JPEG 압축 표준에서 이미지 무결성 인증을 위한 워터마킹 알고리즘

조현우*, 여동규*, 이해연*
*국립금오공과대학교 소프트웨어공학과
e-mail:hwjo@kumoh.ac.kr

Watermarking Algorithm to Authenticate Image Integrity on JPEG Compression

Hyun-Wu Jo*, Dong-Gyu Yeo*, Hae-Yeoun Lee*
*Dept. of Software Engineering, Kumoh National Institute of Technology

요 약

멀티미디어 콘텐츠는 디지털 데이터의 특성상 위·변조 또는 불법유통 등의 문제가 발생할 수 있다. 특히 의료 및 군사, 예술 분야 등 많은 부분에서 멀티미디어 데이터의 보안성이 중요한 이슈가 되고 있다. 본 논문에서는 이러한 기술적 요구에 맞추어 이미지의 무결성을 인증할 수 있는 워터마킹 알고리즘을 제안한다. 제안하는 알고리즘은 JPEG 이미지 압축 과정에서 추가적인 처리를 통해 이미지에 인증코드를 삽입하고, 디코딩 과정에서 삽입 인증코드 추출 및 비교 인증코드 재생성을 통해 이미지의 원본 여부를 블록 단위로 판단할 수 있다. 제안 알고리즘을 통해 생성된 JPEG 이미지 표준 인코딩 이미지 대비 2.44dB 의 화질 저하를 보였고 1.63%의 압축률 차이를 보였다.

1. 서론

멀티미디어 콘텐츠는 디지털 데이터의 특성상 복제와 수정을 통한 재생산이 쉽고, 따라서 위·변조와 불법적인 유통 문제가 발생하기 쉽다. 의료, 군사, 예술 등 많은 분야에서 멀티미디어 데이터의 신뢰성과 보안성 등이 중요한 기준으로 요구된다. 감시카메라 영상이나 차량 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 높은 신뢰성이 요구된다. 이러한 기술적 요구에 맞추어 이미지의 무결성과 순수성을 확인하는 워터마킹 알고리즘이 연구되어지고 있다.

기존에 연구된 대부분의 가역 워터마킹 알고리즘은 압축을 고려하지 않고 설계되어 영상 압축이 적용되는 이미지 포맷에서는 실용성이 떨어졌다. 본 논문에서는 JPEG 영상 압축 표준에 적용할 수 있는 이미지 무결성 인증을 위한 워터마킹 기술을 제안한다. 2장에서는 현재까지 개발된 워터마킹 알고리즘과 인증코드 생성기술에 대해 분석하고, 3장에서는 본 논문에서 제안하는 워터마크 삽입 기술과 인증코드 생성 방법에 대해서 기술한다. 4장에서 알고리즘에 대한 실험 데이터를 제시하고 5장에서 결론을 내린다.

· 본 연구는 문화체육관광부 및 한국저작권위원회의 2011년도 저작권기술개발사업의 연구결과로 수행되었음.

2. 관련 연구

이미지의 무결성 인증에는 작은 조작이나 공격에도 쉽게 손상되는 연성 워터마킹 알고리즘이 주로 사용된다.

Zhou et al. [1]과 Rajendra et al. [2]에서는 의료용 영상에서 원본 여부를 검증하기 위한 인증 데이터나 환자 정보를 기록하기 위한 방법으로 LSB에 데이터를 삽입하는 방법을 제안하였지만 쉽게 위변조가 가능하다는 단점이 있다. Lin et al. [3]은 영상의 위·변조 탐지 및 복구를 위한 계층적 데이터 은닉 기법을 제안하였다. 하지만 이들 방법들은 비가역적 워터마킹 알고리즘이기 때문에 영상의 품질이 중요한 분야에서는 그 활용도가 떨어진다.

가역 워터마킹 기술은 콘텐츠에 대한 원본 여부 인증이나 은닉 정보 추출 과정을 거친 후 콘텐츠의 원본 화질을 일부 또는 전부 복원할 수 있다. Celik et al. [4]은 무손실 압축 기법을 사용하여 비트평면을 압축한 후 빈 공간에 메시지를 삽입하였으며, Lee et al. [5]은 주파수 영역에서의 변환 계수에 데이터를 삽입하였다. Yeo et al. [6]은 영상의 점진적 차이값 히스토그램을 이용하여 데이터를 삽입하는 알고리즘을 제안하였다. 하지만 차이값 히스토그램을 이용하는 방법은 삽입시 발생하는 오버플로우 문제에 대한 대안으로 부가적인 데이터의 은닉 또는 전송을 필요로 한다.

3. 제안 알고리즘

JPEG 압축 알고리즘은 전 세계적으로 가장 많이 쓰이는 이미지 압축 알고리즘 중의 하나이다. 본 논문에서는 JPEG 표준을 따르는 이미지 압축 알고리즘에 적용할 수 있는 워터마킹 기법을 제안한다. JPEG 이미지의 경우 이

미지를 일부 수정 후 재저장 또는 압축 비율 변경 후 재저장 하게 되면 양자화 된 데이터에 삽입한 워터마크 데이터가 손상된다. 본 알고리즘은 이미지가 재저장 되는 상황을 수정 및 위조 공격이라 가정하고 원본 또는 수정본 임을 판단하게 된다.

제안하는 워터마킹 알고리즘은 16x16 영상 블록에 대해 다운샘플링과 이산 코사인 변환을 이용하여 64bit의 고유한 인증 코드를 생성하여 주파수 도메인의 히스토그램을 기반으로 인증코드를 삽입하고 추출한다. 제안 알고리즘에 의한 JPG 이미지 파일은 JPEG 압축 포맷과 호환되므로 전용 뷰어가 필요치 않다.

3.1. 워터마크 삽입 알고리즘

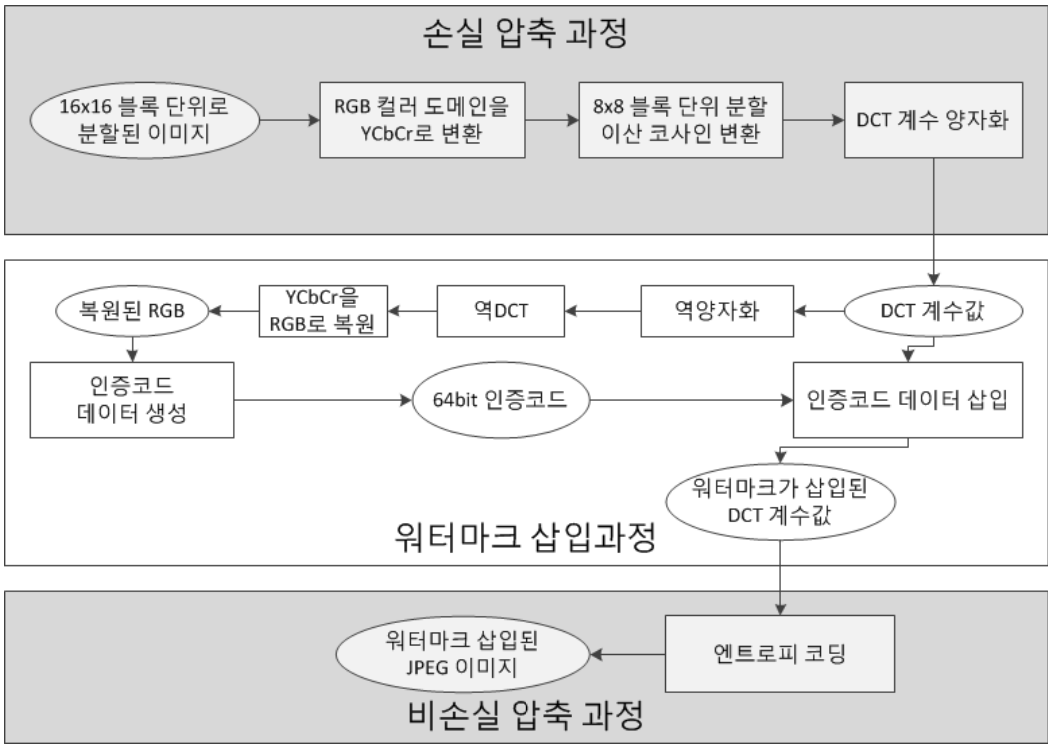
JPEG 압축 알고리즘에서, 손실압축 과정을 거친 후의 데이터는 비손실 압축과정에서 보존 된다. 따라서 JPEG 압축과정 중 양자화가 끝난 데이터에 특정한 워터마크를 삽입하면 영상 압축과 동시에 삽입된 워터마크를 보존하는 것이 가능하다.

워터마크 삽입 알고리즘의 전체적인 과정은 (그림 1)에 나타나 있다. 기존의 JPEG 압축 표준과의 호환성을 고려하여 JPEG 인코딩/디코딩 과정 중간에 인증코드의 생성과 삽입, 추출 및 인증 과정이 추가되었다. 워터마크 데이터의 보존을 위해 손실 압축과정과 비손실 압축 과정 사이의 중간 데이터에 워터마크를 삽입한다.

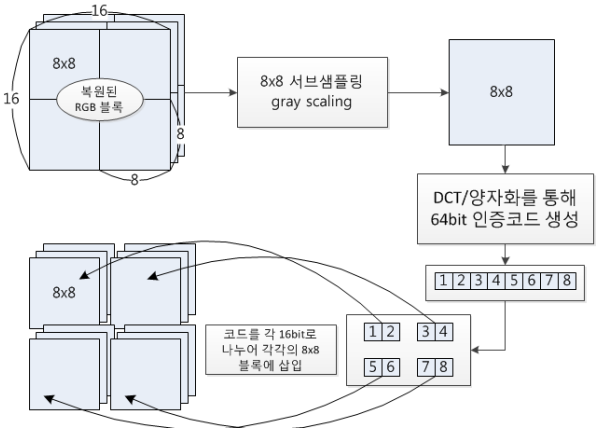
DCT와 양자화를 거친 DCT 블록 데이터는 이전 단계에서 손실 과정을 모두 마친 상태이므로, 양자화된 DCT 블록 데이터의 히스토그램 데이터를 기반으로 인증코드를 삽입한다. 인증코드는 16x16단위의 이미지 블록에 대해 DCT 변환을 이용하여 생성한다. DCT변환을 이용해 생성된 인증코드는 손실 영상에 대한 복원에 이용할 수도 있다. 인증코드 생성 방식은 Yeo et al. [6]의 인증코드 생성방식을 적용하였다.

인증코드는 16x16 블록을 8x8 그레이 이미지 블록으로 다운샘플링한 후 이산 코사인 변환을 통해 양자화 된 DCT 계수를 얻어내고, 이에 대해 zig-zag 순으로 최상위 8개 값을 선택하여 64bit 길이의 인증코드로 사용한다. 인증코드 생성을 위한 양자화 테이블은 Y채널의 DCT 블록 양자화에 이용되는 Luminance Quantization Table을 사용한다.

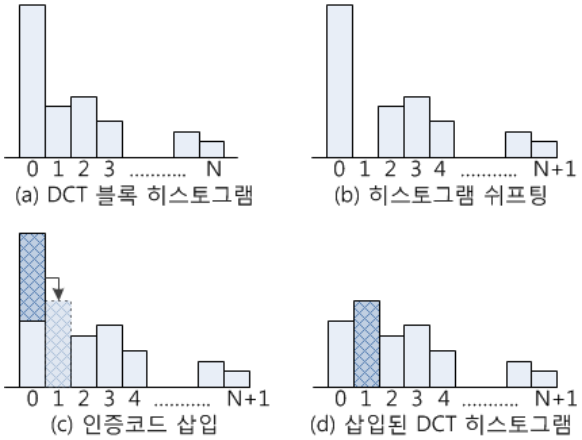
64bit의 인증코드 데이터를 4개의 16bit 데이터로 분할하여 16x16 블록을 구성하는 4개의 8x8 블록에 각각 삽입한다. 분할 삽입 과정은 (그림 2)에 나타나있다. 인증코드 데이터 삽입 방식은 (그림 3)처럼 양자화된 DCT 블록 데이터에 Histogram Shifting 방식으로 삽입된다.



(그림 1) 워터마크 삽입 과정이 추가된 JPEG 인코딩 프로세스



(그림 2) 인증코드 생성 및 분할 삽입



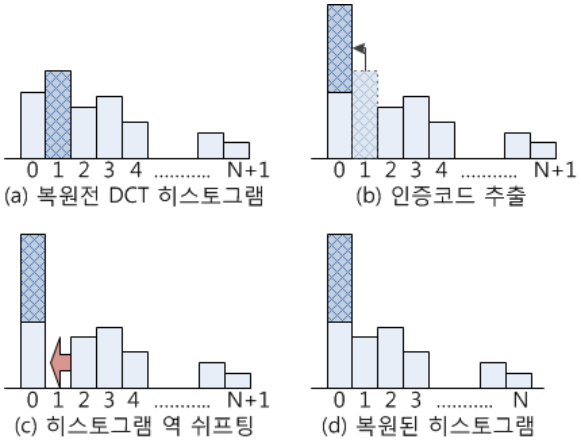
(그림 3) DCT 블록 히스토그램 쉬프팅을 통한 워터마크 데이터 삽입 과정

DCT 블록 데이터를 구성하는 계수값 중 양수 값들을 쉬프팅 한 후, 원래 0이 있던 자리에 0과 1로 구성된 비트 패턴을 삽입한다. Y, Cb, Cr 채널의 DCT 블록 데이터에 각각 8, 4, 4개의 비트 패턴을 삽입한다. 삽입시에 이미지의 변형을 최소화하기 위해 인증코드 데이터가 삽입되는 위치까지의 양수 값들만 쉬프팅한다.

JPEG 이미지 압축 과정에서 양자화된 DCT 블록 데이터는 일반적인 압축비에서 최대 255를 넘지 않는 계수값이 발생한다. 또한 DCT 블록 데이터는 파일로 저장시에 저장 비트수 8비트 이상의 데이터를 허용하기 때문에 일반적인 이미지 워터마크 삽입 알고리즘에서 발생하는 오버플로우 문제는 발생하지 않는다. 따라서 오버플로우 맵과 같은 부가적인 정보의 저장 또는 전달이 필요하지 않다.

3.2 워터마크 검출 및 인증 알고리즘

제안 알고리즘의 목적은 JPEG 포맷에서의 이미지 원본성을 검증하기 위한 것으로, JPEG 포맷의 이미지를 재 저장하면 사용한 도구에 따라 압축 과정에서 사용하는 양자화 테이블이나 압축률의 차이 등으로 인하여 기존의 DCT 계수 데이터가 변경되어 인증이 불가능해진다. 이러한 이



(그림 4) DCT 히스토그램 복원

미지 재저장 과정은 어떠한 공격 시나리오에서든 반드시 거쳐야 하므로 이미지의 원본성이 훼손된 중요한 증거라고 가정한다. 제안 알고리즘에서 삽입된 워터마크는 재저장시에 이미지 전체 부분에 걸쳐 손상되게 되므로 원본/위조본 여부를 민감하게 판단할 수 있다.

이미지의 인증 과정은 JPEG 디코딩 과정을 그대로 이용하되, 인증코드를 추출하는 부분과 비교용 인증코드를 재생성하는 부분, 그리고 수정되었던 DCT 값들을 복원하는 부분이 추가된다.

JPEG 디코딩 과정은 인코딩 과정의 역순으로 진행되고, 비손실 압축의 복원 과정인 엔트로피 디코딩 과정을 거치면 워터마크가 삽입된 8x8픽셀 크기의 양자화된 DCT 블록 데이터를 취득할 수 있다. 인증코드 데이터는 Y채널에서 8비트, Cb 와 Cr 채널에서 각각 4비트씩 총 16비트 데이터를 추출한다. 4개의 블록에서 각각 추출된 16비트 데이터를 조합하여 64bit 인증코드를 추출한다.

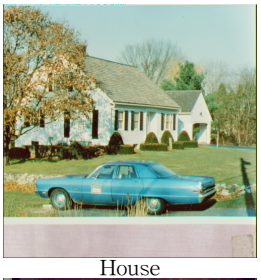
이미지의 원본성 입증을 위해 인증코드 삽입과정과 같은 방식의 인증코드 생성과정을 거쳐, 비교용 인증코드를 재생성한다. 추출된 인증코드와 재생성된 비교용 인증코드를 비교하여 이미지 인증을 수행한다.

제안 알고리즘은 또한 가역 워터마킹 알고리즘으로서, 워터마크가 삽입된 JPEG 이미지 파일에서 인증코드를 제거하여 워터마크가 삽입되지 않고 압축된 JPEG 이미지 파일 수준의 화질로 복원할 수 있다.

zig-zag 순으로 나열된 DCT 블록 데이터에서 최상위 DC성분을 제외한 나머지 성분들을 차례대로 조사하여, 삽입된 비트열 데이터가 채널당 삽입 개수만큼 추출될 때 까지 출현하는 양수를 (그림 4)와 같이 역 쉬프팅하여 삽입 전 데이터로 복원하여 워터마크가 삽입되지 않고 압축된 JPEG 이미지 수준의 화질을 복원한다.

4. 실험 및 성능 평가


Airplane


House


Peppers


Splash

(그림 5) 실험에 사용된 이미지

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

이미지	삽입	미삽입	차이값
Airplane	34.33	37.68	3.35
House	32.95	35.66	2.71
Peppers	33.02	35.16	2.14
Splash	35.18	38.42	3.24
평균	33.13	35.57	2.44

본 논문에서 실험에 사용된 영상은 USC-SIPI 이미지 데이터베이스의 8-bit 컬러 512x512 사이즈 영상 4개이며, (그림 5) 에 나타내었다. 압축 영상과 워터마크 삽입 영상의 품질은 PSNR(dB)로 표시하였다.

인증코드를 삽입한 영상은 시각적으로 미세한 노이즈 상태를 보이나, 영상을 육안으로 식별하는데 문제가 없다. 또한 가역 워터마킹 알고리즘을 사용하여 JPEG 알고리즘 수준의 품질로 복원할 수 있다. 워터마크를 삽입하였을 때와 삽입하지 않았을 때의 JPEG 이미지의 화질 차이를 <표 1>에 나타내었다.

JPEG 압축시의 영상 품질은 원본대비 80% 수준의 품질을 유지하였다. 삽입 이미지에 대해 8bit 3채널 컬러이미지에서 8x8픽셀당 16bit의 데이터를 삽입하였고, 더 많은 용량의 데이터를 삽입할 수 있으나 삽입 이미지의 화질이 저하되게 된다.

워터마크 삽입시에 일어나는 압축영상의 화질 저하는 PSNR을 기준으로 평균적으로 2.44dB로 크게 저하되지 않았음을 확인할 수 있다.

제안 알고리즘은 JPEG 이미지 압축 방식에서 사용하기 위한 워터마크 삽입 방식으로, 워터마크 데이터를 삽입한 후의 영상 압축률 또한 성능평가의 척도가 될 수 있다. 워터마크 삽입영상의 압축률은 삽입하지 않은 이미지에 비하여 평균 1.63%의 압축률 하락을 보였다.

5. 결론

본문에서 제안하는 워터마킹 알고리즘은 JPEG 압축 과정에 삽입하여 활용할 수 있어 높은 활용도가 기대된다. 또한 수정 후 재저장 공격에 민감하여 이미지의 원본성 및 무결성을 인증할 수 있다. 또한 샘플링된 이미지 블록의 DCT 계수를 인증코드로 사용하여 인증코드 삽입 위치에 따라 이미지 손상시에 부분적인 복원이 가능하다.

하지만 제안하는 알고리즘에서 사용하는 워터마크 삽입 방식은 이미지 재압축 및 재저장 공격에 민감하기 때문에 정당하게 일부 수정 후 저장하더라도 이미지 전체 영역의 인증코드 데이터가 손상되어 부분적인 인증이 불가능하다. 현재의 방식으로는 이미지 재압축 및 재저장 시 기존에 존재하는 DCT 블록 데이터와 인증코드 데이터를 보존할 수 없다. 따라서 영상의 부분적인 인증과 손상 복원 등을 가능하게 하기 위해서는 추가적인 연구가 필요하다.

참고문헌

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 여동규, 이해연, "차이값 히스토그램 기반 가역 워터마킹을 이용한 블록 단위 영상 인증 알고리즘", 정보처리학회논문지, 2011 (accepted)