웨이블릿 변환을 이용한 MPEG 디지털동영상 워터마킹에 관한 연구

이 학 찬[†] · 조 철 훈[††] · 송 중 원[†††] · 남궁 재 찬[††††]

요 약

디지털 워터마킹이란 영상이나 비디오, 오디오, 텍스트 등의 저작물에 잘 식별되지 않는 표시를 삽입하여 저작권을 보호하는 방법으로 소유권자의 동의 없이 저작물을 배포, 복사되는 것을 방지하는 방법이다. 본 논문에서는 MPEG 기반의 압축된 영상에 저작권 보호를 위한 시스템의 구현을 위하여 휘도신호에 웨이블릿을 이용한 워터마크 키의 삽입과 추출에 대하여 연구한다. 우선, 원 이미지를 이산 웨이블릿 변환을 이용하여 주파수 영역으로 분해한다. 이 때 RSA(Rivest, Shamir, Aldeman) 공개키(public key)의 암호화 대상을 VLC(variable length coding) 파라메터의 RUN으로 하였다. 이웃하는 RUN파라메터 사이의 높은 연관성은 이미지 전체에 영향을 미치기 때문에 비밀키(private key)를 소유하지 않은 비인가자의 불법적인 행위를 막을 수 있다. 실험 결과, DCT기반의 저주파 대역에 대한 직접적인 암호화 방식[13]보다 더 적은 키를 삽입시키면서 오히려 더 높은 왜곡과 위치가 이동된 이미지를 얻을 수 있었다.

A Study on Digital Watermarking of MPEG Coded Video Using Wavelet Transform

Hack-Chan Lee[†] · Chul-Hoon Cho[††] · Joong-Won Song[†††] · Jae-Chan Namgung[††††]

ABSTRACT

Digital watermarking is to embed imperceptible mark into image, video, audio, and text data to prevent the illegal copy of multimedia data, arbitrary modification, and also illegal sales of the copies without agreement of copyright ownership. In this paper, we study for the embedding and extraction of watermark key using wavelet in the luminance signal in order to implement the system to protect the copyright for image MPEG. First, the original image is analyzed into frequency domain by discrete wavelet transform. The RSA (Rivest, Shamir, Aldeman) public key of the coded target is RUN parameter of VLC (variable length coding). Because the high relationship among the adjacent RUN parameters effect the whole image, it prevents non-authorizer not to possess private key from behaving illegally. The Results show that the proposed method provides better moving picture and the high distortion more key of insert than direct coded method on low-frequency domain based DCT.

키워드 : Wavelet transform, VLC, RSA, DCT

1. 서 론

최근 컴퓨터 및 네트워크에 대한 기술과 인터넷의 비약적인 발전으로 각종 여러 멀티미디어 서비스와 데이터가 급속도로 대중에게 전달되고 있다[13]. 특히, 전자 출판, 컴퓨터, 통신 기술의 발전으로 문서, 음성, 사진 및 비디오 데이터 등 다양한 매체들은 전자기적 장치에 의하여 디지털화 되어 효율적으로 저장, 접근, 이용이 가능하게 되었고, 많은 양의 정보를 디지털 형식으로 저장, 전송하도록 허용되었다. 데이터의 형태가 아날로그 형태에서 디지털 형태로 급속히 변하고 있으며, World Wide Web의 출현으로 더욱 확장되었다. 앞으로 정보는 개인적인 만족을 위한 인터넷 서비스가 발전할 것이며, 여기에서 오는 여러 가지 저작권 문제와 거기에 따르는 해결방안이 심각한 사회문제로 대두되고 있다. 이러한 문제점은 디지털 영상의 소유권 및 저작권 보호와 인증에 대한 분쟁으로 이어지고 있으며 현재까지 이러한 분쟁을 해결하기 위해 학술적으로 여러가지 연구가 진행되어 왔으며 그 중에서도 영상의 소유권 보장과 불법적인 내용 조작을 동시에 막을수 있는 디지털 워터마킹 방법이 가장 활발히 연구되고 있다[1, 2, 5]. 워터마킹은

※ 이 논문은 2000년 광운대학교 교내연구비에 의하여 연구되었음.
† 준 회 원 : 숭실대학교 대학원 컴퓨터학과
†† 준 회 원 : 광운대학교 대학원 컴퓨터공학과
††† 준 회 원 : 광운대학교 정보과학기술대학원 지능정보공학과
†††† 종신회원 : 광운대학교 컴퓨터공학과 교수
논문접수 : 2000년 8월 3일, 심사완료 : 2001년 9월 28일

저작권 보호뿐만 아니라 원본 데이터임을 인증(Authentication)하거나 방송감시(broadcasting monitoring) 및 구매자를 판별(fingerprinting)하는 데에도 응용되고 있다[12]. 본 논문에서는 인터넷 서비스 중 MPEG에서 일어나는 저작권 보호 문제와 불법복제의 방지를 위해 웨이블릿 기반의 RSA 공개키 암호시스템을 이용한 암호화된 워터마크 키 삽입 기술을 제안한다. 워터마크는 모든 멀티미디어 데이터에 적용할 수 있지만, 본 논문에서는 동영상(MPEG)에 대해서만 다루었다. MPEG방식으로 압축된 동영상은 하나의 프레임 내에서 공간적인 중복성을 제거한 I-프레임과 프레임들 사이의 시간적인 중복성을 제거한 P, B-프레임으로 구성된다. I, B, P-프레임은 서로 종속적인 관계를 유지하며 I-프레임의 왜곡은 B, P프레임에 간접적 영향을 미친다. 제안한 알고리즘에서는 I-프레임에 대한 이미지 왜곡을 제안하였다.

워터마킹은 크게 두 가지로 나눌 수 있다. 어떤 개인이 특정한 작품을 만들어 자신의 창작물임을 주장하기 위해 자신만의 독특한 형태의 정보를 영상에 표시해두는 방법과 특정 인가된 사람에게 개인키(private key)를 할당하여 암호화된 이미지를 볼수 있게 하는 방법이 있다. 본 논문에서는 동영상(MPEG)에 워터마크를 삽입시키기 위해 이산 웨이블릿을 기본으로 하는 MPEG를 이용하여 압축된 영상에 워터마크 키를 삽입하는 방법을 제시한다. 먼저, 원 영상을 휘도신호(Y)와 색차신호(CbCr)로 나누고, 그 중 인간의 눈에 민감한 휘도신호를 이산 웨이블릿 변환으로 주파수를 분해한 후 암호화(encription)된 워터마크 키를 해당 RUN 위치에 삽입시키고 비밀키를 가지고 원 이미지를 복원한다. 본 논문의 구성은 1장에서 웨이블릿 변환에 대해, 3장에서 워터마킹과 암호화(encription)에 대해 기술하고, 4장에서 제안한 알고리즘을 소개하고 5장에서는 실험 및 결과를, 마지막으로 6장에서 결론을 맺는다.

2. wavelet transform

2.1 wavelet transform

웨이블릿 변환(wavelet transform)은 퓨리에 변환(fourier transform)과같이 기저 함수(basis function)들의 집합에 의한 신호 분해로써 이해될 수 있다[7]. 이때 웨이블릿 변환에서 하나의 기저함수를 웨이블릿이라 부르며 웨이블릿은 하나의 대역 통과 필터이다. 퓨리에 변환의 기저 함수들과는 다르게 웨이블릿은 유한의 길이를 가지는 기저함수이므로 웨이블릿 변환은 mother wavelet이라 불리는 원형의 웨이블릿의 수축과 팽창에 의해 얻어지는 웨이블릿들의 집합에 의해 구성된다. 그리고 웨이블릿 변환에서는 주파수라는 용어 대신 스케일이라는 용어를 사용하며, 하나의 웨이블릿을 통과한 신호를 스케일의 상세 신호(detail signal)라 한다[15].

웨이블릿 변환은 다운샘플 필터링으로 이루어지며, 원래의 신호를 LPF(Low Pass Filter)와 HPF(High Pass Filter)를 이용하여 분해한다. 분리된 두 개의 신호중 원하는 부분을 다시 필터링(filtering)하여 저주파 성분과 고주파성분으로 나누는데, 이러한 과정을 반복하면 원하는 대역의 주파수 성분을 알수 있다. 웨이블릿 기본함수인 mother wavelet $\Psi(t)$ 함수는 다음과 같은 특성을 가지고 있다.

$$\int_{-\infty}^{\infty} \Psi(t)dt = 0$$

$$\int_{-\infty}^{\infty} |\Psi(t)|^2 dt < \infty$$

이 함수는 아래와 같이 확장과 천이를 통해서 하나의 함수 집합이 된다.

$$\Psi_{a,b}(t) \equiv \frac{1}{\sqrt{|a|}} \Psi\left(\frac{t-b}{a}\right)$$

a와 b는 각각 확장과 천이를 나타내며 웨이블릿변환을 위한 기저함수의 파라메터이다. $\phi(t)$와 $\Psi(t)$를 아래와 같이 쓸 수 있다.

$$\phi(t) = \sum_n h(n)\sqrt{2}\phi(2t-n), \quad n \in Z$$

$$\Psi(t) = \sum_n g(n)\sqrt{2}\phi(2t-n), \quad n \in Z$$

원 신호를 다음과 같은 기저함수의 합으로 나타낼 수 있다.

$$f(t) = \sum_k f_k(t)$$

$$f_k(t) = c_j(k)\phi(t-k) + \sum_j d_j(k)\, 2^{j/2}\Psi(2^j t-k)$$

아래 수식에서의 $c_j(k)$와 $d_j(k)$은 웨이블릿 변환의 필터처럼 사용하는데 이의 근거가 위의 식에 있다고 할 수 있다.

$$c_j(k) = \sum_{m=0}^{N-1} h(m-2k)\, c_{j+1}(m)$$

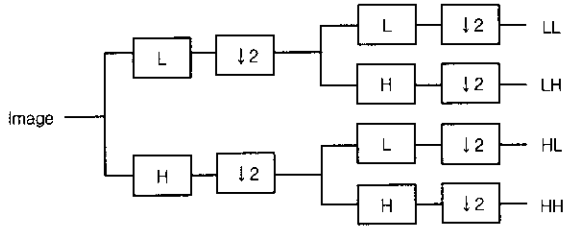
$$d_j(k) = \sum_{m=0}^{N-1} g(m-2k)\, c_{j+1}(m)$$

$$c_{j+1}(k) = \sum_{m=0}^{N-1} h(k-2m)\, c_j(m) + \sum_{m=0}^{N-1} g(k-2m)\, d_j(m)$$

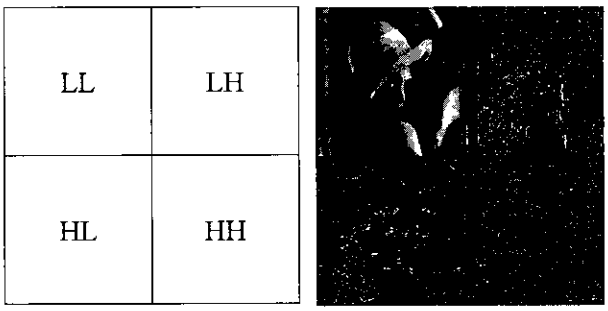
2.2 이미지에서의 웨이블릿 변환

웨이블릿 변환은 원 신호를 먼저 LPF(low pass filter)와 HPF(high pass filter)를 통해 각각 저주파 대역과 고주파 대역으로 분해하고 고주파 대역을 제외한 저주파 대역의 신호를 다시 원하는 레벨의 수준까지 위의 과정을 반복함으로써 다운 샘플링을 한다[6]. 이미지에 대한 웨이블릿 변

환은 가로방향과 세로방향으로 각각 순차적으로 웨이블릿 변환을 수행하여 주파수를 분해한다[15]. (그림 1)은 2-D 이산 웨이블릿 분해를, (그림 2)는 이미지에서의 웨이블릿 분해의 예를 보여주고 있다.



(그림 1) 2-D 이산 신호 웨이블릿 분해



(그림 2) 이미지에서의 웨이블릿 변환

웨이블릿의 변환은 화면을 확대 하거나 축소하더라도 이미지에 거의 손상을 주지 않으면서 DCT(discrete cosine transform)가 가지고 있는 블록킹(blocking) 현상이 없어 고품질의 영상처리가 가능하다.

3 watermarking

3.1 watermarking

워터마킹이란 copyright등과 같은 정보(water mark)를 오디오나 이미지와 같은 미디어에 사람이 인지하지 못하도록 삽입하고 검출할 수 있는 방법을 말한다. 이러한 워터마킹 기법을 그대로 컴퓨터에 적용한 것이 바로 디지털 워터마킹(digital water marking)이다.

이러한 디지털 워터마킹 기법에 기본적으로 요구되는 특징들은 아래와 같다[3, 4].

무감지성(Invisibility) : 디지털 미디어에 삽입된 워터마크는 육안으로는 확인할 수 없어야 한다.

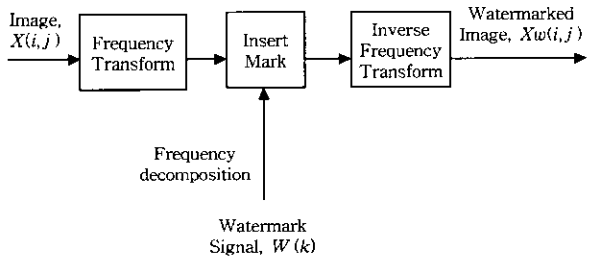
보안성(Security) : 워터마크의 삽입과정이 알려져 있다 해도 관련된 파라메터 값들을 알고 있지 않는 한 불법적으로 워터마크를 삭제하려는 시도는 불가능해야 한다.

강인성(Robustness) : 워터마크가 찍힌 영상은 그 이후의 다양한 의도적 또는 비의도적인 왜곡 방법에 대해 삭제되거나 변형되어서는 안된다. 예를 들어, 전송 및 저장시 발생되는 에러나 JPEG(Joint Photographic Experts Group)과같은 손실 압축 환경에서 발생하는 압축 에러, 그리고 필터링(filtering), 영상 일부만 자르는 크로핑(Cropping), 영상을 축소, 확대하는 스케일링(Scaling), 부가잡음(additional noise) 등의 영상처리 과정에 의해 워터마크가 지워져서는 안된다.

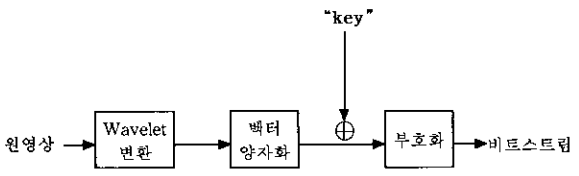
명확성(Unambiguity) : 워터마크가 찍힌 영상에 대해 명확히 소유권을 증명할 수 있는 방법이 있어야 한다. 때에 따라 여러 불법 사용자들이 자신이 임의로 만든 워터마크를 워터마크가 이미 찍힌 미디어에 재삽입하여 소유권을 주장하는 충돌이 발생하는 경우에도 디지털 미디어의 실제 소유권자를 구별할 수 있어야 한다.

워터마킹은 크게 공용 키(public key)를 이용한 암호화 기법과 주파수 확산을 통해 이미지 안에 직접 워터마크를 삽입하는 기법으로 나눌 수 있는데 위의 특징들이 바로, 이 주파수 확산기법에 속한다[14]. 공용 키(public key)를 이용한 워터마크는 이미지의 일부분에 key를 삽입하고 그 키를 수신측에서 받아 이미지를 해독하는데 사용한다. 만약 key를 갖고 않은 비인가자가 이를 해독하려고 시도한다면 이미지는 심한 왜곡이 발생하게 되어 육안으로 식별할 수 없게 된다.

(그림 3)은 주파수 확산 워터마킹을, (그림 4)는 public key를 이용한 워터마킹을 삽입 방법을 보이고 있다.



(그림 3) 주파수 확산을 이용한 워터마킹



(그림 4) public key를 이용한 워터마킹

3.2 RSA(Rivest, Shamir, Aldeman)

RSA 공개키(public key) 암호시스템은 암호화와 전자서명 모두를 제공할 수 있으며, 소인수분해의 어려움에 안전도의 근간을 두고 있다[8, 9]. 즉, 두 소수 p와 q의 곱은 계산하기 쉬우나, 주어진 곱 n = pq로부터 p와 q를 추출하기는 어렵다는 사실에 근간을 두고있다. RSA암호 시스템은 모듈러 지수 연산이 주를 이룬다. 실제 응용에 있어, 작은 암호화 지수를 사용함으로써 복호화보다는 암호화를 더 빠르게 수행 할 수 있도록 설계되고 있다.

< 키 생성 >

1) 두 개의 (서로 다른) 큰 소수 p와 q를 임의로 생성한다.
2) n = pq와 k = (p-1)(q-1)를 계산한다.
3) gcd (*e*, k) = 1인 정수 e (1 < *e* < k)를 임의로 선택한다.
4) 확장된 유클리드 알고리즘을 사용하여 $ed \equiv 1 (\mathrm{mode}\ k)$를 계산한다.
5) A의 공개 키 : (n, *e*), A의 비밀 키 : d

< 암호화 >

1) A의 인증된 공개 키 (n, e)를 얻는다.
2) 메시지 m을 [0, n-1]사이의 정수로 표현한다.
3) $c \equiv m^e \bmod n$를 계산한다.
4) 암호문 c를 A에게 보낸다.

< 복호화 >

1) 비밀 키 d를 이용하여, $m \equiv c^d \bmod n$를 계산한다.

4. 제안한 알고리즘

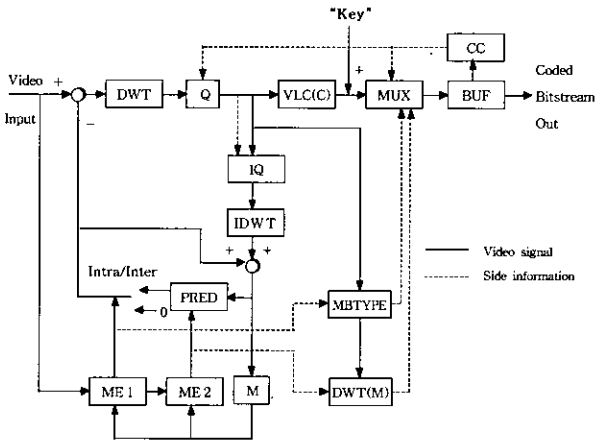
4.1 구조

DCT변환은 알고리즘이 단순하여 매우 큰 입력 데이터를 한번에 처리하지 않고 부분적으로 나누어 처리하기 때문에 반복처리가 가능하며 하드웨어 구현이 간단하다. 그러나 블록단위의 변환을 하기 때문에 블록킹 현상(bolcking effect)이 일어나는 문제점이 있다[10].

DCT변환이 가지고 있는 블록킹 현상을 막아주고 I프레임의 전체 이미지를 한번에 처리할 수 있는 DWT(Discrete Wavelet Transform)를 MPEG에 적용한다. 그리고 공용 키(public key) 암호화 시스템에 의해 생성된 워터마크 키를 VLC블록에 적용함으로써 MPEG비디오에 대해 워터마크를 할 수 있고, 마지막으로 압축하여 전송한다.

웨이블릿은 이웃하는 대역 계수들간의 높은 연관성을 가지고 있다. VLC는 이 계수들을 LAST, RUN, LEVEL의 파라메터들로 부호화하며, 영상에 손실이나 변형을 가하기 위해 이들 파라메터중 RUN파라메터에 RSA공용키 암호화 시스템을 적용하고 생성된 워터마크 키를 해당 RUN위치에 삽입한다. RUN파라메터는 다른 파라메터들에 비해 영향을 미치는 범위가 비교적 넓고, 영상의 위상(위치)까지도 바꾸어 놓을 수 있는 또 하나의 특징을 가지고 있어 영상 암호화에 가장 적당한 파라메터라고 할 수 있다. 반면, LAST파라메터는 0과 1로 값이 제한되어 있어 암호화에 부적당하며, LEVEL은 색의 명암이 왜곡되지만 영상의 위상(위치)는 바꿀 수 없으며, 암호화 수가 VLC 부호화 수에 비례하게 되어 실시간 처리에 부적합하다.

아래 (그림 5)는 제안한 MPEG 디지털 워터마킹 구조를 나타내고 있다.

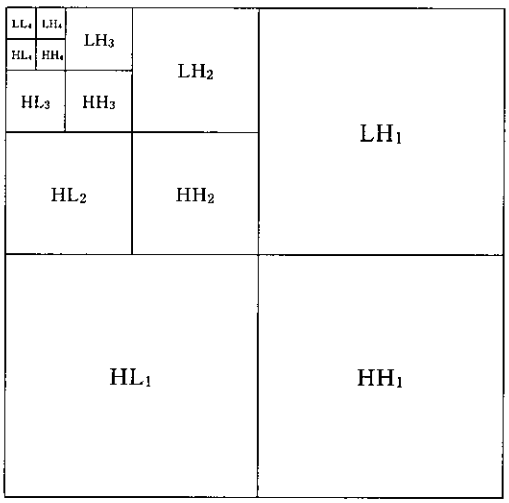


(그림 5) 제안한 MPEG 디지털 워터마킹

Watwrmarking을 위해서 입력된 영상의 휘도 신호와 색차 신호중 인간의 시각에 민감한 휘도 신호를 RSA의 공용키(public key)를 이용하여 메시지를 생성한다. 이렇게 생성된 메시지는 key를 갖지 않은 비인가자에 대하여 육안으로 식별이 어려울 정도의 왜곡이 심한 이미지를 제공한다.

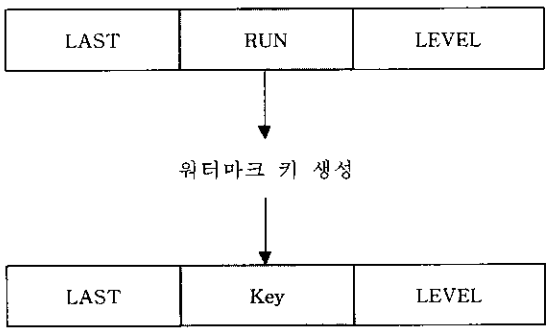
4.2 알고리즘

MPEG이미지는 웨이블릿과 양자화를 거쳐 VLC (variable length coding)[11]로 코딩하여 전송된다. (그림 6)은 이



(그림 6) 다차원 웨이블릿 분해 과정

미지의 다차원 이산 웨이블릿 분해과정을 보여주고 있으며 반복된 분해를 통해 다단계 다운 샘플링과정 볼 수 있다. 본 논문에서는 이미지를 전송하기 위해 4레벨의 웨이블릿 분해로 LL_4 대역을 제외한 나머지 대역에 대하여 VLC(variable length coding)를 처리하였으며 (그림 7)의 (LAST, RUN, LEVEL)에서 RUN 파라메터를 공용키를 사용하여 암호화함으로써 의도적인 이미지 왜곡을 시도하였다.



(그림 7) watermark key 생성 및 삽입

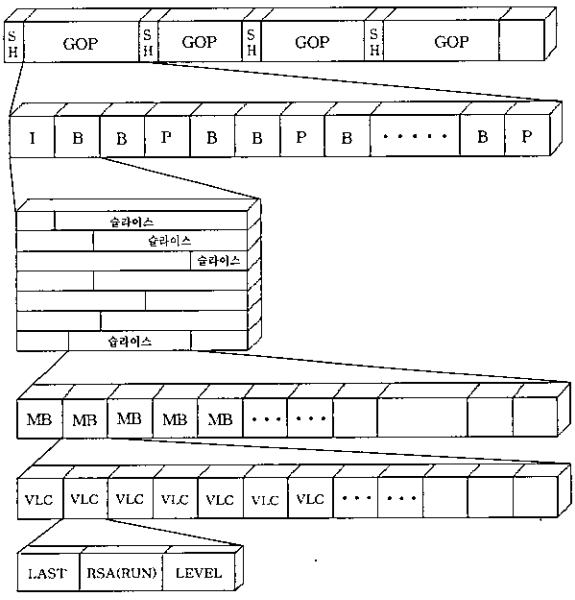
RUN의 계수는 이어지는 계수와의 연관성이 높기 때문에 임의의 계수가 손실되거나 변형된다면 나머지 계수가 갖는 의미는 없어지게 되므로 이미지의 왜곡이 발생하게 된다. 분해의 레벨이 높아질수록 LH, HL, HH대역과의 연관성이 높아지므로 이미지 왜곡의 요인이 된다.

< 워터마크 키 삽입 알고리즘 >

STEP 1 : 원 이미지의 DWT 변환 및 양자화.

STEP 2 : 공용키를 이용한 watermark key 생성

STEP 3 : 해당 RUN파라메터에 key삽입



(그림 8) MPEG 영상 데이터의 워터마킹 계층구조

< 복원 알고리즘 >

STEP 1 : 워터마크 키 추출

STEP 1 : 비밀키를 이용한 해당 RUN파라메터 복원

STEP 2 : IDWT 변환 및 역양자화를 이용한원 이미지 복원

4.3 안전도

제안한 알고리즘의 RSA의 안전도는 메시지(watermark key) 크기에 따라 지수적으로 높아지는 특성이 있다. 본 논문에서는 서로 이웃하는 매크로 블록에 삽입할 워터마크 키를 적당한 수(K)로 묶어 하나의 비트열로 만들어 watermark key를 생성하고, 다시, 생성된 워터마크 키를 하나의 비트열로 잘라 각 해당 위치에 삽입시킴으로써 안전도와 처리속도를 고려하였다.

5. 실험 및 결과

본 논문에서 제안한 웨이블릿에 사용된 영상은 MPEG-4의 영상 중 I 프레임으로 크기는 352 x 240이며, 4레벨 웨이블릿 변환과 RSA 공용키 암호시스템을 적용하여 워터마크 키를 삽입하는 실험을 하였다.

제안한 알고리즘에서는 4레벨의 웨이블릿 분해와 양자화로 얻은 이미지에 RSA 공용키 암호시스템을 이용해 워터마크 키를 삽입한 이미지를 압축, 전송하고 수신측에서는 개인키의 소유 유무에 따라 출력 이미지의 결과를 비교, 분석하였다. (그림 9) (b)는 비밀키 없이 복원한 이미지의 결과이며, (그림 9) (c)는 비밀키가 있는 경우의 결과를 보여주고 있다.

I 프레임은 MPEG동영상에서 가장 중요한 요소이기 때문에 I 프레임에 대해서만 암호화 처리를 하였다. I 프레임은 다른 프레임에 대한 참조 없이 코딩된 프레임으로 스틸영상과 동일하며, P 프레임은 이전의 P또는 I 프레임을 참조하여 macro black의 공간위치 차이를 Motion vector로 Encode되어지며, B 프레임은 이전의 P 프레임과 다음의 P 와 I 프레임을 Encode되어진 것이다. 즉, I, B, P 프레임은 서로 종속적인 관계를 가지고 있기 때문에, 암호화된 I 프레임을 해독하지 못한다면 이어지는 B, P 프레임이 비록 암호화 되지 않았더라도 원하는 영상을 얻지 못하게 된다. 또한, 이미지 전체가 아닌 하나의 RUN파라메터만을 암호화하여 워터마크 키의 수를 조정할 수 있도록 하는 유연성을 제공함으로써 원하는 레벨의 이미지 왜곡을 얻을 수 있도록 하였다.

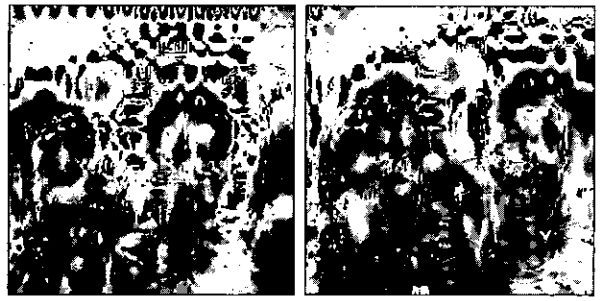
(그림 10)는 MPEG-4영상의 I 프레임의 이미지에 하나의 매크로블럭당 N개의 워터마크 키를 삽입시켜 테스트한 결과이다. 결과에서 볼 수 있듯이 이미지의 왜곡뿐만 아니라 위치에도 영향을 주는 것을 볼 수 있는데, 이것은 RUN 계

(a) 원 이미지

(b) 개인키가 없는 경우 (c) 개인키가 있는 경우

(그림 9) 이미지 복원

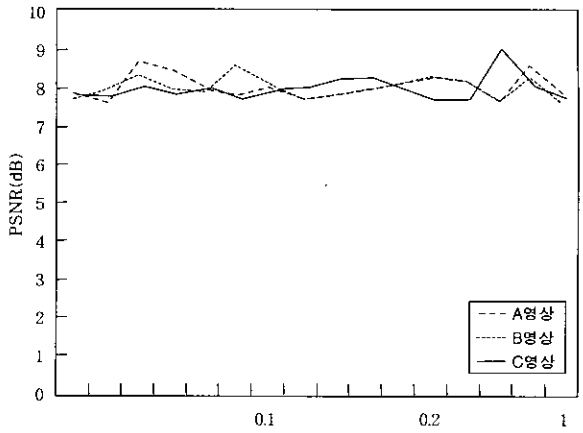
(a) N = 1 인 이미지 (b) N = 1/2 인 이미지



(c) N = 1/4 인 이미지 (d) N = 1/8 인 이미지

(그림 10) 워터마크 키 개수(N)에 따른 이미지 왜곡

수의 또 다른 특성을 보여주는 예이다. 또한, 기존의 DCT 기반의 저주파 계수 암호화 방식보다 적은 수의 워터마크 키를 사용하면서도 더 높은 왜곡을 발생시킬 수 있어 오히려 낮은 결과를 보이고 있다. (그림 11)은 서로 다른 세 개의 영상 A, B, C 영상에 대해 워터마크 수를 변경해 얻은 PSNR값으로써, 공개키를 소유하지 않은 사용자에게는 원 영상이 아닌 손상된 영상만을 제공하게 된다.



매크로 블록당 워터마크 키의 수(N)

(그림 11) 워터마크 처리된 영상의 PSNR

<표 1>은 QCIF(Quarter Common Intermediate Format : 176 x 144)크기의 실제 동영상 200개의 I 프레임을 가지고 실험하여 얻은 평균 PSNR의 결과치를 보여주고 있다.

〈표 1〉 매크로 블록당 워터마크 키의 수에 대한 PSNR

	매크로 블록당 워터마크 키의 수(N)									
	1/10	1/9	1/8	1/7	1/6	1/5	1/4	1/3	1/2	1
PSNR	7.9	8.0	8.0	8.1	8.1	8.3	8.2	8.4	8.7	8.5

5.1 기존 방식과의 비교 분석

기존의 DCT 기반의 워터마크는 DCT 테이블의 저주파 대역에 워터마크를 삽입시키는 방식으로 영상의 번짐 효과를 가져올 수는 있으나 영상을 손상 시키거나 일그러지게 할 수 있는 위상에는 영향을 줄 수 없는 단점을 가지고 있으며, Motion vector 기반의 워터마크는 MPEG 동영상에서의 움직임 벡터에 워터마킹 연산을 함으로써 실제 벡터의 정보가 바뀌게 된다[13]. 현재 복원될 프레임은 전 영상과의 차 영상 그리고 벡터 정보에 의해 복원되며 워터마크가 삽입된 벡터는 영상이 일그러지게 할 수 있지만 모든 매크로 블록의 해당 벡터에 대해 연산이 필요하기 때문에 연산량이 많아진다는 단점을 가지고 있으며, 또한 MPEG로 압축된 동영상 시퀀스에서 움직임 벡터를 갖는 P, B-프레임과는 달리 I-프레임의 경우는 움직임 벡터가 존재하지 않으므로, 움직임 벡터에 워터마크의 키를 삽입하는 이 방법을 I-프레임에 적용하는 것은 불가능하다[13]. <표 2>는 기존 알고리즘과 제안한 알고리즘과의 실험을 통한 비교치를

나타내고 있다.

〈표 2〉 기존 방식과의 비교

	블록킹 현상	위상 변화	매크로 블록당 워터마크키 수(N)
DCT 기반 워터마크	O	X	N ≦ 1
Motion Vector기반 워터마크	-	O	N = 1
제안한 알고리즘	X	O	N ≦ 1

6. 결론 및 향후과제

본 논문에서 제안한 웨이블릿을 이용한 MPEG 동영상 워터마킹 알고리즘은 VLC(RUN)를 공용키를 이용하여 개인키를 소유한 사용자에게만 보여지도록 하였으며 워터마크 키의 수를 줄여 MPEG-4와 같은 동영상의 실시간 전송을할수 있도록 하였다. MPEG 비디오에서 I 프레임은 독립적이고 B, P 프레임은 I 프레임에 종속적이다[16]. 따라서 B, P 프레임에는 워터마크 키를 삽입하지 않고 I 프레임에만 삽입함으로써 암호화 시간을 단축할 수 있었으며, 또한 원하는 정도의 이미지 왜곡을 만들어 내기 위해 워터마크 키의 수를 조정할수 있도록 하였다. 이 알고리즘의 구현으로 공급자는 인가되거나 댓가를 지불한 수요자에게만 개인키를 줌으로써 수요자 층을 넓혀 범용적으로 사용될 수 있으리라 사료되며, 따라서 자신의 재산권을 보호할 수 있을 것으로 기대된다.

향후의 연구과제로는 위의 알고리즘으로 하드웨어를 구현하여 영상회의 시스템과 같은 실시간 전송 시스템이 실용화 되도록 계속적인 연구가 이루어져야 할 것이다.

참 고 문 헌

[1] S. Craver. N. Memon, N. Yeo, and M. Yeung, "Can Invisible Watermarks Resolve Rightful Ownership?" IBM Research Report, RC 20509, July 25, 1996.

[2] Wong, S., "Image security," http : //www.ece.curtin.edu.au/~wongsc/digital.htm, 1997.

[3] Cox I. J., et al., "Secure spread spectrum watermarking for multimedia," NEC Research Institute, Technical Report 95-100, 1995.

[4] Hartung F. and Girod B., "Copyright protection in video delivery networks by watermarking of pre-compressed video," Lecture note in computer science, Vol.1242, pp.423-436, Springer, Heidelberg, 1997.

[5] C. I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," IEEE Journal on Selected Areas in Communications, Vol.16, No.4, pp.525-539, May, 1998.

[6] M. Rao et. al., "Wavelet Transforms," AW, 1998.

[7] D. Kumdur, D. Hatzinakos, "A Robust Digital Image Watermarking Method using Wavelet-Based Fusion," Proceding of ICIP'97, Santa Babara, CA, USA, Oct., 26-29 Vol.I, pp.544-547, 1997.

[8] B. S. Kaliski JR, M.Robshaw, "The secure use of RSA," CriptoBytes, 1(Autumn 1995), pp.7-13.

[9] RSA Data security, "Answer to Frequently Asked Questions About Today's Criptography Ver. 3.0,"

[10] Rafael C. Gonzalez and Richard E. Woods, "Digital Image Processing," Addison Wesley, 1993.

[11] Anil K. Jain. Fundamentals of digital image processing, (Prentice Hall, Inc., 1989)

[12] 표성재, 최창렬, 정제창, "저작권 보호를 위한 디지털 정지영상 워터마킹", 신호처리종합학술대회논문집, 제12권 제1호, pp.261-264, 1999.

[13] 이형훈, 배창석, 최재훈, "MPEG 비디오를 위한 하이브리드 워터마킹 알고리즘", 한국정보처리학회논문지, 제6권 제11호, pp.3157-3164, 1999.

[14] 원치선, "디지털 영상의 저작권 보호", 정보과학회지, 제15권 제12호, pp.22-27, 1997.

[15] 박정빈, 정성환, "이산 웨이블릿 변환을 이용한 칼라 영상 정보 보호 시스템 구현", 한국정보처리학회, 춘계학술발표논문집, 제6권 제1호, pp.1336-1339, 1999.

[16] 이승윤, 유황빈, "대화형 비디오 서비스를 위한 MPEG비디오 기반의 동적 대역폭 관리 기법", 한국정보처리학회논문지, 제6권 제2호, pp.367-376, 1999.

이 학 찬

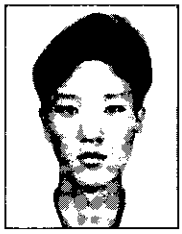
e-mail : war123@hanmail.net

1999년 광운대학교 컴퓨터공학과 졸업 (공학사)

2001년 광운대학교 대학원 컴퓨터공학과 석사졸업

2001년 숭실대학교 대학원 컴퓨터학과 박사과정

관심분야 : 영상처리, MPEG, 신경회로망, 패턴인식, DSP, Watermarking, 암호화, 실시간 처리 등



조 철 훈

e-mail : pangel@hanmail.net

2000년 광운대학교 컴퓨터공학과 졸업 (공학사)

2000년~현재 광운대학교 대학원 컴퓨터공학과 석사과정

관심분야 : 영상처리, MPEG, 신경회로망, wavelet, watermarking 등

송 중 원

e-mail : sjwkw@hanmail.net
1999년 방송통신대학교 전자계산학과 졸업(이학사)
2001년 광운대학교 정보과학기술대학원 지능정보공학과 석사졸업
관심분야 : 영상처리, MPEG, 신경회로망, water-marking 등

남궁 재 찬

e-mail : namjc@daisy.kwangwoon.ac.kr
1970년 인하대학교 전기공학과 졸업(공학사)
1976년 인하대학교 대학원 전자공학과 졸업(공학석사)
1982년 인하대학교 대학원 전자공학과 졸업(공학박사)
1982년~1984년 일본 동북대학 객원교수
1979년~현재 광운대학교 컴퓨터공학과 교수
1989년~현재 정보과학회(전자계산연구회) 전문위원
1991년~현재 전자공학회(전자계산연구회) 전문위원
관심분야 : 영상처리, 신경회로망, MPEG, 문서인식 등