정을 거칠 때 워터마크가 보존될 수 있는 방법을 연구하였다. 영상의 관심

영역(ROI)를 설정하고, 전체 영상에 대해 SHA-256 암호화 알고리즘을 통해 256비트 길이의 해쉬 코드를 생성하여 워터마크로 사용한다. 비 ROI영역의 256개 8x8 블록에 대해 각 블록당 1비트의 워터마크를 삽입한다. 워터마크의 삽입은 각 블록의 LSB에 대해 수행되고, 워터마크의 추출 및 영상 복원을 위해 수신측에서 워터마크가 삽입된 블록의 위치에 대한 정보를 가지고 있어야 한다.

멀티미디어 콘텐츠는 필연적으로 데이터의 양이 크기 때문에 JPEG 압축 등 처리 과정을 포함하게 되고, 이와 같은 처리 과정은 워터마크의 측면에서 공격으로 간주되고, 이들 공격에 강인성을 확보한 영상 인증 기술들에 대한 연구가 진행되고 있다[4], [12]-[14].

### 2.2 가역 워터마킹 기술

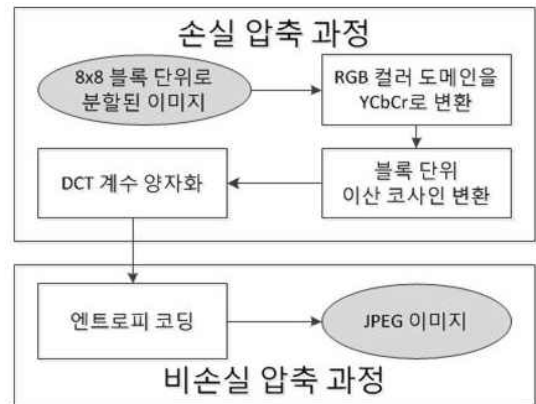
영상의 품질이 중요한 이슈가 되는 영상 콘텐츠를 위한 워터마킹 기술로는 주로 가역 워터마킹 기술이 이용된다. 가역 워터마킹 기술은 콘텐츠에 대한 원본 여부 인증이나 은닉 정보 추출 과정을 거친 후 콘텐츠의 원본 화질을 일부 또는 전부 복원할 수 있다. 가역 워터마킹에 대한 연구들은 지각적 투명성 및 완전한 가역성을 보장하기 위해 각기 다른 영상의 특징을 이용하여 메시지를 삽입한다. Caldelli et al. 은 기존 가역 워터마킹 기술들에 대하여 리뷰하고 개발된 기술들을 종류별로 분류하여 분석하였다[15].

Celik et al. 은 무손실 압축 기법을 사용하여 비트평면을 압축한 후 빈 공간에 메시지를 삽입하였으며, Lee et al. 은 주파수 영역에서의 변환 계수에 데이터를 삽입하였다 [16-17]. Cui et al. 은 JPEG 압축 과정 중 무손실 처리과정상의 데이터에 워터마크를 삽입하는 가역워터마킹 알고리즘을 제안하였는데, 삽입 과정에서 발생하는 화질 저하를 줄이기 위해 양자화 테이블에의 삽입영역을 제한하여 워터마크를 삽입하는 방식을 사용하였다[18]. 이 논문에서는 고정적인 영역에 대해 히스토그램 슈프팅을 이용해 삽입 가능한 용량과 그에 따른 화질 저하를 분석하였는데, 고용량 워터마킹 데이터를 삽입하기에 어려움이 따른다.

Yeo et al. 은 영상 전체에 대해 차이값 히스토그램 슈프팅 방식을 이용하여 워터마크를 삽입하는 기술을 제안하였다[19]. 하지만 차이값 히스토그램을 이용하는 방법은 삽입시 발생하는 오버플로우 및 언더플로우 문제에 대한 대안으로 부가적인 데이터의 은닉 또는 별도 전송을 필요로 한다. 또한 비압축 포맷 영상에 대한 기술로서 범용적으로 사용되는 JPEG 포맷 압축 파일 등을 지원하지 않는다.

### 2.3 JPEG 표준 압축 기술

JPEG 압축 알고리즘은 (그림 1)과 같이 크게 손실 압축 과정과 비손실 압축 과정의 2단계로 이루어진다. 손실 압축 과정은 색공간 변환, 이산 코사인 변환, 양자화 과정 등으로 구성되며, 데이터 손실이 발생하고, 비손실 압축 과정은 run-length encoding과 huffman coding이 포함된 엔트로피 부호화 단계로 구성되며 데이터 손실이 없다.



(그림 1) JPEG 압축 과정

#### 1) 손실 압축 단계

우선 각 픽셀의 RGB 데이터를 YCbCr 데이터로 변환한다. YCbCr 색공간은 NTSC나 PAL 방식의 컬러텔레비전 전송에 쓰이는 색공간과 유사하다. Y 성분은 픽셀의 휘도 정보를 가지고 있으며, Cb와 Cr 성분은 색상 정보를 가지고 있다. 사람의 눈이 색상 성분보다 휘도 성분에 더 민감하기 때문에 색상 정보를 더 많이 압축하기 위해서 YCbCr 색공간으로 변환한다. 색공간 변환 시 실수 연산이 일어나기 때문에 정보가 완전히 보존되지 않는다. 따라서 이후의 양자화 과정을 거치지 않더라도 원본과 완전히 일치하지 않는다.

JPEG 압축 알고리즘에서는 크로마 서브샘플링 과정을 통해 Cb와 Cr 성분의 수를 줄여 압축률을 높이는 과정이 있는데, 제안 알고리즘에서는 워터마크 삽입시의 저장용량과 워터마크 삽입 영상의 화질을 최대한 보존하기 위해 크로마 서브샘플링 과정을 생략한다.

전체 영상을 8x8 사이즈의 블록 단위로 나누고, 각각의 블록에 대해 이차원 이산 코사인 변환을 이용해 주파수 공간으로 변환한다.

사람의 눈은 고주파의 명도 변화에서는 그 구별능력이 떨어진다. 이 사실에 근거하여 주파수 영역의 각 성분에 대해 (그림 2)와 같은 특정한 양자화 테이블로 나누고 정수 몫만을 취함으로써 고주파 성분 정보의 많은 부분을 버릴 수 있다. 전체 JPEG 압축 단계 중 이 단계에서 가장 많은 데이터 손실이 발생한다. 이 단계를 거치면 대부분의 고주파 성분들은 0 또는 0에 근접한 양수, 혹은 음수가 된다.

16	11	10	16	24	40	51	61	17	18	24	47	99	99	99	99
12	12	14	19	26	58	60	55	18	21	26	66	99	99	99	99
14	13	16	24	40	57	69	56	24	26	56	99	99	99	99	99
14	17	22	29	51	87	80	62	47	66	99	99	99	99	99	99
18	22	37	56	68	109	103	77	99	99	99	99	99	99	99	99
24	35	55	64	81	104	113	92	99	99	99	99	99	99	99	99
49	64	78	87	103	121	120	101	99	99	99	99	99	99	99	99
72	92	95	98	112	100	103	99	99	99	99	99	99	99	99	99

(a) Luminance Quantization Table (b) Chrominance Quantization Table

(그림 2) JPEG 압축 과정에 사용되는 표준 양자화 테이블

2) 비손실 압축 단계

JPEG 압축의 기본 단위의 8x8 크기의 DCT 블록 데이터의 격자 성분들에 대해 zig-zag 정렬을 통해 저주파 성분에서 고주파 성분 순으로 정렬한 뒤 반복되는 0에 대해 run-length encoding을 적용하고, 그 결과에 대해 huffman coding을 수행한다. huffman coding 대신에 arithmetic coding도 가능하지만, 제안 알고리즘에서는 huffman coding을 이용한다.

3. 제안 알고리즘

JPEG 압축 알고리즘은 전 세계적으로 가장 많이 쓰이는 영상 압축 알고리즘 중의 하나이다. 본 논문에서는 JPEG 표준을 따르는 영상 압축 알고리즘에 적용할 수 있는 워터마킹 기법을 제안한다. 제안하는 워터마킹 기법은 연성 워터마킹 알고리즘으로, 영상에 대한 수정에 민감하여 워터마크가 쉽게 손상된다. 따라서 영상에 대한 수정 등의 공격이 발생하는 경우에 영상의 변형 여부를 탐지할 수 있다. JPEG 압축표준에서 압축률은 DCT 블록 데이터의 양자화시에 사용하는 양자화 테이블의 배수에 의해 결정되고, 따라서 영상을 일부 수정 후 재저장 또는 압축비를 변경 후 재저장 되게 되면 양자화된 DCT 블록 데이터에 삽입한 워터마크가 손상된다. 본 논문에서는 수정 및 위조 공격의 최종 단계에서 발생하는 영상 재저장시의 손상을 공격의 주요한 근거로 가정하고 영상의 변형을 탐지하게 된다.

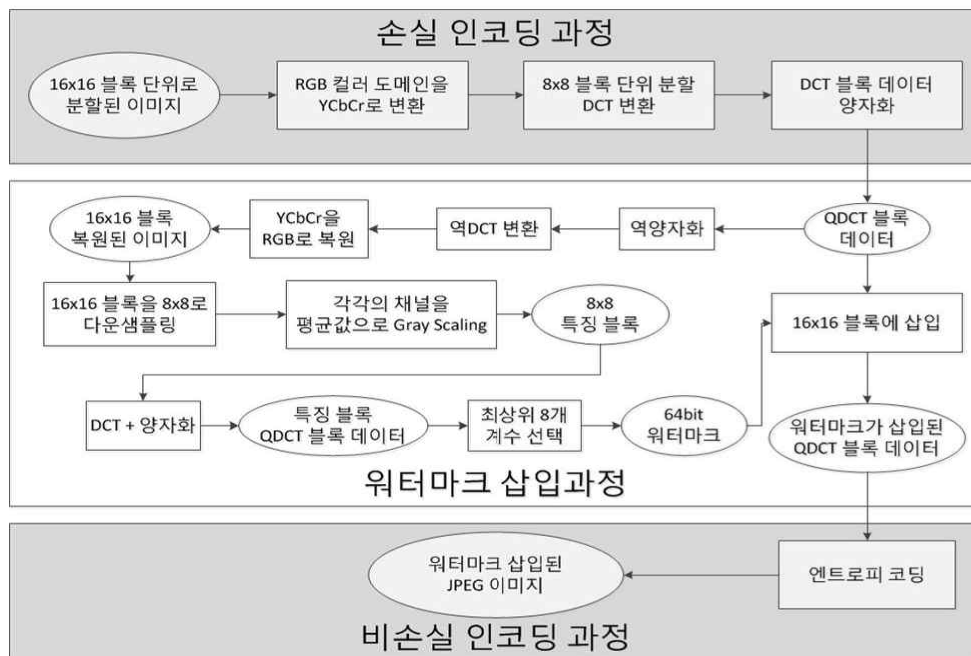
제안하는 알고리즘에 의해 생성된 JPEG 파일은 워터마크 삽입시 영상의 화질 저하나 변형이 크지 않다. 또한 JPEG

압축 과정의 전체적인 프로세스를 보존하면서 DCT 블록 데이터 조정을 통한 워터마킹 과정만 추가되었기 때문에 표준 JPEG 파일의 포맷이나 저장 구조에 영향을 주지 않는다. 따라서 제안 알고리즘을 통해 생성되는 JPEG 파일은 일반적인 영상 뷰어로 영상을 확인하거나 출력할 수 있다.

JPEG 압축알고리즘은 손실 압축 과정 후에 비손실 압축 과정을 거친다. 다시 말해 인코딩 과정에서 데이터 손실이 일어나는 손실 압축 과정을 거친 후의 데이터는 비손실 압축과정을 거쳐 디코딩 과정의 엔트로피 디코딩 과정까지 보존된다. 따라서 JPEG 압축과정 중 양자화가 끝난 데이터에 특정한 워터마크를 삽입하면 영상 압축과 동시에 삽입된 워터마크를 보존하는 것이 가능하다는 점에 착안하여 워터마크 삽입방식을 설계하였다.

3.1 워터마크 생성 및 삽입

JPEG 압축 방식의 기본 블록 사이즈는 8x8 픽셀이고, 제안 알고리즘의 영상 인증 방식은 16x16 픽셀 크기의 블록단위로 이루어진다. 인증률을 높이고 오탐지 확률을 최소화하기 위해서 충분한 길이의 워터마크를 사용해야 하는데, 64비트 길이의 워터마크를 사용할 경우 생성될 수 있는 워터마크의 종류는  $2^{64}$ 가지이므로 우연에 의해 오탐지될 확률은  $1/2^{64}$ , 즉 5.42101E-20로 현실적으로 거의 발생하지 않는다고 볼 수 있다[16]. 그러나 64비트 길이의 워터마크를 8x8 블록에 삽입할 경우 화질의 열화가 심하다는 것을 실험을 통하여 확인하였다. 따라서 본 논문에서는 16x16 블록단위로 워터마크를 생성한 후, 4개의 8x8 서브블록에 16비트씩 분할하여 삽입하는 방식을 사용한다. 워터마크 생성 및 삽입 전체 과정은 (그림 3)에 나타나 있다.



(그림 3) 워터마크 삽입 프레임워크가 추가된 JPEG 영상 인코딩 프로세스

DCT와 양자화를 거친 DCT 블록 데이터는 이전 단계에서 손실이 모두 일어난 상태이므로, 양자화된 DCT 블록(이하 QDCT 블록) 데이터의 히스토그램을 기반으로 워터마크를 삽입한다. 워터마크는 16x16 픽셀 단위의 영상 블록에 대해 DCT를 통하여 생성한다. DCT를 이용해 생성된 워터마크는 영상 일부의 손실이 일어날 경우 손실 영상에 대한 부분적인 복원에 활용될 수도 있다. 워터마크 생성은 Yeo et al. [16]의 방식을 적용한다.

1) 워터마크 생성

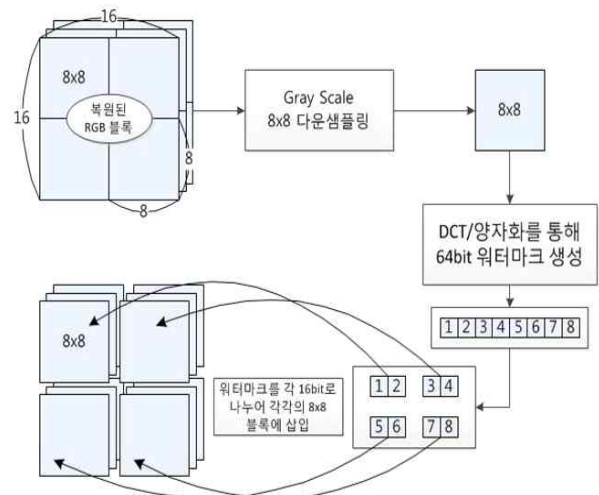
워터마크는 16x16 블록을 8x8 그레이 영상 블록으로 다운샘플링한 후 DCT를 통해 DCT 블록 데이터를 생성한 다음, 이를 양자화 하여 특징블럭에 대한 QDCT 블록 데이터를 얻어내고, 이에 대해 zig-zag 순으로 최상위 8개 값을 선택하여 64비트 워터마크를 생성한다. 워터마크 생성을 위한 DCT 블록 데이터 양자화에 사용되는 양자화 테이블은 JPEG 압축단계에서 Y 채널의 DCT 블록 데이터 양자화에 이용되는 luminance quantization table을 사용한다.

만일 영상의 일부가 공격을 통해 손상되었을 경우, 워터마크가 다른 블록에 보존된 상태라면 손상된 부분을 일부 복원하는데 이를 이용할 수 있다.

2) 워터마크 삽입

워터마크는 16x16 블록에 대해 생성되었고, JPEG 영상 압축은 8x8 블록 단위로 진행된다. 따라서 8x8 픽셀 크기의 블록 4개를 병합하여 하나의 인증 단위로 사용한다. 64비트 워터마크를 4개의 16비트 길이의 워터마크로 분할하여 16x16 블록을 구성하는 4개의 8x8 블록에 각각 삽입한다. 워터마크는 QDCT 블록 데이터에 히스토그램 쉬프팅 방식으로 삽입된다. 워터마크 분할과 히스토그램 쉬프팅에 의한 워터마크 삽입 방식은 (그림 4)와 (그림 5)에 나타나 있다.

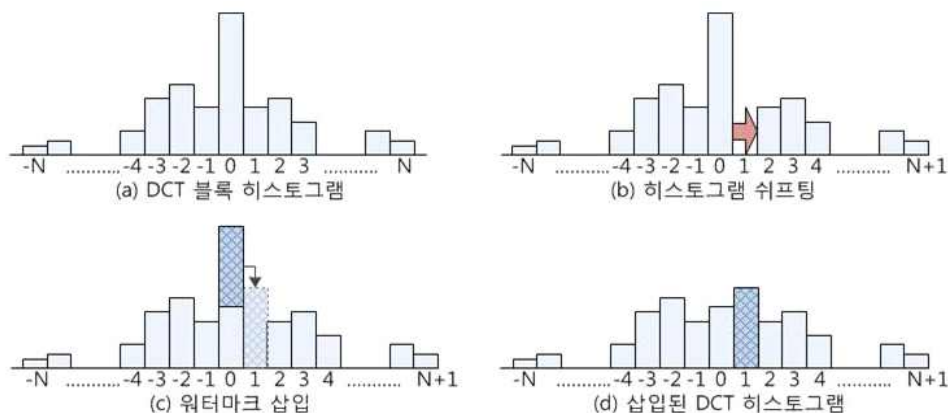
QDCT 블록 데이터에는 워터마크를 삽입하기에 충분한 수의 0이 존재한다. QDCT 블록 데이터를 구성하는 계수값 중 양수 값들을 쉬프팅 한 후, 원래 0과 1이 있던 자리에 워터마크를 삽입한다. 양자화 테이블을 구성하는 상수가 양자



(그림 4) 워터마크 생성, 분할 및 워터마크 삽입 과정

화 과정에서 화질 저하에 미치는 영향을 고려하여 Y, Cb, Cr 채널의 QDCT 블록 데이터에 각각 8, 4, 4개의 비트 패턴을 삽입한다. Cb, Cr 채널의 데이터를 저장하는 QDCT 블록 데이터는 양자화 시에 Y 채널보다 더 큰 양자화 값을 갖는 양자화 테이블을 사용하므로, 상대적으로 Y채널에 비해 QDCT 블록의 계수값을 수정했을 때 삽입 영상에 발생하는 열화가 높게 나타난다. 3개의 채널에 16비트의 워터마크 패턴을 삽입하기 위해 다양한 방법으로 비트 패턴 분배를 분석하였고, 평균적으로 가장 낮은 화질 열화를 보이는 8-4-4 분할 삽입방법을 선택하였다. 삽입시에 쉬프팅으로 인한 화질 저하를 최소화하기 위해 워터마크 삽입이 종료되는 위치까지의 양수 값들만 쉬프팅한다. 워터마크의 삽입은 다음의 규칙을 따른다.

- 1) QDCT 블록을 zig-zag 순서로 진행하며 삽입을 수행한다.
- 2) DC 성분은 삽입, 쉬프팅시에 제외한다.
- 3) 양수값은 우측으로 쉬프팅, 0 값을 수정하여 워터마크 비트패턴을 삽입하고, 음수값은 그대로 둔다.



(그림 5) DCT 블록 데이터 히스토그램 쉬프팅을 통한 워터마크 삽입 과정

- 4) 삽입이 종료된 이후의 양수 값들은 쉬프팅하지 않는다.
- 5) DC 성분은 삽입과 쉬프팅에서 제외한다.

QDCT 블록 데이터는 양자화 테이블 특성상 zig-zag 순서의 앞쪽에 올수록 화질에 미치는 영향이 적다. 따라서 워터마크는 삽입시에 zig-zag 순서에 따라 전방에서 후방 순으로 삽입된다. DC 성분은 화질 저하에 미치는 영향이 크고, 또 0이 발생할 확률이 적기 때문에 DC 성분은 제외하고 쉬프팅이나 삽입이 이루어진다. 워터마크는 0과 1의 비트패턴 형태로 QDCT 블록 데이터의 0 자리에 삽입되고, 삽입이 끝날 때 까지 발견되는 양수만 우측으로 쉬프트 하게 되고, 삽입되지 않는 위치의 계수값들은 조작하지 않는다. 그러므로 원래의 QDCT 블록 데이터에서 '워터마크 삽입이 완료되는 지점까지의 양수 성분'과 '워터마크 삽입 위치 중 1이 삽입되는 위치의 값'만 변경되므로 워터마크 삽입과정이 화질 저하에 미치는 영향은 미미하다. 워터마크 삽입과정은 수식 (1)을 따라 진행된다. ZQDCT는 zig-zag 순서로 배열된 QDCT 블록 데이터이다.  $wm_0$ 는 ZQDCT 데이터에 삽입될 워터마크이며, 0과 1의 이진 데이터로 구성된다.

JPEG 영상 압축 과정에서 QDCT 블록 데이터는 일반적인 압축비에서 최대 255를 넘지 않는 계수값이 발생한다. 또한 QDCT 블록 데이터는 엔트로피 인코딩 과정을 거친 후 파일로 저장하게 될 때 저장 비트수 기준 8비트를 초과하는 데이터를 허용하기 때문에 일반적인 워터마크 삽입 알고리즘에서 발생하는 오버플로우 문제는 발생하지 않는다. 따라서 오버플로우 맵과 같은 부가적인 정보의 저장 또는 전달이 필요하지 않다.

### 3.2 워터마크 추출, 영상 복원 및 인증

제안 알고리즘의 목적은 JPEG 포맷에서의 원본성을 보장하기 위한 알고리즘으로, JPEG 포맷의 영상을 재저장하게 되면 수정 프로그램에 따라 압축 과정에서 사용하는 양자화 테이블이나 프로그램에 따른 압축률의 차이 등으로 기존의 QDCT 블록 데이터가 변경되어 인증이 불가능해진다. 이러한 재저장 과정은 어떠한 공격 시나리오에서든 반드시 거쳐야 하므로 원본성이 훼손된 중요한 증거라고 간주할 수 있다. 제안 알고리즘에서 삽입된 워터마크는 재저장시에 영상

전체 부분에 걸쳐 손상되게 되므로 콘텐츠의 변조 및 위조 여부를 민감하게 판단할 수 있다.

영상의 인증 과정은 JPEG 디코딩 과정을 그대로 이용하되, 워터마크를 추출하는 부분과 비교용 워터마크를 재생성하는 부분, 그리고 QDCT 블록 데이터에서 워터마크를 제거하여 영상의 화질을 일반적인 JPEG 인코딩 영상의 수준으로 복원하는 부분이 추가된다.

JPEG 디코딩 과정은 인코딩 과정의 역순으로 진행되고, 비손실 압축의 복원 과정인 엔트로피 디코딩 과정을 거치면 워터마크가 삽입된 8x8 픽셀 크기의 QDCT 블록 데이터를 취득할 수 있다. 워터마크는 Y 채널에서 8비트, Cb와 Cr 채널에서 각각 4비트씩 총 16비트 워터마크를 추출한다. 16x16 픽셀 크기의 인증블록을 구성하는 4개의 8x8 픽셀 블록에서 추출된 16비트 워터마크를 조합하여 64비트 길이의 워터마크를 복원한다. 영상 인증 및 품질 복원 과정은 (그림 6)에 나타나 있다. 워터마크는 QDCT 블록 데이터에서 수식 (2)를 통해 추출된다.

영상의 원본성 입증을 위해 인코딩 과정에서의 워터마크 생성방식과 같은 방식의 워터마크 생성과정을 거쳐 비교용 워터마크를 재생성한다. RGB 영상으로 복원된 16x16 블록의 영상에 대해 DCT, 양자화 등의 과정을 거쳐 재생성된 비교용 워터마크와 추출된 워터마크를 비교하여 영상 인증을 수행한다.

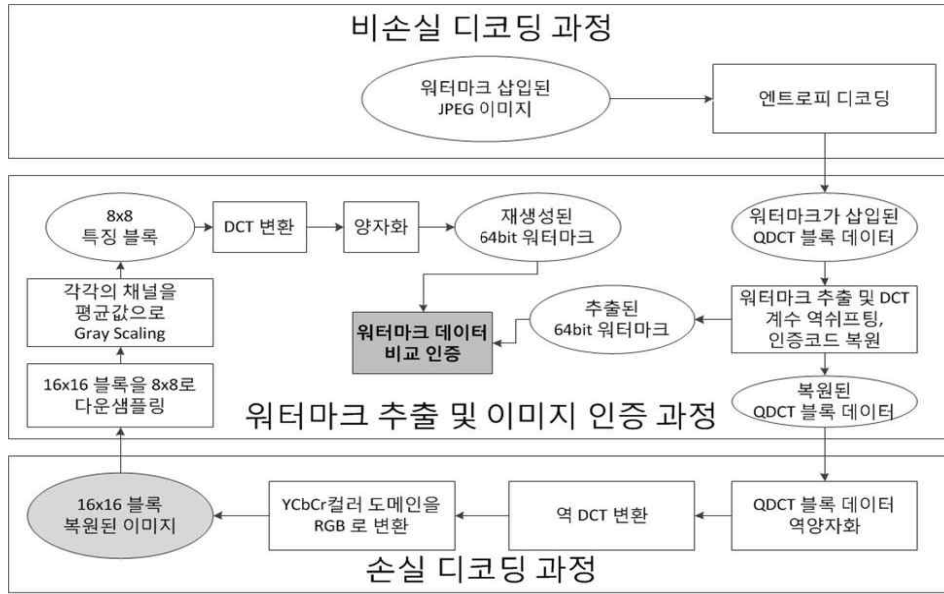
워터마크가 삽입된 QDCT 블록 데이터는 양수 값들을 히스토그램 상에서 역쉬프팅 하는 것으로 원래의 QDCT 블록 데이터를 복원할 수 있다. 따라서 삽입된 워터마크를 추출하는 과정과 동시에 워터마크가 삽입되지 않은 영상을 복원할 수 있다. 워터마크 삽입 과정에서 생성되는 워터마크는 워터마크가 삽입되지 않고 인코딩된 영상을 기준으로 생성되므로, 복원된 영상을 이용해 삽입과 동일한 과정으로 비교용 워터마크를 생성할 수 있고, 이를 추출된 워터마크와 비교하는 것으로 영상 인증을 수행할 수 있다. 정상적으로 워터마크가 삽입되어 인코딩된 영상은 추출된 워터마크와 재생성된 워터마크가 완전히 같아야 한다. 하지만 수정이나 압축 비율 변경 등의 공격을 통해 영상이 변경되면 추출된 워터마크와 재생성된 비교용 워터마크가 달라지고, 따라서 영상의 공격 여부를 판단할 수 있게 된다.

$$ZQDCTw_{(i)} = \begin{cases} ZQDCT_{(i)}, & \text{if } i = 0 \\ ZQDCT_{(i)}, & \text{if } ZQDCT_{(i)} < 0 \\ ZQDCT_{(i)} + 1, & \text{if } ZQDCT_{(i)} > 0 \\ ZQDCT_{(i)} + wm_{(j)}, & \text{if } ZQDCT_{(i)} = 0 \end{cases} \quad (1)$$

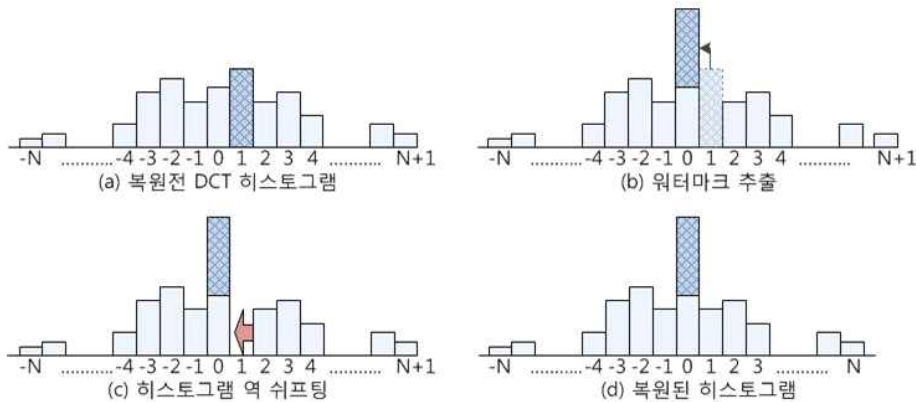
for  $0 \leq j \leq (\text{sizeof}(\text{watermark}) - 1)$ ,  $i = \text{index of Zig-zag reordering}$ .

$$wm_{(j)} = \begin{cases} \text{skip}, & \text{if } i = 0 \\ ZQDCTw_{(i)}, & \text{if } ZQDCTw_{(i)} \in \{0,1\} \end{cases} \quad (2)$$

for  $0 \leq j \leq (\text{sizeof}(\text{watermark}) - 1)$ ,  $i = \text{index of zig-zag reordering}$ .



(그림 6) 영상 인증 및 워터마크 제거를 통한 화질 복원



(그림 7) DCT 히스토그램 복원

제안 알고리즘은 가역 워터마킹 기반으로 개발되어 워터마크가 삽입된 JPEG 영상에서 워터마크를 제거하여 워터마크가 삽입되지 않고 압축된 JPEG 파일 수준의 화질로 복원할 수 있다. QDCT 블록 데이터에서 최상위 DC 성분을 제외한 나머지 성분들을 zig-zag 순으로 진행하면서 차례대로 조사하여, 삽입된 비트열 데이터가 채널당 삽입 개수만큼 추출될 때 까지 출현하는 양수를 (그림 7)와 같이 역 쉬프팅하여 워터마크 삽입전의 QDCT 블록 데이터로 복원한다. 엔트로피 디코딩과 인증 단계 이후의 역 양자화 과정과 역 DCT 등의 과정에서 복원된 QDCT 블록 데이터를 사용하여 워터마크가 삽입되지 않고 인코딩된 JPEG 파일 수준의 화질을 복원한다. 영상 복원은 수식 (3)을 따라 진행된다.

$$ZQDCT_{(i)} = \begin{cases} ZQDCTw_{(i)}, & \text{if } i = 0 \\ ZQDCTw_{(i)}, & \text{if } ZQDCTw_{(i)} < 0 \\ ZQDCTw_{(i)} - 1, & \text{if } ZQDCTw_{(i)} > 0 \end{cases} \quad (3)$$

for  $i = \text{index of Zig-zag reordering}$ .

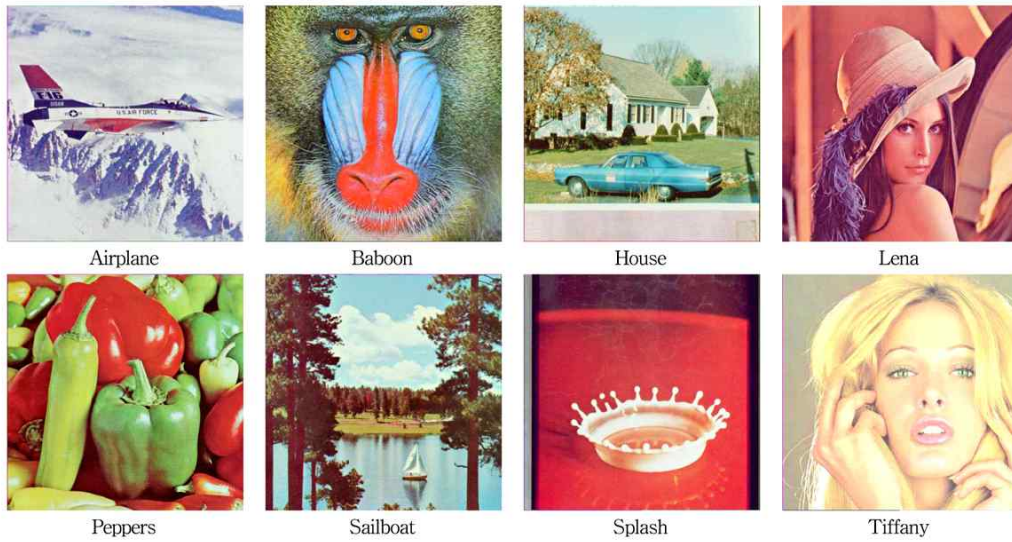
#### 4. 실험 결과

##### 4.1 워터마크 삽입 및 미삽입 JPEG 영상의 화질 비교

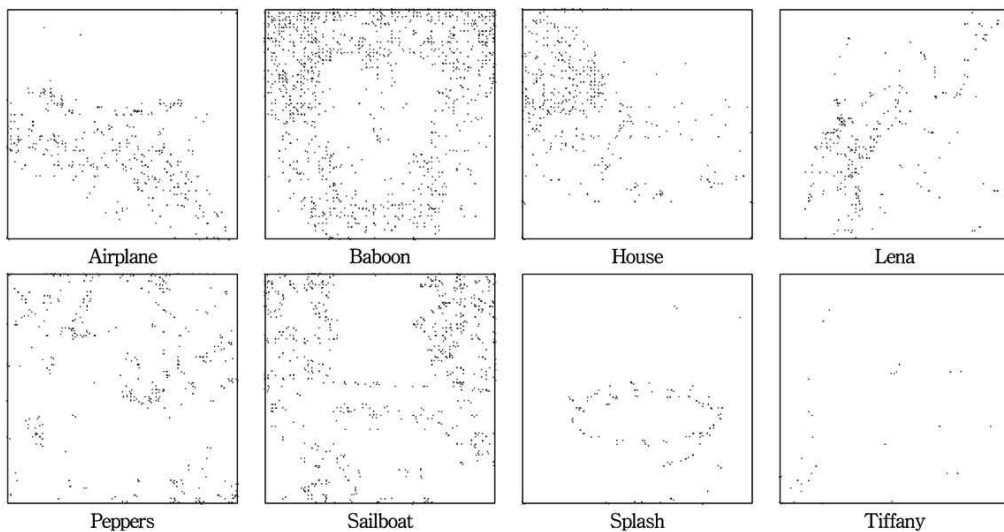
본 논문에서 제안한 알고리즘의 성능 실험을 위해 USC-SIPI(University of Southern California-Signal & Image Processing Institute) 영상 데이터베이스의 8비트 컬러 512x512 사이즈 영상 8개를 사용하였으며 JPEG 포맷으로 압축된 영상을 (그림 8)에 나타내었고, 워터마크 삽입 JPEG 영상과 미삽입 JPEG 영상의 차영상을 (그림 9)에 나타내었다. 압축 영상과 워터마크 삽입 영상의 품질은 수식 (4)과 수식 (5)를 통해 계산된 PSNR(dB)로 측정하였다.

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (p_{(i,j)} - p'_{(i,j)})^2 \quad (4)$$

$$PSNR_{dB} = 10 \log_{10} \frac{(2^n - 1)^2}{MSE} \quad (5)$$



(그림 8) JPEG 압축 영상



(그림 9) 워터마크 삽입 JPEG 영상과 미삽입 JPEG 영상의 차영상

<표 1> 워터마크 삽입 압축 영상과 미삽입 압축 영상의 PSNR 비교 (단위 : dB)

영상	삽입영상	미삽입영상	차이
Airplane	34.33	37.68	3.35
Baboon	30.31	31.64	1.33
House	32.95	35.66	2.71
Lena	33.75	36.34	2.59
Pepper	33.02	35.16	2.14
Sailboat	31.82	33.55	1.73
Splash	35.18	38.42	3.24
Tiffany	33.68	36.13	2.45
평균	33.13	35.57	2.44

변수  $M$ 과  $N$ 은 각각 영상의 너비와 높이를 나타내고,  $p_{(i,j)}$ 는 원본 영상,  $p'_{(i,j)}$ 는 열화된 영상을 나타낸다. 워터마크가 삽입된 영상과 삽입되지 않은 영상은 실제로 아주 미세한 차이를 보이며, 육안으로 확인하기 어려운 정도의 화질 저하가 나타난다. (그림 9)에 제시된 차영상은 노이즈 발생 위치 확인을 위해 노이즈 픽셀 밝기를 조정하였다.

또한 가역 워터마킹 알고리즘을 사용하였으므로, 워터마크 추출후에 JPEG 알고리즘을 사용하여 압축된 파일 수준의 품질을 100% 복원할 수 있었다. 영상의 JPEG 압축과 워터마크 삽입시의 화질 차이를 <표 1>에 나타내었다.

미삽입 영상의 JPEG 압축시의 영상 품질은 원본대비 80~85%의 품질을 유지한다. 삽입 영상에 대해 8비트 3채널 컬러 영상에서 8x8 픽셀당 16비트 데이터를 삽입하였고, 더 많은 용량의 데이터를 삽입할 수 있으나 삽입 영상의 화질



이 저하되게 된다. 워터마크 삽입시에 일어나는 압축영상의 화질 저하는 PSNR을 기준으로 평균적으로 2.44dB로 크게 저하되지 않는다.

4.2 워터마크 삽입 및 미삽입 JPEG 영상의 압축률 비교

제안 알고리즘은 JPEG 영상 압축 방식에서 사용하기 위한 워터마크 삽입 방식으로, 워터마크를 삽입한 후의 영상 압축률 또한 성능평가 척도가 될 수 있다. 압축률은 원본 영상의 비트맵 포맷 파일과 변환된 JPEG 포맷 파일의 헤더 정보를 포함한 용량을 비교하였다.

미삽입 영상의 JPEG 압축률은 원본대비 92.27%의 압축률을 보인다. 워터마크를 삽입한 영상의 경우 평균적으로 90.65%의 압축률을 보여 압축 성능이 크게 저하되지 않음을 <표 2>를 통해 보여 주고 있다. 워터마크 삽입 과정에서 양자화된 DCT 블록 데이터에 포함되는 0의 개수가 적어지므로 비손실 압축 과정 중 run-length encoding 코딩의 특징에 의해 압축 성능 또한 삽입 데이터의 용량이 커질수록 저하될 수 있다.

<표 2> 워터마크 삽입 압축 영상과 미삽입 압축 영상의 원본대비 압축률 비교

영상	삽입영상	미삽입영상	차이
Airplane	92.27%	93.77%	1.50%
Baboon	84.79%	86.69%	1.90%
House	90.26%	91.84%	1.58%
Lena	92.11%	93.77%	1.66%
Pepper	91.18%	92.90%	1.72%
Sailboat	89.37%	91.07%	1.70%
Splash	93.19%	94.59%	1.40%
Tiffany	92.00%	93.55%	1.55%
평균	90.65%	92.27%	1.63%

5. 결 론

본 논문에서는 가역 워터마킹을 이용하여 압축 영상에 대한 무결성을 인증하는 알고리즘을 제안하였다. 제안하는 워터마킹 알고리즘은 JPEG 압축 표준을 기반으로 JPEG 압축 과정에서 삽입하여 활용할 수 있어 높은 활용도가 기대되며, 수정 후 재저장 공격에 민감하여 원본성 및 무결성을 확실하게 판단해 낼 수 있다.

특히, 샘플링된 영상 블록의 DCT 블록 데이터 일부를 워터마크로 사용하여 다른 영상 블록에 삽입함으로써 해당 영상 블록의 손상 시에 다른 영상 블록에 삽입된 워터마크를 검출하여 부분적인 복원이 가능하다. 일반적인 영상편집 프로그램을 써서 영상의 일부분을 변경 후 재압축 및 재저장을 하게 되면 워터마크 삽입된 영상의 모든 블록을 변경하기 때문에, 삽입된 모든 워터마크가 손상되어 부분적인 인증이 불가능하고, 영상 전체가 변경된 것으로 인증한다.

마지막으로, 가역 워터마크 방식을 적용하였기 때문에 삽입된 워터마크를 제거하여 워터마크가 삽입되지 않고 압축된 JPEG 파일 수준의 화질을 복원할 수 있다.

차후에는 블록 간 유사성을 활용한 워터마크 삽입 방식 및 삽입 도메인 등에 대한 연구를 통하여 정량적인 품질을 향상할 필요가 있다.

참 고 문 헌

- [1] F. Mintzer, J. Lotspiech, and N. Morimoto, "Safeguarding digital library contents and users: digital watermarking," D-Lib Magazine, 1997.
- [2] 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.
- [3] P. H. W. Wong, C. Andy, and O. C. Au, "On improving the iterative watermark embedding technique for JPEG-to-JPEG watermarking," Proc. of the International Symposium on Circuits and Systems, pp.161-164, 2004.
- [4] X. Shi, F. Liu, D. Gong, and J. Jing, "An Authentication Watermark Algorithm for JPEG images," Proc. of the International Conference on Availability, Reliability and Security, pp.584-588, 2009.
- [5] X. Q. Zhou, H. K. Huang, and S. L. Lou, "Authenticity and integrity of digital mammography images," IEEE Trans. Medical Imaging, Vol.20, No.8, pp.784-791, Aug., 2001.
- [6] A. U. Rajendra, D. Anand, B. P. Subbanna, and U. C. Niranjana, "Compact storage of medical images with patient information," IEEE Trans. Information Technology in Biomedicine, Vol.5, No.4, pp.320-323, Dec., 2001.
- [7] 강태환, 장호현, 김동서, 주낙근, "이미지 인증과 변형 검출을 위한 DWT기반 다중워터마킹," 한국콘텐츠학회 2005 추계종합 학술대회 논문집, Vol.3, No.2, pp.480-484, 2005.
- [8] P. L. Lin, C. K. Hsieh, and 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.
- [9] 김효철, "히스토그램 보정을 이용한 고신뢰성 영상 인증 기법," Journal of Korea Multimedia Society, Vol.13, No.7, pp.1088-1094, July, 2010.
- [10] S. Emmanuel, H. C. Kiang, and A. Das, "A Reversible Watermarking Scheme for JPEG-2000 Compressed Images," Proc. of the IEEE International Conference on Multimedia and Expo, pp.69-72, 2005.
- [11] J. M. Zain and M. Clarke, "Reversible Watermarking Surviving JPEG Compression," Proc. of the International Conference of IEEE Engineering in Medicine and Biology Society, Vol.4, pp.3759-3762, 2005.

[12] A. Shiozaki, M. Iwata, and A. Ogihara, "Reversible Watermarking Method for JPEG Image," IEICE Trans. on Information and Systems, Vol.E91-D, No.7, pp.2068-2071, 2008.

[13] X. Wang, J. Wang, and H. Peng, "A Semi-fragile Image Watermarking Resisting to JPEG Compression," Proc. of the International Conference on Management of e-Commerce and e-Government, pp.498-502, 2009.

[14] H. Wang and C. Liao, "Compressed-domain fragile watermarking scheme for distinguishing tampers on image content or watermark", Proc. of the International Conference on Communications, Circuits and Systems, pp.480-484, 2009.

[15] R. Caldelli, F. Filippini, and R. Becarelli, "Reversible Watermarking Techniques: An Overview and a Classification," EURASIP Journal on Information Security, Vol.2010, Article ID. 134546, 2010.

[16] 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.

[17] 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.

[18] 최학남, 김종원, 최종욱, 김학일, "JPEG 압축 영역에서의 리버서블 워터마킹", 정보처리학회논문지, Vol.17, pp.121-130, 2007.

[19] 여동규, 이해연, "차이값 히스토그램 기반 가역 워터마킹을 이용한 블록 단위 영상 인증 알고리즘", 정보처리학회논문지, Vol.18-B, No.6, 2011.



**조 현 우**

e-mail : hwjo@kumoh.ac.kr  
 2010년 국립금오공과대학교 컴퓨터공학부  
 소프트웨어공학전공 (학사)  
 2012년 국립금오공과대학교 컴퓨터소프트  
 웨어공학과(공학석사)  
 2012년~현 재 (주)에이티아이 연구원

관심분야: 멀티미디어, 영상처리, 디지털워터마킹 등



**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)셋트랙아이 선임연구원

2006년~2007년 코넬대학교 박사후연구원  
 2008년~현 재 국립금오공과대학교 컴퓨터소프트웨어공학과  
 교수

관심분야: 멀티미디어, 영상처리, 콘텐츠보안, 디지털워터마킹 등