동영상 비디오 워터마킹 기법 성능분석

권순각*, 김진호**
*동의대학교 컴퓨터영상공학부 소프트웨어공학전공
**한국전자통신연구원 컴퓨터-소프트웨어연구소 디지털저작권관리연구팀

Performance Analysis for Video Watermaking Method

Soon-kak Kwon*, Jin-Ho Kim**
*Division of Computer Video Engineering, Dongeui University
**Computer-Software Laboratory / Digital Rights Management Team, ETRI
E-mail : *skkwon@dongeui.ac.kr, **jhokim@etri.re.kr

요 약

본 논문에서는 동영상 신호에 대한 워터마킹 알고리즘의 관점에서 워터마킹 성능, 부호화성능, 실시간 구현 등의 요구조건 사이의 관계를 살펴보고, 모의실험을 바탕으로 재부호화시의 강인성, 필터링공격에 대한 강인성 등 동영상 워터마킹 방법에 대해 성능을 분석한다.

1. 서론

비디오 워터마킹의 요구조건은 이미지 워터마킹의 요구조건과 비슷하지만 요구조건 들간의 trade-off가 많이 달라질 수 있다. 비디오 워터마킹의 경우 호스트 신호 대 워터마크 정보의 비(ratio), 즉 삽입되는 워터마크의 정보량은 비교적 덜 중요한(less critical) 요소가 되는 반면, 시간정보의 추가로 인해 워터마킹으로 인한 시각적 왜곡(visual distortion)이 중요한 요소가 된다. 또한 비디오의 경우 프레임 비율의 변환(frame-rate conversions)과 같은 가능한 공격의 수가 증가될 수 있기 때문에 강인성(robustness)에 대한 고려가 중요하다. 무엇보다도 실시간 처리가 요구되는 비디오 워터마킹의 경우 계산량의 복잡도 문제가 중요한 고려 요소가 된다.

지금까지 워터마킹에 대한 대부분의 연구는 이미지 워터마킹에 관한 것이며, 따라서 오디오나 이미지보다 비디오 워터마킹이 현재 open problem으로 남아있다. 이미지에 대해 정의된 대부분의 기본적인 워터마킹 이론이 비디오 워터마킹에 그대로 적용될 수 있는데 예를 들면 호스트 신호의 DCT 계수에 워터마크 정보를 더하는 방법이 JPEG 스트림 뿐만 아니라 MPEG 스트림의 I 프레임에 그대로 적용될 수 있다. 하지만 비디오의 시간차원의 추가로 인해 발생하는 drift와 같은 문제가 새로이 극복되어야 한다. 즉 I 프레임에 워터마크를 삽입할 때 발생한 왜곡이 MPEG 알고리즘에 포함된 움직임 보상(motion compensation) 모듈로 인하여 주위의 P 및 B 프레임에 영향을 미칠 수 있다.

비디오 워터마킹은 이미지 워터마킹보다 워터마크 정보를 넣을 수 있는 비트의 수가 많다는 장점을 가지고 있지만 실시간 처리가 요구된다. 그리고 워터마크 삽입영역에 따라 비압축영역의 워터마킹과

압축영역의 워터마킹으로 나눌 수 있다. 현재 이미지 워터마킹에서 사용되는 기법들이 조금 변형된 상태에서 비디오 워터마킹에 응용되고 있으며, 주로 압축영역에서의 워터마킹이 사용되고 있다.

본 논문에서는 비디오 워터마킹 기법을 살펴보고, 모의실험을 바탕으로 성능을 분석한다.

2. 비디오 워터마킹 기법

비디오 워터마킹 기술들을 분류하는 가장 일반적 기준은 워터마크가 삽입될 비디오 신호의 압축성 여부이다. 대개의 워터마킹 기법들은 비압축 영역(uncompressed video) 상에서 동작한다[6]~[9]. 일반적으로 디지털 비디오는 방송 또는 분배 시에 WWW이나 VOD 등의 서버상에서 압축 형태로 저장되어 있다. 그러므로 압축된 비디오 신호에 비압축 영역의 워터마킹 기법을 적용하려면 원 비디오 신호를 복구하여 워터마크 정보를 삽입한 후, 이를 다시 재압축(reencoding)하는 복잡한 과정을 거쳐야 하므로 현실성이 떨어진다고 볼 수 있다. 이는 이미지 워터마킹과는 달리 비디오 워터마킹의 경우에는 알고리즘의 견고성 뿐 아니라 실시간 구현을 위한 계산 복잡도가 매우 중요한 설계 요인이기 때문이다. 이점을 고려한다면 비디오 신호의 복호 및 재압축 과정을 필요로 하지 않는 압축 비트스트림 상의 워터마킹 알고리즘 개발이 보다 바람직하다. 압축 영역에서의 비디오 워터마킹 알고리즘으로는 DCT 계수[1][2][3], 코드워드[2], 움직임 벡터[5] 또는 GOP 구조와 같은 부가 정보[4]에 워터마크를 삽입하는 방법 등이 제시되어 있으며, 이 중 DEW (Differential Energy Watermarking) 방법[2] 성능이 우수하다.

DEW 방식은 기본적으로 압축된 데이터 스트림의 고주파 DCT 계수를 선택적으로 제거함으로써 정보를 삽입하는 방식이며, 이때 각 비트는 DCT 블록들 간의 에너지 차의 패턴에 기반하여 삽입된다. 우선, 비디오 신호에 삽입될 정보를 $L_j(j=0,1,\cdots,L-1)$ 라벨 비트들로 구성되는 라벨 비트열 L로 나타낸다. 라벨 비트열은 비트 단위로 MPEG 압축 비디오의

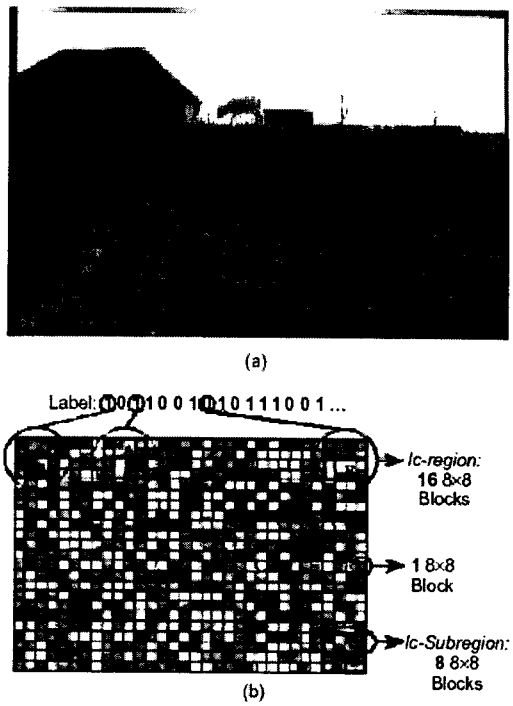


그림1. (a)샘플 영상, (b)블록단위로 셔플링된 영상

I-frame에서 취해진 n개의 8X8 DCT블록 마다 하나씩 삽입된다. 공격에 대한 강인성을 유지하기 위하여 n은 대개 16과 64 사이의 값으로 설정되는데, 이는 각 라벨 비트들이 주어진 영상에서 n개의 블록으로 구성되는 영역(region)에 삽입됨을 의미한다. 그러나, 그림1에서 보듯이 라벨 비트가 삽입되기 전에 영상을 8X8 DCT 블록 단위로 뒤섞어서 배치한다. 이 셔플링(shuffling) 과정은 라벨링 기법에 대한 비밀키(secret key)의 기능을 가지면서 동시에 DCT 블록들 간의 통계 특성을 공간적으로 난수화하는 작용을 한다.

라벨 비트열의 각 비트는 셔플링된 영상의 lc-region(label bit-carrying-region)에 삽입된다. 예를 들어 그림1에서처럼 n=16인 경우 라벨의 첫번째 비트는 영상의 좌상의 16개 DCT 블록으로 구성되는 lc-region에 삽입된다. 각 lc-region은 위, 아래에 따라 n/2=8개 DCT 블록으로 구성되는 두개의 lc-subregion으로 나누어지며, 이 두 lc-subregion들 사이의 에너지 차분을 이용하여 라벨의 비트 값이

삽입된다. 만약 위쪽 lc-subregion(lc-subregion A)이 아래쪽 lc-subregion(lc-subregion B)보다 큰 고주파 에너지를 가지면 0이 삽입된 것이며, 작은 고주파 에너지를 가지면 1이 삽입된 것이다. 압축된 비디오 프레임의 고주파 에너지를 계산하기 위해 다음의 식처럼 zigzag 스캐닝된 DCT 계수의 부집합에 대한 에너지를 계산한다.

$$S(c) = \{i \in \{0,63\} \mid (i > c)\} \quad (1)$$

Zigzag 스캐닝 된 DCT 계수는 그림2와 같이 순서가 정해지며, $i = 0$ 은 DCT 블록의 DC 계수에 해당한다. 에너지 계산에 사용되는 DCT 계수들의 집합 $S(c)$ 는 cut-off 지수 c 에 의해 결정되며, 주어진 lc-region에 적합한 c 의 선택은 라벨 비트의 강인성과 가시성에 있어서 매우 중요한 과정이다. 큰값의 cut-off 지수가 사용될수록 라벨 삽입에 따른 화질의 저하는 적어진다. 그리고, 각각의 lc-region들은 그들의 공간 신호 특성에 따라 서로 다른 cut-off 지수를 갖는다.

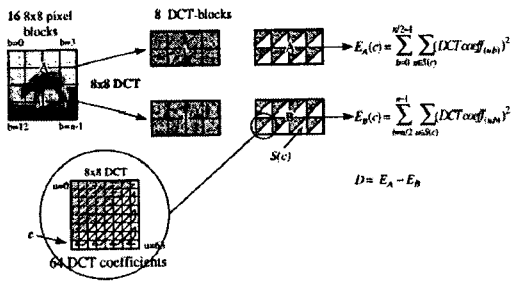


그림2. 고주파 DCT계수에 의한 에너지 차분 계산 예

lc-subregion의 에너지 E_A 는 다음의 식으로 정의된다.

$$E_A(c,n,Q_{jpeg}) = \sum_{b=0}^{n/2-1} \sum_{i \in S(c)} ([\theta_{i,b}]_{Q_{jpeg}})^2 \quad (2)$$

여기서 $\theta_{i,b}$ 는 lc-subregion A의 b번째 DCT 블록의 i번째 DCT 계수를 나타낸다. E_A 를 계산하기 전에 DCT 계수들은 quality factor, Q_{jpeg} 을 이용하여 재양자화된다. 이 양자화는 cut-off 인덱스를 결정하는 과정에서만 사용되며, 라벨 삽입 과정의 실제 영상 데이터에는 적용되지 않는다. E_B 로 표기되는 lc-subregion B의 에너지도 동일하게 정의된다.

두 lc-subregion A와 B 사이의 에너지 차분 D 의 계산식은 다음과 같다.

$$D(c,n,Q_{jpeg}) = E_A(c,n,Q_{jpeg}) - E_B(c,n,Q_{jpeg}) \quad (3)$$

라벨 비트의 값은 에너지 차분 D 의 부호에 삽입된다. 라벨 비트 0은 $D > 0$ 으로, 라벨 비트 1은 $D < 0$ 으로 정의된다. 그러므로, 라벨 삽입 과정은 D 를 계산하기 위한 E_A 와 E_B 를 반드시 조절해야 한다. 만약 0이 삽입되어야 하는 경우에는 lc-subregion B에서 DCT블록의 cut-off 인덱스 c이후의 고주파 계수를 0으로 함으로써 $D = E_A - E_B = E_A - 0 = +E_A$ 가 되도록 만든다. 반대로 라벨 비트 1이 삽입되는 경우에는 lc-subregion A의 DCT블록들에서 cut-off 인덱스 이후의 모든 에너지를 제거함으로써 $D = -E_B$ 가 되도록 한다. 워터마크가 압축된 비트 스트림 상에서 삽입되기 때문에, 두개의 lc-subregion중 한쪽에 속하는 8X8 DCT블록들의 EOB를 선택된 cut-off 인덱스까지 DC계수 방향으로 이동시킴으로써 재압축 없이 DCT 계수들을 0으로 만들 수 있다. 그림2에 $n = 16$ 인 셔플링 되지 않은 8X8 DCT 블록들인 경우에 lc-subregion의 에너지 차분 D 를 계산하는 전체적인 과정이 도시 되어있다. 식(2)에서처럼 DCT계수의 에너지를 계산하는 과정에서 Q_{jpeg} 으로 선양자화를 하기 때문에, DEW 방식은 JPEG/MPEG 압축에 의해 심각하게 영향받지 않는 영상의 중요 부분에 효과적으로 라벨을 삽입할 수 있다. 따라서, 과도한 화질의 열화가 발생하지 않는 한, DEW 워터마크를 제거하기는 거의 불가능하다.

D 값은 라벨링 과정에서 제거되어야 하는 DCT 계수의 개수를 결정할 뿐 아니라, 삽입된 라벨의 가시성과 견고성도 결정하게 된다. 워터마크 삽입과정에서 주요 저주파 DCT 계수가 제거되는 것을 방지하기 위해서는 cut-off 지수 c 가 특정 임계치 $c_{\min}$ 보다는 크게 선택되어져야 한다. 이를 고려할 경우 c 에 대한 결정식은 다음과 같이 표현된다.

$$C(n,Q_{jpeg},D,c_{\min}) = \max\{c_{\min}, \max\{i \in \{0,63\} \mid E_A(i,n,Q_{jpeg}) > D) \wedge (E_B(i,n,Q_{jpeg}) > D)\}\} \quad (4)$$

Ic-region에서 라벨 정보를 추출하기 위해서는 삽입 과정에서 사용된 cut-off 지수를 알아야 한다. 이를 위해 우선 $E_A(c,n,Q_{jpeg})$와 $E_A(c,n,Q_{jpeg})$가 모든 cut-off 지수 $c = 0,\cdots,63$ 에 대해 계산된다. Ic-subregion A 또는 B의 일부 DCT 계수가 워터마크 삽입 과정에서 제거되었기 때문에, 우선 각 Ic-subregion 에 대해 임계값 D' 보다 작은 에너지를 가지는 두개의 최소 지수를 구한다. 그러면 실제 사용된 cut-off 지수는 이 두 값 중에서 큰 값으로 결정된다.

3. 비디오 워터마킹 기법의 성능 분석

기존의 비디오 워터마킹 기술 중에서 가장 많이 인용되고 있는 DEW(differential energy watermarking) 비디오 워터마킹 기법에 대하여 모의 실험을 통해 성능을 분석한다. DEW 방식에서 사용되는 파라미터들은 다음과 같다.

- D : 하나의 Ic-region에서의 에너지 차로서 이 값은 8x8 블록단위의 값으로 정규화될 필요가 있다. 이는 Ic-region의 크기가 영상의 크기 뿐만 아니라 삽입되는 비트량에 따라 변하기 때문이다. 지금부터 사용되는 D는 에너지가 아니라 정규화된 값인 MSE를 의미한다.
- C : 워터마크 삽입시의 cut-off point로서 이는 D에 의해 결정된다.
- T : 워터마크 검출시의 문턱 값으로서 위의 C 파라미터를 검출부에서는 알 수 없으므로 이를 추정하기 위해 사용된다. T는 항상 C보다 작아야 하며, 공격이 없을 경우 T는 어떠한 역할도 수행하지 않으나, 공격이 있는 경우 T는 워터마크 검출 신뢰도에 영향을 미친다.
- B : 삽입 비트수

DEW 방식의 파라미터는 아니지만 성능 분석을 위해 사용되는 파라미터는 다음과 같다.

- QP : 비디오 부호화에 사용되는 양자화 계수로서 비디오 압축 데이터의 비트율을 조절하는 데 사용된다. 양자화 간격 (step-size)은 QP의 두 배로 결정된다. QP는 비디오 데이터를 압축하는 과정에서 뿐만 아니라, 압축된 데이터의 재부호화 (re-encoding) 과정에서도 흔히 사용될 수 있다. 즉, 비디오 데이터를 채널이나 미디어의 용량에 따라 비트율을 가감할 수 있다. 이러한 비트율의 변화는 워터마크된 비디오에서 의도적이든 비의도적이든 워터마크에 영향을 준다.
- RDR (right detection ratio) : 이는 삽입된 워터마크 정보를 검출했을 때, 정확히 검출된 정보량대 삽입된 정보량의 비를 백분율로 표시한 것이다 즉,

$$RDR = \frac{\text{the number of bits correctly detected}}{\text{the number of bits embedded}} \times 100 \quad (5)$$

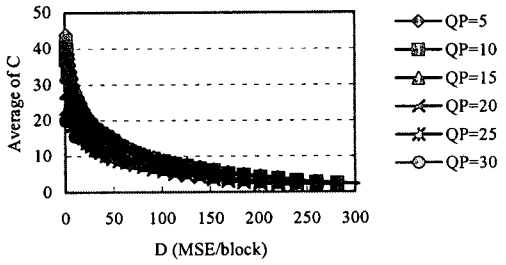
3.1 실험 환경

실험에 사용된 영상은 Coastguard, Container, Mobile 비디오 시퀀스로서, 각 영상은 CIF (352x288) 포맷을 가진다. 양자화기 (quantizer)는 H.263 양자화기로 MPEG-4의 second quantization method의 역양자화와 동일하다.

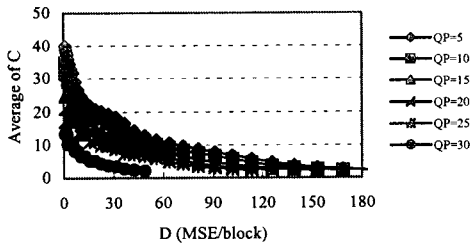
3.2 실험결과

1) D와 C의 관계 : D의 증가에 따른 C의 변화를 보기 위하여 각 영상에 대한 실험을 수행하였다. 그림 3은 각 영상에 대한 실험 결과이다. 그림에서 볼 수 있듯이, D의 증가에 따라 C의 평균값이 지속적으로 감소함을 관찰할 수 있다. 또한, QP의 증가에 따라 C의 평균값이 감소함을 알 수 있다.

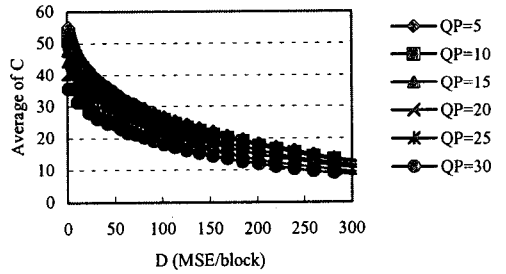
2) QP=10에 대한 각 영상에 있어서 D와 C, D와 PSNR과의 관계로부터의 고찰: 그림4는 QP=10일 때 각 영상에 대한 D-C와 D-PSNR를 한꺼번에 도시한 것이다. 이 그림에서 살펴보면, 영상에 따라 D에 따른 C의 변화가 큰 차이를 보이는 반면, D에 따른 PSNR의 변화가 큰 차이가 없음을 알 수 있으므로 워터마크의 삽입 시 기준으로 사용할 계수를 C보다는 D로 정하



(a) Coastguard000



(b) Container000



(c) Mobile000

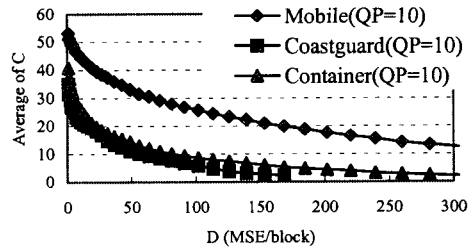
그림3. 실험영상에 대한 D-C의 관계

는 것이 적절하다는 것을 관찰할 수 있다. 즉, 고정된 C를 삽입기의 입력으로 사용하기보다는 고정된 D를 입력으로 사용하는 것이 더 적합할 것 같다.

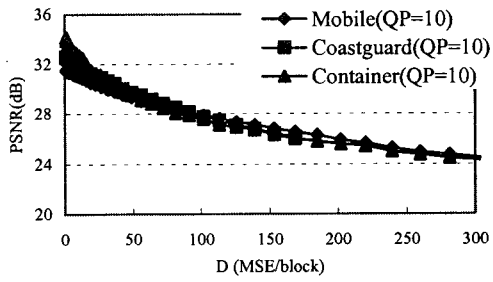
3) 재부호화 공격에 대한 강인성

그림 5 는 Coastguard 영상에 대한 재부호화 공격에 대한 실험 결과이다. 실험 결과에서 관찰할 수 있는 점은 다음과 같다.

- DEW방식이 재부호화 공격에 매우 강인하다. 예를 들어, 그림5(a)의 경우 (QP=10으로 부호화된 비트열에 대해, QP+1 (=11), QP+5 (=15), QP+9(=19),

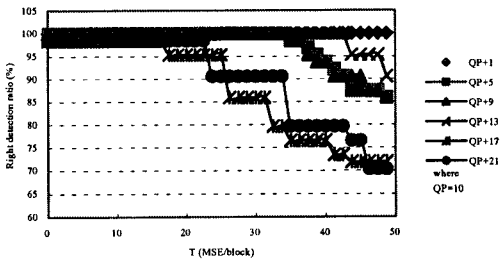


(a) D-Avg[C]

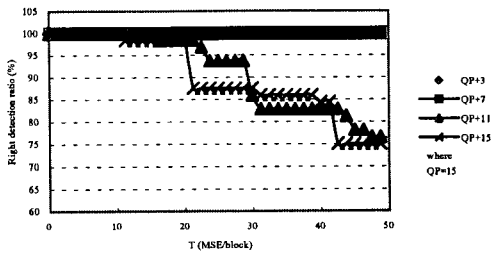


(b) D-PSNR

그림 4. QP=10 일때, D 에 따른 Avg[C], PSNR 의 변화



(a) 재부호화 공격시, T와 RDR과의 관계



(b) 재부호화 공격시, T와 RDR과의 관계

그림 5. 재부호화 공격에 대한 결과

QP+13 (=23), QP+17 (=27), QP+21 (=31)로 재양자화 하는 공격), 적절한 T 의 설정으로 QP+9 (=19) 까지는 RDR=100%임을 관찰할 수 있다. 즉, QP=10 로 부호화된 비트열을 QP=19 로 양자화해도 워터마크가 정확히 검출될 수 있음을 의미한다. QP=10 과 QP=19 는 양자화 계수에 있어서 큰 차이가 있음에도 워터마크가 정확히 검출되는 것은 DEW 방식이 재부호화 공격에 매우 강인함을 말한다. 그림 5(b)의 경우 (QP=15 로 부호화된 비트열에 대한 공격 실험)에도 마찬가지로 유사한 결과를 갖는다.

- 재부호화 공격의 경우 T 의 증가에 따라 RDR 이 단조(monotonically) 감소하는 경향이 있다. 이는 재부호화 공격은 DCT 계수를 첨가하는 공격이 아니라 DCT 계수를 제거하는 공격만 있기 때문이다.

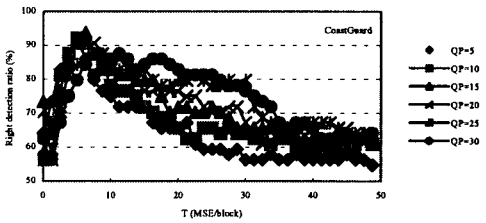
4) 필터링 공격에 대한 강인성

필터링 공격에 대한 강인성 실험에서도 재부호화 공격에서와 마찬가지로 D=50 으로 설정하였다. 필터링 공격이란 다음과 같이 정의된다.

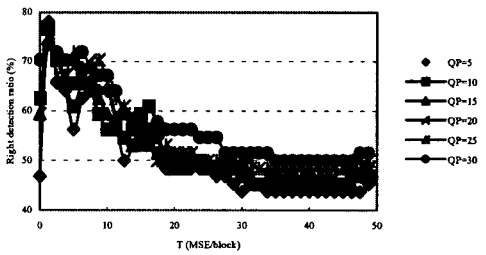
1) QP=A 로 부호화된 비트열을 복호화 하여 영상을 얻는다.
2) 1)에서 얻어진 영상에 대해 필터링을 수행한 결과 영상을 QP=A로 다시 부호화하여 비트열을 얻는다.

그림 6 은 Coastguard 영상에 대한 3x3 mean filter 와 5x5 mean filter 를 적용한 공격에 대한 실험 결과이다. 실험 결과에서 관찰할 수 있는 점은 다음과 같다.

- DEW 방식이 필터링 공격에 비교적 약하다. 정지영상에 대해 적용되는 대부분의 워터마킹 기법들이 필터링 공격에 매우 강인한 것에 비한다면 DEW 방식은 필터링 공격에 약하다고 말할 수 있다.
- 재부호화 공격의 경우 T 의 증가에 따라 RDR 이 단조(monotonically) 감소하는 경향이 있는 반면, 필터링 공격의 경우 T 의 증가에 따라 RDR 이 증가했다가 감소하는 경향을 가지고 있다. 이것은 적절한 T 의 선택이 RDR 의 성능에 영향을 미침을 의미한다. RDR 이 최대값을 가지는 T 를 최적의 T ($T_{optimal}$)라고 정의하자. 그 때, 그림 6(a)와 그림 6(b)를 비교하면 그림 6(a)의 $T_{optimal}$ 가 그림 6(b)의 $T_{optimal}$ 보다 큰 것을 관찰할 수 있다. 3x3 mean filter 는 5x5 mean filter 의 차단 주파수 (cut-off frequency)에 있어서 큰 값을 가진다는 점을 고려한다면, 본 실험 결과에서는 차단주파수가 낮아질 수록 $T_{optimal}$ 이 낮아짐을 관찰할 수 있다. 물론 각각의 $T_{optimal}$ 에서 차단주파수가 낮은 필터링 공격을 수행했을 때의 RDR 이 낮아진다. 이는 차단주파수가 낮을수록 영상 정보가 많이 제거되기 때문이다.



(a) 3x3 mean filtering 공격시, T와 RDR과의 관계



(b) 5x5 mean filtering 공격시, T와 RDR과의 관계

그림6. 필터링 공격에 대한 결과

4. 결론

DEW 방식의 입력 계수, D, C, T, B와 부호화 계수, QP, 그리고 PSNR, RDR에 대한 실험을 수행한 결과로부터 다음과 같은 결론을 내릴 수 있다.

- D의 증가에 따라 C의 평균값이 지속적으로 감소한다. 또한, QP의 증가에 따라 C의 평균값이 감소한다.
- 영상에 따라 D에 따른 C의 변화보다는 D에 따른 PSNR의 변화가 차이가 적으므로 워터마크의 삽입시 기준으로 사용할 계수를 C보다는 D로 정하는

것이 적절하다.

- 워터마크 삽입전의 영상과 삽입 후의 영상에 있어 주과적 화질 저하가 적다.
- DEW방식은 재부호화 공격에 매우 강인하다. 재부호화 공격의 경우 T의 증가에 따라 RDRO이 단조(monotonically) 감소한다. 즉, $T_{optimal} = 0$ 이다.
- DEW방식은 필터링 공격에 비교적 약하다. 필터링 공격의 경우 T의 증가에 따라 RDRO이 증가했다가 감소하는 경향을 가지고 있다. 즉, $T_{optimal} \neq 0$ 이다.
- 재부호화 공격과 필터링 공격의 두 가지 공격에 대한 실험 결과로부터 대략 $T_{optimal} = D/10$ 이면 영상에 관계없이 최적의 결과를 얻을 수 있다.

참 고 문 헌

[1] F.Hartung and B.Girod, " Watermarking of uncompressed and compressed video," Signal Processing, vol.66, no.3, pp. 283-301, 1998.

[2] G.C.Langelaar, R.L.Lagendijk and J.Biemond, " Real-time labeling of MPEG-2 compressed video," Journal of Visual Communication and Image Representation, vol.9, no.4, pp. 256-270, Dec., 1998.

[3] F.Hartung and B.Girod, " Digital watermarking of raw and compressed video," Proc. SPIE Digital Compression Technologies and Systems for Video Commun., vol. 2952, Oct. 1996, pp. 206-213.

[4] J.-P. Linnartz. (1998). MPEG PTY marking. [Online]. Available WWW:http://diva.eecs.berkerly.edu/linnartz/pty.

[5] F.Jordan, M.Kutter and T.Ebrahimi, " Proposal of a watermarking technique for hiding /retrieving data in compressed and decompressed video," ISO/IEC Doc. JTC1/SC29/WG11 MPEG97/M2281, July, 1997

[6] M.Swanson, B.Zhu, and A.Tewfik, " Multiresolution scene-based video watermarking using perceptual models," IEEE J. Select. Areas Commun., vol.16, pp. 540-550, May, 1998.

[7] V.Darmstaedter, J.-F. Delaigle, D.Nicholson, and B.Macq, " A block based watermarking technique for MPEG2 signals: Optimization and validation on real digital TV distribution links," Proc. European Conf. Multimedia Applications, Services, and Techniques-ECMAST ' 98, Berlin, Germany, May 1998

[8] J.Dittmann, M.Stabenau and R.Steinmetz, " Robust MPEG video watermarking technologies," Proc. ACM Multimedia' 98. Bristol U.K., Sept. 1998.

[9] C.Busch, W.Funk, and S.Wolthusen, " Digital watermarking: From concepts to real-time video applications," IEEE computer Graphics and Applications, pp. 25-35, Jan., 1999.