# 허용 가능한 이미지 조작에 대한 내용 적응 시그너쳐 생성 기법

안세정, 정성환
창원대학교 컴퓨터공학과

# Content Adaptive Signature Generation Method for Acceptable Image Manipulation

Se-Jung Ahn, Sung-Hwan Jung
Dept. of Computer Engineering, ChangWon National University

**요 약**

본 논문에서는 JPEG 압축 이외의 블러링(blurring) 및 샤프닝(sharpening) 등의 허용 가능한 이미지 조작에도 정보가 유지될 수 있는 내용 적응(content adaptive) 서명(signature) 기법을 제안하였다. 제안한 방법은 블록의 이미지 내용의 특성을 사용하여, 기존의 이미지 블록 사이의 DCT 계수 차이가 유지되는 DCT를 기반으로 한 Chang의 서명 방법의 단점을 개선하였다. 즉, 허용 가능한 이미지 조작에 대하여 에러 발생 확률이 높은 블록을 피하여 서명을 생성하였다. Lenna를 포함한 여러 표준 영상을 사용하여 실험한 결과, 제안한 방법은 Chang의 방법에서 발생하는 서명의 비트 스트림 에러보다 에러 발생 빈도가 블러링 이미지에서는 평균 약 55%, 샤프닝 이미지에서는 평균 약 51% 더 낮았다.

## 1. 서론

최근 디지털 데이터를 보호하기 위해 디지털 컨텐츠 자체에 소유권 정보를 삽입하여 불법적인 복제를 막는 디지털 워터마킹 방법이 많이 연구되고 있다[1].

예전에는 불법적인 조작에 견딜 수 있는 강인한(robust) 워터마크나 혹은 불법적인 조작이 가해진 이미지에 조작이 가해졌다는 흔적을 남기기 위한 약한(fragile) 워터마크를 주로 연구해 왔다. 그러나 최근에는 그 둘을 결합하여 합법적인 조작이나 왜곡(legitimate distortion)에는 영향을 받지 않지만, 불법적인 왜곡이나 조작에는 파괴되는 semi-fragile 워터마크에 관심을 가지고 많은 연구가 이루어지고 있다[2].

semi-fragile 워터마크는 주로 서명 삽입(signature embedding) 과 워터마크 삽입(watermark embedding) 두 부분으로 나누어진다[3]. 본 논문에서는 이 중 서명 삽입(signature embedding) 부분만을 다루고 있다.

Chang은 인증(authentication)을 얻을 수 있는 허용 가능한 조작에 대해서는 서명이 유지되고, 불법적인 조작이 가해진 이미지들에 대해서는 서명이 파괴되도록 semi-fragile 하게 서명을 만들 수 있는 알고리즘을 연구하였다[3].

최근까지 semi-fragile을 언급하고 있는 논문에서의 허용 가능한 조작은 JPEG 압축(Compression) 에 관한 것이 대부분이었고, 허용 가능한 조작된 이미지에 여러 가지 적응적인(adaptive)방법을 사용하면 semi-fragile한 서명을 유지할 수 있다고 주장하고 있지만 실제적으로 어느 정도까지 보증을 해주는지 정확한 값을 보여주는 사례는 거의 없었다[4].

본 논문은 블러링과 샤프닝과 같은 다양한 허용 가능한 이미지 조작에 대하여 기존 Chang의 방법을 수정하여 블록의 내용에 따라 시그너쳐를 생성하는 내용 적응 시그너쳐 기법을 제안하였다. 또한 실험을 통하여 기존 방법과 성능을 비교 분석하였다.

## 2. 허용 가능한 조작

대용량의 디지털 데이터의 저장과 전송에서는 압축

과 잡음 등이 발생하는데 이런 형태의 이미지 조작은 이미지 프로세싱에서 피할 수 없는 부분으로 인식되고 있다[5].

Chang은 허용 가능한 조작으로 압축(compression), 블러링(blurring), 샤프닝(sharpening), 잘라내기(cropping), 포맷 변형(format transformation), 이동(shifting), 스케일링(scaling) 등을 들고 있다. 이러한 조작들은 이미지의 시각적인 왜곡을 최소화하려고 노력한다[3,6].

하지만 실제로 Chang의 방법에는 JPEG 압축 이외의 허용 가능한 조작된 이미지에 대하여 언급은 있지만 자세히 설명 되어있지 않다. 또한 시뮬레이션 결과, 허용 가능한 조작으로 분류한 미약한 블러링이나 샤프닝 공격에 대하여 시그너쳐를 인증하기에는 취약하다.

다음 장에는 Chang의 방법의 취약점을 분석하고, 허용 가능한 이미지 조작에 대하여 에러를 줄일 수 있는 방법을 고려해 보고자 한다.

## 3. Chang의 블록 기반 시그너쳐 방법

Chang의 서명 생성 방법은 다음과 같다. 먼저 원본 칼라 이미지 I를 그레이 스케일 이미지로 변환한 후, 8×8 블록으로 중첩되지 않게 나눈다.

$$I = \bigcup_{p=0}^{\omega} I_P \qquad (1)$$

$p$는 원본 이미지를 8×8로 나눈 블록의 순서를 나타내고 $\omega$는 전체 블록의 개수이다. 그런 후, 각 블록을 DCT 변환하고 양자화 한다.

$$T_P = DI_P \qquad (2)$$

$D$는 DCT 변환을 나타낸다.

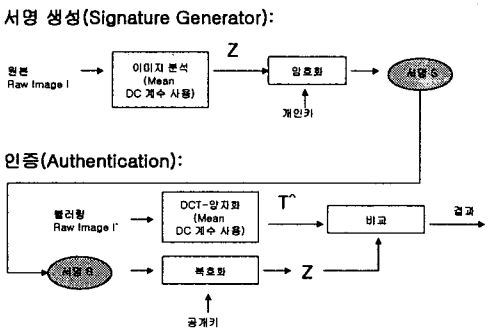
$$\tilde{t}_p(\nu) \equiv \text{Integer Round}\left(\frac{T_p(\nu)}{Q(\nu)}\right) \qquad (3)$$

$Q(\nu)$는 양자화 테이블이고, $\tilde{t}_p(\nu)$는 DCT 변환 후 양자화 테이블을 사용하여 양자화 된 값을 정수로 표현한 값이다.

양자화해서 얻어진 결과를 이웃하는 블록의 같은 위치의 계수의 차를 사용하여 구분한다. 즉, 계수의 차가 0보다 크면 코드에 1을 할당하고, 그렇지 않으면 코드에 0을 할당하여 서명이 될 코드를 얻는다. 결과적으로 DCT 변환 후 이웃하는 블록끼리의 계수 비교 후, 부호(sign)는 양자화 변환 이후에도 유지되기 때문에 이렇게 얻어진 코드가 서명이 될 수 있다[3,7].

이 실험에서는 한 이미지의 두 개의 분리된 블록들 안의 같은 위치의 두 개의 DCT 계수의 차를 지정된 경계값(designated threshold value) 과 비교하여 코드를 생성하였고, 각 블록에서 비교한 계수는 10개씩이다.

<그림 1>은 서명을 얻어서 인증하기까지의 전체 블록도를 보여주고 있다.




<그림 1> Signature Generator 와 Authentication Process

그림에서 서명 생성(Signature Generator) 과정에서, 우선 이웃하는 블록의 같은 위치의 DCT 계수 사이의 관계로 이미지의 특징 코드 Z를 생성한다. 인증(Authentication) 과정에서는 받은 이미지의 DCT 계수를 계산하고, 그 계수들과 디지털 서명 S로부터 복호화 된 Z와 비교한다. 받은 이미지가 원본 이미지의 특징인 DCT 계수 사이의 관계를 만족한다면 인증(authenticate)할 수 있다.

실제 Chang의 방법은 JPEG과 같은 압축에는 강하지만, 블러링과 샤프닝과 같은 허용 가능한 이미지 조작에 대해서는 취약한 점이 발견된다.

예로서 블러링 이미지에 대한 Chang 방법의 Z 코드의 결과를 <표 1>에 보인다.

<표 1> 에지 여부에 따른 에러코드 비교

| | DCT | Original Lena image | Blur Lena image |
|---|---|---|---|
| 에지 없는 block | 286 block | 79 1 0 0 0 0 0 0 0 | 79 1 0 0 0 0 0 0 0 |
| | | ↕ ↕ ↕ ↕ ↕ ↕ ↕ ↕ ↕ ↕ | ↕ ↕ ↕ ↕ ↕ ↕ ↕ ↕ ↕ ↕ |
| | 287 block | 78 0 1 0 0 0 0 0 0 | 78 0 1 0 0 0 0 0 0 |
| | Z-code | 1 1 0 0 0 0 0 0 0 | 1 1 0 0 0 0 0 0 0 |
| | | ←→ (일치함) | |
| 에지 있는 block | 788 block | 50 -53 0 67 2 2 2 0 | 50 -53 0 6 7 2 1 2 0 |
| | | ↕ ↕ ↕ ↕ ↕ ↕ ↕ ↕ ↕ ↕ | ↕ ↕ ↕ ↕ ↕ ↕ ↕ ↕ ↕ ↕ |
| | 789 block | 44 -9 2 -1 -7 7 -5 1 -3 0 | 44 -9 2 -1 -7 6 -5 1 3 0 |
| | Z-code | 1 1 1 1 1 0 1 1 1 1 | 1 1 1 1 1 0 1 1 1 1 |
| | | ←→ (일치하지 않음) | |

<표 1>의 예에서 에지가 없는 블록의 Z 코드보다 에지가 많은 블록의 Z 코드가 에러가 발생할 가능성이 높음을 보이고 있다.

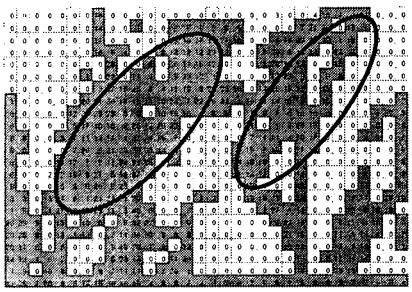
따라서 블록의 내용에 따라 적응적으로 이미지 특징 코드인 시그너쳐를 생성하는 접근 방법이 필요하다.

## 4. 제안한 내용 적응 시그너쳐 방법

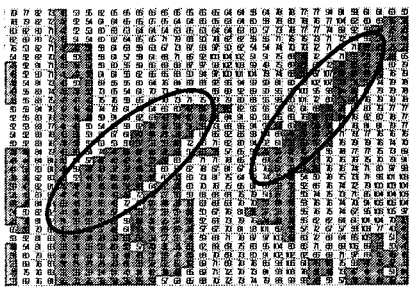
### 4.1 DC 값을 이용한 블록 특성 판별

이미지의 내용에 적응적으로 특징을 추출하여 변환 영역 상에서 서명이 될 수 있는 코드를 얻을 수 있는 알고리즘이 필요하다. 본 연구에서는 DCT 변환 영역 상에서 블록의 특성을 판별하고 시그너쳐를 생성하는 방법을 제안한다.

우선 공간영역에서 에지 블록과 DCT 변환 영역의 위치를 비교하기 위하여 다음 <그림 2>의 예를 보자. <그림 2>의 (a)에서는 에지를 추출하기 위하여 소벨 마스크(Sobel Mask)를 사용하여 블록 당 에지 후보 픽셀의 개수를 보이고 있다.



(a)



(b)

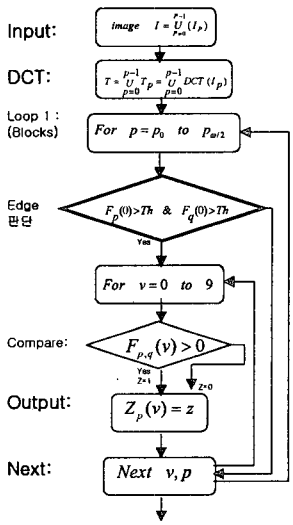
<그림 2> 소벨 연산자로 확인해본 공간 영역의 에지(a)와 DCT 블록 변환 영역의 에지(b) 비교

한편 <그림 2> (b)는 이미지에서 에지가 있는 블록으로 볼 수 있는 위치의 DCT 계수의 DC값이다.

<그림 2> (a)에서의 타원 영역의 위치와 (b)에서의 타원 영역의 위치는 어느 정도 관련이 있음을 볼 수 있다. 따라서 변환 영역에서 DC 값이 낮은 블록들이 공간 영역에서 에지를 포함한 블록들을 어느 정도 나타낸다고 볼 수 있다. 그러므로 이미지를 DCT 변환했을 때 얻을 수 있는 DC의 계수값으로 에지가 있는 블록인지 아닌지를 판별 할 수 있다. 다음 절에서 DC값을 이용하여 에지 블록을 피하면서 서명 코드를 얻는 방법을 보이고자 한다.

### 4.2 내용 적응 시그너쳐 생성 알고리즘

<그림 3>은 제안한 블록 특성 기반의 내용 적응 시그너쳐 생성 알고리즘이다.




<그림 3> 제안한 내용 적응 시그너쳐 알고리즘 흐름도

<그림 3>은 기존의 Chang의 방법을 수정하여 이웃 블록의 DC 계수가 실험에 사용한 Mean DC보다 크다고 할 때 그 블록을 에지가 없는 블록으로 판단한다. 에지가 없는 블록으로 판단된 이웃 블록끼리 지그재그 스캔된 DCT 계수를 10개씩 순서적으로 비교하여 0보다 크면 1을, 그렇지 않으면 0을 코드에 할당한다. 모든 블록을 비교할 때까지 이 과정을 반복한다.

## 5. 실험 및 결과 분석

본 논문에서 에지가 있는 블록으로 판단하기 위해 사용한 경계값은 전체 블록의 DC값의 평균을 사용하였다. 실험 대상이 된 이미지는 256×256 크기였고, 8×8 픽셀로 한 블록을 구성하여 전체 1024개의 블록을 가지고 있다. 그러므로 다음의 수식을 사용하여

평균값 DC를 구하였다.

$$Th=(\sum_{n=0}^{1023} DC_n)/1024 \quad (4)$$

이렇게 얻어진 평균값 DC를 경계값으로 하여 적응적으로 블록의 내용을 판단하여 시그너쳐를 생성하였다.

다음의 <표 2>은 기존의 Chang의 방법과 제안한 방법에 의해 발생하는 에러 비트 수를 보여주고 있다.

<표 2> Chang의 방법과 제안한 방법에 의한 에러 비트 수

| | Chang | | 제안한 방법 | | | |
|---|---|---|---|---|---|---|
| Th=MeanDC | blur | Sharpen | Blur | 향상율 | Sharpen | 향상율 |
| Lenna | 116 | 186 | 56 | 52% | 110 | 60% |
| baboon | 196 | 226 | 85 | 57% | 99 | 56% |
| lake | 130 | 217 | 51 | 61% | 102 | 53% |
| house | 133 | 202 | 64 | 52% | 95 | 53% |
| map | 208 | 265 | 97 | 53% | 176 | 34% |
| average | 156.6 | 219.2 | 70.6 | 55% | 116.4 | 51.2% |

<표 2>는 전체 1024개의 블록에 대해 Z 코드를 생성하였을 때, 제안한 방법이 기존의 Chang의 방법에 비하여 블러링의 경우는 약 55%, 샤프닝의 경우에는 약 51% 이상 에러율이 향상되었음을 볼 수 있다.

제안한 방법에서 에러 비트가 일부 있다는 것은 허용 가능하다고 할 수 있는 조작이 진행되었다는 증거이다. 그러므로 에러코드의 허용 한계를 정해서 그 이상의 에러가 나지 않는다면 허용 가능한 조작이 가해졌다는 것으로 판단할 수 있다.

## 6. 결론

본 논문에서는 JPEG 압축 이외의 허용 가능한 조작에도 유지될 수 있는 내용 적응 서명을 얻기 위한 방법을 제안하였다. 제안한 방법은 기존 Chang의 방법을 수정하여 블록의 특성을 판별하여 비트 스트림으로 된 서명의 에러가 발생할 확률이 높은 에지 부분 블록을 피해서 서명을 생성하였다.

제안한 방법은 Lenna를 비롯한 여러 표준 영상에서 실험한 결과, 기존 Chang의 방법에서 발생하는 서명의 비트 스트림 에러보다 발생 빈도가 블러링에서는 약 55%, 샤프닝에서 약 51.2% 더 낮음을 확인하였다. 또한 에러코드의 허용 한계를 정해서 그 이상의 에러가 나지 않는다면 허용 가능한 조작이 가해졌다는 것으로 판단할 수 있다.

하지만 허용 가능한 조작과 불법적인 조작 사이의 현실적인 명확한 구분이 아직 없어서 그것을 명확히 할 필요가 있다. 그리고 블러링과 샤프닝 이외에도 다양한 허용 가능한 이미지 조작에 대한 내용 적응적인 서명을 얻을 수 있는 연구가 필요하다.

## [참고문헌]


[1] S. Katzenbeisser, F. A. P. Peticolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, 2000.

[2] Eugene T. Lin, Christine I. Podilchuk, Edward J. Delp, "Detection of image alterations using semi-fragile watermarks," SPIE International Conf. on Security and Watermarking of Multimedia Contents II, 3971(14) January 2000.

[3] C. -Y. Lin, S. -F. Chang, "A Robust Authentication Method Distingushing JPEG Compression from Malicious Manipulation," CU/CTR Technical Report 486-97-19, Dec 1997: SPIE Storage and Retrieval of Image / Video Database, San Jose, Jan. 1998.

[4] B. Sankur, "A Comparative Assessment of Semi-Fragile Watermarking Methods," SPIE Conf., Multimedia Systems and Applications IV, vol.4518, Denver, USA, Aug. 2002.

[5]E. T. Lin, C. I. Podilchuk, E. J. Delp, "Detection of Image Alteration Using Semi-Fragile Watermarks," Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents II, Col. 3971, Ed. P. W. Wong, E. Delp, January 23-28, San Jose, CA, 2000.

[6]Quibin Sun, Shih-Fu Chang, Maeno Kurato, Masayuki Suto, "A New semi-fragile image authentication framework combining ECC and PKI infrastructure," ISCA02, phoenix, USA, May, 2002.

[7] Saraju P. Mohanty, K. R. Ramakrishnan, Mohan S Kankanhalli "A DCT Domain Visible Watermarking Technique for Images," IEEE International Conference on Multimedia and Expo2, pp. 1029-10323, 2000.