

JPEG 압축 도메인에서 인증용 워터마킹에 관한 연구

김영남^o 김종원 최기철 최종욱

상명대학교 디지털저작권보호연구소

{ynlsk1^o, jwkim, cuijizhe, juchoi}@smu.ac.kr

A Study on Authentication Watermarking in the JPEG Compression Domain

Jin YongNan^o Kim Jongweon Cui Jizhe Choi Jong-Uk

Copyright Protection Research Institute, Sangmyung University

요 약

본 논문은 이미지 워/변조 검출 및 인증을 위한 고속의 Semi-Fragile 워터마킹 방법을 제안한다. 제안방법은 JPEG 이미지를 허프만 복호화 후에, 양자화 테이블 값에 의한 변화율이 같은 특정 양자화 계수를 비교함으로써 조건을 만족하는 8×8 블록 당 1비트 워터마크 정보를 삽입한다. 이때의 조건은 이미지의 열화를 초래하지 않을 정도의 작은 boundary 값을 기준으로 한다. 제안한 방법이 압축에 강인함을 실험을 통하여 증명하였다.

키워드 : Semi-Fragile Watermarking, Digital Watermarking, Content Authentication, JPEG

1. 서론

21세기에 들어서서 컴퓨터와 인터넷의 급속한 발전과 디지털 카메라와 캠코더의 보급 및 카메라 폰의 출현, 그리고 디지털 콘텐츠의 품질을 보장 및 향상하기 위하여 출현한 각종 소프트웨어에 의하여 디지털 이미지를 저장하거나 편집하기가 더욱 편리하게 되었다. 이것은 디지털 이미지에 대한 워/변조가 용이하다는 단점을 내포하게 된다.

이러한 디지털 이미지에 대한 인증을 위하여 Fragile(깨지기 쉬운) 워터마킹 기법이 연구되어 왔다. 그러나 이런 기법은 이미지에 대한 압축도 워/변조로 간주하기 때문에 압축 이미지의 워/변조 검출은 불가능하다. 따라서 압축 이미지의 워/변조 검출을 위하여 압축에는 강인한 Semi-Fragile 워터마킹 기법을 사용한다.

기존에 JPEG 압축에 강인하게 하기 위하여 미리 높은 압축 계수(Quantization Factor)로 압축 한 후 워터마크 정보를 삽입하는 방법이 있다[1,2]. 이러한 방법은 워터마크 정보를 삽입하기 위하여 높은 압축 계수에 의한 사용자 임의의 Non-Uniform 양자화 테이블을 이용하기 때문에 ISO에서 제안한 표준 양자화 테이블로 워터마크 추출이 불가능 하다. 다른 방법으로, 주파수 도메인의 저주파 대역에 워터마크 정보를 삽입하는 방법이 있다[3]. 이는 계산량은 적지만 많은 DCT 계수에 워터마크 정보를 삽입하기 때문에 이미지 열화가 크다. 또 다른 방법으로, DCT 선형성을 이용하여 임의의 DCT 계수에만 워터마크 정보를 삽입 함으로써 계산량도 줄이고

이미지 손실도 줄일 수 있는 방법이 있다[4]. 하지만 이러한 방법은 Quality Factor 85까지 검출 에러가 0% 이므로 이미지 워/변조에 대한 인증 범위가 많이 제한된다.

본 논문에서는 JPEG 이미지를 허프만 복호화 후 DCT 복호화 과정 없이 양자화 계수에 워터마크를 삽입함으로써 보다 빠른 알고리즘 개발에 초점을 맞췄다.

2. 제안 알고리즘

그림 1에서 나타낸 ISO에서 정한 표준 양자화 테이블에서 $(3,1) = (2,3) = (4,1) = 14$ 이다. 이것은 Quality Factor가 변함에 따라 양자화 계수 $Q(3,1)$, $Q(2,3)$, $Q(4,1)$ 은 동일한 비율로 변한다는 것을 의미한다. 따라서 $Q(2,3)$ 과 $Q(4,1)$ 을 비교하여 제안한 알고리즘의 조건을 만족하면 워터마크를 삽입, 만족하지 않으면 삽입하지 않는다.

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

그림 1 : 휘도 성분용 양자화 테이블

2.1 워터마크 삽입

그림 2는 워터마크 삽입 알고리즘을 나타내며 각 과정은 다음과 같다.

step 1 : JPEG 이미지를 입력 받아서 허프만 복호화 한다.

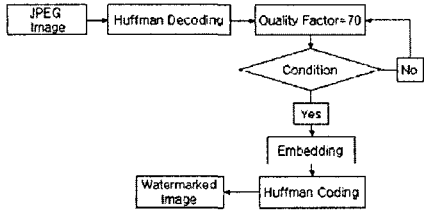


그림 2 : 워터마크 삽입 알고리즘

step 2 : step 1에서 얻은 양자화 계수의 각 8×8 블록의 $Q(3,1)$, $Q(2,3)$, $Q(4,1)$ 을 Quality Factor가 70인 양자화 계수로 바꾼다.

step 3 : 식 (1), (2), (3)을 동시에 만족하는 블록을 찾는다.

$$|Q(2,3) - Q(4,1)| \leq 2 \cdot \text{boundary} \quad (1)$$

$$[\max(Q(2,3), Q(4,1)) + \text{boundary}] \geq Q(3,1) \quad (2)$$

$$[\min(Q(2,3), Q(4,1)) - \text{boundary}] \leq Q(3,1) \quad (3)$$

step 4 : 워터마크 추출 시 양자화 과정의 사사오입에 의한 오차를 없애기 위하여 다음과 같이 변환한 후 $Q(3,1)$ 에 워터마크 정보를 삽입한다.

if $Q(4,1) > Q(2,3)$

$$Q(4,1) = Q(4,1) - 1; \quad Q(2,3) = Q(2,3) + 1$$

elseif $Q(2,3) > Q(4,1)$

$$Q(4,1) = Q(4,1) + 1; \quad Q(2,3) = Q(2,3) - 1$$

여기서 워터마크 정보가 1이면 원래의 $Q(3,1)$ 값 대신에

$$\text{round}\{Q(2,3) + Q(4,1)/2\} + 1 \quad (4)$$

을 대입하고, 워터마크 정보가 0이면

$$\text{round}\{Q(2,3) + Q(4,1)/2\} - 1 \quad (5)$$

을 대입함으로써 워터마크 정보를 삽입한다.

step 5 : 워터마크가 삽입된 양자화 계수를 원래의 Quality Factor로 변환 후 허프만 부호화 하여 워터마크 된 JPEG 이미지를 얻는다.

2.2 워터마크 추출

본 논문에서 워터마크 정보의 추출은 원 이미지를 필요로 하지 않는다. 그림 3은 워터마크 추출 알고리즘을 나타내며 각 과정은 다음과 같다.

step 1' : 워터마크 정보가 삽입된 이미지 또는 위/변조된 이미지를 허프만 복호화 한다.

step 2' : step 1'에서 얻은 각 8×8 블록의 양자화 계수 가운데서 $Q(3,1)$, $Q(2,3)$, $Q(4,1)$ 을 Quality Factor가 70인 양자화 계수로 바꾸어 식 (1), (2), (3)을 동시에 만족하는 블록을 찾는다.

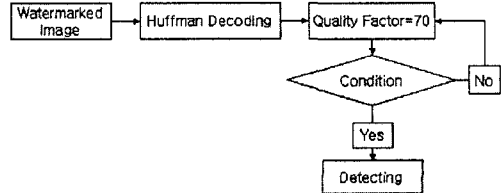


그림 3 : 워터마크 추출 알고리즘

step 3' : step 2'를 만족하는 블록에서 워터마크 정보를 추출한다[표 1].

표 1 : 워터마크 추출

워터마크 추출조건	추출된 워터마크
$\text{round}\{Q(2,3) + Q(4,1)/2\} \geq Q(3,1)$	1
$\text{round}\{Q(2,3) + Q(4,1)/2\} < Q(3,1)$	0

3. 제안된 알고리즘에 의한 인증

제안 알고리즘은 실험에 의하여 Quality Factor가 77~99 사이에서 변할 때 워터마크 추출이 100% 가능하다. 따라서 본 논문은 Quality Factor가 77~99인 JPEG 이미지에 대한 인증이 가능하다. 이미지의 위/변조 여부 및 위/변조된 위치를 확인하기 위하여 워터마크된 이미지 $C_w(x, y)$ 와 삽입된 워터마크 $W_r(x, y)$ 사이의 상호상관관계 $R_{xy}(u, v)$ 를 구한다.

$$R_{xy}(u, v) = \iint C_w(x, y) W_r(x - u, y - v) dx dy \quad (6)$$

그리고 본 논문에서는 키 값에 의한 랜덤 난수를 워터마크 정보로 사용하였다. 이 키 값은 이미지 위/변조 여부 판단 및 위/변조된 위치를 검출할 때 사용되는 중요한 파라미터로써 이미지의 저작자나 소유권자가 항상 비밀로 보관해야 한다.

그림 4는 변조 전과 변조 후의 이미지를 보여주고 있다.



그림 4 : 변조 전 이미지와 변조된 이미지

그림 5, 6은 그림 4에서 나타난 두 이미지의 변조 전과 변조 후의 상호상관관계를 나타낸다.

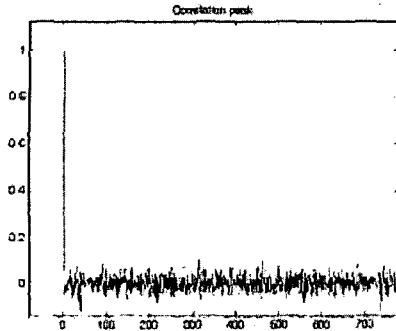


그림 5 : 변조 전 상호상관관계

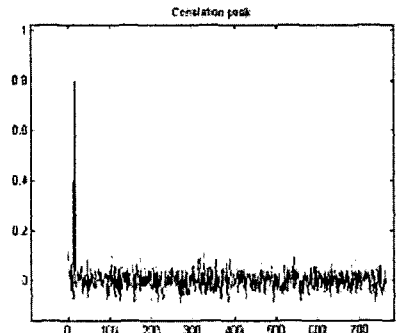


그림 6 : 변조 후 상호상관관계

그림 6에서 변조된 이미지에 대한 삽입 워터마크와 추출된 워터마크 사이의 유사도가 0.8인데 이것은 이미지가 변조되었다는 것을 나타내며, peak 값이 0이 아닌 다른 위치에서 나타났다는 것은 그 위치에서 변조되었다는 것을 나타낸다.

4. 실험결과 및 성능분석

본 논문에서는 256×256 JPEG gray 이미지를 실험으로 이용하였으며, seed 값이 1024이고 크기가 1024인 랜덤 난수를 워터마크 정보로 사용하였다. 그림 7은 boundary 값이 2 일 때 삽입된 워터마크의 강인성을 보여주고 있다.

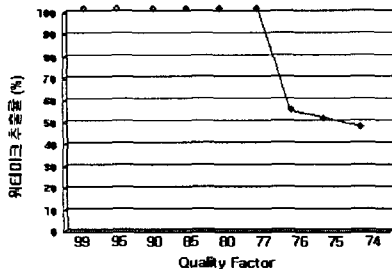


그림 7 : JPEG 압축에 대한 강인성

표 2는 워터마크 정보 삽입 후, 워터마크된 이미지의 화질

저하 정도를 살펴보기 위하여 원 이미지와 워터마크된 이미지의 PSNR을 구하였다.

표 2 : PSNR 비교

Quality Factor	PSNR (dB)			
	Lena	Barbara	Baboon	Goldhill
77	42.31	41.84	42.27	41.49
80	42.29	41.85	42.30	41.46
85	42.64	42.27	42.08	42.21
90	42.68	42.16	42.18	42.10
95	42.67	42.16	42.28	42.23
99	42.60	42.18	42.25	42.12

5. 결론 및 향후 연구과제

본 논문에서는 Quality Factor가 변함에 따라 양자화 계수 Q(3,1), Q(2,3), Q(4,1)이 동일한 비율로 변한다는 것을 이용하여 인증용 Semi-Fragile 워터마크 기법을 제안하였다. 제안방법에 의하여 Quality Factor 77까지 예러 없이 워터마크 검출이 가능하였다.

본 논문에서 제안한 워터마크 기법에서는 워터마크 삽입 여부를 판단하기 위한 boundary 값 및 워터마크 검출의 정확성을 높이기 위하여 워터마크 정보의 불확화에 관하여 추후 연구가 필요하다.

[참고문헌]

- [1] C.-Y. Lin and S.-F. Chang, "Semi-Fragile Watermarking for Authentication JPEG Visual Content", Proc. SPIE, Security and Watermarking of Multimedia Contents, San Jose, California, pp.140-151, January 2000
- [2] Kurato Maeno, et al, "New Semi-Fragile Image Authentication Watermarking Techniques Using Random Bias and Non-Uniform Quantization", Proc. SPIE, Security and Watermarking of Multimedia Contents, San Jose, California, pp.659-670, January 2002
- [3] Eugene T.Lin, et al. "Detection of image alterations using semi-fragile watermarking", Proc. SPIE, Security and Watermarking of Multimedia Contents, San Jose, California, pp.23-28, January 2000
- [4] 변영배, 유세근, 김중원. "이산코사인변환의 선형성을 이용한 Semi-Fragile 워터마크", 제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 2003.5