블록 인덱싱을 이용한 블라인드 워터마킹 기법

A Novel Blind Watermarking Scheme Using Block Indexing

한승우*, 강현호**, 신상욱***

부경대학교 전자계산학과*, 전기통신대학 정보시스템학연구과**, 부경대학교 전자컴퓨터정보통신공학부***

Seung-Wu Han(swhanmarine@hotmail.com)*, Hyun-Ho Kang(kang@ice.uec.ac.jp)**,
Sang-Uk Shin(shinsu@pknu.ac.kr)***

요약

본 논문에서는 멀티미디어 콘텐츠에 정보를 은닉시키기 위해 블록의 인덱스 값을 이용한 워터마킹 알고리즘을 제안한다. 제안된 알고리즘은 대역확산통신 기반에서 인덱스화된 워터마크를 이용하는 새로운 블라인드 워터마킹 기법이다. 워터마크 삽입은 원 영상을 서브블록으로 분할한 후 각 블록에 인덱스 값을 할당한 후, 삽입하고자하는 워터마크를 블록의 인덱스 값과 매핑시키고, 매핑 된 블록을 DCT로 변환시킨 다음 DCT 공간의 중간 주파 주파수 영역에 PN시퀀스를 삽입한다. 결과적으로 워터마크를 인덱스 값으로 표현하는 기법이다. 워터마크의 추출은 원 영상 없이 PN시퀀스와 워터마크가 삽입된 영상의 상관관계에 의해서 가능하다. 실험결과 워터마크가 삽입된 영상은 시각적으로 손상을 감지하기 어려울 정도로 화질열화는 적었으며, 다양한 신호처리 적인 공격에도 강인성을 보였다.

■ 중심어 : | 워터마킹 | 블록 인덱싱 | DCT | 대역확산통신 |

Abstract

In this paper, we propose an efficient watermarking algorithm using block indexing. The proposed algorithm is a novel blind watermarking scheme using the indexed watermark value based on the spread spectrum method. The watermark insertion is allocated into index value of each block after dividing original image into sub-blocks. The watermark embedded in mappinged with index values of blocks, And the mappinged blocks convert to DCT and then the PN sequence embedded to middle frequency band. Consequently the watermark is expressed by index value of sub-blocks. The watermark extracted from the correlation of between PN sequence and watermarked image. Experimental results demonstrate that the watermarked image has a good quality in terms of imperceptibility and is robust against various attacks.

■ keyword : | Watermarking | Block Indexing | DCT | Spread Spectrum |

I. 서 론

오늘날 급격한 네트워크 기술의 발달로 인터넷을 통한 디지털 영상물의 배포가 일반화 되고 있다. 디지털 데이터가 아날로그 데이터에 비해 저장 및 편집이 용이하고 온라인상에서 쉽게 유통되어 편리성을 제공하지

접수번호 : #050621-002
접수일자 : 2005년 06월 21일
심사완료일 : 2005년 09월 27일
교신저자 : 한승우, e-mail : swhanmarine@hotmail.com

만, 누구나 디지털 데이터의 내용을 쉽게 변형 및 복제할 수 있기 때문에 각종 멀티미디어 서비스와 환경이 개인에게까지 제공되고 있다. 디지털 영상은 원본과 복사본의 구별이 불가능하기 때문에 저작권보호가 쉽지 않다. 따라서 이러한 디지털 영상물의 저작권 보호를 위해 저작권 정보를 나타내는 마크를 저작물에 삽입해 저작권을 보호하는 디지털 워터마킹 기법이 연구되어지고 있다.

디지털 워터마킹이란 원 영상에 비밀정보를 눈에 띄지 않게 숨겨 넣고 저작권 분쟁시 이를 추출하여 영상의 소유권을 주장하는 방법이다. 워터마킹은 크게 공간영역에 삽입하는 방법과 주파수 영역에 삽입하는 방법으로 나뉘는데, 공간영역에 워터마크를 삽입하는 방법은 변환식을 사용하지 않고 영상의 특정화소 값을 변화시키는 방법으로 간단하지만 각종 영상처리와 잡음 등의 공격에 취약하다는 단점을 가지며, 주파수 영역에 워터마크를 삽입하는 방법은 영상을 주파수 계수로 변환시켜 워터마크를 삽입하는 방법이다.

이때 주로 사용되는 주파수 변환 방법으로는 Discrete Cosine Transform(DCT), Discrete Fourier Transform(DFT), Discrete Wavelet Transform(DWT) 등이 있다. 주파수 영역에 워터마크를 삽입하는 방법은 공간영역보다 공격에 강인하다는 장점이 있다. 본 논문에서 제안하는 워터마킹 방법은 DCT를 이용한 주파수 영역에서의 워터마킹 기법이다. 워터마킹이 영상의 저작권 보호를 보다 효율적으로 수행하기 위해서는 다음과 같은 특성을 가져야 한다.

- **비가시성** : 워터마크가 삽입된 영상은 원 영상과 시각적으로 구별이 불가능해야 한다.
- **강인성** : 워터마크를 제거하려는 공격에 대해 워터마크는 강인해야 한다.
- **명확성** : 추출된 워터마크가 저작권을 명확히 나타낼 수 있어야 한다.
- **보안성** : 관련된 키 값의 정보를 알고 있는 사람만이 워터마크를 검출할 수 있어야 한다.

본 논문에서는 원 영상을 서브블록으로 분할하여 각 블록에 인덱스 값을 할당하고, 삽입하고자하는 워터마크를 블록의 인덱스 값과 매핑시킨 후 매핑 된 블록을 DCT해서 중간 주파수 영역에 Pseudo-random Noise Sequence(PN시퀀스)를 삽입함으로서 워터마크가 인덱스 값이라는 것을 표현하는 블라인드 워터마킹 기법을 제안한다.

제안된 방법에서는 워터마크가 삽입된 후 화질 열화를 최소화하기 위하여 워터마크가 매핑된 인덱스 값을 가지는 블록의 중간 주파수 대역을 적절하게 결정해야 한다. 이를 위해 본 논문은 2장에서 디지털 워터마킹에 대한 소개를 하고, 3장에서 제안하는 워터마킹 알고리즘을 설명하고, 4장에서 실험 및 고찰을 통해서 제안한 알고리즘의 특성을 살펴본 후 마지막으로 5장에서 결론을 제시한다.

II. 관련연구

DCT변환을 이용한 워터마킹의 대표적인 방법으로 Cox[1], Piva[2], Barni[3] 등이 제안한 방법이 있다. Cox가 제안한 DCT를 이용한 워터마킹 기법의 경우 대역확산 통신기법을 이용한다. 대역확산 통신기법이란 협대역의 신호를 광대역의 신호에 걸쳐서 전송함으로써 외부환경에 영향을 덜 받으면서 전송할 수 있는 방식을 말한다. 영상 데이터를 주파수 형태로 변환했을 때 가질 수 있는 주파수 대역을 통신채널이라고 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 도입한다.

워터마크를 영상이 갖고 있는 여러 주파수 영역으로 확산시킴으로서 특정 주파수 대역의 에너지는 감지하기 어렵게 한다. 그러나 주파수의 위치와 변화량을 알고 있는 소유권자에 의해 주파수 성분을 추출하면 높은 신호대 잡음비로 워터마크를 검출할 수 있다. 또한 영상을 주파수 성분으로 변환하여 워터마크의 삽입 시 영상에 의미 있는 부분에 워터마크를 삽입하기 위하여 인간 시각적 특성을 고려한 특정 주파수 성분을 이용하게 된다.

원 영상을 DCT를 이용한 주파수 변환 후 DC를 제외한 AC계수 부분에 평균이 0이고 분산이 1인 정규분포를 갖는 가우시안 시퀀스의 워터마크를 삽입하게 된다. AC계수 중에서도 주파수 성분의 특성을 고려하여 워터마크를 삽입해야 하는데 대역확산 된 주파수 성분 중 인간시각에 크게 영향을 미치지 않는 주파수 성분에 워터마크를 삽입한다. 이 때 워터마크의 강인성을 유지하면서 화질 열화를 최소화하도록 워터마크를 삽입해야 한다. 이와 같은 DCT를 이용한 워터마크 삽입 및 검출 과정의 흐름은 [그림 1]과 [그림 2]에서 나타낸다.

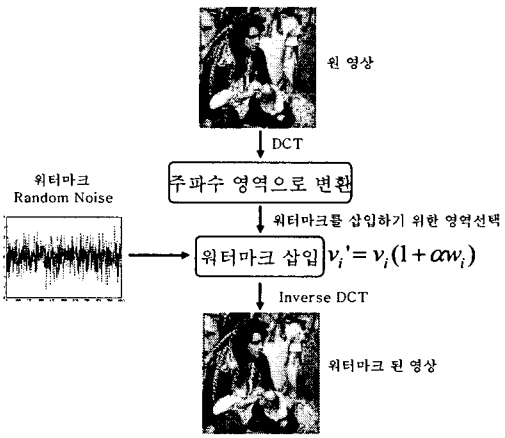

그림 1. DCT를 이용한 워터마크 삽입과정

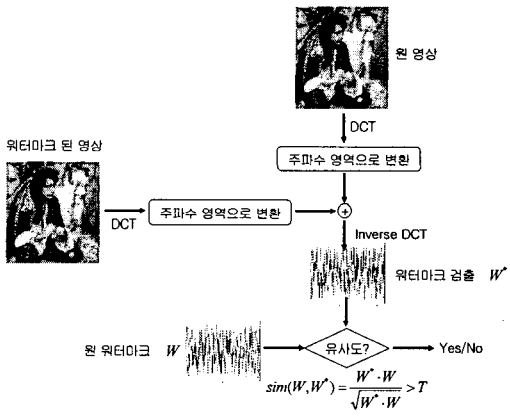

그림 2. DCT를 이용한 워터마크 추출과정

Piva와 Barni에 의해 제안된 DCT 기반 워터마킹 기법은 원 영상에 삽입하고자 하는 워터마크가 M개의 PN시퀀스로 구성되며, 그 값은 식(1)과 같다.

$$X = x_1, x_2, \cdots, x_M \tag{1}$$

X를 이루고 있는 각 x_i의 값은 표준정규분포 N(0,1)에 의해 발생된 랜덤한 실수값이다. 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. 원 영상 없이 워터마크의 검출은 통신로 상에서 잡음이 부가된 영상을 수신하여 검출하는 것이다[4].

1. 워터마크 삽입

워터마크를 영상에 삽입하는 방법은 크기가 N×N인 원 영상 I를 N×N DCT 취하여 DCT 계수를 구한다. 계산된 DCT 계수를 zig-zag scan하여 정렬된 DCT 계수 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 선택, 식(2)와 같은 벡터를 구성한다.

$$T = t_1, t_2, \cdots, t_L, t_{L+1}, \cdots, t_{L+M} \tag{2}$$

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(3)과 같이 생성한다.

$$t'_{L+i} = t_{L+i} + \alpha |t_{L+i}| x_i \tag{3}$$

이러한 방법은 원 신호에 워터마크된 신호를 더하여 진폭계수 α를 증가시켜도 워터마크에 대한 영상의 시

각적인 감지를 방지하고, 공격자로부터 워터마크가 지워지는 것을 방지할 수 있다[6]. 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 DCT 하여 DCT 계수를 구하고, 구해진 DCT 계수를 zig-zag scan한 후, 그 계수 중 하나의 워터마크가 삽입된 대역인 L+1번째부터 L+M번째까지를 택하여 식(4)와 같이 벡터를 구성한다.

$$T^* = t^*_{L+1}, t^*_{L+2}, \cdots, t^*_{L+M} \quad (4)$$

워터마크된 DCT 계수에 삽입할 때 사용된 워터마크 X를 곱하여 상관계수 Z를 식(5)에 의해서 구한다.

$$Z = \frac{1}{M} \sum_{i=1}^{M} x_i \cdot t^*_{L+i} \quad (5)$$

Z값으로부터 워터마크의 존재여부를 판단하는데, 임계값 Sz를 미리 정의하여 상관계수 Z와 비교해서 워터마크가 존재하는지 그렇지 않은지를 확인한다. Sz는 워터마크 된 영상을 이용하여 식(6)에 의해 계산된다.

$$S_z = \frac{\alpha}{3M} \sum_{i=1}^{M} |t^*_i| \quad (6)$$

III. 블록 인덱싱을 이용한 워터마킹

본 논문에서 제안한 워터마킹 기법은 원 영상에 대한 화질 열화를 최소화하면서 다양한 영상에 적용하기 위하여 m*m 원 영상을 n*n 크기를 가지는 서브블록 단위로 나누어 각 블록에 1부터 (m*m)/(n*n)까지의 인덱스 값을 할당한 후, 삽입하고자 하는 워터마크 정보를 블록의 인덱스 값으로 표현하는데 이를 워터마크 정보가 서브블록의 인덱스 값으로 인덱스화 되었다라고 하며, 블록 인덱싱이라 칭한다. 그런 다음 인덱싱 된 블록의 중간 주파수 대역에 특정한 비밀 키에 의해 생성된 PN시퀀스를 삽입함으로써 PN시퀀스가 삽입된 블록의 인덱스 값이 워터마크 정보를 나타내는 기법이다.

본 논문에서 워터마크는 따로 생성하지 않으며, 특정인이나 특정한 정보를 가르키는 0과 1로 구성된 64bits의 이진수로 가정한다.

1. 워터마크 삽입

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

• 1단계

- 먼저 512*512의 원 영상을 32*32의 256개 서브블록으로 나누고 각각의 블록에 1부터 256까지의 인덱스 값을 할당한다. 여기서 서브블록은 삽입하고자 하는 워터마크 정보가 삽입되는 단위 블록이다.
- 원 영상에 직접 워터마크 값을 인덱싱하는 것은 블록 인덱싱 과정에서 원 영상의 고정된 블록에만 워터마크가 삽입될 수 있기 때문에 본 논문에서는 콘텐츠상의 서브블록들을 비밀 키 값을 가지고 스크램블하여 블록의 위치를 뒤섞은 다음 워터마크 삽입과정을 수행한다.
- 삽입하고자 하는 64bits의 워터마크 정보를 단위블록의 인덱스 값으로 매핑시킨다. 각각의 단위블록에 삽입되는 정보는 8비트로 구성되는데, 앞의 4비트는 워터마크 정보의 순서를 나타내는 동기화 비트로 사용되고, 실제 저작권을 나타내는 워터마크 정보는 나머지 4비트가 된다. 제안된 알고리즘에서는 64bits의 워터마크 정보를 256개의 서브블록 중에서 16개의 단위블록에 워터마크를 삽입하며, 멀티미디어 콘텐츠에는 128비트(워터마크 정보순서 64비트, 워터마크 정보 64비트)의 정보가 삽입된다. 멀티미디어 콘텐츠에 삽입되어지는 정보의 구성은 [그림 3]과 같다. 여기서 0과 1로 구성된 8bits의 인덱스화된 워터마크 값을 10진수로 나타내면 앞서 설명한 서브블록의 인덱스 값이 된다.

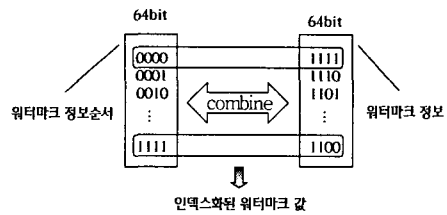

그림 3. 인덱싱된 워터마크의 구성

• 2단계

- 원 영상을 서브블록으로 분할한 후 스크램블 과정을 거친 영상을 살펴보면 16개의 단위블록 행과 열로 나타난다. 행이 가지는 16개의 단위블록을 이진수 0000~1111로 나타내면, 각 행은 16개의 열에 대한 단위블록을 가진다. 이때 16개의 단위블록 열 중에서 하나의 단위블록씩만 블록 인덱싱 된다. [표 1]은 워터마크 값을 서브블록의 인덱스 값으로 표현할 수 있는 범위를 나타낸다.

표 1. 워터마크 값의 인덱싱 범위

워터마크 정보의 순서표현	워터마크 정보표현	8비트로 표현된 인덱스 값 (워터마크 정보의 블록 인덱싱)
1행 = 0000 (Binary)	0000 (Binary)	00000000 = 1 (Binary) = (indexed block)
2행 = 0001	0001	00010001 = 18
3행 = 0010	0010	00100010 = 35
4행 = 0011	0011	00110011 = 52
5행 = 0100	0100	01000100 = 69
6행 = 0101	0101	01010101 = 86
7행 = 0110	0110	01100110 = 103
8행 = 0111	0111	01110111 = 120
9행 = 1000	1000	10001000 = 137
10행 = 1001	1001	10011001 = 154
11행 = 1010	1010	10101010 = 171
12행 = 1011	1011	10111011 = 188
13행 = 1100	1100	11001100 = 205
14행 = 1101	1101	11011101 = 222
15행 = 1110	1110	11101110 = 239
16행 = 1111	1111	11111111 = 256

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

• 3단계

- 2단계 과정을 거쳐 64비트의 워터마크 정보가 인덱싱된 16개의 단위블록에 평균 0, 분산 1의 분포를 이루는 M개의 실수 값을 Piva의 알고리즘을 이용해 삽입하게 된다(PN 시퀀스는 특정한 비밀 키에 의해서 생성된다). [그림 4]는 저작권 보호를 위해 삽입하고자 하는 64비트의 워터마크 정보가 콘텐츠 상에서 단위블록의 인덱스 값으로 표현되는 예를 설명하고 있다. 인덱싱된 이진수 8비트의 정보를 10진수로 표기하면 15와 같으며, 이는 스크램블 된 영상에서 16번째의 단위블록을 나타낸다. 이와 같은 과정을 거쳐서 워터마크 된 영상을 얻을 수 있다.

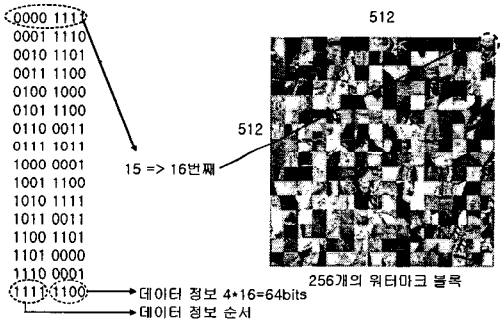

그림 4. 인덱싱된 워터마크 블록

예제의 경우에서는 단위블록 당 4비트의 워터마크를 삽입한 경우이고, 서브블록의 크기를 줄여서 분할된 블록의 개수가 많아지게 할 경우 콘텐츠 상에 삽입할 수 있는 정보량 또한 증가시킬 수 있다. 추출 시 삽입된 PN시퀀스와 삽입된 대역의 유사도 값을 계산하여 워터마크 정보를 추출하므로 블록의 크기가 작아지면 검출율이 낮을 수 있으므로 서브블록은 정확한 워터마크 검출을 위해서 적절한 크기를 유지하여야 한다.

워터마크 정보가 인덱싱된 단위블록들이 Piva의 방법을 이용하기에는 PN시퀀스의 길이가 상당히 짧은 것이 사실이다. 하지만 워터마크가 표현된 단위블록의 인덱스 값 중에서 워터마크 정보의 순서를 결정하는 64비트의 정보들이 존재하기 때문에 몇 개의 불명확한 블록이 있다 하더라도 워터마크를 유추할 수 있다. [그림 5] (a)는 PN시퀀스의 삽입대역을 나타내고 있으며 [그림 5]

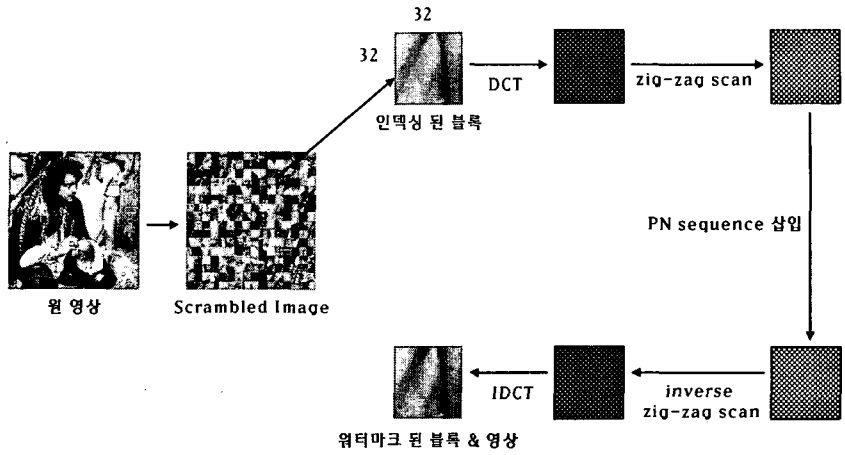

그림 5(b). 제안방법의 워터마크 삽입과정

(b)는 저작권 보호를 위해 워터마크 정보 64비트를 원 영상에 삽입하는 과정을 나타내고 있다.

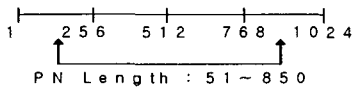

그림 5(a). PN시퀀스 삽입대역

2. 워터마크 추출

워터마크 추출은 삽입과정에서 사용된 PN 시퀀스를 이용하기 때문에 원 영상을 필요치 않으며, 삽입과정의 역으로 워터마크 정보를 추출하게 된다.

◦ 1단계

- 저작권을 증명하기 위한 워터마크 정보를 검출하기 위해서 먼저 대상이 되는 m*m의 원 영상을 n*n의 서브블록으로 나눈다. 분할된 서브블록은 워터마크 추출을 위한 단위블록이다.
- 서브블록들을 삽입과정에서 사용한 비밀 키를 가지고 스크램블 한 후 2단계 과정과 같이 n*n의 모든 서브블록에 대해서 워터마크 검출을 시도한다.

◦ 2단계

- 삽입과정에서 사용한 평균 0, 분산 1의 분포를 이루는 M개의 실수 값을 생성한다.
- 생성된 실수와 삽입과정에서 삽입한 대역이 가지는 값 사이의 유사도 값을 식(7)에 의해 계산한다.

$$(W, W^*) = \frac{W^* \cdot W}{\sqrt{W^* \cdot W}} \qquad (7)$$

W : Original PN시퀀스, W^* : PN시퀀스 삽입대역

- 계산된 유사도 값으로부터 워터마크가 서브블록의 인덱스 값으로 표현된 블록인지 아닌지를 확인, 워터마크가 존재하는 블록은 인덱스 값을 8비트 이진수로 변환해서 삽입한 워터마크 정보를 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)와 [그림 6] (b)는 삽입된 워터마크 정보 64비트를 대상이 되는 콘텐츠 상에서 추출하는 과정을 나타낸다.

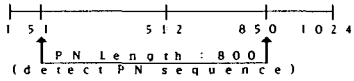

그림 6(a). PN시퀀스 추출대역

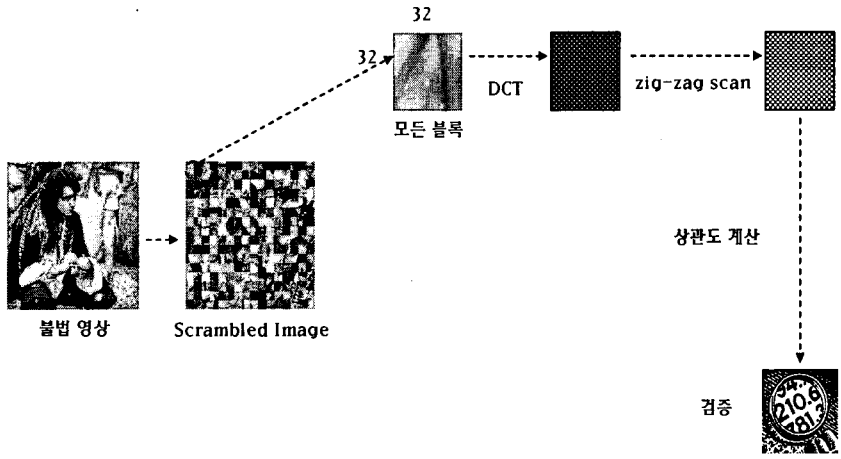

그림 6(b). 제안방법의 워터마크 추출과정

Ⅳ. 실험결과 및 고찰

제안방식의 효율성을 확인하기 위하여 다음 그림과 같은 몇 가지 gray scale의 Man영상, Lena영상, Bridge영상, Couple영상, House영상을 대상으로 하여 128비트(워터마크 정보순서 64비트 & 워터마크 정보 64비트)를 삽입하고 추출하는 과정을 수행하고, 여러 가지 신호처리 적인 왜곡을 가하여 공격으로부터의 강인성을 실험한다.

[그림 7]은 알고리즘에서 사용한 원 영상이다.

그림 7. 원 영상

[그림 8] (a) 그림은 Piva의 알고리즘에 따라 α=0.2, L=25000, M=16000을 적용한 워터마크된 영상을 나타내고 있으며, [그림 8] (b)는 제안방법에 따라 32×32크기의 블록으로 나누어 α=0.5, L=50, M=800개가 삽입되어진 영상을 나타내었다.


(PSNR : 47.01)

그림 8(a). Piva방식의 워터마크 된 영상


(PSNR : 44.21)

그림 8(b). 제안방식의 워터마크 된 영상

Piva의 워터마크 검출 알고리즘에 의해 Original 워터마크로 검출한 결과와 1000회 정도 랜덤하게 워터마크를 발생시켜 검출한 결과를 [그림 9]에서 나타낸다. 결과에서 보는바와 같이 상관계수 값은 삽입 시에 사용된 정확한 워터마크를 가지고 검출하였을 때 가장 큰 값을 나타내고, 다른 신호 값들에 대해서는 아주 낮은 값을 나타내었다.

[그림 10] (a)는 제안 방식의 검출 알고리즘에 의한 블록 당 결과 값을 그래프로 나타내고 있다. 워터마크가 인덱싱된 16개의 블록에서 상대적으로 높은 유사도 값을 보인다. [그림 10] (b)는 PN 시퀀스 길이를 달리한 결과이다.

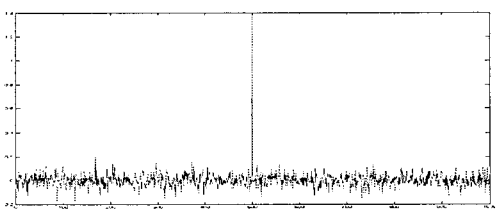

그림 9. Piva방법의 워터마크 검출 response

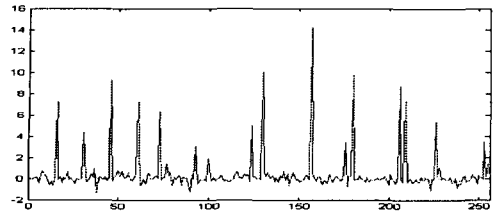

그림 10(a). 제안방법의 워터마크 검출 시 각 블록에 대한 response (PN length : 800)

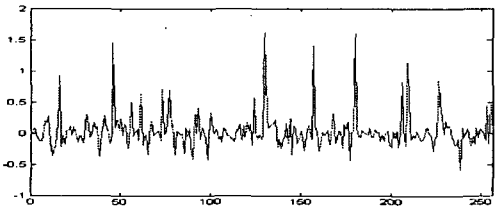

그림 10(b). 제안방법의 워터마크 검출 시 각 블록에 대한 response (PN length : 500)

제안기법에서 사용한 PN 시퀀스의 길이는 800으로 32*32 단위블록에서 인간의 지각성을 고려하되 최대한의 크기로 중간주파수 대역에 삽입된다. PN 시퀀스의 길이는 워터마크 검출에 있어 중요한 요소로 PN 시퀀스의 길이가 너무 길면 워터마크 된 영상에서 비지각성을 만족시키지 못하며, 너무 짧으면 워터마크 검출을 제대로 할 수 없다는 점을 고려해야 한다.

신호처리적인 내성에 대해서는 추출된 16개의 블록(실제 PN시퀀스가 삽입되어진 블록)에 대해 삽입과정에서 사용한 Original PN시퀀스와 500회의 랜덤하게 생성한 다른 실수 열과의 상관도 값을 구하여 제시하였다. 적색으로 상관도가 높게 나타나는 부분이 Original PN시퀀스와의 상관도를 나타내며 청색으로 나타난 상관도는 전현 다른 랜덤한 PN시퀀스와의 상관도를 나타낸다. [그림 11]에서 계산된 결과를 보이고 있으며 X축은 500회의 랜덤 시퀀스 빈도를 나타내며 Y축은 상관도를 나타낸다. Original PN시퀀스를 사용해서 계산된 유사도 값이 다른 랜덤한 실수 열과의 계산보다 높은 유사도 값을 가짐으로 신호처리 적인 내성을 가진다.

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 제거하기 위한 filter

② Histogram Equalization

: 영상처리에 의해 화질이 향상될 수 있다. 히스토그램 평활화는 명암 값 분포를 재분배하여 보다 균일한 분포를 갖게 함으로 인해 화질을 향상시

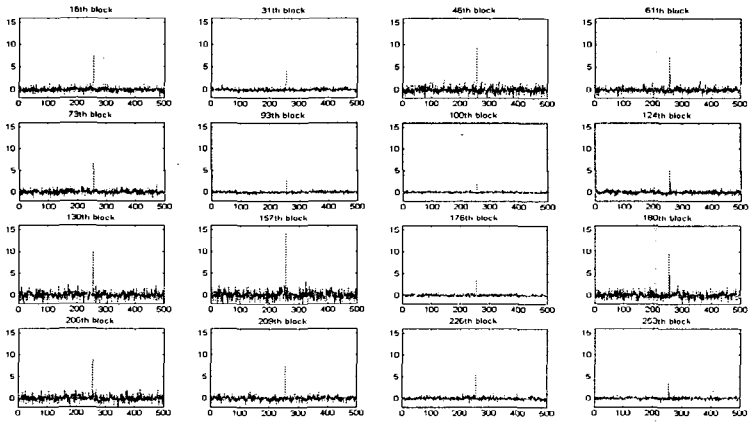

그림 11. 검출된 블록에 대한 검증

킬 수 있는 영상처리기법.

③ JPEG Compression 90%

: 영상의 압축으로 인해 정보의 데이터양을 줄임으로써 전송시 효율적인 영상처리기법.

④ JPEG Compression 70%

⑤ Low pass Filter

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

⑥ Sharpening

: 영상의 Detail information를 향상시키기 위한 영상처리기법.

Gaussian Filter | Histogram Equalization | JPEG 90% Compression | JPEG 70% Compression | Low pass Filter | Sharpening

그림12(a). 신호처리 공격에 의해 생성된 영상

신호처리 공격에 의해 생성된 영상은 [그림 12] (a)에서 확인할 수 있으며, [그림 12] (b)에서 워터마크의 강인성을 간과할 수 있는 PSNR(Peak Signal to Noise Ratio) 값을 나타내고 있다.

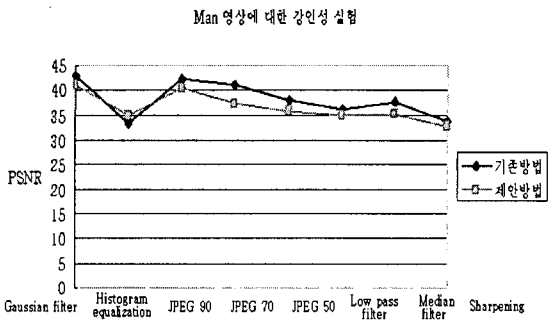

그림 12(b). 신호처리 공격된 영상에 대한 PSNR

다양한 신호처리 적인 왜곡에도 PSNR 값은 35[dB] 전후로 화질 열화는 크지 않다.

[그림 13]에서 18까지는 Piva기법과 제안기법에 대해 신호처리적인 공격(Stirmark 3.1의 대표적인 공격)에 의해 왜곡된 영상을 대상으로 한 워터마크 검출 response를 나타내고 있다.

PN 시퀀스가 삽입된 16개 블록의 상관도 값이 다른 블록에 비해 높은 값을 가지는 것을 확인할 수 있다.

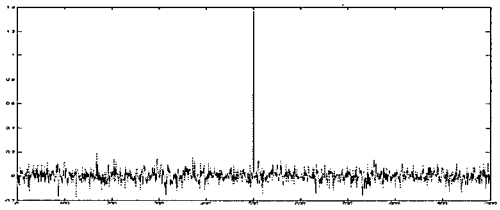

그림 13(a). Gaussian Filter 공격에 대한 검출 response(Piva기법)

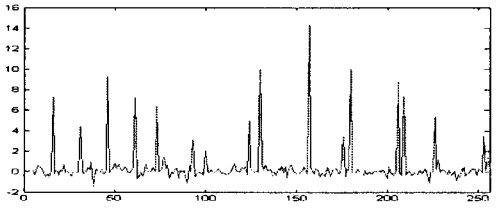

그림 13(b). Gaussian Filter 공격에 대한 검출 response(제안기법)

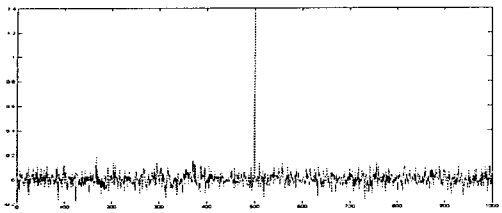

그림 14(a). Histogram Equalization 공격에 대한 검출 response(Piva기법)

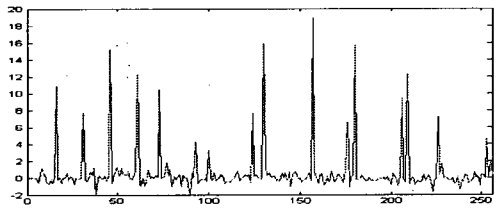

그림 14(b). Histogram Equalization 공격에 대한 검출 response(제안기법)

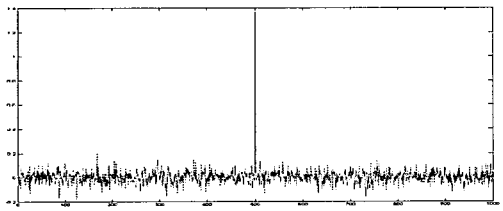

그림 15(a). JPEG 90% Compression 공격에 대한 검출 response(Piva기법)

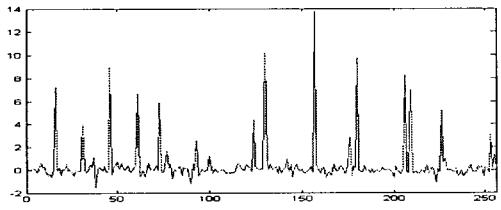

그림 15(b). JPEG 90% Compression 공격에 대한 검출 response(제안기법)

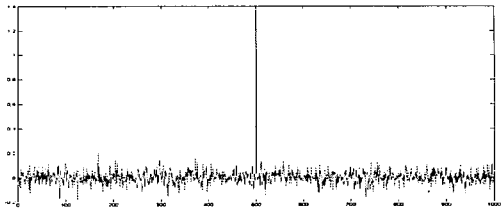

그림 16(a). JPEG 70% Compression 공격에 대한 검출 response(Piva기법)

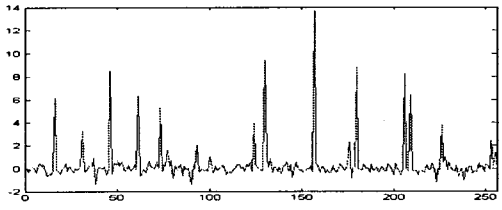

그림 16(b). JPEG 70% Compression 공격에 대한 검출 response(제안기법)

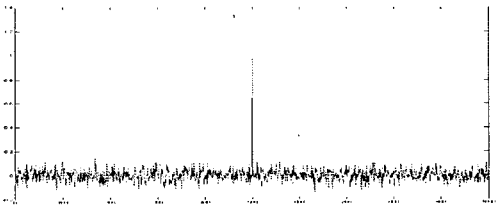

그림 17(a). Low pass Filter 공격에 대한 검출 response(Piva기법)

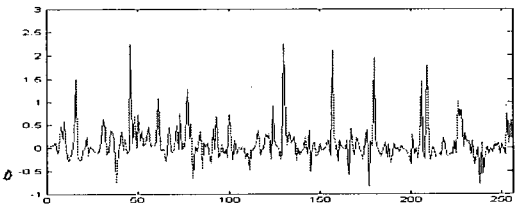

그림 17(b). Low pass Filter 공격에 대한 검출 response(제안기법)

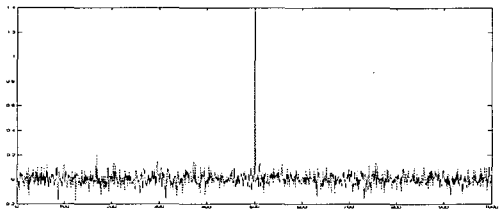

그림 18(a). Sharpening 공격에 대한 검출 response(Piva기법)

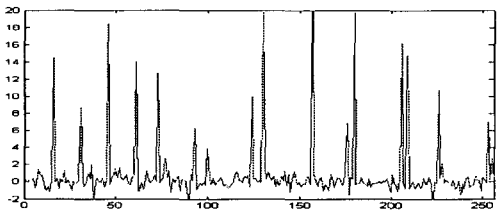

그림 18(b). Sharpening 공격에 대한 검출 response(제안기법)

실험결과에서 나타난 것처럼 각각의 공격영상에 대한 상관계수 값은 대체로 높은 상관계수 값을 보여 신호처리적인 내성을 가지고 있음을 확인할 수 있다.

삽입된 워터마크가 각 영상의 화질에 미치는 영향을 확인하기 위해 Piva기법과 제안기법의 워터마크 된 영상에 대해 식(8)에 의해서 PSNR값을 비교하였다.

삽입된 워터마크가 각 영상의 화질에 미치는 영향에 대한 비교를 위해 Piva기법과 제안된 기법의 워터마크 된 영상에 대해 식(8)에 의해서 PSNR값을 비교하였다.

$$PSNR = 10 \log_{10} \frac{M_i^2 \max X}{MSE} [dB] \qquad (8)$$

$$MSE = \frac{1}{M \times M} \sum_{i=1}^{M} (X_i - X_i')^2 \qquad (9)$$

식(9)에서 M은 원 영상의 너비와 높이 크기이고, X는 원 영상을, X'는 워터마크 된 영상을 나타내고 있으며, PSNR의 결과 값이 클수록 원 영상과 화질의 차이가 적음을 나타낸다.

[표 2]에서 Piva, 제안방식 모두 PSNR 값은 40[dB] 이상으로 워터마크 삽입에 의한 화질의 열화가 거의 없음을 보여주고 있다. 사용된 PN 시퀀스의 길이가 달라 Piva 방식의 PSNR값이 다소 높으나 삽입되는 워터마크의 정보의 양은 제안방식이 효율적이다.

표 2. Piva방식과 제안방식의 PSNR 비교

실험영상	Piva방식[dB]		제안방식[dB]	
Man	47.07	워터마크 삽입량 : 1bit PN 시퀀스 길이 : 16000	44.21	워터마크 삽입량 : 64bit PN 시퀀스 길이 : 800
Lena	42.43		41.12	
Couple	50.79		43.29	
Bridge	50.22		42.98	
House	45.49		41.43	

V. 결 론

본 논문에서는 디지털 멀티미디어 데이터의 저작권 보호를 위해 멀티미디어 콘텐츠의 단위블록에 인덱스 값을 할당한 후, 이를 워터마크 정보와 매핑시키는 새로운 방법을 이용하고 있으며, 워터마크 정보가 매핑된 단위블록에 DCT기반의 대역확산 기법을 적용하여 워터마크 정보를 표현하는 블록 인덱싱 워터마킹 기법을 제안하고, 그 유용성에 대해 살펴보았다. 실험을 통해 통신로 상에서 발생 가능한 신호처리공격에 대해서도 워터마크를 검출할 수 있는 내성을 입증하였다. 삽입과정에서 원 영상을 서브블록으로 분할하고, 분할된 블록 중에서 워터마크 값을 표현하는 인덱스 값을 가지는 단위 블록을 대상으로 워터마크를 삽입하는 과정에서 계산 량은 다소 증가하지만 화질 열화를 최소화할 수 있고 공격에 대한 안전성을 보장할 수 있다.

제안된 블록 인덱싱이란 새로운 기법을 이용한 워터마킹 알고리즘은 현실적이고 효율적인 기법으로 보다 확장된 응용에 적용할 수 있을 것으로 기대된다.

참 고 문 헌

[1] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE

Transactions, Vol.6, No.12, pp.1673-1687, Dec. 1997.

[2] A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "DCT-based Watermarking Recovering without Resorting to the Uncorrupted Original Image," IEEE International Conference, Vol.1, No.26, pp.520-523, Oct. 1997.

[3] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT-Domain System for Robust Image Watermarking," IEEE Transactions, Vol.66, No.3, pp.357-372, May. 1998.

[4] Gangyi Jiang, Mei Yu, Shoudong Shi, Xiao Liu, and Yong-Deak Kim, "New blind image watermarking in DCT domain," IEEE Transactions, Vol.2, No.26, pp.1580-1583, Aug. 2002.

[5] E. Y. Lam and J. W. Goodman, "A Mathematical Analysis of the DCT Coefficients Distributions for Images," IEEE Transactions, Vol.9, No.10, pp.1661-1666, Oct. 2000.

[6] M. Eyadat, "Factors that affect the performance of the DCT-block based image watermarking algorithms," International Conference on information technology, Vol.1, No.2, pp.650-654, Dec. 2004.

저 자 소 개

한 승 우(Seung-Wu Han) 준회원

- 2003년 2월 : 동명정보대학교 정보통신공학과(공학사)
- 2005년 2월 : 부경대학교 대학원 전자계산학과(이학석사)
- 2005년 3월~현재 : 부경대학교 lacuc 연구원

<관심분야> : 멀티미디어 컨텐츠 보호, 신호처리

강 현 호(Hyun-Ho Kang) 정회원

- 1999년 2월 : 동의대학교 컴퓨터공학과(공학사)
- 2001년 2월 : 부경대학교 대학원 전자계산학과(이학석사)
- 2004년 2월 : 부경대학교 대학원 전자계산학과(박사수료)
- 2005년 4월~현재 : 일본 전기통신대학(電氣通信大學) 박사과정

<관심분야> : 멀티미디어 컨텐츠 보호 및 응용, 신호처리, 오류정정부호

신 상 욱(Sang-Uk Shin) 정회원

- 1995년 2월 : 부경대학교 전자계산학과(이학사)
- 1997년 2월 : 부경대학교 대학원 전자계산학과(이학석사)
- 2000년 2월 : 부경대학교 대학원 전자계산학과(이학박사)
- 2000년 4월~2003년 8월 : 한국전자통신연구원 선임연구원
- 2003년 9월~현재 : 부경대학교 전자컴퓨터정보통신공학부 전임강사

<관심분야> : 암호이론, 정보보호, 이동통신 정보보호