정확한 위치를 측정할 수 있는 연성 워터마킹

이혜란, 박지환
부경대학교 전자계산학과

Fragile Watermarking Capable of Accurate Localization

Hye-Ran Lee, Ji-Hwan Park
Dept. of Computer Science, PuKyong Nat'l University

요 약

일반적으로 인증과 무결성 증명을 목적으로 하는 연성 워터마킹은 영상의 블록별로 워터마킹을 수행하게 된다. 블록별로 워터마킹을 수행하는 기법은 블록 cut-and-paste 공격 또는 collage 공격이 발생하게 되면 영상의 변조에도 워터마크가 깨어지지 않고 정상적으로 추출되는 문제점이 발생한다. 몇 몇 기법은 영상의 각 블록을 워터마킹 할 때에 이웃하는 블록들의 정보를 이용한 워터마킹으로 이러한 공격에 대응하고 있다. 하지만 이웃하는 블록을 이용하는 기법에도 변조된 위치 측정이 정확하지 않다는 단점이 있다. LIU[1]가 제안한 기법은 블록을 이등분하여 반은 이웃 블록의 정보와 해당 블록의 정보를, 나머지 반은 해당 블록의 정보를 삽입함으로서 위치 측정을 향상시키는 기법을 제안하였다. 하지만, LIU의 기법에서 해당 블록의 이전 블록과 이후의 블록이 동시에 변조되면 해당 블록의 변조 여부가 정확해지지 않는다는 문제점이 발생한다. 본 논문에서는 블록을 3등분하여 해당 블록의 이전 블록과 이후 블록의 정보를 사용함으로 LIU 기법의 문제점을 해결하면서 위치 측정을 정확하게 하는 기법을 제안한다.

1. 서론

디지털 워터마킹은 크게 견고한 워터마킹과 연성 워터마킹 두 가지로 분류할 수 있다. 견고한 워터마킹은 일반적으로 저작권, 소유권을 증명하는데 사용하며 연성 워터마킹은 인증과 무결성을 증명하는 용도로 사용된다. 군사적으로 중요한 영상, 법적 증거가 되는 영상 혹은 의료 영상과 같이 미세한 변조조차도 허용하지 않는 영상의 경우, 워터마크를 삽입하여 변조 발생 시 워터마크가 쉽게 깨어지도록 하므로 영상의 변조 유무 및 변조 위치를 측정하는 것이 연성 워터마킹 기법이다.

연성 워터마킹 기법 중 Wong의 기법[2]은 디지털 서명 기법을 도입하여 인증과 무결성을 증명하는 방법으로 블록별로 워터마킹을 수행한다. 블록마다 독립적으로 워터마킹을 수행하므로 cut-and-paste 공격과 Holliman and Memon's counterfeiting 공격[3]에 취약함을 볼 수 있다. 이러한 공격에 대응하기 위해 contextual 정보를 사용하여 워터마킹을 수행하는 기법들이 등장하게 되었다. Li의 기법[4]은 블록을 지그재그 스캔하여서 블록을 이등분 한 후 해당 블록의 오른쪽 반에 다음 블록의 오른쪽 반을 가지고 와서 워터마킹을 수행한다. 해당 블록을 워터마킹 할 때에 다음 블록의 오른쪽 반의 정보가 들어가기 때문에 블록 cut-and-paste 공격 및 counterfeiting 공격을 막을 수 있다. 하지만 해당 블록을 워터마킹 할 때에 이웃 블록의 정보를 활용하는 것은 contextual 정보를 활용할 수 있다는 장점이 있지만, 변조가 발생하게 되면 변조의 위치 측정이 정확하지 않다는 단점이 있다. 즉 해당 블록의 변조가 발생하면 해당 블록과 이웃 블록이 모두 변조된 위치로 측정되기 때문에 변조의 위치 측정이 정확하지 않다는 문제점이 생기게 된다.

이러한 문제점을 해결하기 위해 LIU의 기법[1]에서는 블록을 이등분 한 후 두 개의 시리즈를 생성하여 블록의 반에 첫 번째 시리즈를, 나머지 블록의 반에 두 번째 시리즈를 각각 삽입하게 된다. 첫 번째 시리즈의 생성은 해당 블록의 모든 픽셀의 LSB를 제외한 7MSBs 정보와 이전 블록의 모든 픽셀의 모든 비트 정보의 입력으로 이루어진다. 두 번째 시리즈의 생성은 해당 블록의 모든 픽셀의 LSB를 제외한 7MSBs 정보를 입력으로 이루어지게 된다. 결과적으로 블록의 반쪽으로 해당 블록의 변조를 측정

하며 나머지 반쪽은 이웃 블록을 contextual 정보로 사용하므로 블록 cut-and-paste 공격 및 counterfeiting 공격에 대응할 뿐 아니라 변조된 위치 측정의 정확도를 향상시키고 있다. 하지만 LIU의 기법에서 해당 블록의 이전 블록과 이후의 블록이 함께 변조되면 해당 블록은 변조되지 않았음에도 불구하고 변조되었다는 잘못된 검출을 하게 된다. 이러한 잘못된 검출을 줄이기 위해서 워터마킹을 수행하기 이전에 블록을 뒤섞어서 연속적인 블록의 변조 발생률을 떨어뜨리게 된다. 하지만 어떠한 경우에는 잘못된 검출이 일어날 수 있고 변조가 발생하지 않았음에도 불구하고 변조되었다고 위치 측정이 될 수도 있다는 것이다. 군사적 용도, 법적 증거용, 의료 영상 등의 정확성을 요하는 영상에서는 심각한 문제를 일으킬 수도 있게 된다.

본 논문에서는 이러한 LIU의 문제점을 해결하기 위하여 블록을 3등분하여 각각에 해당 블록의 정보, 이전 블록의 정보, 이후 블록의 정보를 삽입하여 잘못된 검출이 발생하지 않도록 하며, 블록을 뒤섞을 필요도 없게 된다. 2장에서는 LIU의 기법을 기본으로 수정한 본 제안 기법의 워터마크 삽입에 대해 설명하며, 변조 검출에 대해서는 3장에서 기술하며 4장에서는 본 제안 기법의 실험 결과 및 결론을 내리게 된다.

2. 워터마크 삽입

먼저 본 제안 기법의 기반이 되는 LIU의 기법을 살펴보면 다음과 같다.

· $M*N$ 원 영상을 $k*l$의 블록으로 분할하고 워터마크도 마찬가지로 분할한다. $m=M/k$, $n=N/l$.

· *key 1*을 사용하여 블록을 랜덤하게 섞는다. 원영상의 정렬된 블록 *(B(1), B(2), ...B(i)...B(mn))*, 블록 $B(i)$는 $B_1(i)$와 $B_2(i)$로 분할한다. 해당하는 워터마크 블록 *(W(1), W(2), ...W(i)...W(mn))*이며, 워터마크 블록 $W(i)$는 $W_1(i)$와 $W_2(i)$로 분할한다.

· 첫 번째 블록을 제외하고, 블록 $B(i)$와 이전 블록 $B(i-1)$는 두 개의 시리즈를 생성하기 위해 처리된다. 첫 번째 비트 스트림 시리즈는 블록 $B(i-1)$의 모든 픽셀의 모든 비트와 블록 $B(i)$의 모든 픽셀의 7 MSBs의 정보를 *key 2*로 암호화 한 후 MD5 해쉬 함수를 수행한다. 128비트 출력 H를 얻게 되고 H는 $p=128/(kl/2)$를 가지고 $H_1...H_p$으로 나눈 후 $W_1(i)$과 *XOR* 연산을 수행하게 된다. 그 결과가 식(1)처럼 첫 번째 시리즈 M_1이 된다.

$$M_1=H_1\oplus...\oplus H_p\oplus W_1(i) \quad (1)$$

두 번째 비트 스트림 시리즈는 블록의 모든 픽셀의 모든 7 MSBs 정보를 *key* 3으로 암호화 한 후 MD5 해쉬 함수를 수행한다. 128비트 출력 HH를 얻게 되고 HH는 $p=128/(kl/2)$를 가지고 $HH_1...HH_p$으로 나눈 후 $W_2(i)$와 *XOR* 연산을 수행한다. 그 결과가 식(2)처럼 두 번째 시리즈 M_2가 된다.

$$M_2=HH_1\oplus...\oplus HH_p\oplus W_2(i) \quad (2)$$

· M_1, M_2를 블록 $B_1(i)$과 $B_2(i)$의 LSB에 각각 삽입한다.

LIU의 기법은 해당 블록에 의존적일뿐만 아니라 이전 블록에도 의존적이므로 동일 영상의 다른 곳에서 워터마크를 식별하는 것이 불가능하며 다른 영상의 동일한 위치에서도 워터마크를 식별하는 것이 불가능하다. LIU 기법의 변조 검출은 해당 블록의 LSB를 추출한 결과와 삽입 시와 동일하게 M_1, M_2를 생성하여 비교하므로 변조를 확인할 수 있다. 변조 검출 시 해당 블록 이전의 블록과 이후의 블록이 동시에 변조되면 해당 블록이 변조되지 않았음에도 불구하고 변조된 것으로 나타나게 된다. 이러한 문제점을 해결하기 위해 블록을 뒤섞는 방법으로 이웃한 블록들이 동시에 변조되는 것을 줄이려하지만, 블록을 뒤섞었다 하더라도 어떠한 경우에는 이웃한 블록들이 동시에 변조되는 경우가 발생하게 되고 그림 3의 (e)와 (g)처럼 변조의 위치 측정에 정확도가 떨어지게 된다.

제안 기법에서는 기존의 LIU의 기법을 토대로 하지만, 블록을 3등분하여 해당 블록의 이전 블록 정보와 이후 블록 정보를 삽입하여 위치 측정의 정확도를 향상시킬 뿐만 아니라, 블록을 뒤섞을 필요도 없어지게 된다. 제안 기법의 워터마크 삽입과정은 다음과 같다.

[단계 1] $M*N$ 원 영상을 $k*l$의 블록으로 분할하고 워터마크도 마찬가지로 분할한다. $m=M/k$, $n=N/l$. 분할된 블록 *(B(1), B(2), ...B(i)...B(mn))*이고, 블록 $B(i)$는 다시 $B_1(i)$, $B_2(i)$, $B_3(i)$로 분할한다. 해당하는 워터마크 블록 *(W(1), W(2), ...W(i)...W(mn))*이고, 워터마크 블록 $W(i)$도 $W_1(i)$, $W_2(i)$, $W_3(i)$로 분할한다.

[단계 2] 블록 $B(i)$, 이전 블록 $B(i-1)$, 이후 블록 $B(i+1)$를 이용해 세 개의 시리즈를 생성한다. 첫 번째 비트 스트림 시리즈는 블록 $B(i-1)$의 모든 픽셀의 모든 비트와 블록 $B(i)$의 모든 픽셀의 7 MSBs의 정보를 *key* 1로 암호화 한 후 MD5 해쉬 함수를

수행한다. 128비트 출력 H를 얻게 되고 H는 p=*128/(kl/3)*를 가지고 $H_1...H_p$으로 나눈 후 $W_1(i)$과 *XOR* 연산을 수행하게 된다. 그 결과 식(4)처럼 첫 번째 시리즈 M_1이 생성된다.

$$M_1=H_1\oplus...\oplus H_p\oplus W_1(i) \quad (4)$$

두 번째 비트 스트림 시리즈는 블록의 모든 픽셀의 모든 7 MSBs 정보를 *key* 2로 암호화 한 후 MD5 해쉬 함수를 수행한다. 128비트 출력 HH를 얻게 되고 HH는 p=*128/(kl/3)*을 가지고 $HH_1...HH_p$으로 나눈 후 $W_2(i)$와 *XOR* 연산을 수행하게 된다. 그 결과가 식(5)처럼 두 번째 시리즈 M_2가 된다.

$$M_2=HH_1\oplus...\oplus HH_p\oplus W_2(i) \quad (5)$$

세 번째 비트 스트림 시리즈는 블록 $B(i)$의 모든 픽셀의 7 MSBs의 정보와 블록 $B(i+1)$의 모든 픽셀의 7 MSBs의 정보를 *key* 3로 암호화 한 후 MD5 해쉬 함수를 수행한다. 128비트 출력 HHH를 얻게 되고 HHH는 p=*128/(kl/3)*을 가지고 $HHH_1...HHH_p$으로 나눈 후 $W_3(i)$과 *XOR* 연산을 수행하게 된다. 그 결과가 식(6)처럼 세 번째 시리즈 M_3이 된다.

$$M_3=HHH_1\oplus...\oplus HHH_p\oplus W_3(i) \quad (6)$$

[단계 3] 구해진 M_1, M_2, M_3을 블록 $B_1(i)$, $B_2(i)$, $B_3(i)$의 LSB에 각각 삽입한다.

그림 1은 제안 기법의 워터마크 삽입 과정을 나타낸 것이다.

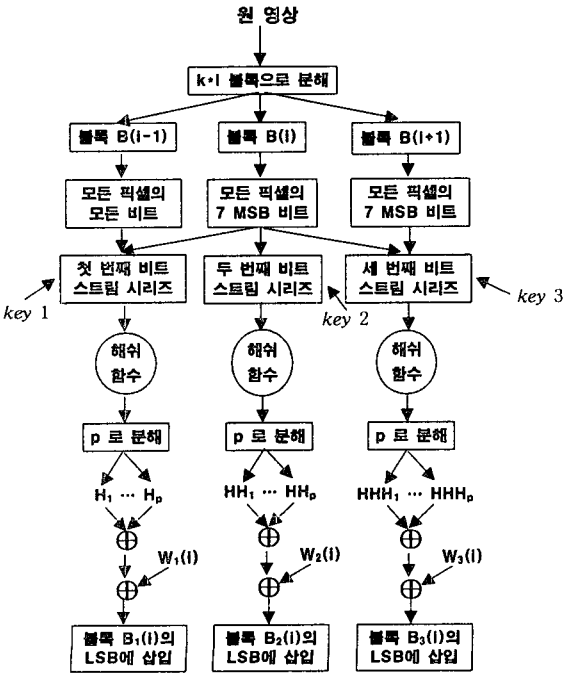

그림 1. 워터마크 삽입 과정

3. 변조 검출

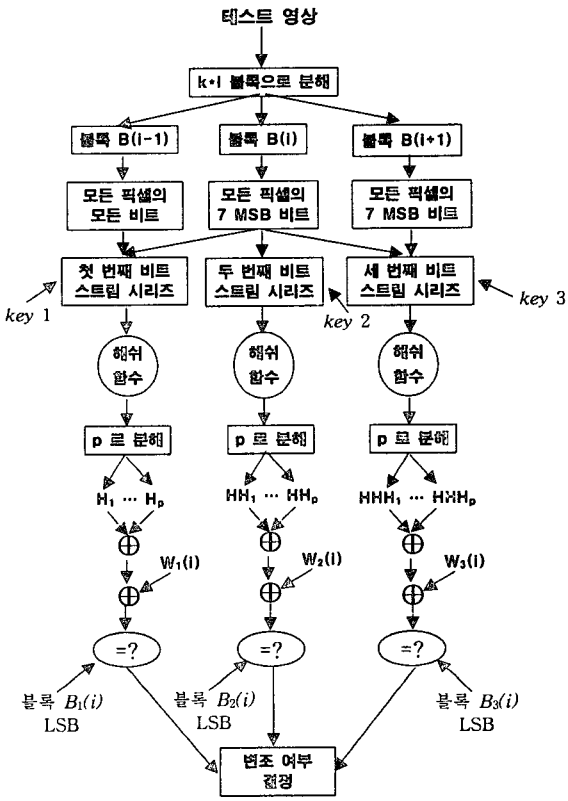

그림 2. 변조 검출 과정

변조 검출 과정은 다음과 같은 단계로 구성된다.

[단계 1] 워터마크 삽입 시처럼 세 개의 시리즈 M_1, M_2, M_3을 생성한다.

[단계 2] 블록$B_1(i)$, $B_2(i)$, $B_3(i)$의 LSB와 세 개의 시리즈를 각각 비교한다.

그림 2는 워터마크가 삽입된 테스트 영상의 변조 검출 과정을 그림으로 나타낸 것이다.

4. 실험 및 결론

본 실험은 두 가지 형태로 나눌 수 있다. 첫 번째는 영상의 픽셀 값을 임의로 변경시키는 경우와 두 번째는 영상의 다른 부위 혹은 또 다른 워터마크된 영상에서 블록을 cut-and-paste하는 collage 공격을 가 한 경우이다. 원 영상은 실험에 많이 사용되는 256*256 그레이 레벨의 Lena 영상으로 그림 3의 (a)이며, (b)와 (c)는 제안 기법으로 워터마크된 영상이다. (d)는 Lena 영상 모자의 장식부분의 픽셀 값을 변조한 영상이며 (e)는 모자의 꽃 장식 부분의 블록

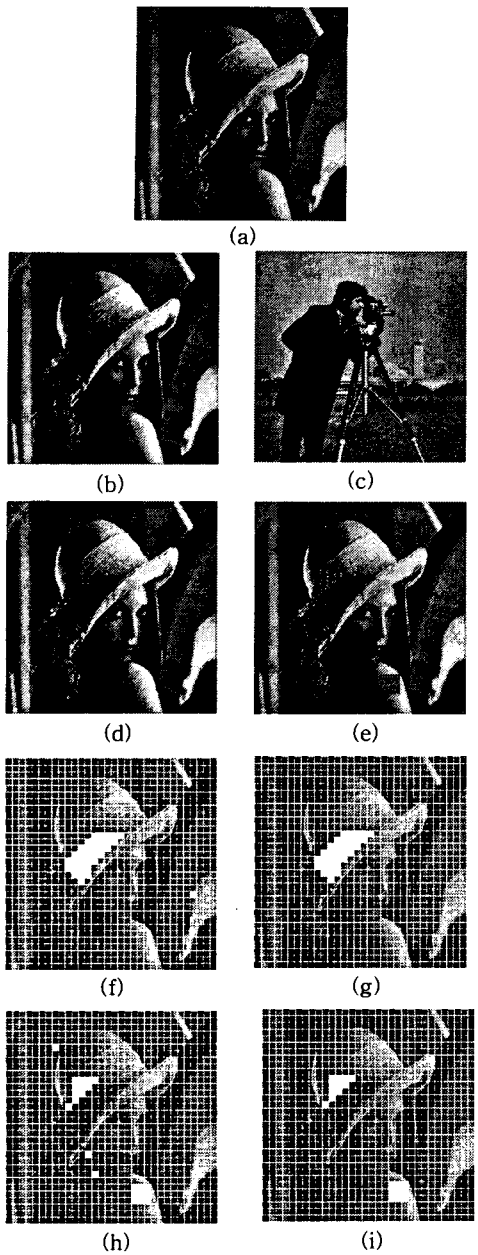

그림 3. (a) 원 영상, (b) 워터마크된 영상 I, (c) 워터마크된 영상 II (d) 변조된 영상, (e)collage attack, (f) (c)에서 LIU의 기법으로 변조 검출, (g) (c)에서 제안 기법으로 변조 검출, (h) (d)에서 LIU의 기법으로 변조 검출, (i) (d)에서 제안 기법으로 변조 검출

을 cut-and-paste, 또 다른 워터마크된 영상 (c)로부터 동일한 위치의 9개의 블록을 cut-and-paste하여 collage 공격을 가 한 영상이다. (f)는 픽셀 값을 변조한 영상(d)에서 LIU가 제안한 기법으로 변조 검출을 한 결과를 나타낸 것으로 거울의 비친 모자 부분이 실제로 변조되지 않았음에도 불구하고 변조된 것처럼 위치 측정된 그림이다. (g)는 제안 기법으로 변조 검출을 한 것으로 위치 측정이 블록별로 정확한 것을 알 수 있다. (h)는 블록 cut-and-paste 공격을 가 한 영상 (e)로부터 LIU의 기법으로 변조 검출을 한 영상으로 변조되지 않은 몇 개의 블록이 변조 된 것으로 위치 측정된 것을 알 수 있다. 반면 제안된 기법으로 변조 검출을 한 영상(i)은 실제로 변조된 위치에만 위치 측정된 것을 알 수 있다.

영상의 블록별로 워터마킹을 수행하는 기법은 블록 cut-and-paste 공격 또는 collage 공격이 발생하게 되면 영상의 변조에도 워터마크가 깨어지지 않고 정상적으로 추출된다는 문제점이 발생하므로 이웃하는 블록들의 정보를 이용한 워터마킹으로 이러한 공격에 대응하고 있다. 하지만 이웃하는 블록을 이용하는 기법에도 변조된 위치 측정이 정확하지 않다는 단점을 가지고 있으므로 LIU의 기법은 블록을 이등분하여 반은 이웃 블록의 정보와 해당 블록의 정보를, 나머지 반은 해당 블록의 정보를 삽입함으로서 위치 측정을 향상시키는 기법을 제안하였다. 하지만, LIU의 기법에서 해당 블록의 이전 블록과 이후의 블록이 동시에 변조되면 해당 블록이 변조되지 않았음에도 불구하고 변조된 것으로 위치 측정이 되었다. 본 논문에서는 이러한 LIU의 기법을 보완하는 기법으로 블록을 3등분하여 해당블록의 이전 블록과 이후 블록의 정보를 함께 사용함으로 위치 측정의 정확성을 향상시키는 기법을 제안하였다.

[참고문헌]

[1] F. Liu, Y. Wang, "An Improved Block Dependent Fragile Image Watermark," in *Proc. IEEE ICME*, vol. 2, pp.501-504, July 2003.

[2] P. W. Wong, "A Public Key Watermark for Image Verification and Authentication," in *Proc. IEEE ICIP*, Chicago, IL, Oct. 1998

[3] M. Holliman and N. Memon, "Counterfeiting Attacks on Oblivious Block-wise Independent Invisible Watermarking Schemes," *IEEE Trans. Image Processing*, vol. 9, pp.432-441, Mar. 2000.

[4] C. T. Li, D. C. Lou, and T. H. Chen, "Image Authentication and Integrity Verification via Content-based Watermarks and a Public Key Cryptosystem," in *Proc. IEEE int'l conference on Image Processing*, vol.3, pp. 694-697, 2000.