영상 위·변조 검출과 인증을 위한 Fragile 워터마킹

김미애, 송근실, 이원형
중앙대학교 첨단영상대학원 영상공학과
e-mail:kimma@dreamwiz.com

Fragile Watermarking for Image Tamper-Proofing and Authentication

Mi-Ae Kim, Geun-Sil Song, Won-Hyung Lee
Dept of Image Engineering Graduate School of A.I.M.
Chung-Ang University

요 약

본 논문에서는 디지털 영상의 인증 및 무결성을 위한 Fragile Watermarking 기법을 제안한다. 이 기법은 원 영상과 워터마크 영상을 각각 랜덤하게 섞고, 랜덤수와 LUT를 이용하여 워터마크를 LSB에 삽입하므로 보안성을 갖는다. 또한, 워터마크 삽입·추출과정에서 두 개의 비밀키와 XOR를 이용하여 간단히 처리할 수 있다. 실험을 통하여 영상의 변형 여부 및 조작 위치를 검출하였다.

1. 서론

최근 통신 기술의 발달과 인터넷의 대중화로 멀티미디어 정보의 유통이 활성화 되고 있다. 디지털화된 미디어 데이터는 복사가 용이하고 원본과 구별할 수 없으며, 편집이 가능한 이점이 있으나 악의적인 목적으로 소프트웨어를 이용하여 손쉽게 위·변조를 할 수 있다. 이에 따라 영상의 인증과 조작을 판별하기 위한 효율적인 방법이 요구되고 있다.

본 논문에서는 영상의 변형 여부 및 조작 위치를 검출하는 디지털 영상에 대한 인증(Authentication)과 무결성(Integrity)을 위한 Fragile Watermarking 기법을 제안한다. Fragile Watermarking은 약간의 변형에도 쉽게 깨지는 워터마킹 기법으로 영상의 변형 유·무와 조작된 위치를 검출할 수 있기 때문에 영상의 위·변조를 방지할 수 있다. 이것은 주로 법정 증거 자료, 상업적인 용도 그리고 저널 자료에 활용되고 있다[1]. 일반적으로 효과적인 영상의 인증과 무결성을 위해서는 다음의 조건을 만족해야 한다[2-3]. 첫째는 영상의 변형 여부를 판단할 수 있어야 하고, 둘째는 영상의 조작 위치를 검출할 수 있어야 하며, 셋째는 원 영상 없이도 검출이 가능해야 하며,

넷째는 삽입된 워터마크는 비가시적이어야 한다.

기존의 Fragile Watermarking에 대한 연구를 공간영역에 워터마크가 삽입되는 방법을 중심으로 살펴보면, Yeung과 Mintzer[4]는 LUT(Look-Up Table)을 이용하여 영상의 인증 및 무결성을 확인하였으나, 동일한 워터마크와 LUT를 여러 영상에 적용하는 경우 공격에 노출된다[5]. Wong과 Memon[6]은 해쉬 함수와 암호화 시스템을 이용하여 영상의 변조 여부와 위치를 파악하였으나, 조작 위치의 검출이 블록 단위이고 매 블록마다 MD5와 RSA 알고리즘을 수행하므로 속도면에서 효율적이지 못하다. 공간적 영역이 아닌 주파수 영역에 워터마크를 삽입하는 방법으로 DCT(Discrete Cosine Transform) 영역[2]과 DWT(Discrete Wavelet Transform) 영역[7]을 이용하는 기법이 있다.

본 논문에서는 상기에서 다룬-공간영역에 워터마크를 삽입하는 방법들-문제를 해결하기 위한 기법을 제안한다. 즉, 원 영상의 각 픽셀을 랜덤하게 뒤섞고, 이진 Gray 값과 Key 값으로 XOR를 한 후, LUT을 참조하여 워터마크를 픽셀의 LSB(Least Significant Bit)에 삽입한다. 실험 결과로 영상 조작에 대한 변조 여부 및 위치를 검출할 수 있었다.

2. 제안한 방법

그레이 영상을 기준으로 워터마크를 삽입·추출하며, 워터마크는 이진 로고 영상을 사용한다. 두 개의 비밀키(K_1, K_2)를 생성하여 한 개는 영상의 픽셀들을 랜덤하게 만드는데 사용하고 다른 한 개는 이진 픽셀 값과 XOR 연산하는 값을 생성하는 Seed로 사용한다. 워터마크 영상도 랜덤하게 섞는다. LUT은 0~127값을 이진(0 또는 1)으로 변환하는데 이용한다.

2.1 워터마크 삽입

워터마크 삽입 과정은 다음과 같다.

1단계: - 비밀키 K_1을 이용하여 원 영상의 모든 픽셀을 랜덤하게 섞는다.
- 워터마크 영상은 원 영상과 같은 크기(워터마크 영상이 원 영상보다 작은 경우는 반복하여 똑같은 크기로 만들어 사용할 수 있다)로 만들고 역시 무작위로 섞는다.

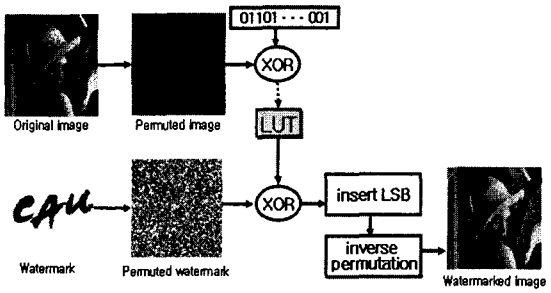
2단계: 비밀키 K_2를 이용하여 영상 크기(MxN) 개수의 이진 랜덤수를 생성한다.

3단계: 각 픽셀의 LSB를 제외한 7bit와 2단계에서 생성한 랜덤수를 XOR 연산한다. 이 때, 랜덤수는 한번 연산에 7개가 사용되는데, 다음 연산은 하나씩 뒤로 이동을 하고, 끝에서는 다시 첫 번째 랜덤수부터 반복하여 사용한다.

4단계: LUT을 참조하여 3단계의 연산 결과(0~127)에 해당하는 이진 값을 구한다.

5단계: 4단계의 결과와 워터마크의 픽셀 값을 XOR 연산하여 LSB에 삽입한다.

3단계에서 5단계 과정을 모든 픽셀에 차례대로 수행한다.

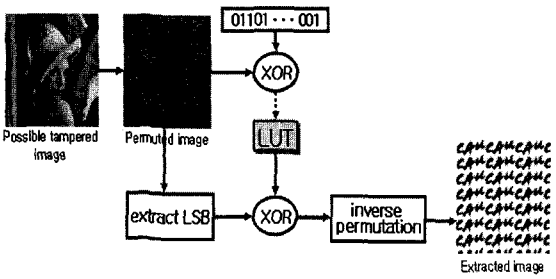


(그림 1) 워터마크 삽입 과정

6단계: 랜덤하게 뒤섞인 영상을 원래 영상으로 복구한다.

2.2 워터마크 추출

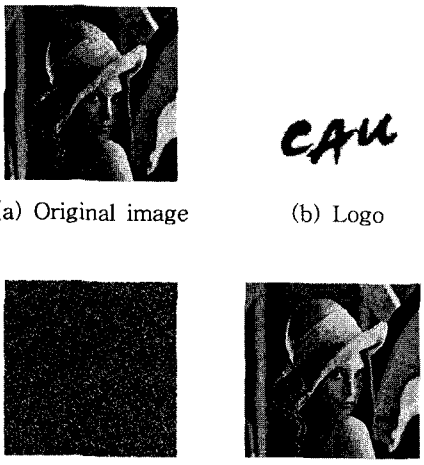
워터마크를 삽입할 때와 같은 방법으로 비밀키(K_1, K_2)를 이용하여 영상을 랜덤하게 섞고, 랜덤수를 생성하여 XOR 연산을 수행한다. LUT를 참조하여 얻은 결과와 LSB를 XOR 연산을 하여 해당 워터마크 픽셀을 구한다. 이렇게 워터마크 영상의 모든 픽셀 값을 얻은 후, 뒤섞인 워터마크 영상을 원래의 영상으로 복구한다.



(그림 2) 워터마크 추출 과정

3. 실험 및 분석

본 논문에서는 실험 영상으로 (그림 3) (a)와 같은 256x256 크기의 Lena 영상과 워터마크는 (b)와 같은 80x35 크기의 이진 로고 영상을 사용하였다. (c)와 (d)는 각각 원 영상을 랜덤하게 섞은 영상과 워터마크가 삽입된 영상이며, PSNR은 54.2dB로 비가시성을 갖는다.



(a) Original image (b) Logo

(c) Permuted image (d) Watermarked image

(그림 3)

(그림 4) (a)는 워터마크가 삽입된 영상의 모자 부분이 조작된 것으로 (b)의 추출한 워터마크 영상에서 변조 위치를 정확히 검출하였다.

(a) Tampered image (b) Extracted watermark

(그림 4)

픽셀 단위로 워터마크를 삽입·추출하기 때문에 블록 단위로 처리되는 Wong[6]의 방법보다 더욱 정확하게 조작 위치를 검출할 수 있으며, 암호학적 시스템을 적용하지 않으므로 검출 속도를 보다 빠르게 할 수 있다. 또한, 원 영상과 워터마크 영상을 무작위로 섞고 랜덤수와 연산하므로 LUT 값을 추정하는 것은 어렵다.

4. 결론

본 논문에서는 디지털 영상의 인증과 무결성 검증을 위해 공간 영역에서 두 개의 비밀키와 XOR를 사용하는 Fragile Watermarking 기법을 제안하였다.

비밀키를 사용하여 원 영상과 워터마크 영상을 랜덤하게 섞고, 이를 랜덤수와 LUT를 이용하여 워터마크를 삽입하므로 보안성을 갖는다. 또한, 워터마크 삽입·추출과정에서 암호학적 알고리즘을 적용하지 않은 간단한 수행 과정으로 빠르게 처리할 수 있다. 실험 결과로 영상의 변형 여부와 조작 위치를 정확하게 검출하였다. 향후 연구 과제로 악의 없는 변형에는 워터마크가 깨지지 않는 기법에 대한 연구가 수행되어야 할 것이다.

감사의 글

본 연구는 교육부의 BK21 사업의 지원으로 수행된 결과의 일부임.

참고문헌

[1] Inoue H., Miyazaki A., Katsura T., "Wavelet-based watermarking for tamper proofing of still images", *Proc. IEEE International Conference on Image Processing*, vol.2, pp.88-91, Sept. 2000.

[2] Min Wu, Bede Liu, "Watermarking for image authentication", *Proc. IEEE International Conference on Image Processing*, vol.2, pp.437-441, Oct. 1998.

[3] E. T.Lin, E. J. Delp, "A Review of Fragile Image Watermarks", *Proc. Multimedia and Security Workshop at ACM Multimedia*, pp.36-39, Oct. 1999.

[4] Yeung M.M, Mintzer F., "An invisible watermarking technique for image verification", *Proc. IEEE International Conference on Image Processing*, vol.2, pp.680-683, Oct. 1997.

[5] Holliman M., Memon N., "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes", *IEEE Transactions on Image Processing*, vol.9, pp.432-441, March 2000.

[6] P. W. Wong, Memon, N., "Secret and public key image watermarking schemes for image authentication and ownership verification", *IEEE Transactions on Image Processing*, vol.10, pp.1593-1601, Oct. 2001.

[7] Kundur D., Hatzinakos D., "Digital watermarking for telltale tamper proofing and authentication", *Proc. IEEE*, vol.87, pp.1167-1180, July 1999.