

하다마드 도메인에서의 손실압축에 강인한 워터마킹

Robust Watermarking against Lossy Compression in Hadamard Domain

최 학 남* 김 중 원** 이 덕*** 최 중 욱****
Xue-Nan Cui Jong-Weon Kim Li De Jong-Uk Choi

요 약

본 논문에서는 하다마드 변환을 이용하여 워터마크 정보를 삽입 및 추출하는 손실압축에 강인한 워터마킹 방법을 제안한다. 하다마드 행렬은 1과 -1로 구성된 행렬이므로 계산이 빠르고 또한 역변환이 가능한 행렬이므로 워터마크 구현에 사용 가능하다. 워터마크 삽입과정에서, 워터마크는 하다마드 계수중의 중간 주파수 계수 10개를 선택하여 워터마크 패턴을 이용하여 삽입하였다. 워터마크 추출과정에서는, 삽입 시 사용했던 워터마크 패턴을 이용하여 비교하는 방법을 사용하여 워터마크 정보를 추출하였다. 실험결과, 하다마드 도메인에서 4096비트의 이진 로고영상을 삽입하였을 때 PSNR(Peak Signal To Noise Rate)이 36-46dB사이에서 BER(Bit Error Rate)이 3.9-12.5%에 달하는 성능을 나타내었고 JPEG 압축에 대해서는 QF(Quality Factor)가 30에서부터 육안으로 구분할 수 있을 정도의 로고를 추출해 낼 수 있었다. 본 논문에서는 하다마드 도메인에서의 성능을 증명하기 위하여 DCT, FFT, DWT등과 비교하여 실험한 결과 하다마드 도메인에서 가장 좋은 성능을 나타냄을 알 수 있었다.

Abstract

In this paper, we proposes a robust watermarking against the lossy compression in the Hadamard domain. The Hadamard matrix consists of only 1 or -1 and can be computed very fast. The Hadamard transform has the inverse transform therefore it is able to be applied into the watermarking technology. In embedding process, we select 10 coefficients from intermediate frequency domain and create two watermark patterns. In extraction process, we use the watermark patterns and compare them to detect the watermark information. When we use the standard image (512x512) and binary watermark image (64x64), the results of these examines are PSNR for 38-42dB and BER for 3.9-12.5%. The JPEG QF between 30 and 100, naked human eyes can detect to watermark image easily. The experimental results show that performance of Hadamard domain is better than those of DCT, FFT, and DWT.

Key word : Hadamard, reversible, watermarking, jpeg, shift

서 론

최근 들어 콘텐츠의 불법 사용, 저작권침해 방지 등을 위한 많은 기술들이 개발되고 있는데 그중에서 대표적인 기술들로는 워터마킹, 핑거프

린팅이 있다. 워터마킹 기술은 저작권자의 정보를 콘텐츠에 삽입하여 콘텐츠의 저작권을 주장하는 기술이고 핑거프린팅 기술은 사용자의 정보를 콘텐츠에 삽입하여 콘텐츠의 불법유통을 방지하는 기술로써 삽입하는 정보의 차이에 의해 다를 뿐 기술상에서는 거의 비슷하게 처리된다.

인터넷 사이트는 대부분 전송효율을 높이고 저장량을 줄이기 위해서 압축 이미지들을 사용한다. 이미지를 압축하게 되면 삽입되었던 워터마크가 손상될 수 있다. 때문에 이러한 압축에 강인한 워터마크 알고리즘을 개발하여야 한다. 물론 이미지에 대한 공격이 압축만 존재하는 것이 아니다. 기

* 준 회 원 : 인하대학교 정보통신공학과 박사과정
xncui@vision.inha.ac.kr

** 정 회 원 : 상명대학교 디지털저작권보호연구센터
전임연구교수 jwkim@smu.ac.kr

*** 정 회 원 : 상명대학교 디지털저작권보호연구센터
전임연구교수 lide@smu.ac.kr

**** 정 회 원 : 상명대학교 소프트웨어대학 교수
juchoi@smu.ac.kr

[2006/10/09 투고 - 2006/10/11 심사 - 2007/02/27 심사완료]

하학적 공격이라든가 신호처리 공격도 존재한다. 본 논문에서는 손실압축 공격에 대한 부분만 다룬다. 기존에는 워터마크를 Spatial 영역이나, DCT, FFT, DWT를 한 주파수 영역에 많이 사용하였다. Spatial 영역에 워터마크를 삽입하면 쉽게 깨지는 현상이 나타나기 때문에 강인한 워터마크에서는 주로 DCT (Discrete Cosine Transform)나 FFT(Fast Fourier Transform), DWT(Discrete Wavelet Transform)을 이용하여 영상을 주파수 영역으로 전환시켜서 워터마크정보를 삽입하는 방법을 사용한다. Fei 등이 제안한 알고리즘은 압축에 강인하게끔 설계하였고[6], Kii 등은 패치워크를 이용하여 이미지 크로핑에 강인한 알고리즘을 설계하였고[7], Kang 등은 DWT도메인에 워터마크 정보를 삽입하고, DCT도메인에 템플릿을 삽입하는 방법으로 기하학적 공격과 JPEG 압축에 강인한 워터마크 알고리즘을 제안하였다[8].

워터마크정보는 랜덤함수를 이용하여 생성하는 방법, 로고이미지를 사용하는 방법 주로 두 가지 방식을 사용한다. 랜덤함수를 이용하여 생성된 워터마크정보는 랜덤특성을 가지고 있기에 보편성을 가지고 있고, 로고영상을 워터마크 정보로 추출 시 사람의 육안으로 판단가능하다는 장점이 있다. 본 논문에서는 이 두 가지 장점을 살리기 위해서 로고영상을 랜덤함수에 의해서 랜덤하게 섞은 다음 워터마크정보로 사용하여 삽입하였다. 실험결과 하다마드 도메인에서는 PSNR이 36~46dB사이에서 BER이 3.9~12.5%에 달하였고, JPEG 압축 30에서도 살아남아서 DCT나 FFT, DWT보다 JPEG압축에 더 강인한 것을 알 수 있었다[2~5].

1. 관련 기술

2.1 하다마드 행렬

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (1)$$

하다마드 행렬은 -1과 1로 이루어진 내적의 합이 0이고 즉 직교되고 대칭되는 특징을 가지고 있으며 -1과 1로만 구성되었기 때문에 계산이 빠른 특징을 가지고 있다. [식 1]은 2차원 하다마드 행렬이다. 2차원 하다마드는 모든 행렬의 근원 행렬이 된다. 1차원 하다마드 행렬은 1로 표현할 수 있다. 1은 유일한 홀수차 하다마드 행렬이다. 다음의 [식 2]는 하다마드 확장공식이다[1].

$$H_N = \begin{bmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & -H_{N/2} \end{bmatrix} \quad (2)$$

하다마드 행렬은 근원 행렬인 2차원 하다마드 행렬로부터 시작하여 확장하여 무수히 많은 하다마드 행렬들을 만들어 낼 수 있다.

하다마드 행렬은 실수범위 내에서 존재하며 대칭되며 직교된다. 즉

$$H = H^* = H^T = H^{-1} \quad (3)$$

하다마드 행렬은 1과 -1 두 원소만 포함하고 있기 때문에 곱셈 연산이 필요하지 않기에 계산이 고속으로 처리되고 양호한 에너지집중특성을 가지고 있다.

2.2 하다마드 변환

$$I = HH^T \quad (4)$$

여기서 I는 단위행렬을 가리킨다. 하다마드 변환의 일반 공식은 다음의 [식 5]와 같다. [식 5]에서 I는 원본신호이고 \hat{I} 는 하다마드 변환된 신호이다.

$$\hat{I} = H I H^T \quad (5)$$

하다마드 변환은 역변환이 가능한 변환이다. 역변환은 [식 6]과 같이 표현할 수 있다.

$$I = inv(H) \times \hat{I} \times inv(H^T) \quad (6)$$

여기서 $inv(H)$ 는 HM (Hadamard Matrix)의 차원분의 1을 나타낸다. 즉 4×4 하다마드 행렬로 표시하면 다음과 같다.

$$H_{4 \times 4} = \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{vmatrix} \quad (7)$$

$$inv(H_{4 \times 4}) = \frac{1}{4} \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{vmatrix} \quad (8)$$

2.3 워터마킹의 일반식

압축에 강인한 워터마크 방식은 흔히 스프레드 스펙트럼 방식을 이용하여 구현한다. 이는 1 비트의 워터마크 정보를 표현하기 위하여 8×8 혹은 16×16 혹은 영상 전체만큼 크기의 의사난수를 생성하여 사용하는데 이렇게 하면 일정한 애러들을 보정할 수 있어 강인한 워터마크 구현에 사용된다. 본 논문에서 제안한 알고리즘 역시 스프레드 스펙트럼 방식을 이용하여 구현하였다.

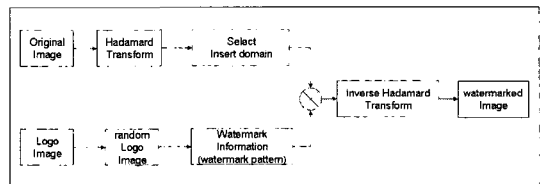
$$I_w(n) = I(n) + \alpha W(n) \quad (9)$$

$$I_w(n) = I(n) + \alpha(n) W(n) \quad (10)$$

[식 9]와 [식 10]에서 $I_w(n)$ 은 워터마크가 삽입된 영상을 나타내고, $I(n)$ 은 원본영상을 나타내고, α 는 삽입강도를 나타내며, $W(n)$ 은 워터마크 정보를 나타낸다. [식 9]은 워터마크 전체에 삽입강도를 줘서 워터마크를 삽입하는 방식이고, [식 10]은 영상의 특성에 따라 삽입영역을 정하고 각각의 삽입영역에서의 삽입강도를 조절하여 워터마크를 삽입하는 방식이다. [식 9]와 [식 10]은 모든 워터마크 삽입이 이 두 식을 통해서 이루어진다고 해도 과언이 아닐 정도로 많이 사용되는 수식이다.

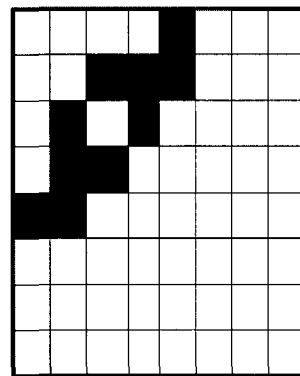
2. 제안 알고리즘

[그림 1]은 전체 삽입과정을 도식한 그림이다. 워터마크 삽입과정을 간략히 설명하면 다음과 같다. 우선 원본영상에 대해 삽입 도메인을 정하고 원본영상을 하다마드 영역으로 변환시킨다. 다음으로 워터마크 정보가 삽입될 삽입영역을 선정하고 하다마드 계수에 워터마크를 삽입하게 된다. 마지막으로 워터마크 삽입된 계수에 역 변환을 적용하면 워터마크가 삽입된 영상을 얻을 수 있다.



(그림 1) 워터마크 삽입

변환 된 각 영역의 8×8 블록에서 10개의 위치를 선택하여 워터마크 삽입 영역을 정한다.



(그림 3) 삽입영역

[그림 2]는 워터마크 패턴이 삽입 될 영역을 나타낸 그림이다. 워터마크 패턴은 하나의 워터마크 정보를 표시하기 위하여 삽입되는 시퀀스이다. 즉 스프레드 스펙트럼과 유사한 방법이다. 워터마크 정보가 0이면 W_{P_0} 이 삽입되고 1이면 W_{P_1} 이

삽입된다. 실제 삽입하게 될 워터마크 패턴은 다음과 같다.

$$W_{P_0} = \{1010101010\}$$

$$W_{P_1} = \{0101010101\}$$

워터마크 패턴은 삽입영역에 다음과 같은 알고리즘에 의해 삽입 되게 된다.

$$Y_i = \text{sign}(X_i)(|X_i| + \alpha W_{P_k}) \quad (11)$$

$$i = 1, 2, \dots, 10, k = 0, 1$$

여기서 α 는 삽입 강도 이고, X_i 와 Y_i 는 각각 원본 삽입계수와 워터마크 된 삽입계수를 나타낸다. 워터마크 된 삽입계수에 역변환을 하게 되면 최종적으로 워터마크 된 영상을 얻는다.

삽입 될 워터마크정보는 이진 로고영상이고 이 이진 로고영상은 랜덤기를 거치게 되는데 이때 Secret key를 이용하여 로고 영상을 뒤섞는다. 이렇게 하면 만일 공격자가 워터마크 추출기를 가지고 있다고 할지라도 key가 없으면 추출된 로고 영상은 무의미한 영상이 되게 된다. 이렇게 생성된 이진 영상은 워터마크 삽입 알고리즘을 통해서 영상의 전 영역에 삽입되게 된다.

다음은 이진 로고영상을 랜덤하게 섞는 방법이다.

```

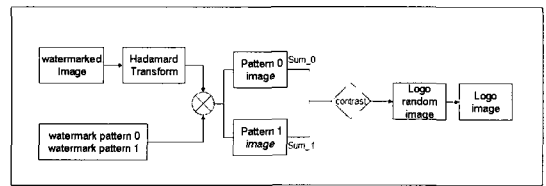
randseed(key);
rand_i = randperm(64);
rand_j = randperm(64);

for i = 1 : 64
    for j = 1 : 64
        m = rand_i(i);
        n = rand_j(j);
        logo_T(i,j) = logo(m,n);
    end
end
    
```

여기서 key는 Secret key를 말하고 randperm은 seed값에 의하여 랜덤하게 섞어주는 함수이다. 여

기서 64값을 준 것은 1부터 64까지의 값을 랜덤하게 섞기 위함이다. logo는 이진 로고영상을 나타내고 logo_T는 변환된 즉 랜덤하게 섞인 이진 로고 영상을 나타낸다.

[그림 3]은 워터마크 추출 과정을 도식화한 그림이다. 워터마크 추출과정에서도 우선 워터마크 영상을 하다마드 영역으로 변환한다. 변환된 하다마드 계수에 각각 삽입 할 때 사용했던 워터마크 패턴을 적용하게 된다.



(그림 4) 워터마크 추출

다음 두 패턴에 의해 계산된 값을 비교하게 된다. W_{P_0} 을 적용했을 때 값이 W_{P_1} 을 적용했을 때와 어떤 차이를 보이는데에 따라서 0이나 1을 판단한다. 수식으로 표현하면 다음과 같다.

$$S_0 = \sum_{i=0}^{10} |Y_i| W_{P_0} \quad (12)$$

$$S_1 = \sum_{i=0}^{10} |Y_i| W_{P_1} \quad (13)$$

```

if S_0 > S_1
    WM = 0;
else
    WM = 1;
    
```

추출된 로고영상은 랜덤하게 뒤섞인 상태로 추출된다. 랜덤하게 섞인 로고영상을 의미 있는 로고영상으로 바꾸기 위해서 삽입할 때와 비슷한 형태의 다음과 같은 처리를 해준다.

```

randseed(key);
rand_i = randperm(64);
rand_j = randperm(64);

for i = 1 : 64
    for j = 1 : 64
        m = rand_i(i);
        n = rand_j(j);
        logo(i,j) = logo_T(m,n);
    end
end
end
    
```

추출된 이진 영상이 랜덤변환기를 거치게 되면 삽입했던 이진 로고영상을 얻을 수 있다.

3. 실험결과

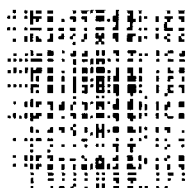
본 논문에서 사용한 원본영상은 512x512 영상이고 삽입 할 이진 로고영상은 64x64 영상이다. 강인성 실험에 사용된 공격은 StirMarkBenchmark 툴을 이용하여 공격하였다. [그림 4]는 원본영상이고, [그림 5]는 삽입될 이진 로고영상이며, [그림 6]은 랜덤기를 거친 이진 로고영상으로써 실제 삽입될 영상이다.



(그림 5) 원본영상



(그림 6) 로고



(그림 7) 랜덤로고

아래의 표들에서 Strength는 삽입강도를 나타내고 PSNR은 영상들 사이의 신호대잡음비를 나타내고, BER(Bit Error Rate)는 원본로고영상과 추출된 로고영상의 비트에러율을 나타낸다.

1) HT Domain인 상에서의 실험

다음은 본 논문에서 제안한 하다마드 영역에서의 실험결과이다. [표 1]은 삽입강도에 따른 실험 결과들을 나타내는 도표이다.

(표 1) 삽입강도에 따른 실험결과

Strength	PSNR(dB)	BER(%)
30	46.95	12.5
40	44.48	10.7
50	42.55	7.70
70	39.62	6.30
100	38.44	4.50
110	36.52	3.90

하다마드 매트릭스 성질로 부터 삽입 강도가 100일지라고 실제 Spatial 영역에서 영상의 픽셀이 변하는 범위는 12 이내라고 볼 수 있다. 왜냐하면 하다마드 역변환을 할 때 inv()연산을 사용하기 때문이다. 아래의 그림에서의 수치는 각각 삽입강도를 나타낸다.



30

40

50



70

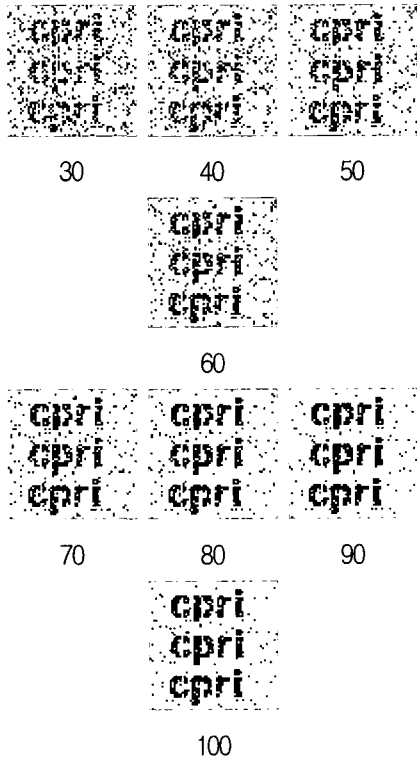
100

110

다음은 삽입강도 100으로 하여 삽입된 워터마크 영상을 JPEG압축 했을 때의 실험결과이다. [표 2]에서 PSNR은 워터마크 영상과 압축된 워터마크 영상의 신호대잡음비를 나타낸다.

(표 2) JPEG 압축에 따른 실험결과(HT)

Quality Factor	PSNR(dB)	BER(%)	Remarks
30	32.16	18	판단가능
40	32.71	17.3	"
50	33.15	16.1	"
60	33.57	14.4	"
70	34.23	10.2	"
80	35.66	5.8	"
90	39.11	4.1	"
100	62.33	4.4	"



위의 그림에서의 수치는 JPEG압축 Quality Factor이고 각각의 그림은 추출된 이진 로고영상

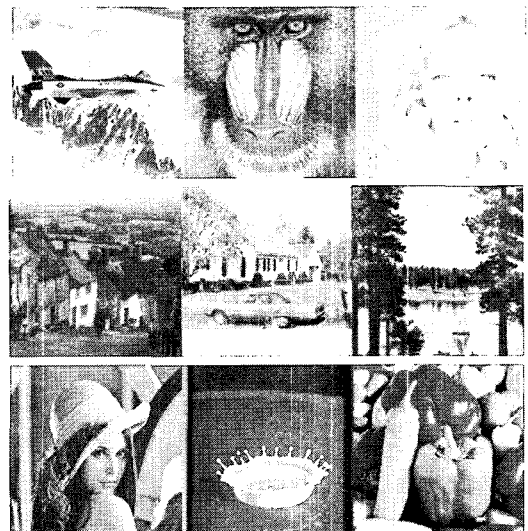
이다. 실험결과 HT Domain에서 삽입강도를 30까지 하였을 때 이진 로고영상이 추출되었고 삽입강도를 100 즉 PSNR이 38.44인 워터마크 영상에 대해 JPEG 압축하였을 때 QF(Quality Factor)가 30에서도 이진 로고영상이 검출되었다.

다음은 워터마크 실험에서 가장 많이 사용하고 있는 표준영상 9가지를 선택하여 실험한 결과이다.

[표 3]은 삽입강도를 60으로 하였을 때 각 원본영상과 워터마크영상의 PSNR과 추출 시 발생하는 BER에 대한 도표이다. Lena영상을 제외한다면 나머지 영상에서도 Lena영상과 JPEG 압축에 대하여 비슷한 결과를 얻을 수 있었다.

(표 3) 9가지 영상에서의 실험결과

Image	Strength	PSNR(dB)	BER(%)
Airplane	60	41.73	10.67
Baboon	"	38.38	13.06
Girl	"	38.47	3.27
Goldhill	"	41.81	16.99
House	"	38.45	14.11
Lake	"	38.39	10.25
Lena	"	41.69	7.67
Milk	"	38.44	3.47
Pepper	"	38.40	6.86

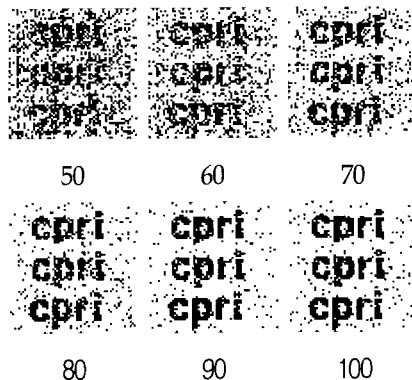


(그림 7) 실험에 사용된 영상들

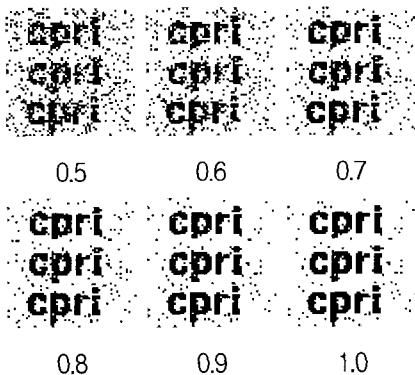
2) DCT Domain인 상에서의 실험

(표 4) 삽입강도에 따른 실험결과 (DCT)

Strength	PSNR(dB)	BER(%)
0.5	42.24	14.4
0.6	40.71	10.1
0.7	39.41	6.80
0.8	38.27	4.70
0.9	37.26	3.20
1.0	36.37	2.50



다음의 영상은 삽입강도에 따른 워터마크 영상들과 추출된 로고영상이다. 수치들은 각각 삽입강도를 나타낸다.



다음은 삽입강도 0.8로 하여 삽입된 워터마크 영상을 JPEG압축 했을 때의 실험결과이다. [표 5]에서의 PSNR은 워터마크 영상과 압축된 워터마크 영상의 신호대잡음비를 나타낸다.

(표 5) JPEG 압축에 따른 실험결과 (DCT)

Quality Factor	PSNR(dB)	BER(%)	Remarks
50	35.43	25.60	판단불가
60	36.16	18.20	판단가능
70	37.12	17.51	"
80	38.39	12.06	"
90	40.76	7.47	"
100	60.57	7.42	"

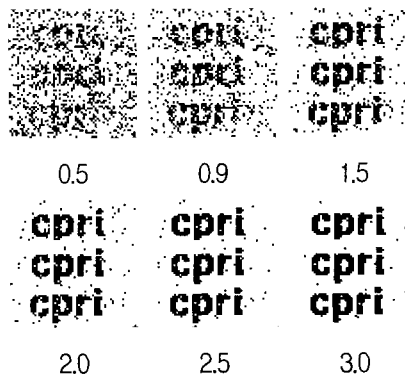
실험결과 DCT Domain에서 삽입강도를 0.5 가지 하였을 때 로고영상이 희미하게 추출되었고 삽입강도를 0.8 즉 PSNR이 38.27인 워터마크 영상에 대해 JPEG 압축하였을 때 QF(Quality factor) 60에서부터 검출이 가능하였다[2][4].

3) FFT Domain인 상에서의 실험

(표 6) 삽입강도에 따른 실험결과 (FFT)

Strength	PSNR(dB)	BER(%)
0.5	50.47	25.00
0.9	45.44	15.00
1.5	41.05	6.00
2	38.58	3.00
2.5	36.68	1.50
3	35.15	0.70

다음은 삽입강도에 따른 워터마크 영상과 추출된 이진 로고영상이다.



다음의 영상은 삽입강도 2.0으로 하여 삽입된 워터마크 영상을 JPEG압축 했을 때의 실험결과이다.

(표 7) JPEG 압축에 따른 실험결과 (FFT)

Quality Factor	PSNR(dB)	BER(%)	Remarks
80	36.58	14.89	판단불가
90	39.59	9.40	판단가능
100	58.43	3.10	"

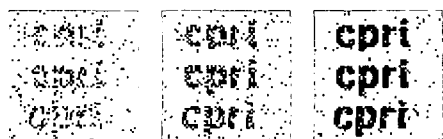


4.5 5.5 6.5

다음의 영상은 삽입강도 5.5로 하여 삽입된 워터마크 영상을 JPEG압축 했을 때의 실험결과이다.

(표 8) JPEG 압축에 따른 실험결과 (DWT)

Quality Factor	PSNR(dB)	BER(%)	Remarks
80	35.98	43.85	판단불가
90	38.50	7.37	판단가능
100	58.45	2.64	"



80 90 100

실험결과 FFT Domain에서 삽입 강도를 0.9 까지 하였을 때 이진 로고영상이 추출되었고 삽입 강도를 2.0 즉 PSNR이 38.58dB인 워터마크 영상에 대해 JPEG 압축하였을 때 QF가 90과 100에서 겨우 검출되었다. FFT Domain에서는 JPEG 압축에 매우 취약함을 알 수 있다.



80 90 100

4) DWT Domain인 상에서의 실험

(표 7) 삽입강도에 따른 실험결과 (DWT)

Strength	PSNR(dB)	BER(%)
1.5	49.42	14.33
2.5	44.86	7.71
3.5	42.00	4.74
4.5	39.87	3.20
5.5	38.15	2.1
6.5	36.64	1.44

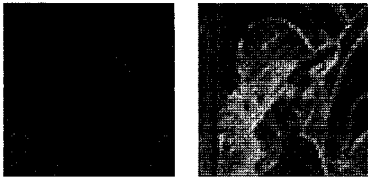
다음은 삽입강도에 따른 워터마크 영상과 추출된 이진 로고영상이다.



1.5 2.5 3.5

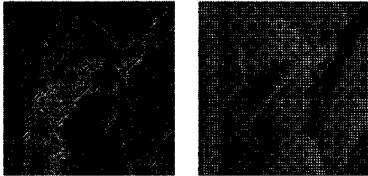
실험결과 DWT Domain에서 삽입 강도를 1.0 까지 하였을 때 이진 로고영상이 추출되었고 삽입 강도를 5.5 즉 PSNR이 38.15dB인 워터마크 영상에 대해 JPEG 압축하였을 때 QF가 90과 100에서 겨우 검출되었다. DWT Domain에서는 공격받지 않은 영상에서는 아주 좋은 성능을 나타내고 있지만 JPEG 압축에 매우 취약함을 알 수 있다.

본 논문에서는 하마다드 영역과 기타 영역에서의 워터마크 실험결과를 비교하기 위하여 같은 삽입알고리즘으로 HT(Hadamard Transform), DCT (Discrete Cosine Transform), FFT(Fast Fourier Transform), DWT(Discrete Wavelet Transform) 변환 영역에 워터마크를 삽입하여 실험을 진행하였다. 다음의 [그림 8], [그림 9], [그림 10], [그림 11]은 Lena영상을 8x8 블록 단위로 각각 DCT, FFT, HT, DWT 변환을 적용한 그림이다.



(그림 8) DCT

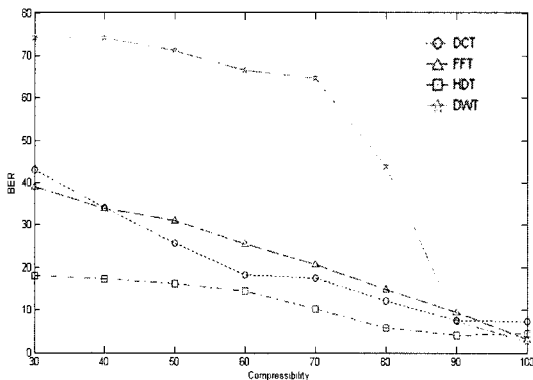
(그림 9) FFT



(그림 10) HT

(그림 11) DWT

[그림 12]는 HT, DCT, FFT, DWT Domain 상에서 JPEG압축을 했을 때의 실험결과를 도식화 그림이다. 그림에서 x축은 압축률을 표시하고 y축은 BER을 나타낸다. 사용된 워터마크 영상은 각 Domain에서 PSNR이 약 38.5인 영상을 선정하여 압축을 진행하였다. 실험결과 대부분 표준영상에서 원본이진 로고영상과 추출된 이진 로고영상의 BER이 20미만일 때 육안으로 판단 가능하였다. 실험결과 HT Domain에서는 QF가 30이상일 경우 모두 검출 가능하였고, DCT Domain에서는 QF가 60이상일 경우 검출이 가능하였으며, FFT Domain과 DWT Domain에서는 QF가 80이상일 경우 검출이 가능하였다.



(그림 12) HT, DCT, FFT, DWT Domain 실험결과 비교

4. 결론

본 논문에서는 하다마드 변환영역에 워터마크를 삽입 및 추출하는 방법을 제안하였다. 워터마크는 정보는 64x64 이진 로고영상을 사용하였고 원본영상은 512x512 크기의 표준영상들을 사용하여 실험을 진행하였다. 공격을 받지 않았을 때 DCT는 PSNR이 36~42사이에서 BER이 2.5~14.4%에 달하였고, FFT는 PSNR이 36~45사이에서 BER이 1.5~15%에 달하였고, DWT는 PSNR이 36.5~50dB 사이에서 BER이 1.5~14.5%에 달하였으며, HT는 PSNR이 36~46 사이에서 3.9~12.5%에 달하였다. 본 논문에서는 HT Domain에서 JPEG 압축에 강인하다는 것을 증명하기 위하여 각 Domain에서의 삽입강도를 조절하여 원본영상과 워터마크 삽입된 영상사이의 PSNR이 약 38.5를 기준으로 하여 JPEG압축을 진행하여 실험한 결과 HD에서 가장 좋은 성능을 보여주었다. 또한 하다마드 행렬을 사용하면 연산과정에서 고속으로 처리되기 때문에 처리속도에서도 DCT, FFT, DWT보다 우월성을 가진다.

참고 문헌

- [1] Saeid Saryazdi, Hossein Nezamabidi-pour, "A Blind Digital Watermark in Hadamard Domain", Transactions on engineering, computer in gand technology V3 December, 2004 ISSN 1305-5313
- [2] J.Hernandez, M.Amado, F.Perez-Gonzalez, "DC T-domain watermarking technique for still images; Detector performance analysis and a new structure", IEEE Trans. Image Processing, Vol.9, pp.55-68, Jan.2000
- [3] N. Nikolaidis, I. Pitas, "Robust image watermarking in the spatial domain", Signal Processing archive Volume 66 , Issue 3 (May 1998) table of contents. pp.: 385 - 403

- [4] 최병철, 김용철, "DCT 기반의 최대용량 블라인드 워터마킹", 한국통신학회논문지, 01-5 Vol.26 No.5B
- [5] G. Langelaar, I. Setywan, R. Lanendijk, "Watermarking digital image and video data", IEEE Signal Processing Magazine PP.20-46 SEP 2000
- [6] Fei.C., Kundur. D., Kwong. R.H., "Analysis and design of watermarking algorithms for improved resistance to compression.", IEEE Trans. On Image Processing 13(2004) 126-144
- [7] Kii. H., Onishi. J, Ozawa.S., "The digital watermarking using zerotree of DCT", IEEE International Conference on Multimedia Computing and System 1999, pp.7-11
- [8] Kang. X, Huang.J, Shi.Y.O, Lin.Y, "A DW T-DFT composite watermarking scheme robust to both affine transform and jpeg compression", IEEE Transactions on Circuits and Systems for Videl Technology 13, 2003, pp.776-786

◎ 저 자 소 개 ◎



최 학 남(Xue-Nan Cui)

2004년 연변대학교 수학과 졸업(학사)
2005년~2006년 상명대학교 디지털저작권 보호연구센터 연구원
2007년 상명대학교 일반대학원 컴퓨터과학과 졸업(석사)
2007년~현재 인하대학교 정보통신공학과 박사과정
관심분야 : 디지털 워터마킹, 저작권관리기술, 디지털 영상처리, etc.
E-mail : xncui@vision.inha.ac.kr



김 종 원(Jong-Weon Kim)

1989년 서울시립대학교 전자공학과 졸업(학사)
1991년 서울시립대학교 대학원 전자공학과 졸업(석사)
1995년 서울시립대학교 대학원 전자공학과 졸업(박사)
1996~2000년 주성대학 정보통신학과 조교수
2000~2004년 (주)마크애니 부설연구소장
2004년~2005년 상명대학교 소프트웨어대학 초빙교수
2006년~현재 상명대학교 디지털저작권보호연구센터 전임연구교수
관심분야 : 디지털워터마킹, 저작권보호 및 관리기술, 디지털신호처리, etc.
E-mail : jwkim@smu.ac.kr



이 덕(Li De)

1996년 할빈이공대학교 전기공학과 졸업(학사)
2001년 상명대학교 대학원 전자계산학과 졸업(석사)
2005년 상명대학교 대학원 컴퓨터과학과 졸업(박사)
2006년~현재 상명대학교 디지털저작권보호연구센터 전임연구교수
관심분야 : 디지털워터마킹, 저작권관리기술, 디지털신호처리, 컴퓨터네트워크보안, etc.
E-mail : lide@smu.ac.kr



최 종 욱(Jong-Uk Choi)

1982년 아주대학교 산업공학과 졸업(학사)
1982년 서울대학교 대학원 경영학과 수료(석사)
1988년 University of South Carolina (MIS. Ph.D)
1988~1991년 한국과학기술연구원 시스템공학연구소 선임연구원
2000년~현재 (주)마크애니 대표이사
1991년~현재 상명대학교 소프트웨어대학 교수
관심분야 : 디지털워터마킹, 저작권보호 및 관리기술, 정보보호응용기술, 인공지능, etc.
E-mail : juchoi@smu.ac.kr