

논문 2006-43CI-5-7

정수 블록 변환을 이용한 디지털 이미지 워터마킹 알고리즘

(Digital Image Watermarking Algorithm using Integer Block Transform)

오 관 정*, 호 요 성**

(Kwan-Jung Oh and Yo-Sung Ho)

요 약

디지털 워터마킹(watermarking) 기법은 디지털 콘텐츠에 워터마크라고 하는 사용자 ID(identification)나 자신만의 정보를 삽입시킴으로써 불법적인 복제를 막고, 지적 재산권 및 저작권을 보호하며, 소유권을 주장할 수 있는 근거를 제시할 수 있도록 하는 기술이다. 일반적으로 주파수 영역에서 워터마크를 삽입하고 검출하는 주파수 영역 워터마킹 알고리즘이 선호된다. 그러나 주파수 영역으로 변환된 값은 정수 값이 아니므로 조작이 쉽지 않고 알고리즘도 현실적으로 많은 제약을 받는다. 본 논문에서는 위와 같은 문제점을 해결하기 위해 정수 블록 변환을 이용하고, 더불어 공간 영역과 변환 영역 모두에서 워터마크를 검출할 수 있는 알고리즘을 제안한다. 본 논문에서 제안한 알고리즘은 블록 단위로 정수 DCT 변환한 후, 변환 영역 블록의 중간 주파수 대역 계수의 특정 비트 평면에 워터마크를 삽입한다. 이는 공간 영역에서는 DEW(differential energy watermarking)로 반영된다. 실험을 통해 제안한 알고리즘이 주파수 영역만을 이용한 방법에 비해 다양한 공격에 강인함을 확인했으며, 비가시성이나 워터마크 삽입 용량 면에서도 우수함을 알 수 있었다.

Abstract

Intellectual property rights are gathering strength these days. Because digital contents are easily reproduced and distributed by advanced computers and networks. Digital watermarking is one of the best solutions for this problem. Generally, frequency-domain watermarking algorithms are preferred since they are more robust than spatial-domain algorithms. However, coefficients in the frequency domain are floating-point numbers. Thus, it is not easy to manipulate those floating-point coefficients and frequency-domain watermarking algorithms have some limitations in their applications. In order to overcome this difficulty, we employ an integer transform in this paper. In addition, our proposed algorithm can extract the watermark from both the spatial and frequency domains. We embed the watermark into a specific bit-plane of mid-frequency coefficients. This is equivalent to the differential energy watermarking (DEW) in the spatial domain. Our simulation results show that the proposed algorithm is imperceptible, good for the watermark payload, and robustness against various attacks. Moreover, it is more efficient than any other algorithm working in only one domain.

Keywords: 워터마킹, 정수 변환, DEW

I. 서 론

컴퓨터와 네트워크의 발달과 함께 디지털 이미지, 음악, 비디오, 문서 등 디지털 콘텐츠의 불법적인 복제나 유통으로 인한 지적재산권 문제가 크게 대두되고 있다.

디지털 콘텐츠의 불법 복제와 유통은 콘텐츠 제작자의 창작 의욕을 상실시키며, 심각한 경제적 손실을 입히므로 불법적인 복제를 막고, 저작권을 효과적으로 보호하기 위한 콘텐츠 보호 기술이 요구되고 있다^[1-2].

이전까지는 암호화 기법이 많이 이용되었지만 이 기법은 암호화되지 않는 상황에서는 의미가 없고, 한번 암호가 풀려 버린 콘텐츠는 보호받을 수 없다. 따라서 디지털 콘텐츠 자체에 워터마크라고 하는 사용자 ID나 자신만의 정보를 삽입시켜 효율적으로 저작권을 보호하는 디지털 워터마킹에 대한 관심이 집중되고 있다^[3-4].

워터마크는 비가시성, 강인성, 보안성 등을 만족해야 하며, 일반적으로 공간적 영역보다는 주파수 영역 알고

* 학생회원, ** 평생회원, 광주과학기술원 정보통신공학과 (Gwangju Institute of Science and Technology, Department of Information and Communications)

※ 본 논문은 광주과학기술원(GIST) 실감방송연구센터(RBRC)를 통한 정보통신부 대학 IT연구센터(ITRC)와 교육인적자원부 두뇌한국21(BK21) 정보기술사업의 지원으로 수행되었다.

접수일자: 2006년2월2일, 수정완료일:2006년9월1일

리즘들이 다양한 공격에 보다 강한 특성을 가진다. 그러나 주파수 영역으로 변환된 값은 정수 값이 아니므로 조작성이 쉽지 않고 알고리즘도 현실적으로 많은 제약을 받는다. 이러한 문제점을 극복하기 위해 웨이블릿이 이용되었으나, 조작 후 공간영역으로 변환시의 잘림 현상을 해결할 수 없었다.

본 논문에서는 위와 같은 문제점을 해결하기 위해 정수 블록 변환을 이용하고, 잘림 현상으로부터 자유로운 조건을 제시한다. 더불어, 공간 영역과 변환 영역 모두에서 워터마크를 검출할 수 있는 알고리즘을 제안한다. 기존의 알고리즘들이 삽입 및 검출 과정이 동일한 영역에서 이루어진 반면에, 본 논문에서 제안한 알고리즘은 워터마크를 주파수 영역에서 비트평면을 이용하여 삽입한 후, 검출 과정에서 공간 영역은 DEW 방법을 이용하고, 주파수 영역은 해당 비트 평면에서 정보를 검출하는 비대칭적인 워터마킹 시스템이다.

본 논문에서는 정수 변환을 이용하여 잘림 현상으로부터 자유로운 비대칭 구조의 워터마킹 알고리즘을 제안한다. 제II장에서 정수 변환, DEW, 제안한 워터마킹 시스템에 대해 설명하고, 제III장에서 제안한 알고리즘의 성능을 평가하기 위한 실험결과를 보인다. 그리고 제IV장에서 본 논문의 결론을 맺는다.

II. 제안한 알고리즘

본 장에서는 정수 블록 변환을 이용하여 주파수 영역 계수의 값이 정수형이 아닌 경우 발생하였던 기존 알고리즘들의 문제점들을 극복하고, 또한 주파수 영역 알고리즘들이 안고 있는 고질적인 문제인 잘림 현상에 대해 아무런 구애도 받지 않으면서 정보를 삽입할 수 있는 워터마킹 시스템을 설명한다.

기존의 알고리즘들이 대부분 동일 영역에서 워터마크의 삽입과 검출이 이루어졌지만, 본 장에서 제안한 알고리즘은 주파수 영역에서 워터마크를 삽입하고 검출은 공간 영역과 주파수 영역 모두에서 이루어질 수 있도록 하여 보다 쉽게 워터마크를 검출할 수 있다.

1. 정수 블록 변환

현재 영상에 이용되는 변환은 DCT, 웨이블릿, KL 변환 등 다양한 종류가 있다. 이러한 변환들은 각각의 정의에 따라 에너지의 압축 효과가 다르다. 디지털 워터마크 분야에서는 이러한 변환들을 이용하여 주파수 영역 워터마킹 알고리즘들을 개발하였다. 그러나 이러

한 변환들은 압축을 목적으로 만들어진 변환들이기 때문에 워터마킹에 이용되었을 경우 여러 가지 문제점들이 발생한다^[5].

대표적인 문제점이 주파수 영역 계수의 형태이다. 이전의 공간 영역 워터마킹의 경우 공간 영역의 계수 값들이 정수형이기 때문에 알고리즘의 개발에 대한 제약이 적고, 계수값에 대한 조작성이 간단하고 쉬웠다. 그러나 주파수 영역의 경우 계수 값이 정수형 아닌 경우가 많아, 알고리즘을 전개하는데 현실적으로 많은 제약이 따른다. 즉, 히스토그램 방법, 비트 평면 조작법, 홀짝법 등 정수형인 경우 사용되었던 많은 알고리즘의 직접적인 적용이 힘들다. 그림 1은 일반적인 주파수 영역 워터마킹 알고리즘의 워터마크 삽입 과정을 보여준다.

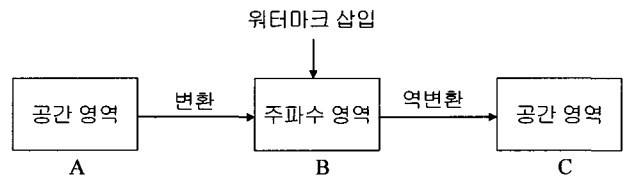


그림 1. 주파수 영역 워터마크 삽입 과정
Fig. 1. Frequency Domain Watermark Embedding.

그림 1에서 보듯이, 워터마크 삽입 과정의 영역은 크게 A, B, C 세 영역으로 나뉜다. 실제 주파수 영역 워터마킹의 경우 워터마크의 삽입과 검출은 B영역에서 이루어진다. 따라서 B 영역의 계수값이 정수형일 경우 알고리즘의 개발 과정에서 보다 많은 이득이 있다. 표 1은 현재 이미지 변환에 많이 사용되는 DCT, 웨이블릿 변환, 정수 변환에 대해 각 영역에서 갖는 계수 값의 형태를 비교한 것이다.

표 1. 각 변환에 대한 A, B, C 계수 값의 형태
Table 1. Coefficient Type in A, B, C for Each Transform.

변환	A	B	C
DCT	정수	소수	정수
웨이블릿	정수	정수	정수
정수	정수	정수	정수

표 1에 보인 것처럼, DCT의 경우 B영역에서 소수형태의 값을 갖지만, 웨이블릿 변환과 정수 변환의 경우 B영역에서 정수 형태의 계수 값을 갖는다. 따라서 웨이블릿 변환이나 정수 변환을 이용했을 경우 주파수 영역 워터마킹 알고리즘을 전개하는데 보다 편리하다.

본 논문에서는 이미지 워터마킹에 정수 변환을 사용했는데, 정수 변환은 블록 변환이기 때문에 워터마크

삽입 용량을 고려하여 4×4 블록 크기를 이용하였다. 식 (1)과 식 (2)는 4×4 정수 변환식과 역변환 식이다^[6].

$$Y = (C_f X C_f^T) \otimes E_f = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 1 & -1 & -2 \\ 1 & -1 & -1 & 1 \\ 1 & -2 & 2 & -1 \end{pmatrix} (X) \begin{pmatrix} 1 & 2 & 1 & 1 \\ 1 & 1 & -1 & -2 \\ 1 & -1 & -1 & 2 \\ 1 & -2 & 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} a^2 & \frac{ab}{2} & a^2 & \frac{ab}{2} \\ \frac{ab}{2} & \frac{b^2}{4} & \frac{ab}{2} & \frac{b^2}{4} \\ a^2 & \frac{ab}{2} & a^2 & \frac{ab}{2} \\ \frac{ab}{2} & \frac{b^2}{4} & \frac{ab}{2} & \frac{b^2}{4} \end{pmatrix} \quad (1)$$

$$X = C_f^T (Y \otimes E_i) C_i = \begin{pmatrix} 1 & 1 & 1 & \frac{1}{2} \\ 1 & \frac{1}{2} & -1 & -1 \\ 1 & -\frac{1}{2} & -1 & 1 \\ 1 & -1 & 1 & -\frac{1}{2} \end{pmatrix} (Y) \otimes \begin{pmatrix} a^2 & ab & a^2 & ab \\ ab & b^2 & ab & b^2 \\ a^2 & ab & a^2 & ab \\ ab & b^2 & ab & b^2 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \frac{1}{2} & -\frac{1}{2} & -1 \\ 1 & -1 & -1 & 1 \\ \frac{1}{2} & -1 & 1 & -\frac{1}{2} \end{pmatrix} \quad (2)$$

where, $a = \frac{1}{2}$, $b = \sqrt{\frac{2}{5}}$, $d = \frac{1}{2}$

위와 같이 정수 변환을 이용하여 주파수 영역에서 조 작이 간편한 정수형 계수 값을 얻을 수 있지만, 주파수 영역 워터마킹 알고리즘들은 공통적으로 역변환 과정에 서 잘림 현상이 생긴다. 즉, 원 이미지는 공간 영역의 값이기 때문에 워터마크를 삽입하기 위해 조작한 뒤에는 반드시 다시 공간 영역으로 되돌려져야 한다. 이 과 정에서 주파수 영역과 공간 영역의 매칭이 완전하게 이 루어지지 않아 값이 잘리는 현상이 발생한다.

그림 2에서 보듯이, 워터마크 검출을 위해서는 워터 마크가 삽입된 영상을 주파수 영역으로 변환해야 하는 데, 삽입 과정 중 공간 영역으로의 역변환 과정 중에 생 긴 잘림 현상으로 인해 검출 과정에서 정확한 값을 얻 어낼 수가 없게 된다. 이 때문에 주파수 영역의 알고리 즘들은 현실적으로 많은 제약을 갖는다.

이를 극복하기 위해 본 논문에서는 잘림 현상으로부터 자유로운 조건을 찾는다. 즉, 주파수 영역에서의 조 작이 공간 영역에서 정수형으로 변할 수 있는 조건을 찾는다. 이를 위해 먼저 주파수 영역과 공간 영역간의 관계에 대해 알아본다.

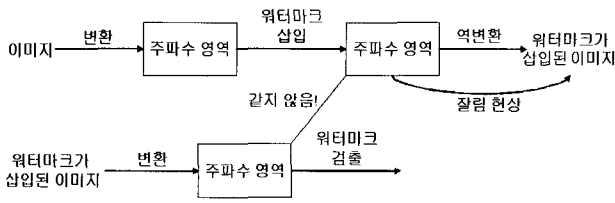


그림 2. 잘림 현상 문제
Fig. 2. Problem of Truncation Error.

$$C_f(i, j) \rightarrow C_f(i, j) \pm 1 \quad (3)$$

식 (3)과 같이 주파수 영역의 특정 계수를 1만큼 증 가시키거나 감소시키면 공간 영역의 계수 값들은 식 (4)와 같이 변화한다. 여기서 첨자 f 는 주파수 영역을 의미한다.

$$\begin{aligned} C_{S1}(i, j) &\rightarrow C_{S1}(i, j) \pm \alpha \\ C_{S2}(i, j) &\rightarrow C_{S2}(i, j) \pm \beta \\ C_{S3}(i, j) &\rightarrow C_{S3}(i, j) \pm \gamma \\ 0 < \alpha, \beta, \gamma < 1 \end{aligned} \quad (4)$$

식 (4)와 같이 각 계수값들은 주파수 계수의 위치에 따라 최대 3가지의 다른 형태로의 변화가 발생한다. 여 기서 첨자 S 는 주파수 영역을 의미한다.

$$m \times \min(\alpha, \beta, \gamma) = 1 \quad (5)$$

이러한 변화를 바탕으로 식 (5)와 같이 세 변화의 값 중 가장 작은 값의 변화가 1을 만족하는 m 값을 구하여 식 (3)과 식 (4)를 식 (6)과 식 (7)로 바꾸어 표현한다.

$$C_f(i, j) \rightarrow C_f(i, j) \pm m \quad (6)$$

$$\begin{aligned} C_{S1}(i, j) &\rightarrow C_{S1}(i, j) \pm m\alpha \\ C_{S2}(i, j) &\rightarrow C_{S2}(i, j) \pm m\beta \\ C_{S3}(i, j) &\rightarrow C_{S3}(i, j) \pm m\gamma \end{aligned} \quad (7)$$

여기서 $m\alpha, m\beta, m\gamma$ 은 모두 정수 값이다. 만약 우리 가 주파수 영역의 계수값을 m 의 배수만큼 변화시키면 공간 영역에서의 변화도 정수로 발생한다. 이러한 m 값 은 주파수 영역 계수의 위치에 따라 다르다. 식 (8)은 주파수의 각 위치에 따른 m 값을 보여주고 있다.

$$\begin{pmatrix} 16 & 40 & 16 & 40 \\ 40 & 100 & 40 & 100 \\ 16 & 40 & 16 & 40 \\ 40 & 100 & 40 & 100 \end{pmatrix} \quad (8)$$

식 (8)에서 보듯이 (1,1), (1,3), (3,1), (3,3)이 그 변화 의 정도가 가장 작아 워터마크 삽입에 적합함을 알 수 있다. 또한 16의 배수는 2^n 의 형태로 표현이 가능하므로 비트 평면 조작법을 통해 워터마크의 삽입이 가능하다. 비트 평면 조작법은 해당 비트평면의 비트를 삽입 하고자 하는 비트로 치환시키는 방법으로 자세한 내용은 제안한 워터마킹 시스템에서 다루도록 하겠다.

2. DEW(differential energy watermarking)

앞 절에서는 잘림 현상으로부터 자유롭고 값의 차이가 가장 작아서 워터마크 삽입에 적당한 4개의 계수를 결정하였다. 이 절에서는 4개의 계수 중 워터마크 삽입에 가장 적합한 하나의 계수를 찾는다.

원래 DEW 알고리즘은 비디오 워터마킹에서 연속하는 블록의 에너지 값이 비슷한 것에 착안하여 화질에 영향이 미비한 고주파 부분의 값을 조작하여 인위적으로 두 블록간의 에너지차를 발생시켜 정보를 삽입하는 방법이었다^[7].

$$|E(A) - E(B)| < T \rightarrow 0 \tag{9}$$

$$|E(A) - E(B)| \geq T \rightarrow 1 \tag{10}$$

식 (9)와 식 (10)에서처럼 두 영역의 에너지 값의 차이를 이용해 워터마크를 삽입한다. 4개의 계수의 위치에 따른 공간 영역에서의 변화는 식 (11)과 같다. δ 는 워터마크의 강도를 나타낸다.

$$\begin{aligned} \delta \times 16 \times \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} &\rightarrow \delta \times \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \\ \delta \times 16 \times \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} &\rightarrow \delta \times \begin{pmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \\ \delta \times 16 \times \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} &\rightarrow \delta \times \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \\ \delta \times 16 \times \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} &\rightarrow \delta \times \begin{pmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \end{aligned} \tag{11}$$

식 (11)의 결과에서 보듯이, (1,1)을 제외한 세 개의 계수들에서 어떤 위치의 계수 값은 증가하고 어떤 위치의 계수 값은 감소하는 것을 알 수 있다. 이를 이용하여 검출 과정에서 DEW 알고리즘을 적용할 수 있다.

(1,1)을 제외한 3개의 계수에 대해 공간 영역에서 값이 증가하는 부분을 A 영역, 감소하는 부분을 B 영역이라 하면, 영상의 특성상 인접한 화소들의 모임인 두 영역의 에너지 값은 대체로 유사한 값을 갖게 된다. 그러나 워터마크 삽입을 통해 조작이 되는 경우 두 영역 중 한 영역의 값이 증가하거나 감소하여 두 영역간의 에너지 차는 커지게 된다. 이를 통해 DEW 알고리즘에 대한 적용이 가능하다.

DEW 알고리즘이 좋은 성능을 내기 위해서는 무엇보다도 정보 삽입에 이용될 두 영역의 에너지 값이 유사해야 한다. 세 계수 중 워터마크 삽입에 적합한 한 계수만을 선택하기 위해 각 계수에 대해 원 영상에서 두 영역의 에너지 값이 얼마나 유사한지를 통해 DEW의 안정성을 검사했다. 이를 위해 8개의 실험 영상에 대해 두 영역의 에너지 차가 10 이하인 경우가 전체에서 차지하는 비율을 조사했다.

표 2. 세 계수에 대한 DEW의 안정성
Table 2. DEW Stability of 3 Coefficients.

실험 영상 (512×512)	DEW의 안정성 (%)		
	(1,3)	(3,1)	(3,3)
Airplane	53.69	52.86	71.30
Baboon	17.29	14.67	22.62
Bacteria	91.14	92.00	99.98
Blood	58.89	48.72	95.42
Lena	49.45	59.92	68.23
Peppers	44.94	46.84	54.85
Sailboat	35.43	32.76	39.33
Tiffany	50.52	56.70	63.82
평균	50.17	50.56	64.44

표 2에서 알 수 있듯이, (3,3)의 경우가 가장 안정적인 성능을 보였다. 따라서 (3,3)을 워터마크 삽입에 이용하도록 한다. 식 (11)의 (3,3)의 경우에서 알 수 있듯이, (3,3)의 경우 공간 영역에서의 변화가 연속적으로 일어나지 않는다. 따라서 DEW 관점에서 보다 안정적인 성능을 보였으며, 실제 워터마크 삽입에서도 조작으로 인한 변화가 연속적으로 일어나지 않기 때문에 (1,3)이나 (3,1)의 경우보다 사람 눈의 관점에서 화질이 더 좋아 보인다.

또한 (3,3)은 4개의 계수 중 중간 주파수 대역에 가장 가까운 특성을 보인다. (1,3)이나 (3,1)의 경우 중간 주파수 대역이긴 하나 블록의 방향성에 크게 구애를 받는 값이다. 따라서 16개의 계수 중 워터마크 삽입에 가장 적합한 계수는 (3,3)이다.

3. 제안한 워터마킹 시스템

지금까지 정수 변환과 DEW를 이용하여 주파수 영역에서 잘림 현상으로부터 자유로우며 공간 영역에서 DEW 알고리즘의 효과를 낼 수 있는 계수를 찾았다. 이 절에서는 본 논문에서 제안하는 워터마킹 시스템의 특징인 비대칭 워터마킹 시스템에 대해 살펴보고, 이전 결과를 바탕으로 하여 실제 워터마크의 삽입 및 검출 과정에 대해 자세히 알아본다.

가. 비대칭 워터마킹 시스템

이전의 워터마킹 시스템들은 대부분 워터마크의 삽입과 검출이 동일한 영역에서 이루어졌다. 이를 바탕으로 워터마킹 알고리즘들은 공간 영역 워터마킹과 주파수 영역 워터마킹으로 구분된다. 이렇게 워터마크 삽입과 검출을 동일한 영역에서 할 수 밖에 없었던 이유는 변환의 특성상 한 영역에서의 변화는 다른 영역의 전체에 영향을 미치기 때문이었다.

그러나 본 논문에서 제안하는 알고리즘은 이러한 특징을 고려하여 주파수 영역의 조작을 공간 영역에서 DEW 알고리즘으로 적용시켜, 검출 과정에서 주파수 영역뿐만 아니라 공간 영역에서도 워터마크를 검출할 수 있는 시스템을 제안한다. 이러한 비대칭 워터마킹 시스템은 워터마크가 삽입된 영상이 공격을 받은 경우 한쪽 영역만을 이용한 경우와 비교하여 보다 좋은 성능의 워터마크를 검출할 수 있다.

나. 워터마크 삽입

워터마크 삽입 과정은 그림 3에서와 같이 크게 워터마크의 랜덤화 과정과 워터마크 삽입 과정으로 나뉜다.

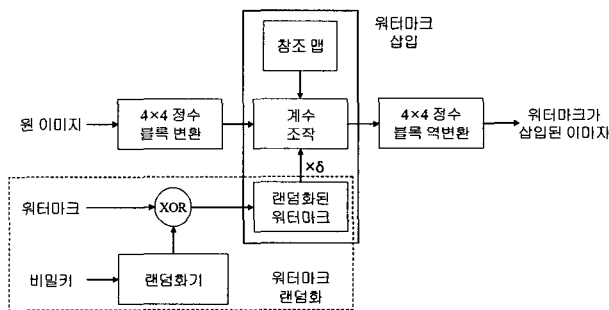


그림 3. 워터마크 삽입 과정
Fig. 3. Watermark Embedding Process.

그림 3을 바탕으로 한 실제 워터마크의 삽입 과정은 다음과 같다.

1. 랜덤화기를 통해 워터마크를 랜덤화시킨다.

$$W_R = W_O \oplus R$$

랜덤화된 워터마크 W_R 은 원 워터마크 W_O 와 비밀키를 통해 랜덤화기에서 발생된 랜덤 비트 R 을 XOR한 것이다. 이를 통해 워터마크에 대한 보안성을 보장할 수 있다.

2. 참조맵을 만든다. 참조맵은 워터마크 삽입 과정에서 삽입되는 워터마크의 위치를 다시 한번 섞어주는 역할을 한다. 즉, 랜덤화된 워터마크를 1, 2, 3, 4,... 의 순서로 읽어서 삽입하는 게 아니라, 5, 47, 12, 1... 의 순서처럼 랜덤하게 삽입하도록 해 준다. 따라서 삽입되는 워터마크의 지역적인 특성을 랜덤화시켜 잘림과 같은 공격에 강인한 특성을 갖는다.
3. 4x4 블록 변환을 수행한다.
4. 블록의 (3,3) 계수의 해당 비트 평면 값($B(3,3)$)과 삽입하고자 하는 비트를 비교하여 조작한다.
삽입할 비트와 비트 평면의 값이 같은 경우
 $\rightarrow B(3,3) = B(3,3)$
삽입할 비트와 비트 평면의 값이 다른 경우
 $\rightarrow B(3,3) = B(3,3) \pm 16 \times 2^{\delta-1}$
5. 각 블록에 대해 역변환을 수행하여 공간 영역으로 되돌린다.

다. 워터마크 검출

그림 4는 워터마크의 검출 과정을 보여준다.

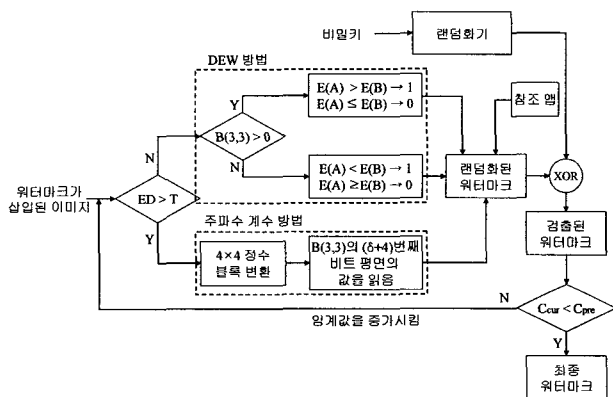


그림 4. 워터마크 검출 과정
Fig. 4. Watermark Extraction Process.

그림 4를 바탕으로 한 워터마크의 검출 과정은 다음과 같다.

1. 블록의 A영역과 B영역의 에너지 차이를 계산한다.
 $|E(A) - E(B)| > T \rightarrow$ 주파수 계수 방법
 $|E(A) - E(B)| \leq T \rightarrow$ DEW 방법

2. 아래의 두 가지 방법을 이용하여 랜덤화된 워터마크를 검출한다.
 DEW 방법
 $E(A) > E(B) \rightarrow 1$ 을 검출
 $E(A) \leq E(B) \rightarrow 0$ 을 검출
 주파수 계수 방법
 (3,3)계수의 $(\delta+4)$ 값이 1 \rightarrow 1을 검출
 (3,3)계수의 $(\delta+4)$ 값이 0 \rightarrow 0을 검출

3. 랜덤화기와 참조맵을 이용하여 워터마크 검출한다.

4. 원 워터마크의 상관도를 계산한다. 이를 통해 보다 성능이 좋은 워터마크를 검출할 수 있다.
 $C_{cur} \geq C_{pre} \rightarrow$ 임계값을 증가 시킨다.
 $C_{cur} < C_{pre} \rightarrow$ 최종 워터마크를 검출한다.
 C_{cur} 과 C_{pre} 는 현재 임계값과 이전 임계값에 대한 상관도를 의미한다. 상관도는 검출된 워터마크와 원 워터마크의 유사도를 이용하였다. 일반적으로 임계값에 따른 유사도 함수가 블록 함수의 형태를 갖기 때문에 위와 같은 식을 통해서 유사도가 가장 높은 임계값을 찾아낼 수 있다.

III. 실험 및 분석

본 논문에서 제안한 정수 변환을 이용한 이미지 워터마킹 알고리즘의 성능을 평가하기 위해 512×512 크기의 8개의 흑백 영상에 대해 비가시성, 워터마크 삽입용량, 다양한 공격에 대한 강인성에 대해 실험하였다. 또한 비대칭 워터마킹 시스템의 성능 실험을 위해 DEW를 고려하지 않은 경우와 비교하였다. 그림 5는 본 실험에 워터마크로 이용된 200×80 크기의 이진 영상이며, 이는 16,000 비트에 해당된다^[8].



그림 5. 200×80 크기의 이진 로고 영상
 Fig. 5. Binary Logo Image of 200×80 Pixels.

1. 비가시성

비가시성은 워터마크 삽입으로 인한 변화의 정도를 의미한다. 기본적으로 워터마킹 알고리즘은 워터마크 삽입 후에도 원본과의 차이가 거의 없어야 하며, 워터마크의 삽입 여부를 쉽게 감지할 수 없어야 한다. 즉,

컨텐츠의 품질을 저하시키지 않는 범위 내에서 워터마크를 삽입해야 한다. 응용되는 목적에 따라 가시적인 워터마킹을 이용하는 경우도 있으나, 일반적인 경우의 워터마킹은 비가시적인 워터마킹을 말한다.

이미지 워터마킹의 경우 비가시성은 흔히 PSNR 값을 통해 평가되는데, 이는 식 (12)와 같이 정의된다.

$$PSNR(dB) = 10 \log \left(\frac{255^2}{MSE} \right) \tag{12}$$

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (W(i,j) - O(i,j))^2$$

여기서 W 는 워터마크가 삽입된 영상을, O 는 원 영상을 나타낸다. 본 논문에서 제안한 알고리즘의 경우 PSNR 값은 워터마크의 강도(δ)에 크게 영향을 받는다. 워터마크의 강도를 크게 하면 영상의 왜곡이 커져서 화질은 나빠지지만, 워터마크를 보다 쉽게 검출할 수 있다. 본 논문에서 제안한 워터마크 알고리즘의 PSNR 하한값은 식 (13)과 같다.

$$PSNR \text{ 하한값} = 10 \log \left(\frac{255^2}{\delta} \right) \tag{13}$$

여기서 δ 는 워터마크의 강도를 나타낸다.

표 3은 각 영상에 대해 워터마크의 강도에 따른 PSNR 값을 보여준다. 표 3에서 알 수 있듯이, 영상에 관계없이 워터마크의 강도에 의존하는 값을 보였다. 이는 영상의 특성에 관계없이 안정적인 화질을 보장한다는 의미이다. 그림 6은 워터마크의 강도가 3인 경우의 Lena 영상의 원 영상과 워터마크가 삽입된 영상을 보여주고 있다.

그림 6에서 보듯이, 원 영상과 워터마크가 삽입된 영상의 화질의 차이는 눈으로 확인하기 힘들다. 워터마크가 삽입된 영상에 대한 화질의 열화는 식 (13)에서처럼 삽입되는 워터마크의 강도에 의존한다.

표 3. 워터마크가 삽입된 경우의 PSNR 값
 Table 3. PSNR of Watermarked Images.

실험 영상 (512×512)	PSNR (dB)		
	$\delta = 1$	$\delta = 2$	$\delta = 3$
Airplane	51.23	45.19	39.14
Baboon	51.15	45.13	39.13
Bacteria	51.20	45.19	39.17
Blood	51.19	45.18	39.16
Lena	51.22	45.21	39.17
Peppers	51.23	45.16	39.16
Sailboat	51.21	45.17	37.14
Tiffany	51.18	45.19	39.17



그림 6. 원 영상(상), 워터마크가 삽입된 영상(하)
Fig. 6. Original Image(T), Watermarked Image(B).

2. 워터마크 삽입 용량

워터마크 삽입 용량은 보통 크게 중요한 요소는 아니지만, 워터마킹 알고리즘들의 성능을 비교하는 하나의 척도로 사용될 수 있다. 본 논문에서 제안한 알고리즘은 4x4 블록 기반이기 때문에 워터마크의 삽입 용량은 영상의 크기에 상당히 좌우된다.

$$\text{삽입 용량} = (M/4) \times (N/4) \tag{14}$$

여기서 M과 N은 원 영상의 가로와 세로의 화소수다.

3. 다양한 공격에 대한 강인성

워터마킹 알고리즘에 요구되는 조건 중 가장 중요한 것이 바로 공격에 대한 강인성이다. 강인성이란 워터마크가 삽입된 영상이 공격을 받더라도 그 공격을 받은 영상에서도 워터마크를 검출할 수 있는 능력을 말한다.

워터마크를 삽입하는 사람들은 저작권 보호나 복제 방지 등을 목적으로 콘텐츠에 워터마크를 삽입하지만, 워터마크가 삽입된 콘텐츠를 다시 불법적으로 이용하려는 공격자들은 워터마크가 삽입된 영상에 다양한 영상 처리를 수행하여 워터마크를 제대로 검출할 수 없도록 한다. 따라서 워터마크 알고리즘은 가급적 다양한 공격에 강인해야 하지만, 모든 공격에 강인한 알고리즘을 만들기는 매우 어렵다.

본 실험에서는 잡음 추가, 잘림, 저대역 필터링, 고대역 필터링, JPEG 압축과 같은 일반적인 공격에 대해 제안한 알고리즘의 강인성을 실험했고, 강인성의 정도를 원 워터마크와의 유사도를 이용하여 측정하였다.

가. 잡음 추가

잡음의 추가는 가장 흔한 공격 중의 하나인데, 워터마크가 삽입된 영상의 전 영역에 임의로 잡음을 추가하여 영상에 삽입된 워터마크의 검출을 방해하는 공격이다. 잡음 추가에 대한 제안한 알고리즘의 강인성의 정도는 표 4와 같다. 본 실험에서는 워터마크가 삽입된 영상에 대해 일반적인 균일 잡음을 1%, 3%, 5% 추가한 후 잡음이 삽입된 영상에서 검출된 워터마크와 원 워터마크와의 유사도를 측정하였다.

표 4. 잡음 추가에 대한 강인성
Table 4. Robustness against Noise Addition.

실험 영상 (512x512)	δ = 1			δ = 2			δ = 3		
	1 %	3 %	5 %	1 %	3 %	5 %	1 %	3 %	5 %
Airplane	74.70	55.78	51.29	90.61	72.57	61.65	97.98	91.39	80.61
Baboon	57.39	51.10	50.51	70.47	61.14	55.29	85.37	78.58	71.92
Bacteria	78.32	56.28	51.13	96.34	71.65	61.19	100	92.81	79.03
Blood	78.72	58.31	52.12	95.78	73.34	61.99	99.93	92.13	79.39
Lena	73.15	56.54	52.16	90.94	72.41	61.61	98.25	91.16	79.99
Peppers	68.68	53.46	52.05	88.78	72.36	62.43	98.33	90.94	80.27
Sailboat	63.45	53.63	50.95	81.94	67.66	59.60	95.56	88.04	79.93
Tiffany	72.28	55.91	50.63	83.88	68.69	57.96	97.13	89.96	80.59
평균	70.84	55.13	51.36	87.34	69.98	60.22	96.57	89.38	78.97

표 4에서 보듯이, 워터마크의 강도가 클수록 잡음 공격에 더 강함을 알 수 있다. 또한 실험 영상의 특성에 따라 워터마크 검출율의 차이가 크게 나는데, 이는 영상의 공간적인 복잡도에 따라 DEW의 안정성이 차이가 나기 때문이다.

그림 7은 워터마크의 강도가 3인 경우의 워터마크가 삽입된 Peppers 영상과 이에 5% 잡음을 추가한 경우의 영상과 그때 검출된 워터마크를 보여주고 있다. 표 4와 그림 7에서 알 수 있듯이, 워터마크의 강도에 따라 가시적인 워터마크를 검출할 수 있었다.

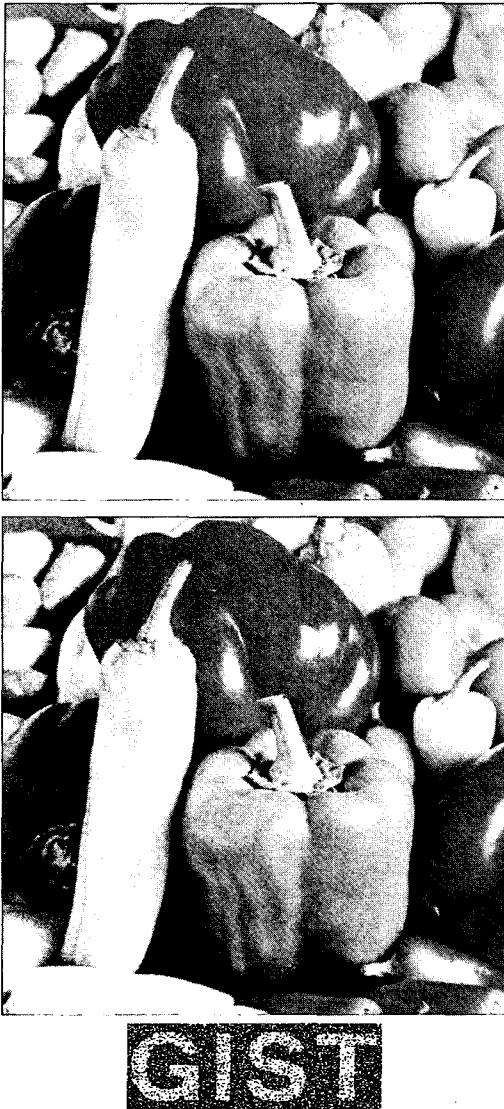


그림 7. 워터마크가 삽입된 영상(상), 잡음이 추가된 영상(중), 검출된 워터마크(하)
 Fig. 7. Watermarked Image(T), Noisy Watermarked Image(M), Extracted Watermark(B).

나. 영상 잘림

영상 잘림은 워터마크의 강도에 영향을 받지 않는다. 영상 잘림에 대한 강인성은 참조 맵에 의해 보장된다. 참조맵을 사용하지 않으면 영상의 윗부분이 잘려나가면 검출된 워터마크도 윗부분이 잘리게 된다. 그러나 참조맵을 이용하면 이 영향을 전체에 분산시키는 효과가 있다. 영상 잘림에 대한 강인성의 결과를 표 5에 보였다.

표 5. 영상 잘림에 대한 강인성
 Table 5. Robustness against Image Clipping.

	12.5 %	25 %	50 %	75 %
Airplane	92.92	86.18	73.06	61.91



그림 8. 잘림 공격 후 영상(상)과 추출 워터마크(하)
 Fig. 8. Clipped Image(T) and Extracted Watermark(B).

표 5에서 보듯이, 심지어 영상의 75%가 잘려나가도 61.91%의 워터마크 검출율을 보였다. 그림 8은 Airplane 영상이 50%의 잘림 공격을 받은 경우와 그때 검출된 워터마크를 보여주고 있다.

다. 저대역 필터링

저대역 필터링은 영상의 저주파 대역의 값을 취하고 고주파 성분은 버리는 동작이므로 영상을 자세히 나타낼 수 없다. 그림 9에 보인 것처럼, 저대역 필터링 공격을 받은 영상은 원래 영상에 비해 흐려진다.

표 6. 저대역 필터링에 대한 강인성
 Table 6. Robustness against LPF.

실험 영상 (512×512)	저대역 필터링에 대한 검출율 (%)		
	$\delta = 1$	$\delta = 2$	$\delta = 3$
Airplane	61.54	73.64	85.69
Baboon	50.83	55.15	64.33
Bacteria	72.12	82.08	95.99
Blood	69.09	82.84	94.72
Lena	60.96	74.89	87.10
Peppers	56.33	71.93	86.19
Sailboat	53.67	63.05	77.18
Tiffany	59.75	72.80	85.73
평균	60.54	72.05	84.62

표 6에 보인 것처럼, 워터마크의 강도에 따라 저대역 필터링에 대한 강인성도 커짐을 알 수 있다. 그림 9는 워터마크의 강도가 2인 경우의 Airplane 영상과 저대역 필터링 공격을 받은 후의 영상, 그때 검출된 워터마크를 보여준다. 그림 9와 같이 저대역 필터링된 영상에서도 가시적인 워터마크를 검출할 수 있었다.



그림 9. 워터마크가 삽입된 영상(상), 저대역 필터링된 영상(중), 검출된 워터마크(하)
 Fig. 9. Watermarked Image(T), LPFed Watermarked Image(M), Extracted Watermark(B).

라. 고대역 필터링

고대역 필터링은 영상의 고주파 성분을 강조하여 영상을 선명하게 하는 영상처리로 고주파 부분에 대한 변화를 주어 고주파 영역에 삽입된 워터마크를 공격한다. 고대역 필터링에 대한 강인성은, 표 7에 보인 것처럼, 워터마크의 강도에 따라 커짐을 알 수 있다. 그림 10은 워터마크의 강도가 2인 경우의 Tiffany 영상, 고대역 필터링 공격을 받은 후의 영상과 그때 검출된 워터마크를 보여주고 있다.

표 7. 고대역 필터링에 대한 강인성
 Table 7. Robustness against HPF.

실험 영상 (512×512)	고대역 필터링에 대한 검출율 (%)		
	$\delta = 1$	$\delta = 2$	$\delta = 3$
Airplane	74.86	87.01	94.09
Baboon	56.57	63.86	70.29
Bacteria	99.16	99.99	100
Blood	88.51	97.96	99.91
Lena	73.52	86.00	94.68
Peppers	68.88	80.61	91.14
Sailboat	63.89	74.10	82.98
Tiffany	72.25	82.20	91.94
평균	74.71	83.97	90.63



그림 10. 워터마크가 삽입된 영상(상), 고대역 필터링된 영상(중), 검출된 워터마크(하)
 Fig. 10. Watermarked Image(T), HPFed Watermarked Image(M), Extracted Watermark(B).

마. JPEG 압축

JPEG 표준은 정지영상의 용량을 줄이기 위해 흔히 사용되는데, 이는 사람의 눈에 덜 민감한 부분에 대한 정보를 줄이는 손실 압축 방식이다. 표 8은 압축비가 3.5:1인 JPEG 압축에 대한 강인성을 보여주고 있다.

표 8. JPEG 압축에 대한 강인성
Table 8. Robustness against the JPEG.

실험 영상 (512×512)	JPEG 압축에 대한 검출율 (%)		
	$\delta = 1$	$\delta = 2$	$\delta = 3$
Airplane	55.64	69.99	89.34
Baboon	51.15	61.73	78.57
Bacteria	53.13	67.30	87.59
Blood	58.19	67.66	89.79
Lena	55.38	69.14	89.17
Peppers	53.34	69.41	90.06
Sailboat	51.94	66.29	87.71
Tiffany	55.73	70.04	89.20
평균	54.31	67.70	87.68

표 8에서 보듯이, 일반적인 JPEG 압축에 대해서도 워터마크의 강도에 따라 비교적 강인함을 보였다.

4. 비대칭 워터마킹 시스템의 성능

본 논문에서 제안한 대칭 워터마크 시스템의 성능 평가를 위해 공간 영역의 DEW 알고리즘을 고려한 경우와 그렇지 않은 경우에 대한 각 공격에 대한 워터마크의 검출율을 비교했다. 표 9에서 보듯이, DEW를 이용한 경우가 그렇지 않은 경우보다 좋은 성능을 보임을 알 수 있다.

표 9. DEW를 사용한 경우와 사용하지 않은 경우의 다양한 공격에 대한 성능 비교

Table 9. Robustness Comparison between with DEW and without DEW.

공격	DEW 이용하지 않음	DEW 이용
잡음 추가	66.32	69.98
잘림	85.37	87.41
저대역 필터링	49.50	72.05
고대역 필터링	70.96	83.97
JPEG 압축	60.32	67.70

IV. 결 론

본 논문에서는 정수 변환을 이용한 이미지 워터마킹 알고리즘을 제안하였다. 제안한 알고리즘은 정수 변환을 통해 주파수 영역에서 잘림 현상으로부터 자유롭고

조작이 간편한 정수값을 이용할 수 있다. 또한 주파수 영역의 조작이 공간 영역에서는 DEW로 반영되어 검출 과정에서 두 영역을 모두 고려하는 비대칭 워터마킹 시스템이므로, 대칭 워터마킹 시스템에 비해 검출이 용이하며 성능을 향상시킬 수 있다. 컴퓨터 실험을 통해 제안된 알고리즘이 비가시성과 워터마크 삽입 용량 면에서 안정적으로 우수함을 보였고, 잡음 추가, 영상 잘림, 저대역 필터링, 고대역 필터링, JPEG 압축과 같은 공격에도 비교적 우수함을 확인할 수 있었다.

참 고 문 헌

- [1] G.C. Langelaar, I. Setyawan, and R.L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 20-46, Sept. 2000.
- [2] I. J. Cox, M. L. Miller, and J. A. Bloom, "Digital Watermarking," Morgan Kaufmann Publishers, 2002.
- [3] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," *Int. Conf. on Image Processing*, vol. 2, pp. 86-90, 1994.
- [4] S. Katzenbeisser and F. A. P. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking," Artech House, 2000.
- [5] A. G. Bors and I. Pitas, "Image watermarking using DCT domain constraints," *IEEE Int. Conf. on Image Processing*, 1996.
- [6] L. E. G. Richardson, "H.264 and MPEG-4 Video Compression," Wiley, 2003.
- [7] G. C. Langelaar and R. L. Lagendijk, "Optimal differential energy watermarking of DCT encoded images and video," *IEEE Transactions on Image Processing*, vol. 10, no. 1, Jan. 2001.
- [8] M. Kutter and F. A. P. Petitcolas, "Fair benchmarking for image watermarking systems," *Proceedings of SPIE 3657, Security and Watermarking of Multimedia Contents*, pp. 226-239, 1999.

저 자 소 개



오 관 정(학생회원)
 2002년 8월 전남대학교 정보통신
 공학과 졸업(학사).
 2005년 2월 광주과학기술원 정보
 통신공학과 졸업(석사).
 2005년 3월~현재 광주과학기술원
 정보통신공학과 박사과정.

<주관심분야: 다시점 비디오 부호화 (MVC),
 H.264, 워터마킹, 영상신호 처리 및 압축>



호 요 성(평생회원)
 1981년 2월 서울대학교
 전자공학과 졸업(학사).
 1983년 2월 서울대학교 대학원
 전자공학과 졸업(석사).
 1983년 3월~1995년 9월 한국전자
 통신연구원 선임연구원.

1989년 12월 미국 University of California, Santa
 Barbara Department of Electrical and
 Computer Engineering(박사),
 1990년 1월~1993년 5월 미국 Philips 연구소
 Senior Research Member.
 1995년 9월~현재 광주과학기술원 정보통신
 공학과 교수.

<주관심분야: 디지털 신호처리, 영상신호 처리 및
 압축, 초저속 영상통신, 디지털 TV와 고선명 TV,
 MPEG 표준, 다시점 비디오 부호화, 실감방송>