이학석사 학위논문

블록 인덱싱을 이용한 DCT 기반 워터마킹

지도교수 신 상 욱

이 논문을 [illegible] 제출함

2005년 2월

부경대학교 대학원

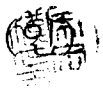
전 자 계 산 학 과

한 승 우

한승우의 이학석사 학위논문을 인준함

2004년 12월 23일

주심 공학박사 김 창 수 

위원 공학박사 여 정 모 

위원 이학박사 신 상 욱 

<차례>

<표차례>

<그림차례>

DCT Based Watermarking Using Block Indexing

Seung-Wu Han

Dept. of Computer Science, Pukyong Nat'l University

Abstract

Digital watermarking is the enabling technology to prove ownership on copyrighted material, detect originators of illegally made copies, monitor the usage of the copyright multimedia data and analyze the spread spectrum of the data over networks and server.

In this thesis we propose a novel blind watermarking algorithm for digital contents. The proposed algorithm is a watermarking scheme using a indexed watermark value based on the spread spectrum method, and is more efficient than any other watermarking schemes. In case that the whole watermark is 128 bit, it is embedded in the 16 sub-blocks out of 256 sub-blocks of original image. Each block is indexed by 8 bit binary value from 00000000 to 11111111. The first 4 bits are used to represent the order of watermark information and the remaining 4 bits mean the watermark information. An index value of sub-blocks is a decimal value of 8 bit binary value combined the watermark information of 4

bit with the order of watermark information of 4 bit. The scheme embeds PN Sequences in selected 16 sub-blocks; the watermark value is indexed in relevant sub-blocks. The indexed watermark value includes the order of watermark information; the scheme can detect some blocks have low correlation value in extracting process. The watermarking scheme based on DCT and indexed watermark value has invisibility property. It is also robust to image signal processing techniques such as Gaussian filtering, Histogram Equalization, JPEG compression, Low pass filtering, Median filtering, Sharpening.

1.서론

컴퓨터 기술의 발달과 인터넷의 급속한 보급으로 인하여 디지털 미디어의 제작 및 정보 교환이 활발히 이루어지고 있다. 온라인상에 쉽게 유통되어 편리성을 제공하지만, 누구나 디지털 데이터의 내용을 쉽게 변형 및 복제가 가능하기 때문에 저작권 침해가 생겨나게 되었으며 이를 해결하기 위한 기술을 필요로 한다.

1.1 연구배경 및 목적

빠른 속도로 발전하는 네트워크 기술과 인터넷의 활성화로 인해 다양한 멀티미디어의 디지털화가 이루어졌고 디지털 데이터가 아날로그 데이터에 비해 저장 및 편집이 용이하고 온라인상에 쉽게 유통되어 편리성을 제공하지만, 누구나 디지털 데이터의 내용을 쉽게 변형 및 복제가 가능하기 때문에 각종 멀티미디어 서비스와 환경이 개인에게까지 제공되고 있다. 디지털 데이터는 원본과 복사본의 구별이 불가능하기 때문에 저작권 침해의 문제가 발생하게 되었으며, 이에 따라 저작권 침해를 방지 및 억제하기 위한 방법으로 저작권 정보를 나타내는 마크를 저작물에 삽입해 저작권을 보호하는 디지털 워터마킹 기법이 연구되고 있다.

워터마킹이란 디지털 콘텐츠에 사용자의 ID(Identification)나 자신만의 정보를 삽입하여 불법적인 복제를 막고, 데이터의 소유자의 저작권과 소유권을 효율적으로 보호하기 위한 방법으로써 데이터에 일정한 암호를 숨겨서 부호화 하는 과정으로 이러한 부호를 워터마크라 한다. 디지털 콘텐츠에 삽입되는 워터마크로 사용될 수 있는 정보들은 소유자, 시간,

날짜, 웹 주소, 이메일 주소, 복사권한 등으로 이러한 정보들을 검출하여 저작권 보호나 콘텐츠의 위·변조 여부를 가리는 데 사용하고 있다.

대표적인 초기 워터마킹 기법으로 Piva[1]와 Cox[2]의 기법을 들 수 있다. DCT(Discrete Cosine Transform)를 사용하여 영상을 변환한 후, 가장 큰 DCT계수 1000개를 선택하여 워터마크 신호를 삽입한다. 가장 큰 계수들을 사용한 이유는 큰 값을 지닌 DCT계수가 에지나 고주파 성분이 많은 부분에 해당한다는 HVS(Human Visual System)를 활용하기 위함이다. 즉, 픽셀 값을 조금 변형시켜도 눈에 띄지 않는다는 특성을 사용하기 위함이다. 다양한 신호처리 변화에도 워터마크를 검출할 수 있지만 검출 시에 원 영상이 필요하며, 워터마크의 존재 유·무만을 판단할 수 있는 1비트 정보밖에 제공하지 못하고 있다.

본 논문에서는 멀티미디어 콘텐츠에 기밀정보를 은닉시키기 위하여 블록 인덱싱을 이용한 영상 워터마킹 기법을 제안한다. 제안기법은 DCT 기반의 대역확산 방법을 이용하고 있으며, 저작권 보호에 초점이 맞추어져 있는 워터마크 기술을 효율적으로 설계하고 현실적인 응용에 확대시키기 위함이 목적이다.

1.2 연구내용 및 구성

본 논문은 기밀정보 은닉을 위해 블록의 인덱싱을 이용해서 워터마크 값을 표현하는 영상 워터마킹을 제안하고 있다. 512 * 512 크기의 원 영상을 32 * 32 크기로 분할시켜 256개의 블록을 만들 수 있으며, 각 블록은 1부터 256까지의 인덱스로 표시된다. 각 블록의 인덱스는 8비트로 표현 가능하다. 앞의 4비트는 워터마크 정보의 순서로 워터마크 값의 동기를 맞추는데 사용되며, 뒤의 4비트가 저작권을 표시하기 위해 삽입되는

워터마크 정보가 된다. 따라서 64비트의 워터마크 값이 256개의 서브블록 중에서 16개의 블록으로 인덱싱 된다. 삽입하고자 하는 워터마크 정보가 특정한 블록의 인덱스 값으로 표현되었다는 것을 나타내기 위해서 Piva의 워터마킹 방법을 이용하여 인덱싱된 블록에 PN(Sheudo Noise) 시퀀스를 삽입한다. 워터마크 추출은 삽입 시 사용된 PN 시퀀스와 PN 시퀀스가 삽입된 대역간의 상관도 값을 구한 후 상관관계가 높은 블록의 인덱스 값을 구하는 것으로 가능하며, 다양한 신호처리적인 공격에 대한 내성을 제시한다. 본 연구의 핵심적인 제안은 삽입하고자 하는 워터마크를 서브블록의 인덱스 값으로 매핑시키는 것이며, 워터마크가 서브블록의 인덱스 값으로 인덱싱되었다는 것을 표현하기 위해 해당되는 블록마다 Piva의 워터마크 기법을 이용하여 PN 시퀀스를 삽입하고, 삽입된 PN 시퀀스의 자기상관도를 이용한 추출방법을 사용하고 있다.

본 논문의 구성은 다음과 같다. 먼저 2장은 디지털 워터마킹에 대한 소개를 하고 있으며, 3장에서 기존의 연구기법 중에서 본 논문에서 제안한 알고리즘의 바탕이 되는 Piva의 워터마크 기법을 설명한다. 4장은 제안방법에 대한 설명으로 정보 은닉을 위해 워터마크 값을 블록의 인덱스 값으로 사용하는 방법 설명하고, 5장에서 제안방법에 대해 다양한 공격에 따른 실험결과를 제시함으로서 제안된 방법의 효율성을 확인한다. 마지막으로 6장에서 결론을 맺는다.

2.디지털 워터마킹

워터마크(watermark)의 사전적 의미는 "물이 흔들릴 때 밝게 빛나는 부분", "종이나 서류에 투명한 표시를 하여 빛에 밝게 비추어 보면 나타나는 무늬 문양"으로, 700년 전 이태리의 여러 제지 제조업자들이 각자 자신들이 제조한 종이를 구분하기 위하여 눈에 잘 띄지 않게 자신들만의 문자나 기호 등을 삽입한 표시가 그 유래이다.

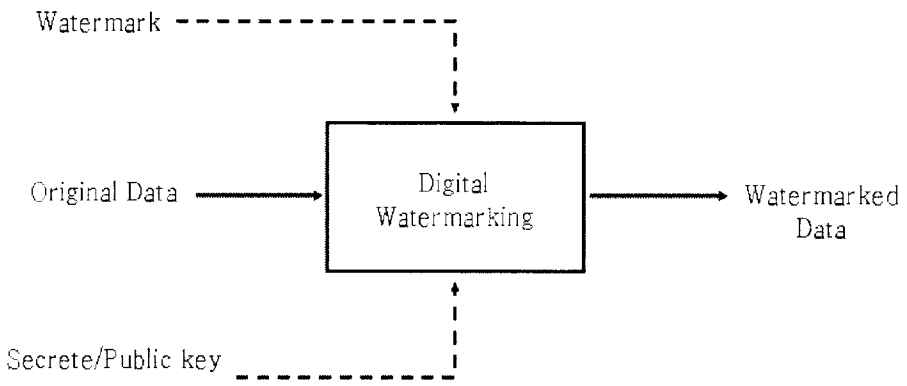
2.1 디지털 워터마킹의 정의

디지털 워터마크란 음악, 영상, 동영상 등의 디지털 데이터에 삽입되는 정보를 말하고, 저작권 보호를 위해 멀티미디어 콘텐츠에 공격자에 의해 인지되지 않도록 특별한 식별기능을 가지는 신호 또는 정보를 삽입하는 기술을 디지털 워터마킹이라 한다. 멀티미디어 콘텐츠에 삽입되어지는 워터마크에 싣는 정보로는 제작자, 소유자, 판매자, 거래자의 고유번호 등이 되고 이는 멀티미디어 콘텐츠를 불법 유통 시켰을 경우 네트워크 상에서 역 추적이 가능하게 된다. 워터마크는 여러 분야에서 응용이 되고 있는데 멀티미디어 저작물의 저작권 보호뿐만 아니라 각종 저작물의 인증(변조가 없었음을 보장), 무단 배포 방지, 불법 배포자 확인, 소유권 확인 등에 이용되고 있다.

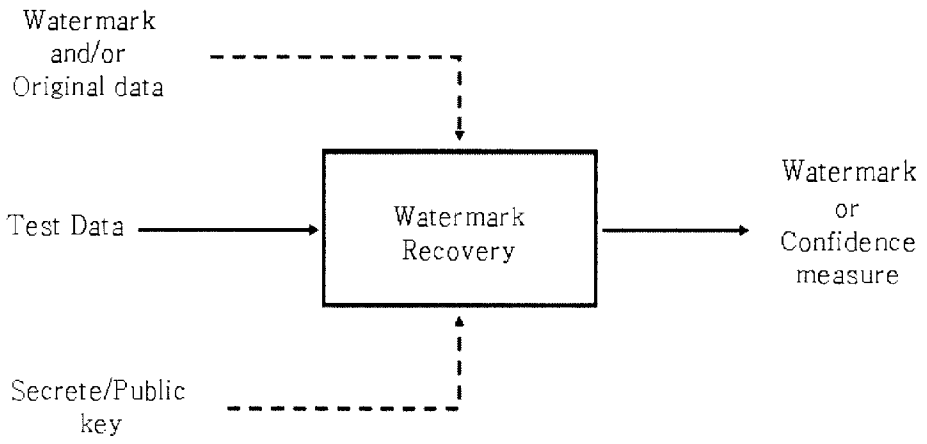
디지털 워터마킹 알고리즘은 워터마크를 멀티미디어 콘텐츠에 싣는 삽입 알고리즘과 저작권 확인을 위해 삽입된 워터마크를 검증하는 검출/추출(detection/extraction) 알고리즘으로 구성된다. 삽입 알고리즘은 원영상 X에 대하여, 워터마크 신호 W와 사용자 키 k가 주어졌을 때, 영상

X에 키 k를 이용하여 워터마크 W가 삽입되고 워터마크 되어진 영상 Y를 얻게 된다. 워터마크 검출 알고리즘은 검출 시 원 영상 X가 필요한 경우와 그렇지 않은 경우로 분류될 수 있으며, 검출 시 X가 필요한 경우는 원 영상을 가진 저작자만이 워터마크를 추출할 수 있다.

1) 워터마크 삽입



2) 워터마크 추출



2.2 디지털 워터마킹의 분류

디지털 워터마킹은 관점에 따라서 다양한 방법으로 분류할 수 있으나 일반적으로 다음과 같이 분류된다.

1) 견고성에 의한 분류

- 강인한 워터마킹(Robustness Watermarking)
  원 영상의 데이터를 파괴하지 않고서는 도저히 삽입된 워터마크를 없앨 수 없도록 하는 것으로 저작물의 원 소유자 확인 및 불법 제공자의 신원 확인 등에 사용되는 기법.

- 연성 워터마킹(Fragile Watermarking)
  원 영상에 대한 약간의 변형에도 워터마크가 쉽게 사라지도록 함으로써 무결성 확보 및 위조, 변조를 방지하기 위해 사용된다. 변형된 부분의 워터마크가 사라짐으로써 어떤 형태의 위조, 변조를 가했는지 파악하기 쉽고, 법정에서 무결성 주장의 근거를 제시하는 기법

- Semi-Fragile 워터마킹
  Fragile워터마크와 Robust워터마크의 중간단계로 사용자가 규정한 임계치를 초과하는 경우에 워터마크가 손상되는 기법으로 압축과 같이 영상의 내용을 변화시키지 않는 공격에 대해서는 워터마크가 살아남고 특정부분을 바꾸는 것과 같은 악의적인 공격에 대해서는 워터마크가 사라져서 위조, 변조 되었다고 판단하는 기법.

2) 영역에 의한 분류

- 공간영역 워터마킹(Spatial Domain Watermarking)
  공간영역에서 워터마킹이 이루어지는 기법.

- 주파수영역 워터마킹(Frequency Domain Watermarking)
  주파수 영역에서 워터마킹이 이루어지는 기법.

3) 검출 알고리즘의 공개여부에 의한 분류

- 공개 워터마킹(Public Watermarking)
  워터마크 검출 알고리즘을 공개하여 모든 사용자가 워터마크를 검출할 수는 있지만 제거나 생성을 할 수 없는 기법.

- 비공개 워터마킹(Private Watermarking)
  워터마크 검출 알고리즘을 공개하지 않아 다른 사용자가 워터마크를 검출할 수 없는 기법.

4) 추출 시 원 영상의 필요 여부에 의한 분류

- Blind 워터마킹
  원 영상 및 원 워터마크 없이도 워터마크를 추출할 수 있는 기법.

- Non-Blind 워터마킹
  원 영상을 사용해서 워터마크를 추출할 수 있는 기법.

2.3 디지털 워터마킹의 요구조건

일반적으로 디지털 멀티미디어 데이터의 저작권을 보호하기 위해서 삽입되는 워터마크는 다음과 같은 요구조건을 만족해야 한다.

1) 무감지성(Imperceptibility)

워터마크의 삽입으로 인해 저작권을 보호하고자 하는 저작물의 품질이 저하되어서는 안된다는 것이다. 워터마크를 시각적으로 인지하지 못하게 하는 것은 악의적인 공격자로부터 워터마크가 제거되지 않도록 하기 위함이다.

2) 강인성(Robustness)

워터마크 된 영상은 의도 또는 비의도적 영상 변형에 의해 제거되지 않아야 하고, 의도적인 워터마크 제거 공격에 대해서 강인해야 한다. 영상의 중요한 부분에 워터마크를 삽입하게 되면 워터마크 제거 시 심각한 화질열화가 발생된다. 비의도적인 공격에 대해서 워터마크가 손실되어서는 안된다. 필터링(filtering), 압축(compression-JPEG & MPEG), 축소/확대, cropping, translation, rotation, AD/DA변환, 양자화(resampling) 등의 각종 변환 공격에 강인해야 한다.

3) 보안성(Security)

워터마크 삽입 알고리즘이 공개되어진 경우라도 정확한 키를 알고 있지 않으면 워터마크의 삭제가 불가능해야 한다는 것이다, 즉 키는 사용자만이 가지고 있어야 한다.

4) 명확성(Unambiguousness)

워터마크 된 영상에 대해서 명확한 소유권을 주장할 수 있어야 한다. 공격자에 의해 임의로 만들어진 워터마크를 삽입하여 소유권을 주장할 경우 이들의 허위 사실을 증명할 수 있어야 한다.

5) 전환(Invertibility)

필요에 따라 기존의 정보를 삭제하고 새로운 정보의 삽입이 필요하나 상대적으로 공격에 약하다.

6) 충분한 정보의 삽입(Number of bits which can be hidden)

저작물의 번호, 구매자에 대한 정보 등을 수록하여 저작권을 나타냄으로 많은 정보의 삽입을 필요로 한다.

7) 낮은 검출 오류 확률(Low decision error probability)

워터마크는 극히 작은 오차일지라도 법적으로 문제가 심각함으로 워터마크 검출 시에 오류발생률이 낮아야 한다.

8) 워터마크의 빠른 검출(Fast watermark detection)

워터마크 삽입 시 계산 량은 중요하지 않지만 web searching을 통한 불법 저작물의 체크비용은 감소되어야 하므로 검출 시 계산 량은 작아야 한다.

3. 관련연구

디지털 영상/동영상 워터마킹 기술은 1990년대 초에 처음 소개되어 1990년대 중반부터 활발히 연구되어 현재까지 짧은 시간 사이에 많은 방법들이 개발되고 있으며 발전하고 있다.

3.1 일반적인 디지털 워터마크 기법

디지털 워터마킹 기술은 워터마킹 생성, 워터마크 삽입, 워터마크 검출단계 기술로 구분할 수 있다. 워터마크 생성과정은 삽입하고자 하는 워터마크를 어떤 형태로 대상 콘텐츠에 삽입할 것인지를 결정하는 방법으로 사용되는 워터마크는 이진(binary) 영상, 키(key)값에 의해 변환된 이진 영상, 키 정보에 의해 암호화된 문자열 또는 PN 시퀀스 등이 있다. 이러한 워터마크는 워터마크의 유무 정보뿐만 아니라 저작권, 소유자, 콘텐츠 내용 등을 포함할 수 있으며, 이렇게 워터마크로 삽입되는 내용을 워터마크 페이로드(payload)라 정의한다.

$$I_w(x) = I(X) + k(I(x)) \cdot W(x) \qquad \text{식(1)}$$

$I(x)$: 원본 콘텐츠

$I_w(x)$: 워터마크 삽입 콘텐츠

$W(x)$: 워터마크

$k(I(x))$: 워터마크 강도

워터마크 삽입과정은 생성된 워터마크를 어떻게 원본 영상에 삽입할 것인지를 결정하는 과정으로 대부분이 공간영역이나 주파수 영역에서 식(1)과 같이 인간 시각 시스템을 참조한 삽입강도를 정하여 더하는 방식을 사용한다. 워터마크 검출은 원본을 필요로 하는 경우 원본 콘텐츠와 대상 콘텐츠의 차분 값을 이용하는 방법과 식(2)와 같이 유사도를 측정하는 워터마크 검출법이 있다.

$$sim(X, X^*) = \frac{X^* \cdot X}{\sqrt{X^* \cdot X}} \qquad \text{식(2)}$$

X : Original image

X^* : Watermarked image

원본이 필요 없는 경우는 워터마크 신호의 자기상관도를 구사는 방식을 사용한다.

3.2 DCT를 이용한 워터마크 기법

DCT를 이용한 워터마크 기법의 경우 대역확산 기법(Spread Spectrum)을 이용한 워터마크 기법이 일반적이다. 대역확산 통신기법은 협 대역(Narrow Band)의 신호를 광 대역(Wide Band)의 신호에 걸쳐서 전송함으로 외부 환경에 영향을 받지 않고 전송할 수 있는 방식이다.

영상 데이터를 주파수 형태로 변환했을 때 가질 수 있는 주파수 대역을 통신 채널이라고 가정하면 워터마크는 그 통신 채널로 통과하는 협대역의 신호라고 볼 수 있다. 그 신호가 잡음, 필터링, 압축전송 등에 영향을 받지 않고 효과적으로 전송이 될 수 있도록 대역확산통신 방식을 도

입한다. 즉, 워터마크(신호)를 영상(전송채널)이 갖고 있는 여러 주파수 영역으로 확산시킴으로써 특정 주파수 대역의 에너지는 감지하기 어렵게 한다. 그러나 주파수의 위치와 변화량을 알고 있는 소유권자에 의해 주파수 성분을 추출하면 높은 신호 대 잡음비로 워터마크를 검출 할 수 있다. 또한 영상을 주파수 성분으로 변환하여 워터마크의 삽입 시 의미 있는 부분에 워터마크를 삽입하기 위한 시각적 특성을 고려해야 한다.

원 영상을 DCT를 이용한 주파수 변환 후 DC를 제외한 AC계수 부분에 평균이 0이고 분산 값이 1인 정규분포를 갖는 가우시안 시퀀스(Gaussian sequence)의 워터마크를 삽입하게 된다. AC계수 중에서도 주파수 성분의 특성을 고려하여 워터마크를 삽입해야 하는데 대역확산된 주파수 성분 중에서 인간시각에 크게 영향을 미치지 않는 중간 주파수 성분에 워터마크를 삽입한다. 이와 같은 DCT를 이용한 워터마크 삽입 및 검출 과정의 흐름은 그림 1과 2에서 나타내고 있다.

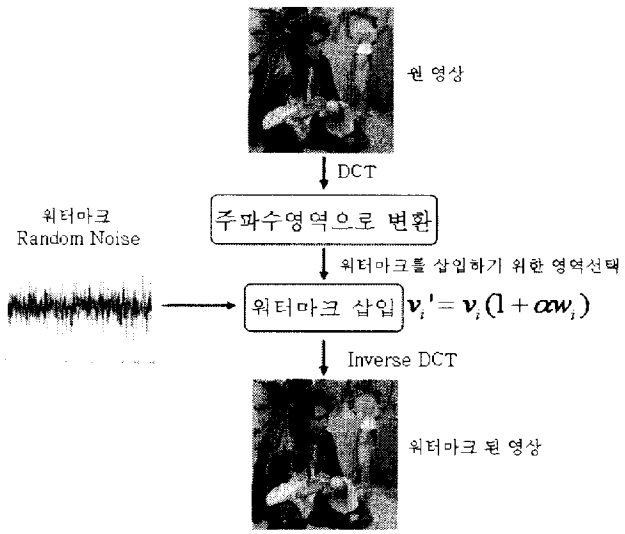
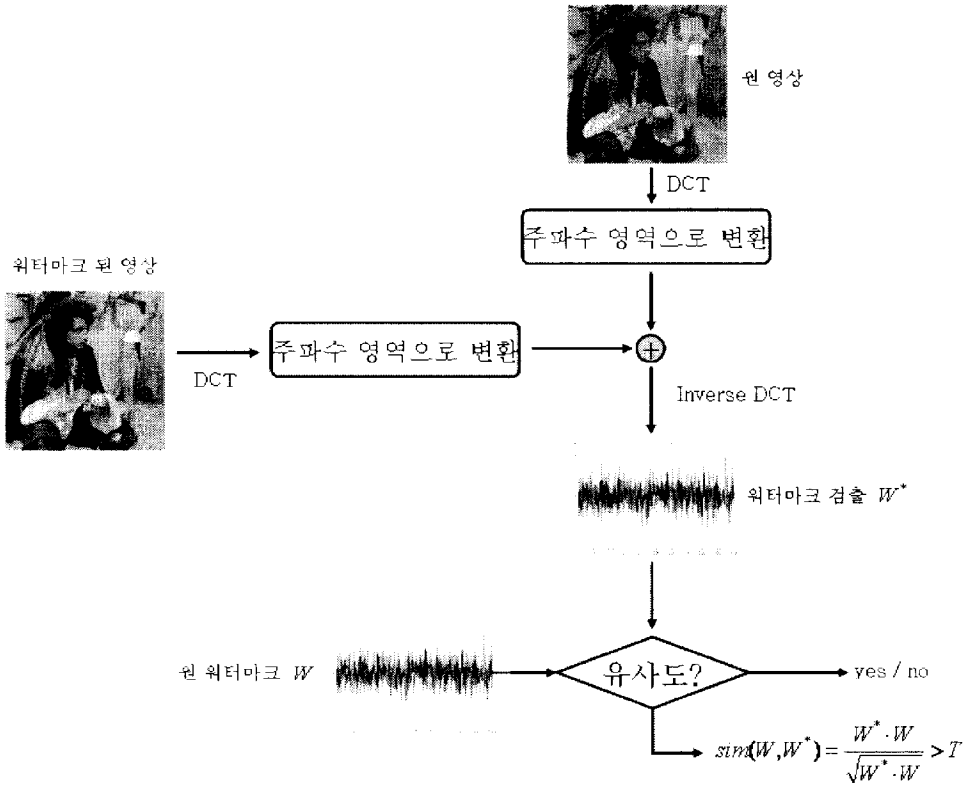


그림1. DCT를 이용한 워터마크 삽입과정



그그림2. DCT를 이용한 워터마크 추출과정

3.3 Piva의 워터마킹 기법

Piva에 의해 제안된 DCT 기반 워터마킹 기법[3][4]은 원 영상에 삽입하고자 하는 워터마크가 M개의 PN 시퀀스로 구성되어 있고 그 값은 식(3)과 같다.

$$X = \{x_1, x_2, \cdots, x_M\} \qquad \text{식(3)}$$

X를 이루고 있는 각 x_i의 값은 표준정규분포 N(0,1)에 의해 발생된 랜

덤한 실수 값이다. 워터마킹의 처리방법은 일반적으로 통신로 상에서 일어나는 것과 유사한데, 원 영상에 삽입되는 워터마크는 채널을 통해 전송되어 신호가 되고, 채널 잡음은 워터마크에 대해 행해지는 고의적인 공격이나 왜곡에 비유될 수 있다. 워터마크의 검출은 통신로 상에서 잡음이 부가된 영상을 수신하여 검출하는 것이다.

1) 워터마크 삽입

워터마크를 영상에 삽입하는 방법은 크기가 N×N인 원 영상 I를 N×N DCT를 취하여 DCT 계수를 구한다. 계산된 DCT 계수를 zig-zag scan하여 정렬된 DCT계수 중 워터마크 시퀀스 $X = \{x_1, x_2, \cdots, x_M\}$가 삽입될 대역 L과 M을 결정하게 된다. 만약, L의 크기가 작아지면 저주파 영역에 워터마크가 삽입되어 시각적으로 쉽게 인식되고, M이 커지면 고주파 영역에 워터마크가 삽입되어 시각적으로 인식이 어려워진다[5]. 처음부터 L+M번째까지의 계수를 선택하여 식(4)와 같은 벡터를 구성한다.

$$T = \{t_1, t_2, \cdots, t_L, t_{L+1}, \cdots, t_{L+M}\} \qquad \text{식(4)}$$

시각적인 인지도와 강인성간의 trade off를 고려하여 워터마크 시퀀스 X를 가장 저역인 L은 제외하고 M까지 삽입하여 새로운 벡터 $T = \{t_1, t_2, \cdots, t_L, t'_{L+1}, \cdots, t'_{L+M}\}$을 식(5)과 같이 생성한다.

$$t'_{L+i} = t_{L+i} + \alpha | t_{L+i} | x_i \qquad \text{식(5)}$$

이러한 방법은 원 신호에 워터마크 된 신호를 더하여 진폭계수 α를 증가시켜도 워터마크에 대한 영상의 시각적인 감지를 방지하고, 공격자로부

터 워터마크가 지워지는 것을 예방한다. 그런 다음에 계수 T'를 inverse zig-zag scan하고, 다시 IDCT를 하여 워터마크 된 영상 I'를 생성한다.

2) 워터마크 검출

워터마크의 검출은 변조된 영상 I'을 N×N DCT를 하여 DCT 계수를 구하고, 구해진 DCT 계수를 zig-zag scan한 후, 그 계수 중 하나의 워터마크가 삽입된 대역인 L+1번째부터 L+M번째까지를 택하여 식(6)과 같이 벡터를 구성한다[6][7].

$$T^* = \{t^*_{L+1}, t^*_{L+2}, \cdots, t^*_{L+M}\} \quad \text{식(6)}$$

워터마크 된 DCT 계수에 삽입할 때 사용된 워터마크 X를 곱하여 상관계수 Z를 식(7)에 의해서 구한다[8][9][10].

$$Z = \frac{1}{M}\sum_{i=1}^{M} y_i \cdot t^*_{L+i} \quad \text{식(7)}$$

Z값으로부터 워터마크의 존재여부를 판단하는데, 임계값 Sz를 미리 정의하여 상관계수 Z와 비교해서 워터마크가 존재하는지 그렇지 않은지를 확인한다[11][12]. Sz는 워터마크 된 영상을 이용하여 식(8)에 의해 계산된다.

$$S_z = \frac{\alpha}{3M}\sum_{i=1}^{M} | t^*_i{}' | \quad \text{식(8)}$$

4. 블록 인덱싱을 이용한 DCT 기반 워터마킹

Piva에 의해 제안된 DCT-Based 워터마킹 기법은 기본적으로 주파수 영역에 삽입하고자 하는 워터마크가 잡음형태로 삽입되므로 화질저하를 감소시키고 간단한 공격에 공간영역에서의 워터마킹 기법보다 강하다는 장점이 있지만, 의도적으로 가해질 수 있는 기하하적 공격 등에는 약한 단점이 있다. 또한, 삽입 알고리즘이 DCT계수를 이용하고 중간대역에 워터마크 정보가 삽입된 것이 공개된다면 영상에 대한 공격이 쉽게 이루어질 수 있다[13].

본 논문에서 제안한 워터마킹 알고리즘은 원 영상에 대한 화질열화를 최소화하면서 다양한 영상에 적용하기 위하여 워터마크를 삽입할 영상을 n by n의 크기를 가지는 블록단위로 나누어 각각의 블록에 인덱스 값을 할당한 후, 삽입하고자 하는 워터마크 정보를 블록의 인덱스 값으로 표현하고, 워터마크정보가 인덱싱된 블록의 중간 주파 대역에 PN 시퀀스를 삽입함으로써 워터마크 정보를 삽입하는 기법이다.

4.1 워터마크 삽입

제안된 워터마크 알고리즘은 워터마크 정보를 원 영상의 서브블록에 대한 인덱스 값으로 표현하는 기법으로 3단계 과정을 거쳐 워터마킹을 수행하고 있다.

1단계

• 먼저 원본 영상을 여러 개의 서브블록으로 나눈다. 여기서 서브블록은

삽입하고자 하는 워터마크 정보가 삽입되는 단위 블록이다.

- 워터마크 정보를 단위블록의 인덱스 값으로 매핑시킨다. 삽입되는 하나의 단위블록에 삽입되는 정보는 8비트로 구성되는데, 앞의 4비트는 정보의 순서를 나타내는 동기화 비트로 사용되고, 실제 저작권을 나타내는 워터마크 정보는 나머지 4비트가 된다(데이터 정보순서 4비트 & 데이터 정보 4비트). 제안된 알고리즘에서는 분할된 256개의 블록 중에서 16개의 단위블록에 대해 워터마크를 삽입하므로 멀티미디어 콘텐츠 상에는 총 128비트(워터마크 정보순서 64비트 & 워터마크 정보 64비트)의 정보가 삽입된다. 멀티미디어 콘텐츠에 삽입되어지는 정보의 구성은 그림 3과 같다.

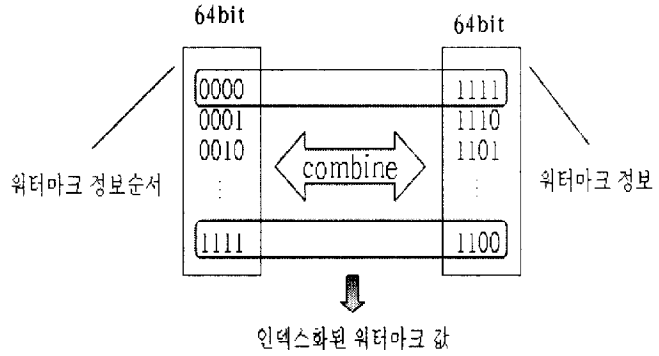


그림3. 인덱싱된 워터마크 구성

- 원 영상에 직접 워터마크 값을 인덱싱하는 것은 영상의 특성에 따라 시각적인 문제를 야기할 수 있기 때문에 본 논문에서는 콘텐츠상의 서브블록들을 스크램블과정을 거쳐 블록의 위치를 뒤섞는다.

2단계

• 스크램블 된 콘텐츠를 살펴보면 16개의 행을 가진다. 각 행을 이진수로 표현하면 0000(step1)부터 1111(step16)로 나타낼 수 있는데, 이때 각 step은 16개의 블록에 대해서 인덱싱 할 수 있으나, 각 행에서 하나의 블록만이 사용되어진다. 표1은 워터마크 값을 콘텐츠 상에서 서브 블록의 인덱스 값으로 표현할 수 있는 범위를 표 1에서 나타내고 있다.

표1. 워터마크 값의 인덱싱 범위

워터마크 정보의 순서표현	워터마크 정보표현	8비트로 표현된 인덱스 값
step1 = 0000(Binary)	0000(Binary)	00000000(Binary)
⋮	⋮	⋮
step16 = 1111(Binary)	1111(Binary)	11111111(Binary)

예를 들어, 멀티미디어 콘텐츠에 삽입하고자 하는 워터마크 정보가 이진수 0000부터 1111까지의 64비트라 가정하면, 이는 0부터 15까지의 10진수로 표현할 수 있다. step1의 1번째 단위 블록에 0000의 워터마크가 표현되는 것을 시작으로 해서 step16의 16번째 단위블록에 1111의 워터마크 값이 단위블록의 인덱스 값으로 표현되는 것이다.

3단계

• 2단계 과정을 거쳐서 64비트의 워터마크 정보를 표현하고 있는 16개의 단위 블록에 대해서 평균 0, 분산 1의 분포를 이루는 M개의 실수

값을 Piva의 방법을 이용해 삽입하게 된다[14][15]. 그림 4는 저작권 보호를 위해 삽입하고자 하는 64비트의 워터마크 정보가 콘텐츠 상에서 단위 블록의 인덱스 값으로 표현되는 예를 설명하고 있다. 이와 같은 과정을 거쳐서 워터마크 된 영상을 얻을 수 있다.

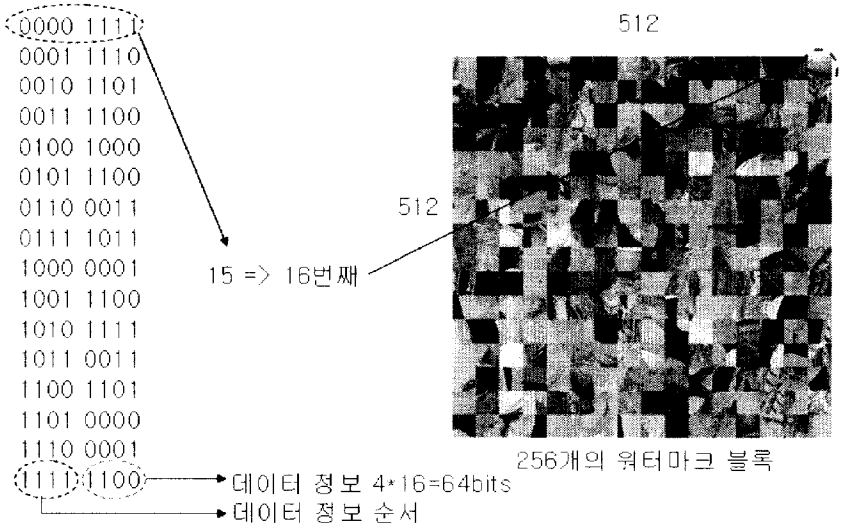


그림4. 인덱싱된 워터마크 블록

예제의 경우에서는 하나의 블록 당 4비트를 삽입한 경우이고, 서브블록의 크기를 줄여서 분할된 블록의 개수가 많아지게 할 경우 콘텐츠 상에 표현할 수 있는 정보량 또한 증가시킬 수 있다. 그러나 추출 시 삽입된 PN 시퀀스와 삽입된 특정대역의 유사도 값을 구해서 워터마크 정보를 추출하므로 블록의 크기가 작아지면 검출율이 낮을 수 있으므로 서브블록은 정확한 워터마크 검출을 위해서 적절한 크기를 유지하여야 한다.

본 논문에서는 512 by 512의 원 영상에 대해 워터마크 정보순서 64비트와 워터마크 정보 64비트를 원 영상이 가지는 256개 블록 중에서 16개 단위블록의 인덱스 값으로 표현한다.

원 영상을 32*32크기의 서브블록으로 나눈 것은 그림에서 보듯이 단위 블록의 정보가 8비트로 구성되므로 2^8개의 블록 인덱스 값이 필요하다.

워터마크 값에 의해 인덱싱된 단위블록들이 Piva의 방법을 이용하기에는 PN 시퀀스의 길이가 상당히 짧은 것이 사실이다. 하지만 워터마크가 표현된 단위블록의 인덱스 값 중에서 워터마크 값의 순서를 정하는 64비트의 정보들이 존재하기 때문에 약간의 불명확한 블록에 대해서도 워터마크를 유추할 수 있다. 그림5(a)는 PN 시퀀스의 삽입대역을 나타내고 있으며 그림5(b)는 저작권 보호를 위해 워터마크 정보 64비트를 원 영상에 삽입하는 과정을 나타내고 있다.

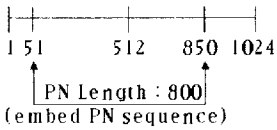


그림5(a). PN 시퀀스 삽입대역

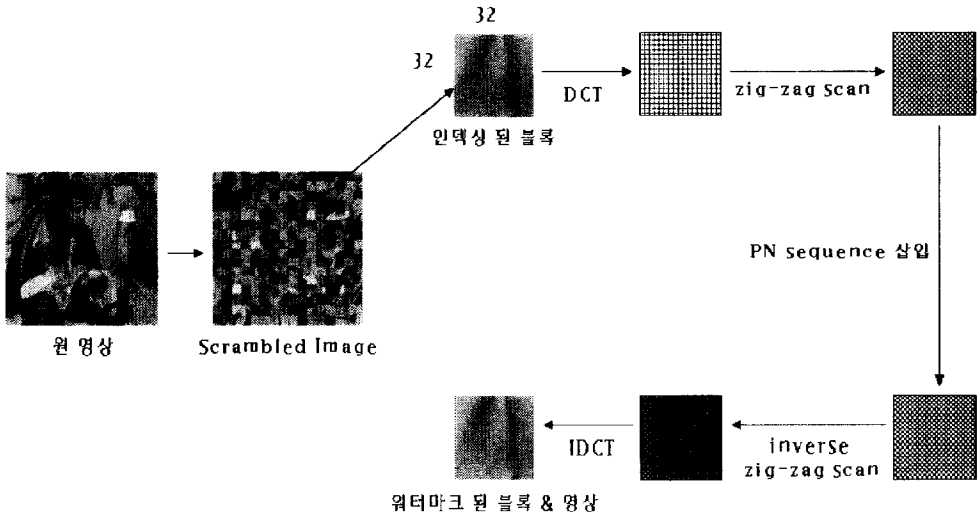


그림5(b). 제안방법의 워터마크 삽입과정

4.2 워터마크 추출

워터마크 추출 시에는 삽입과정에서 사용된 PN 시퀀스를 이용하기 때문에 원본 영상을 필요로 하지 않으며[16], 삽입의 역 과정을 거쳐서 삽입된 워터마크 정보를 추출하게 된다.

1단계

- 저작권을 증명하기 위한 워터마크 정보를 검출하기 위해서 먼저 대상이 되는 영상을 여러 개의 서브블록으로 나눈다. 분할된 서브블록은 워터마크 추출을 위한 단위 블록이다.

- 대상이 되는 영상을 서브블록으로 나눈 후, 서브블록들을 삽입과정과 동일한 형태로 스크램블 하여 블록의 위치를 뒤섞는다.

2단계

- 256개의 단위 블록에 대해서 삽입과정에서 사용한 평균 0, 분산 1의 분포를 이루는 M개의 실수 값을 생성한다.

- 생성된 실수와 삽입과정에서 삽입한 대역이 가지는 값 사이의 유사도 값을 식(9)를 이용해 계산한다.

$$sim(W, W^*) = \frac{W^* \cdot W}{\sqrt{W^* \cdot W}} \qquad \text{식(9)}$$

W : Original PN 시퀀스

W^* : PN 시퀀스가 삽입된 대역

• 계산된 유사도 값으로부터 워터마크 정보가 서브블록의 인덱스 값으로 표현된 블록인지 아닌지를 확인하고, 워터마크가 존재하는 블록은 인덱스 값을 8비트 이진수로 변환해서 워터마크 추출한다.

• 추출된 각 단위블록의 8비트 정보 중 앞의 4비트를 워터마크 동기비트로 사용했기 때문에 각 단위블록의 뒤쪽 4비트를 동기비트의 정렬에 의해 나타내면 삽입한 워터마크 정보를 검출할 수 있다. 그림 6(a)는 워터마크 추출대역을 나타내며, 그림 6(b)는 저작권 보호를 위해 삽입된 워터마크 정보 64비트를 대상이 되는 콘텐츠 상에서 추출하는 과정을 나타내고 있다.

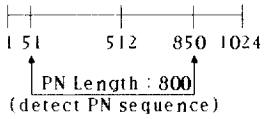


그림6(a). PN 시퀀스 추출대역

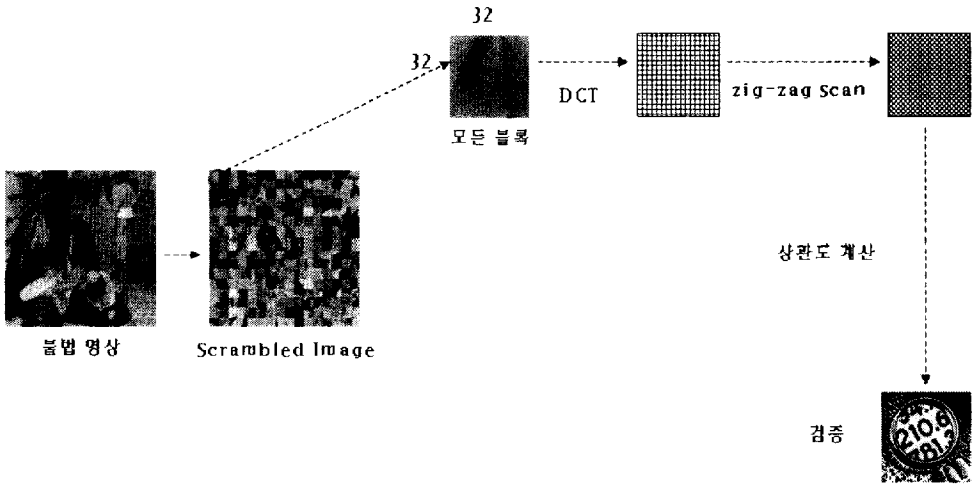


그림6(b). 제안방법의 워터마크 추출과정

5. 실험결과 및 고찰

제안 방식의 효율성을 확인하기 위하여 다음 그림과 같은 몇 가지 gray scale의 Man(512×512)영상, Lena영상, Couple영상, Bridge영상, House영상을 대상으로 하여 128비트의 코드를 삽입하고 추출하는 과정을 수행하고, 여러 가지 신호처리적인 왜곡을 가하여 공격으로부터의 강인성을 실험한다. 그림 7은 알고리즘에서 사용한 원 영상이다.

그림7. 원 영상

그림 8(a)그림은 기존의 Piva 알고리즘에 따라 α=0.2, L=25000, M=16000을 적용한 워터마크 된 영상을 나타내고 있으며, 8(b)그림은 제안방법에 따라 32×32크기의 블록으로 나누어 α=0.5, L=50, M=800개가 삽입되어진 영상을 나타내었다.

그림8(a). 기존방식의 워터마크 된 영상 (PSNR : 47.01)

그림8(b). 제안방식의 워터마크 된 영상 (PSNR : 44.21)

기존 방식의 워터마크 검출 알고리즘에 의해 삽입과정에서 사용된 워터마크로 검출한 결과와 1000회 정도 랜덤하게 발생시켜 검출한 결과를 그래프로 나타내면 그림 9와 같다. 그 결과로 나타난 상관계수 값은 삽입 시에 사용된 정확한 워터마크를 가지고 검출하였을 때 가장 큰 값을 나타내고, 다른 신호 값들에 대해서는 아주 낮은 값을 나타내었다.

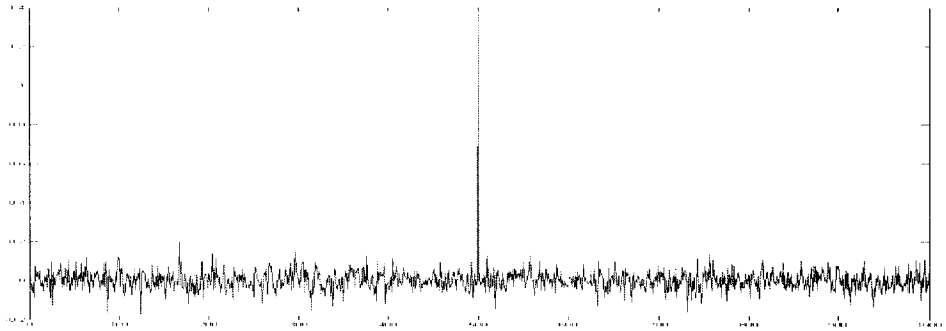


그림9. 기존방법에서의 워터마크 검출 response

그림 10은 제안 방식의 검출 알고리즘에 의한 블록 당 결과 값을 그래프로 나타내고 있다. 워터마크가 인덱싱된 16개의 블록에서 상대적으로 높은 유사도 값을 보인다.

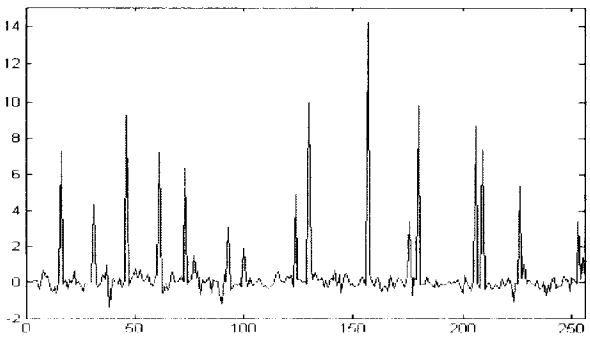


그림10. 제안방법에서의 워터마크 검출 시 각 블록에 대한 response

신호처리적인 내성에 대해서는 추출된 16개의 블록(실제 PN 시퀀스가 삽입되어진 블록)에 대해 삽입과정에서 사용한 Original PN 시퀀스와 500회의 랜덤하게 생성한 다른 실수 열과의 상관도 값을 구하여 제시하였다. 그림 11에서 계산된 결과를 보인다. Original PN 시퀀스를 사용해서 계산된 유사도 값이 다른 랜덤한 실수 열과의 계산보다 높은 유사도 값을 가짐으로 신호처리적인 내성을 가진다.

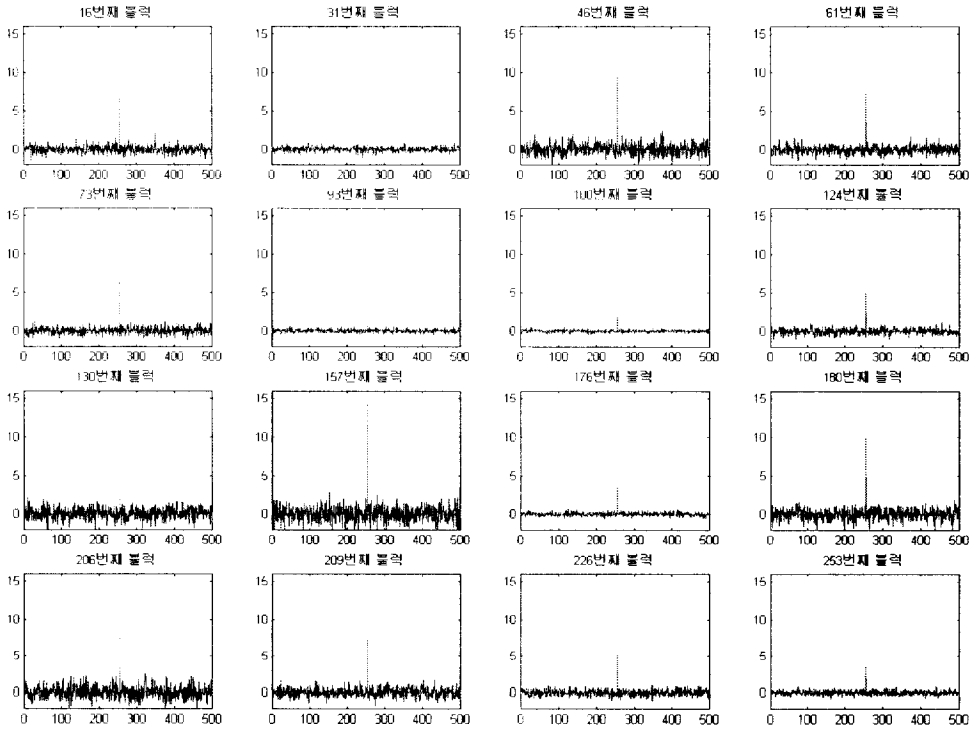


그림11. 검출된 블록에 대한 검증

제안된 워터마킹 기법으로 워터마크 된 영상에 대하여 신호처리적인 공격을 시도해 보았다. 공격은 벤치마크 툴로 알려진 Stirmark 3.1의 대표적인 공격 파라메터를 이용하여 강인성을 평가하였다.

① Gaussian Filter

: 표준분포로부터 끌어낸 noise를 제거하기위한 filter

② Histogram Equalization

: 영상처리에 의해 화질이 향상될 수 있다. 히스토그램 평활화는 명암값 분포를 재분배 하여 보다 균일한 분포를 갖게 함으로 인해 화질이 향상시킬 수 있는 영상처리기법.

③ JPEG Compression 90%

: 영상의 압축으로 인해 정보의 데이터양을 줄임으로써 전송 시 효율적인 영상처리기법.

④ JPEG Compression 70%

⑤ JPEG Compression 50%

⑥ Low pass Filter

: 주로 고주파 신호를 걸러내어 저주파의 필요한 신호만을 골라낼 때 많이 사용되는 filter.

⑦ Median Filter

: 영상 detail을 유지하는 동안 salt and pepper(희고 검은 작은 점이 희끗희끗 뒤섞여 있는 영상)와 noise 충격을 제거하기 위한 영상처리기법.

⑧ Sharpening

: 영상의 Detail information를 향상시키기 위한 영상처리기법.

각종 신호처리적인 공격에 의해 생성된 영상은 그림 12(a)에서 확인할 수 있으며, 그림 12(b)에서 워터마크의 강인성을 간과할 수 있는 PSNR 값을 나타내고 있다.

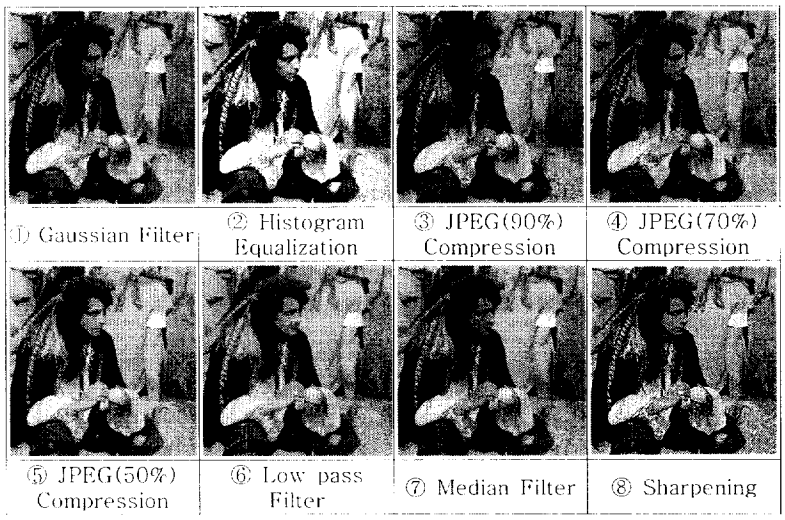


그림12(a). 신호처리 공격에 의해 생성된 영상

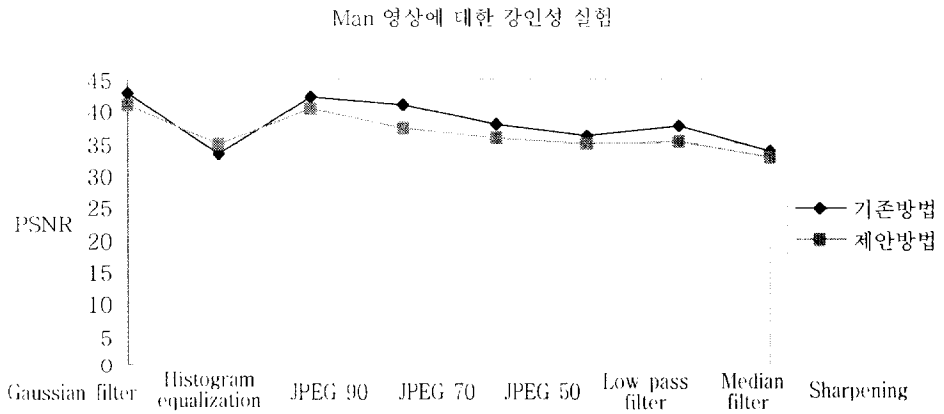


그림12(b). 신호처리 공격된 영상에 대한 PSNR 값

그림 13, 14, 15, 16은 Lena, Couple, Bridge, House 영상에 대해서 실험한 결과를 나타낸다. 기존방법과 제안방법 모두 대부분의 신호처리적인 왜곡에도 PSNR 값은 35[dB]전후로 화질열화는 크지 않다.

그림13(a). Lena 영상

그림14(a). Couple 영상

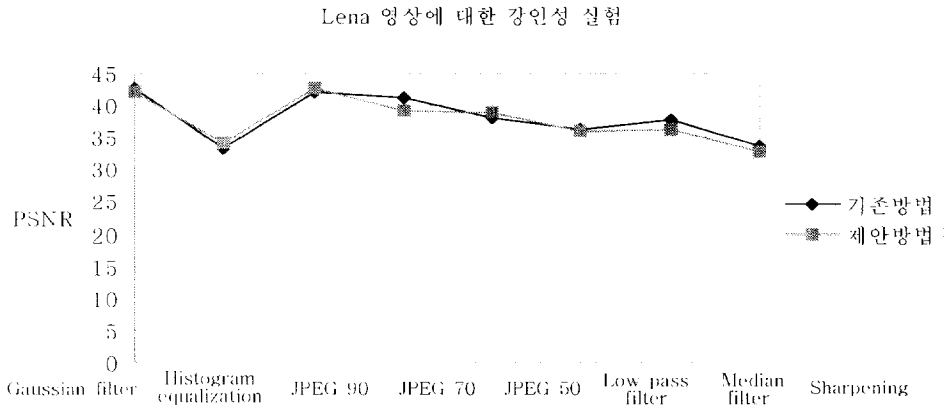


그림13(b). 신호처리 공격된 Lena 영상에 대한 PSNR 값

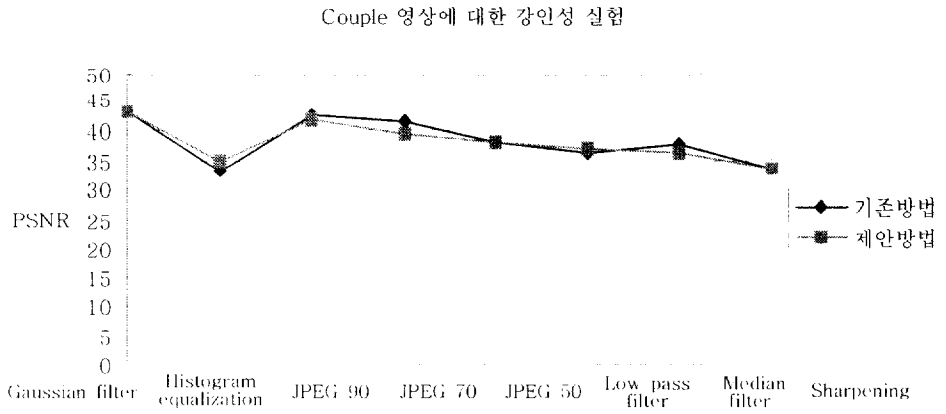


그림14(b). 신호처리 공격된 Couple 영상에 대한 PSNR 값

그림15(a). Bridge 영상

그림16(a). House 영상

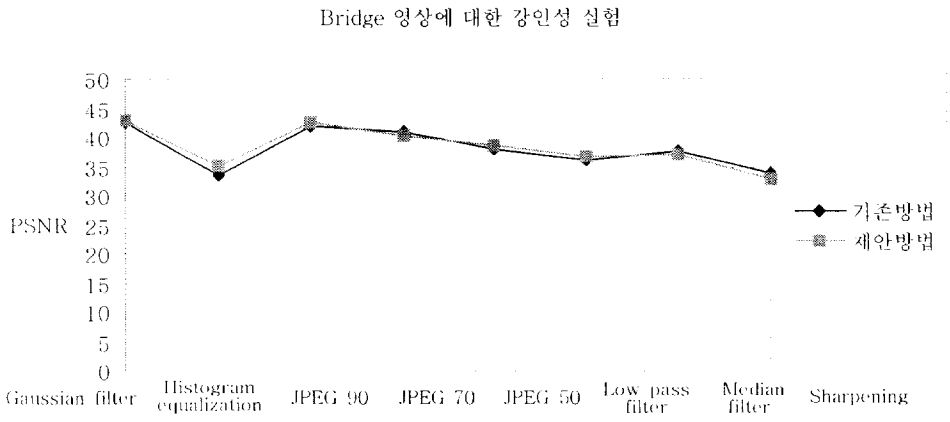


그림15(b). 신호처리 공격된 Bridge 영상에 대한 PSNR 값

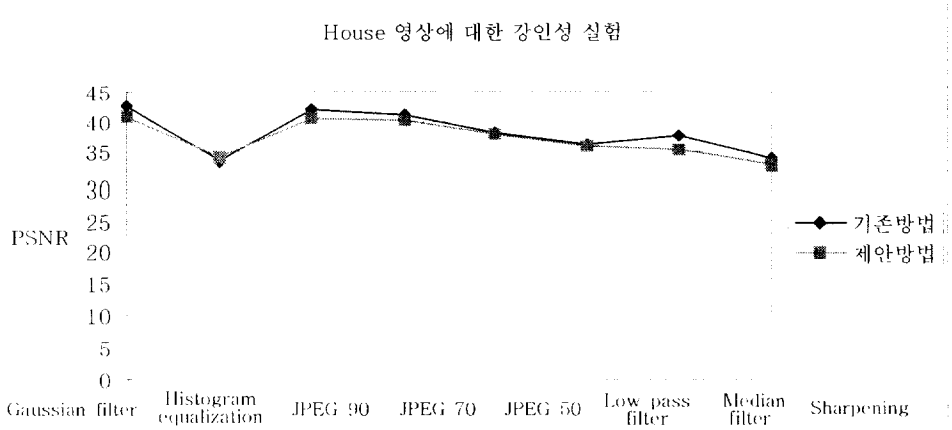


그림16(b). 신호처리 공격된 House 영상에 대한 PSNR 값

그림 17에서부터 그림 24까지는 신호처리적인 공격(Stirmark 3.1의 대표적인 공격)에 의해 왜곡된 영상을 대상으로 한 워터마크 검출 response 그래프를 나타내고 있다. PN 시퀀스가 삽입된 16개 블록의 상관도 값이 다른 블록에 비해 높은 값을 가지는 것을 확인할 수 있다.

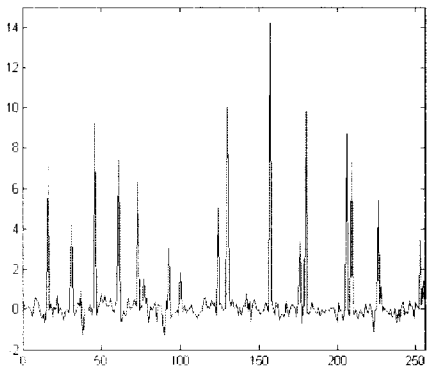


그림17. Gaussian Filter 공격에 대한 검출 response

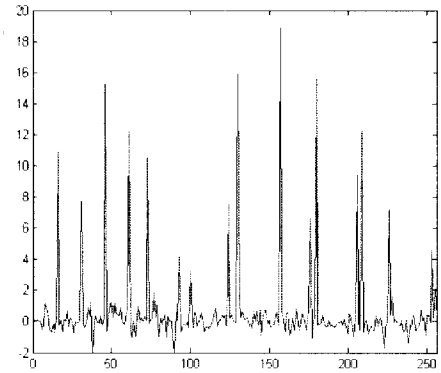


그림18. Histogram Equalization 공격에 대한 검출 response

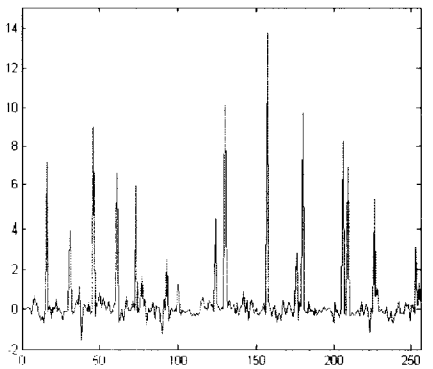


그림19. JPEG 90%compression 공격에 대한 검출 response

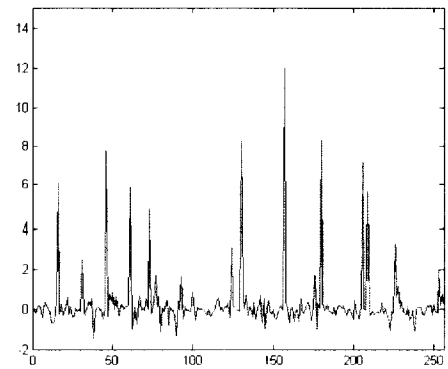


그림20. JPEG70% Compression 공격에 대한 검출 response

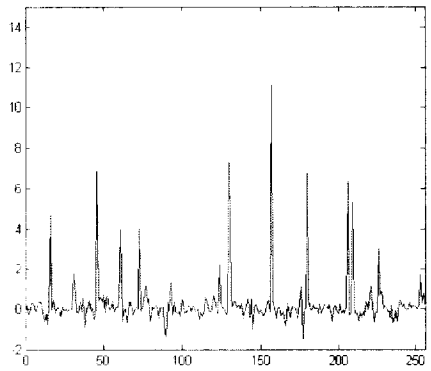


그림21. JPEG50% Compression 공격에 대한 검출 response

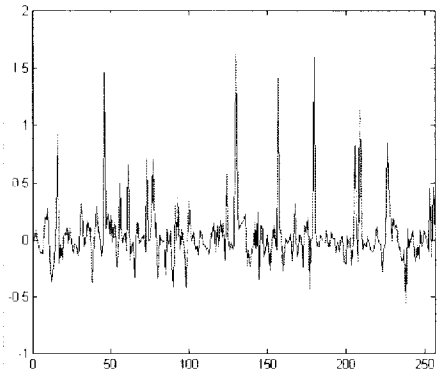


그림22. Low pass Filter 공격에 대한 검출 response

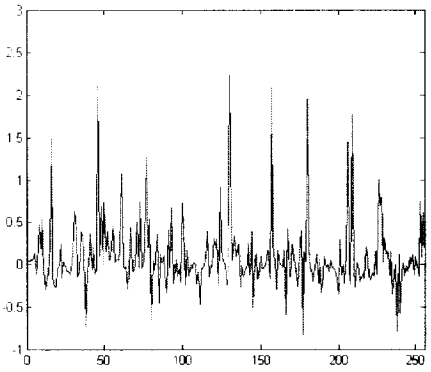


그림23. Median Filter 공격에 대한 검출 response

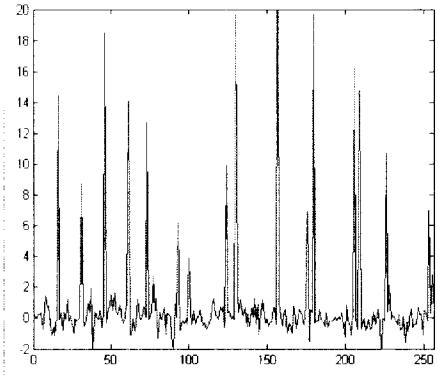


그림24. Sharpening 공격에 대한 검출 response

실험결과에서 나타난 것처럼 각각의 공격영상에 대한 상관계수 값은 대체로 높은 상관계수 값을 보여 신호처리적인 내성을 가지고 있음을 확인할 수 있으나, DCT 단위블록을 사용하는 제안 알고리즘의 특성으로 인해 그림 25(a), 26(a)의 cropping과 general linear geometric등의 공격에

대해서는 취약성을 가지고 있다. 그림 25(b)의 결과를 보면 높은 상관도를 보이고 있지만 워터마크가 삽입된 영역의 단위블록이 cropping된 부분에 대해서는 검출이 불가능하다. 또한, 그림 26(b)의 결과를 보면 대부분의 블록이 낮은 상관도 값을 가진다. 이는 제안방법이 인덱스 값을 사용하기 때문에 디지털 콘텐츠의 인덱스 위치가 변경되면 검출을 할 수 없다.

그림25(a). cropping 공격된 영상

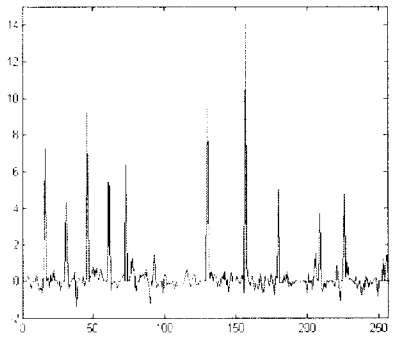


그림25(b). cropping 공격된 영상에 대한 검출 response

그림26(a). rotate공격된 영상

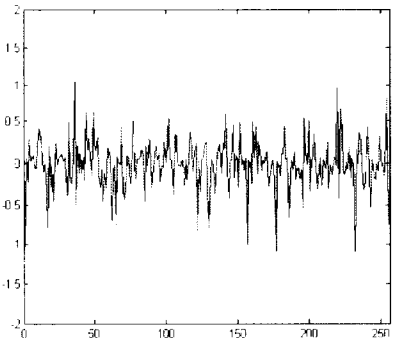


그림26(b). rotate공격에 대한 검출 response

삽입된 워터마크가 각 영상의 화질에 미치는 영향에 대한 비교를 위해 기존의 기법과 제안된 기법의 워터마크 된 영상에 대해 식(10)에 의해서 PSNR(Peak Signal to Noise Ratio)값을 비교하였다.

$$PSNR = 10\log_{10}\frac{M_i^2 \max X}{MSE}[dB] \qquad \text{식(10)}$$

$$MSE = \frac{1}{M \times M}\sum_{i=1}^{M}(X_i - X_i')^2 \qquad \text{식(11)}$$

식(11)에서 M은 원 영상의 너비와 높이 크기이고, X는 원 영상을, X'는 워터마크 된 영상을 나타고 있으며, PSNR의 결과 값이 클수록 원 영상과 화질의 차이가 적음을 나타낸다. 표 2에서 기존방식과 제안방식 모두 PSNR 값은 40[dB]이상으로 워터마크 삽입에 의한 화질의 열화가 거의 없음을 보여주고 있다.

표2. 기존방식과 제안방식의 PSNR 비교

실험영상	기존방식	제안방식
Man	47.07[dB]	44.21[dB]
Lena	42.43[dB]	41.12[dB]
Couple	50.79[dB]	43.29[dB]
Bridge	50.22[dB]	42.98[dB]
House	45.49[dB]	41.43[dB]

현재까지 나타낸 실험들은 일반적으로 영상처리에 사용되는 Classics image에 대한 결과를 나타내었다.

영상은 특성에 따라 분류할 수 있는데, 여러 가지 특성을 가지는 다른 영상에 대한 실험결과를 제시한다. 그림 27(a)는 각각 다른 특성을 가지는 5가지 영상을 나타낸다. 또한 그림 27(b)에서 신호처리적인 공격에 대하여 실험결과를 제시한다. 대체적으로 동일한 형태의 결과 값을 가진다.

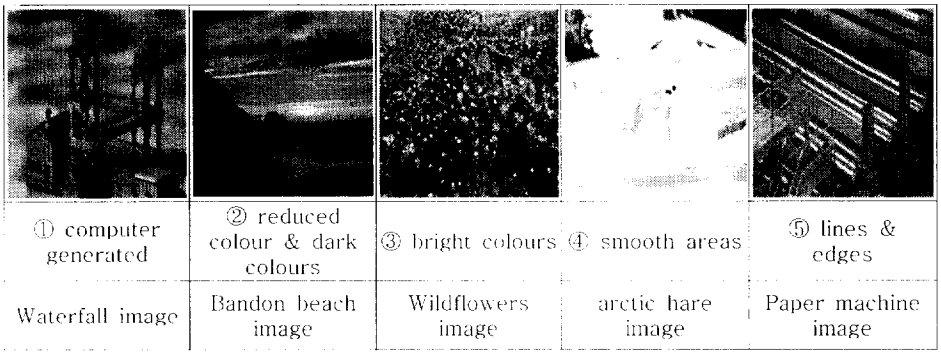


그림27(a). 여러 가지 특성을 가지는 영상

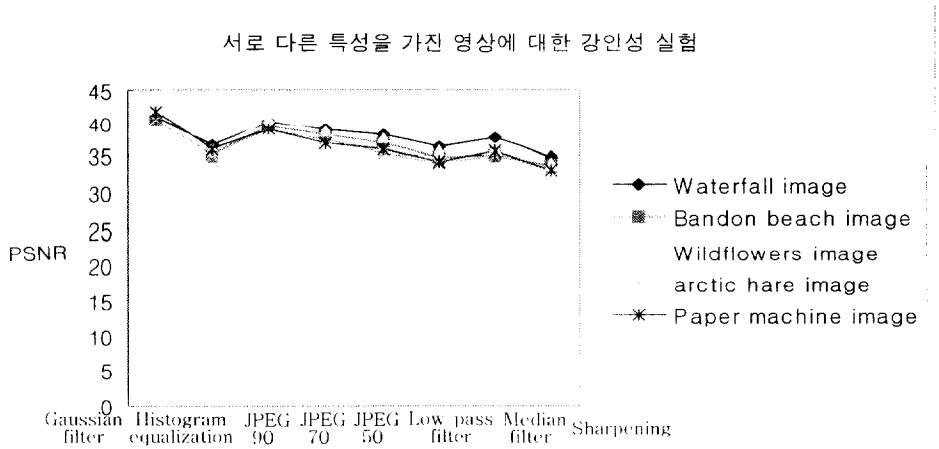


그림27(b). 신호처리 공격된 영상에 대한 PSNR 값

6. 결론

디지털화된 멀티미디어 데이터의 사용 증가에 따라 저작권 침해 및 불법 위조, 변조와 같은 문제점이 발생하고 되었으며, 이러한 문제점을 해결하고자 디지털 워터마킹 기술이 활발히 연구되고 있다. 이 기술은 디지털 데이터의 저작권 보호뿐만 아니라, 인증/무결성, 불법 유통자 추적 등의 다양한 응용분야도 점차적으로 늘어나고 있다.

본 논문에서는 디지털 멀티미디어 데이터의 저작권 보호를 위해멀티미디어 콘텐츠의 단위블록에 인덱스 값을 할당하여 이를 워터마크 정보와 매핑시키는 방법을 이용하며, 워터마크 정보가 매핑된 단위블록에 DCT 기반의 대역확산 기법을 적용하여 워터마크 정보를 표현하는 워터마킹 기법을 제안하고, 그 유용성에 대해 살펴보았다. 워터마크의 삽입 시 사용되는 PN 시퀀스는 잡음과 같은 형태로 워터마크 된 영상의 화질에 영향을 미치지 않으며, 삽입과 검출 시 알고리즘이 간단하여 디지털 데이터의 불법유통에 대한 검증비용을 줄일 수 있다. 실험을 통해 통신로 상에서 발생 가능한 가우시안 노이즈, 샤프닝, 필터링 등의 각종 공격에 대해서도 워터마크를 검출할 수 있는 내성을 입증하였다.

삽입과정에서 512 by 512의 원 영상을 32 by 32의 2^8개 블록으로 분할하고, 분할된 256개의 블록 중에서 워터마크 값을 표현하는 인덱스 값을 가진 단위블록 16개를 대상으로 워터마크를 삽입하기 때문에 기존방식보다 계산 량은 다소 증가하지만, 화질 열화를 최소화 할 수 있고 공격에 대한 안정성을 보장할 수 있다. 대상이 되는 16개의 블록에는 워터마크 정보 순서 4bits 워터마크 정보 4bits로서 하나의 블록 당 정보 삽입 량은 8bits이며, 콘텐츠 전체(16개 블록 선택)에 삽입되는 정보량은 워터마크 정보 순서 64bits와 워터마크 정보 64bits로 128bits의 정보가 된다. 정보량

이 증가할 경우 분할된 블록의 크기를 줄여 블록의 개수를 증가 시킬 수 있지만 워터마크 추출 시 신뢰성을 감소시킬 수 있으므로 적절한 블록의 크기를 고려해야 한다.

본 논문에서 제안된 블록 인덱싱을 이용한 워터마킹 알고리즘은 현실적이고 효율적인 기법이라 할 수 있으며 보다 확장된 응용에 적용할 수 있을 것으로 기대된다.

참고문헌

[1] Piva, A., Barni, M., Bartolini, F. and Cappellini, V.: DCT-based Watermarking Recovering without Resorting to the Uncorrupted Original Image. IEEE International Conference. On Image Processing. 1 (1997) 520-523

[2] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, t.: Secure Spread Spectrum Watermarking for Multimedia. IEEE Trans. on Image Processing. 6(1997) 1673-1687

[3] M.Barni,M., Bartolini,F., Cappellini, V., Piva,A.: A DCT Domain System for Robust Image Watermarking. Signal Processing. 3(1998)357-372

[4] M.Barni, F.Bartolini, V.Cappellini, A.Piva: Statistical Modeling of Full Frame DCT Coefficients. Proceedings of EUSIPCO'98, Rhodes, Greece, 1998

[5] Wolfgang, R. and Podilchuk, C.: Perceptual watermarks for digital images and video. Proceeding of IEEE. 87 (1999) 1108-1126

[6] Barni, M., Bartolini, F., De Rasa, A., and Piva, A.: Capacity issues in digital image water-marks. IEEE Trans. On Image Processing, 9(2000) 445-449

[7] Lam, E.Y., Goodman, J. W.: A Mathematical Analysis of the DCT Coefficients Distributions for Images. IEEE Trans. On Image Processing, 10(2000) 1661-1666

[8] Xiaochen Bo, Lincheng Shen, Wensen Chang.: Sign Correlation Detector for Blind Image Watermarking in the DCT Domain. Proceedings of the Second IEEE Pacific Rim Conference on Multimedia. Advances in Multimedia Information Processing, 2195(2001) 780-787

[9] Retsas, I.; Pieper, R.; Cristi, R.; Watermark recovery with a DCT based scheme employing nonuniform imbedding. System Theory, 2002. Proceedings of the Thirty-Fourth Southeastern Symposium on, 3(2002) 157 - 161

[10] Rangsanseri, Y.; Thitimajshima, W.; Copyright protection of images using human visual masking on DCT-based watermarking. Circuits and Systems, 2002. APCCAS '02. 2002 Asia-Pacific Conference on, 10(2002) 419 - 422

[11] Gangyi Jiang; Mei Yu; Shoudong Shi; Xiao Liu; Yong-Deak Kim; New blind image watermarking in DCT domain. Signal Processing, 2002 6th International Conference on, 8(2002) 1580 - 1583

[12] Chu, W. C.:DCT-based Image Watermarking using sub sampling. IEEE Trans. on Multimedia. 5(2003) 34-38

[13] Suhail, M.A.; Obaidat, M.S.; Digital watermarking-based DCT and JPEG model, Instrumentation and Measurement. IEEE Transactions on, 10(2003) 1640 - 1647

[14] Min-Jen Tsai; Hsiao-Ying Hung; DCT and DWT-based image watermarking by using subsampling. Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on, 3(2004) 184 - 189

[15] Emek, S.; Pazarci, M.; Yucel, M.; A DWT-DCT based digital watermarking technique. Signal Processing and Communications Applications Conference, 2004. Proceedings of the IEEE 12th, 4(2004) 33 - 36

[16] Ahmidi, N.; Safabakhsh, R.; A novel DCT-based approach for secure color image watermarking. 2004. Proceedings. ITCC 2004. International Conference on, 4(2004) 709 - 713

감사의 글

학업에 대한 의욕만으로 정말 열심히 해보겠다는 자신감과 기대로 시작된 대학원 생활은 뒤돌아보면 아쉬움이 많이 남는 소중한 시간들이었습니다. 어느새 2년이라는 대학원 생활이 지나고 졸업을 앞두고 있습니다. 대학원 생활을 무사히 마칠 수 있도록 곁에서 도움을 주신 모든 분들에게 감사드립니다.

먼저 부족하기만 한 저를 조언과 격려로, 때로는 채찍으로서 항상 이끌어 주시고 감싸주셨던 지금은 고인이 되신 박지환 교수님..., 교수님의 얼굴을 맞대며 감사드린다는 말을 전해드리지 못해 아쉬움이 너무 큽니다. 교수님께 고개 숙여 깊이 감사드립니다.

본 논문이 완성될 때까지 노고를 아끼지 않으시고 따뜻하게 조언을 해주신 김창수 교수님, 여정모 교수님, 신상욱 교수님과 대학원 공부를 알차게 할 수 있도록 지도해주신 윤성대 교수님, 이경현 교수님, 김영봉 교수님께 진심으로 감사드립니다.

또한 함께 동고동락하며 많은 힘이 되어준 동기 서병만님, 연구실 생활을 하면서 격려와 도움을 아끼지 않으신 강현호 선배님, 이진흥 선배님, 임태훈 선배님, 박영란 선배님, 최재귀 선배님, 이혜란 선배님, 김소진 선배님, 김태정 선배님, 항상 밝은 얼굴의 박수완님, 성지혜님, 류영희님, 이병욱님 그 외 연구실 모든 가족들에게 감사의 마음을 전합니다.

끝으로 저의 뒤에서 항상 사랑으로 걱정해 주시고 크나큰 힘이 되어주신 사랑하는 부모님께 이 논문을 바칩니다.

2005년 2월

한 승 우