Modulus Blind Watermarking 알고리즘 및 최적 파라미터 추정

장용원, 김인택, 한승수
명지대학교 전기정보제어공학부
*전화: (031) 330-6345, 016-690-2721

Modulus Blind Watermarking Algorithm and Parameter Optimization

Yong-Won Jang, Intaek Kim, Seung-Soo Han
Division of Electrical and Information Control Engineering
Myongji University
*E-mail : shan@mju.ac.kr

Abstract - 최근 인터넷과 컴퓨터의 보급 확대로 디지털 매체의 수요가 늘어나면서 불법복제의 증가로 디지털 정보에 대한 저작권 보호가 큰 문제로 대두되고 있다. 이를 위한 디지털 매체의 소유권을 주장하는 방법 중에 하나가 워터마크를 삽입하는 것이다. 본 논문에서는 원본 이미지를 DCT 변환하여 DC 성분에 modulus 연산을 이용하여 워터마크를 삽입하는 알고리즘을 제시하였고, 강인성에 영향을 주는 파라미터 값을 최적화하였다.
새로운 알고리즘은 삽입한 워터마크를 추출할 때 원본 이미지가 필요치 않은 blind 워터마킹 방법이며, 워터마크를 삽입할 때 사용된 key값만을 가지고 삽입된 워터마크를 추출한다. 본 알고리즘을 이용하여 워터마크를 삽입한 이미지에 JPEG압축, clipping, noise 삽입, resize 등의 4가지 공격을 가하였을 때 워터마크의 검출률이 90% 이상이 되는 강인성을 보였다.

1. 서 론

최근 인터넷과 컴퓨터의 보급 확대로 디지털 정보의 보급이 급격히 증가하고 있다. 이로 인해 디지털 매체의 수요가 늘어나면서 불법복제가 증가하기에 디지털 정보에 대한 저작권 보호가 큰 문제로 대두되고 있다. 현재까지 디지털 영상매체에 대한 저작권보호 기술로 가장 주목받고 있는 것이 워터마크(watermark)방법이다[1].
디지털 워터마크의 요구되는 특성은 삽입 정보가 영상에 나타나지 않아야 하고 영상의 화질 또한 감쇠되지 말아야 하며, 변형을 가해도 소유권자에 의한 추출이 쉬워야한다. 워터마크의 삽입 방법은 크게 공간영역과 주파수 영역에 삽입하는 방법으로 나눌 수 있으나, 변형에 대한 강인성과 화질 면에서 주파수 영역에 삽입하는 방법을 많이 이용하고 있다.
공간영역에서의 워터마킹 방법으로 Osborne등은 m-sequence를 이용한 워터마킹 알고리즘을 제안했고[1], Bendor등은 확률을 이용한 워터마킹 방법인 "patchwork"를 제안하였는데, 이는 추출할 때 원본이미지를 필요로 하지 않는 것이 특징이다[2]. 주파수 방식의 워터마킹 기법으로 Koch, Rindfrey와 Zhao는 이미지를 8×8의 블록 단위로 구분하고 각 블록에 DCT을 계산하여 워터마크를 삽입하는 방법을 제안했고[3], Cox등은 이미지 전체를 DCT변환한 후 대역확산을 이용한 워터마킹 하는 방법을 제안했으며[4], Xia등은 웨이블릿 변환을 이용한 워터마킹 방법을 제안했다[5].
원본 이미지를 참조하는 알고리즘은 원본 이미지를 저장해야 하는 단점 때문에 원본 이미지가 필요 없는 blind-watermark 방법이 필요하게 되었다. 워터마크 삽입 정보로 Osborne 등이 삽입한 가우시안 시퀀스로는 명확한 소유권 주장이 힘들어 더욱 명확한 소유권 주장을 위해 가시적인 로고 이미지를 삽입할 필요가 있다.
본 논문은 DCT를 이용하여 원본 이미지를 주파수영역으로 변환한 후 DC성분에 워터마크 정보를 삽입하는 알고리즘을 제안한다. DC성분은 주파수의 정보가 밀집된 곳으로 워터마크시 화질의 저하가 심해 피하는 부분이지만, 일반적으로 JPEG 압축시 사용되는 양자화테이블의 값이 16로 일정한 값을 갖기 때문에 균일한 특성을 보일 수 있는 장점이 있다[6]. 이진수[0,1]로 구성된 워터마크 정보를 원본 이미지의 DC성분 값에 modulus 연산을 이용하여 삽입[7]하는 본 알고리즘은 워터마크를 추출할 때 원본 이미지 없이 key만을 사용하여 삽입한 로고 이미지를 추출하는 blind-watermarking 방법이며, 1/10(압축률90%)이상의 JPEG압축에도 강인함을 보인다. 워터마크된 이미지에 JPEG, clipping, noise, resize 등 4가지 공격에 대한 강인성을 갖도록 하기위해서 워터마킹시 사용되는 파라미터를 최적화하였다.

2. 제안한 워터마킹 알고리즘

2.1 워터마크 삽입 알고리즘

제안한 알고리즘은 blind-watermarking 방법으로써 정보를 추출하기 위해 modulus 연산을 이용한다. modulus 연산은 항상 나누는 특정값(S)보다 작은 수를 가지므로 S값을 정하여 삽입하고자하는 워터마크의 종류를 선택할 수 있는 특징이 있다.
DCT 변환 후 AC성분에 워터마크를 삽입하는 경우는 JPEG 압축 과정에서 양자화 값이 일정하지 않아 강인성을 상실하는 단점이 있다. 반면 DC성분은 양자화 값이 16으로 일정하고, DC계수 값이 커서 양자화과정에도 변화가 작은 장점이 있다[6]. 제시한 알고리즘에는 quantization step-size(Q)를 이용하여 노이즈나 압축 및 각종 공격에 강인하도록 선택할 수 있으며, 삽입로고 이미지를 추출할 때 소유자만이 올바르게 추출할 수 있도록 특정 key에 따라 random permutation을 수행하고 있다.
Vw×Vh 크기의 원본 이미지를 V, Ww×Wh 크기의 삽입할 로고 이미지를 W, 삽입되는 워터마크 정보를 wk=0,1,…,(S-1)라 하고, k=0,1,…,K(=Ww×Wh)를 인덱스로 사용한다. S는 삽입할 워터마크의 종류를 정하는 인자고, k는 워터마크의 수이다. JPEG압축에 대한 강인성을 갖기 위해, JPEG에서 DCT블록으로 사용하는 8×8블록의 DC성분에 한 비트의 워터마크 정보를 삽입한다. 삽입될 로고 이미지는 원본이미지의 1/8×1/8이어야 한다. 즉 Vw=8×Ww, Vh=8×Wh이다. 그림 1은 워터마크를 삽입하는 블록도이며, 워터마크의 삽입 알고리즘은 다음과 같다.
Step1: 원본 이미지를 8×8블록으로 DCT한다.
Step2: 삽입할 로고 이미지를 검정색은 0, 흰색은 1로 변환시킨다.

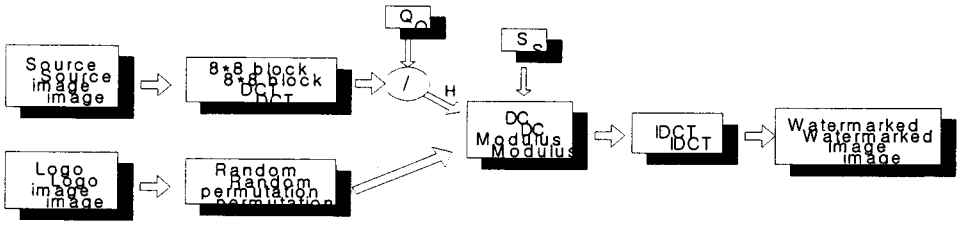

그림 1. 워터마크 삽입 블록도

Step3: Key를 이용해서 로고 이미지를 random permutation시킨다.

Step4: 잡음에 강인성을 주기 위해 DC_k값을 Q로 나누고 나온 값을 반올림하여 정수로 만든다. Q는 quantization step-size이다.

$$H_k = \mathrm{int}\{DC_k/Q\}$$

Step5: 삽입하고자하는 워터마크 wk_k와 $\mathrm{mod}(H_k,S)$의 값이 일치하면 q_k는 H_k값을 취하고, 일치하지 않으면 q_k는 H_k+1값을 취한다.

```
if(wk_k == mod(H_k,S))
    q_k = H_k;
else
    q_k = H_k + 1;
end
```

Step6: $DC_k' = q_k \times Q$값으로 DC값을 대치한다.

Step7: 대치된 DC_k'값을 블록에 적용한 후 IDCT해서 워터마크된 이미지를 얻는다.

2.2 워터마크 추출 알고리즘

추출과정은 워터마크된 이미지를 DCT변환한 후 Q와 S인자를 이용하여 삽입한 워터마크 정보를 추출하고, 입력으로 받은 key를 가지고 추출 정보를 재배치하여 로고 이미지를 만든다(그림 2). 본 추출 알고리즘은 복잡하지 않기 때문에 워터마크의 빠른 추출이 장점이다.

Step1: Permutation할 때 사용된 key를 이용해서 inverse random permutation한다.

Step2: 워터마크된 이미지를 DCT변환한다.

Step3: DC_k'을 Q로 나누고 반올림하여 정수로 만든다.

$$H_k' = \mathrm{int}\{DC_k'/Q\}$$

Step4: H_k'를 S로 나눈 후 나머지 값을 이용하여 삽입한 워터마크 정보를 추출한다.

$$wk_k' = H_k' \bmod S$$

Step5: 입력으로 받은 key로 추출한 워터마크 wk_k'를 재배열하여 로고 이미지를 만든다.

3. 실험 과정 및 결과

본문에서 제안한 알고리즘을 이용하여 quantization step-size(Q)에 따른 JPEG, noise, resize, clipping 등 4가지 실험을 한 후 최적의 Q값을 선택한다.

V는 256×256 크기의 Lena 이미지, W는 32×32 크기의 2색 로고이미지를 사용하였다. 2색 로고이미지를 사용하였기 때문에 S는 2가지되고, K는 로고이미지의 크기이므로 1024(=32×32)가 된다. Q값은 양자화 크기를 정하는 인자로 이 값에 따라서 공격에 대한 강인성의 변화가 가장 민감하다. Q값이 작으면 JPEG의 양자화단계에서 정보 손실이 많으며, Q값이 크면 공격에는 강하나 화질의 손상이 심한 특성이 있다.

그림 3은 Lena, Baboon, Cameraman 등의 서로 다른 3가지 이미지에 각기 다른 로고 이미지를 삽입하여 워터마크된 이미지와 검출된 로고 이미지가 90% 인 경우를 보여주고 있다. 삽입된 로고 이미지의 90%이상만 검출되면 로고 이미지를 눈으로 식별하는데 문제가 없는 수준임을 알 수 있다. 워터마크된 이미지에 공격을 가하지 않았을 때의 PSNR과 Q, 워터마크 검출률과의 관계를 그림 4에 나타내었다. 그림 4에서 보면 3가지 이미지에 대한 결과가 거의 일치하므로 본 알고리즘은 원본 이미지나 로고 이미지의 변화에 영향을 받지 않음을 알 수 있다.

그림 4의 Q에 따른 PSNR을 보면 전 범위가 38dB이상으로 워터마크된 이미지의 PSNR값은 좋은 편이다. 그리고 검출률과 Q의 결과를 보면, 공격을 가하지 않을 때 검출률이 100%가 되는 Q값은 8이상의 값이다. 두 결과를 보면 Q의 범위는 8에서 35사이의 값을 갖는다.

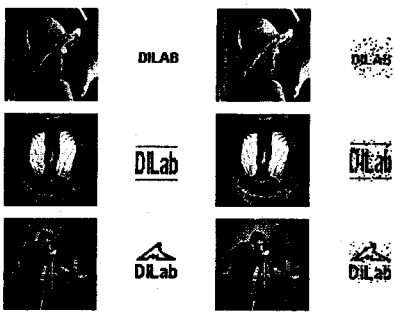

그림 3. "Lena", "Baboon", "Cameraman"의 원본 이미지, 삽입 로고 이미지, 워터마킹된 이미지,90% 검출 로고 이미지

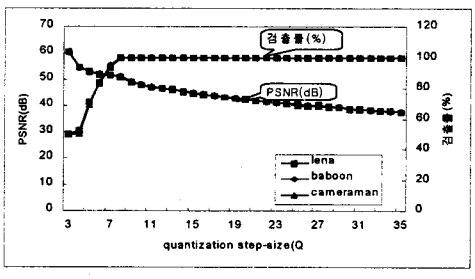

그림 4. 공격을 가하지 않은 경우 PSNR과 Q 및 검출률의 관계

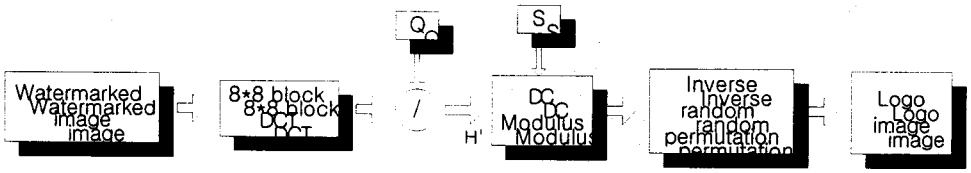

그림 2. 워터마크 추출 블록도

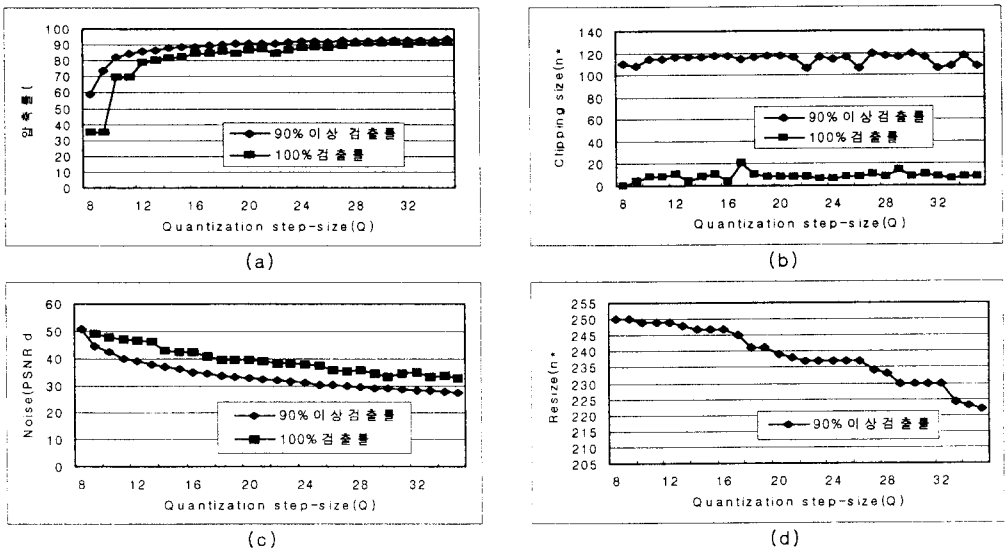

그림 5. 공격을 가한 경우 (a) Q와 JPEG압축에 따른 결과 (b) Q와 clipping에 따른 결과
(c) Q와 noise에 따른 결과 (d) Q와 resize에 따른 결과

강인성을 실험하기 위해 워터마크된 이미지에 JPEG, clipping, noise, resize 등의 4가지 공격을 가한 후 검출되는 워터마크를 살펴보았다. 그림 5(a)-(c)는 JPEG, clipping, noise 등의 공격을 가하였을 때 삽입한 워터마크가 100% 검출되는 경우와 90% 이상 검출되는 경우의 Q에 대한 관계를 보여주는 그래프이다. 그림 5(d)에서는 resize공격에 대한 결과를 보여주고 있는데, resize공격을 가할 때에는 워터마크가 100% 검출이 되지 않으므로 90%이상 검출될 때의 Q에 대한 관계만을 나타내었다. 삽입한 워터마크가 각종 공격에 대한 강인성을 갖아야 하는 기준을 JPEG 은 90%이상, clipping은 100×100이상, noise은 30dB이하, resize는 235×235이상으로 정했다(표 1 참조).

표 1. 기준 공격값

공격방법	기준값
JPEG 압축	압축률 90% 이상
Clipping 크기	100×100 이상
Noise 삽입	PSNR 30dB 이하
Resize	235×235 이상

그림 5(a)의 Q와 압축에 따른 결과를 보면 약 90% 압축을 했을 때 90% 이상의 워터마크 검출률을 갖기 위해서는 Q는 12 이상이어야 하고, 100%의 검출률을 갖기 위해서는 Q는 20 이상일 때가 좋음을 알 수 있다. 그림 5(b)의 Q와 clipping공격에 따른 결과를 보면 원본 이미지의 크기인 256×256의 1/4보다 조금 작은 120×120까지만 clipping공격에 강인함을 보이며, Q에 대한 강인성의 변화는 별로 없음을 알 수 있다. 또한 워터마크를 100% 추출하기 위해서는 clipping 크기가 20이하의 극히 작은 부분만 잘라내야 한다. 그림 5(c)의 Q와 noise에 따른 결과를 보면 노이즈의 경우는 30dB이하를 기준으로 정했는데, 이를 만족하는 Q는 25 이상이다. 그림 5(d)의 Q와 resize에 따른 결과를 보면 전체적으로 나쁜 결과를 보이고 있지만 기준을 만족하는 Q의 값은 27이상이다.

결과를 종합적으로 정리하면 JPEG압축 공격에 강인함을 유지하기 위해서는 Q값이 20이상, clipping공격에 대해서는 Q값의 영향이 적으며, noise공격에 대해서는 Q값이 25이상, resize공격에서는 Q값이 27이상일 때 기준에 만족하고 있다. 공격을 가하지 않은 경우와 공격을 가한 경우를 종합하여 보면 Q는 24일 때 가장 좋은 성능을 보인다.

Ⅳ. 결론

제안된 워터마킹 방법은 워터마크 삽입시 사용된 key만을 사용하여 삽입한 로고 이미지를 추출할 수 있으며, 워터마크된 이미지에 여러 가지 공격을 가하였을 때 강인함을 갖도록 파라미터를 최적화하였다. 제안한 알고리즘을 이용하여 삽입한 후 공격을 가한 결과 Q값을 24로 하였을 때가 가장 좋은 성능을 보였으며, JPEG에는 90%이상의 압축을 가해도 워터마크의 추출이 가능하며, clipping 에서는 원 이미지 크기의 약 1/4 이상을 잘라내도 워터마크가 검출되며, PSNR이 30dB 정도가 되도록 noise를 가하여도 워터마크가 검출되며, resize를 235×235크기로 줄여도 워터마크가 검출되는 강인함을 보였다. 본 연구에서 개발한 알고리즘은 특히 JPEG 압축을 90%이상 가해도 검출률이 100%가 나오는 강인성을 가지므로 동영상 워터마크 알고리즘으로 적용하기에 적합하다.

[참 고 문 헌]

[1] C. F. Osborne, R. G. Schyndel and A. Z. Tirkel, "A Digital Watermarking," *Int. Conf. on Image Processing*, Vol.2, pp.86-90, Nov. 1994

[2] W. Bendor, D. Gruhl, N. Morimoto, and A.Lu, "Techniques for Data Hiding," *IBM Systems Journal*, Vol.38, No.3&4, pp.313-336, 1996

[3] E. Koch, J. Rindfrey, J. Zhao, "Copyright protection for multimedia data," *in Proc. Int. Conf. Digital Media and Electronic Publishing*, 1994

[4] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermaking for multimedia," *IEEE Trans. on Image Processing*, Vol6, No.12, pp.1673-1687,Dec. 1997

[5] X. Xia, C. G. Boncelet, G. R. Arce, "A Multiresolution Watermark for Digital Images," *Proc. IEEE ICIP*, Vol.3, pp.548-551, 1997

[6] 후지와라 히로시, 그림으로 보는 최신 MPEG, 교보문고, 2000, pp.77-91

[7] Hisashi Inoue, Akio Miyazaki, Takashi Araki, Takashi Katsura, "A Digital Watermark Method Using the Wavelet Transform for Video Data," *IEICE TRANS. FUNDAMENTALS*, Vol.E83-A, pp.90-95, 2000