

Forensic Watermarking

최종발표

2020203040 최진우

2020203087 이정현

INDEX

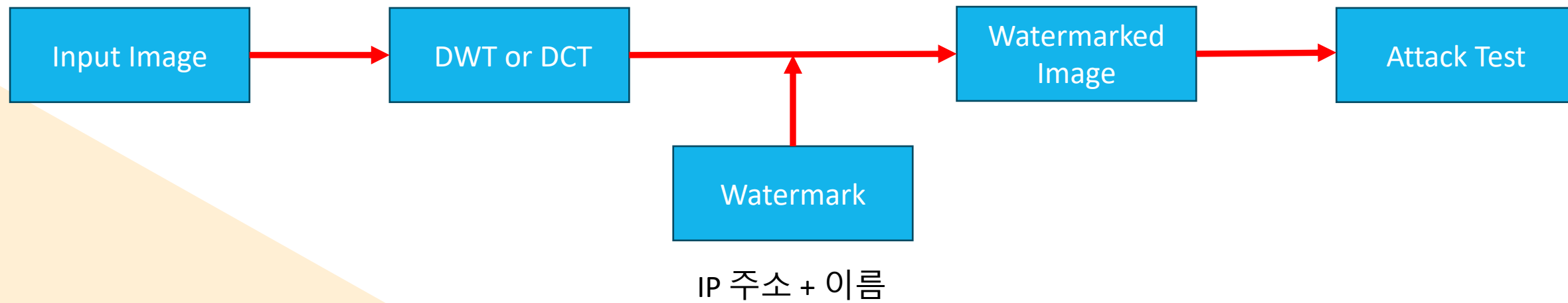
1. 포렌식 워터마킹
2. 프로젝트 과정
3. 한계 및 개선점
4. 팀원 별 역할

포렌식 워터마킹

- 콘텐츠 사용자의 정보를 삽입해 불법 유포를 추적하기 위한 용도로 사용
- 워터마크를 읽어냄으로서 특정 콘텐츠를 구매한 사람이 누구인지를 역추적 할 수 있음



프로젝트 구조



입력 이미지

- 사용 이미지(512x512)



lena.jpg



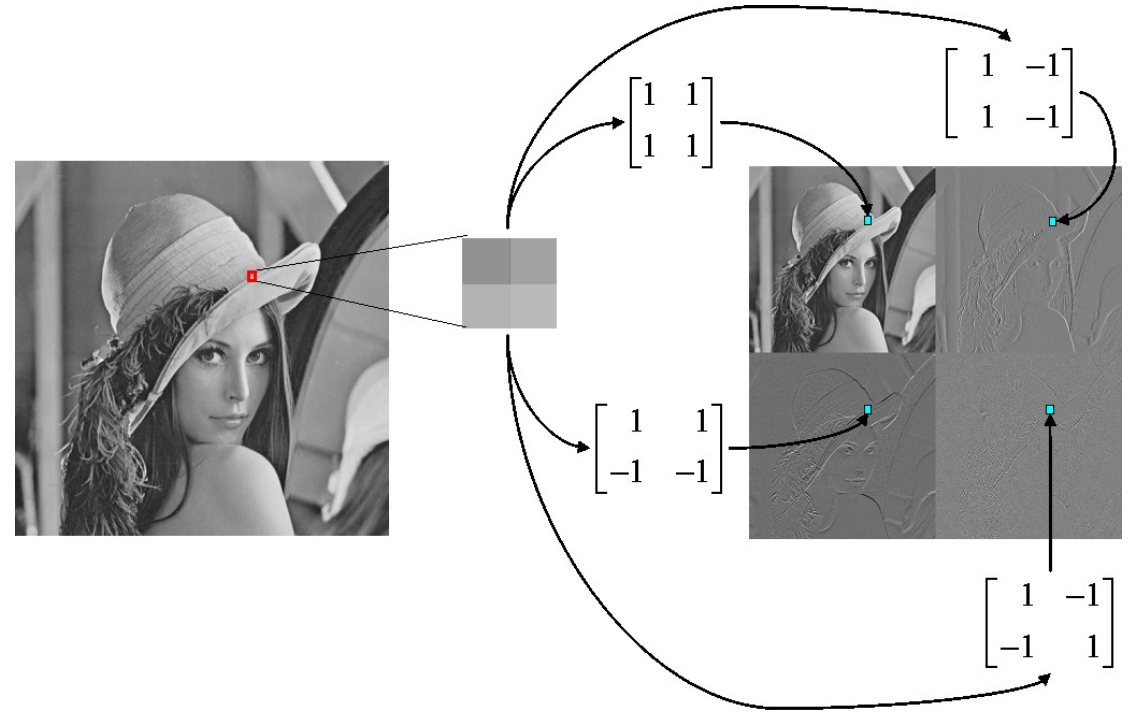
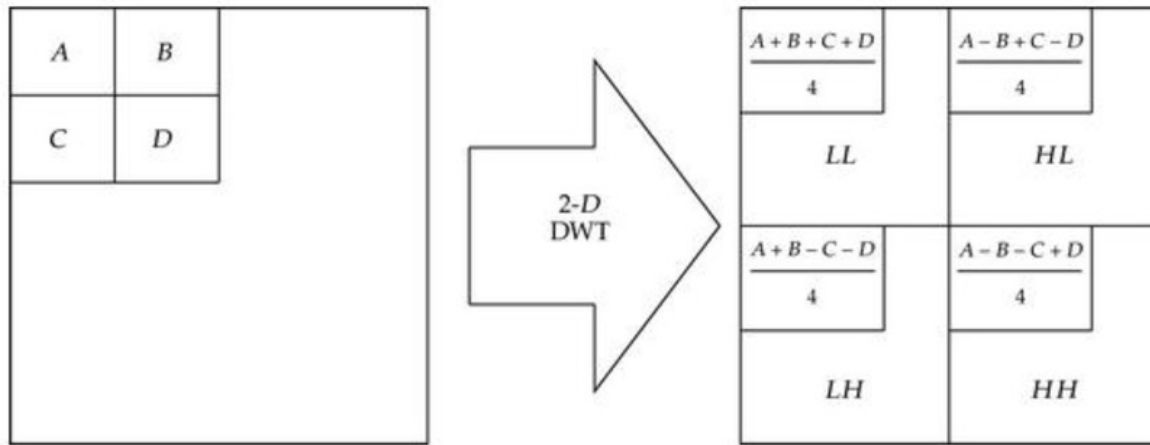
landscape.jpg



IU.jpg

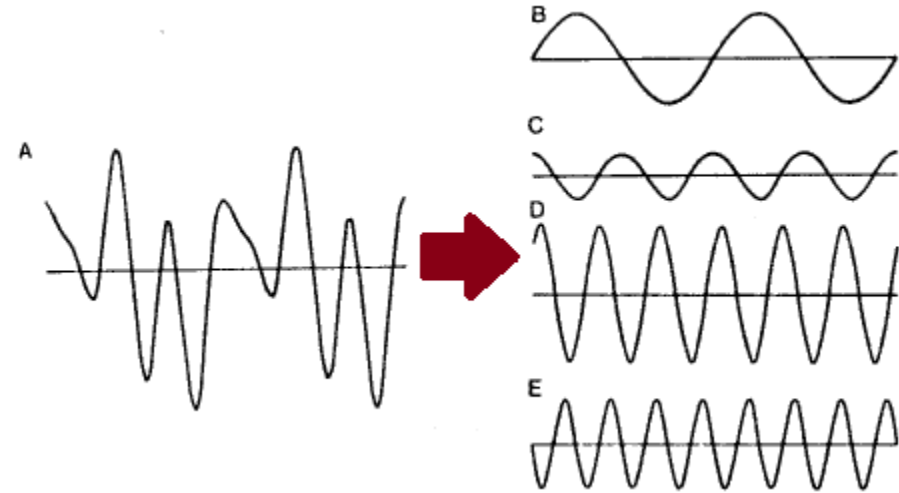
DWT(Discrete Wavelet Transform)

- DWT: 신호를 분석하고 분해하여 고주파, 저주파 대역으로 나누는 수학적 변환
- 고주파 성분의 HH 대역에 워터마크 삽입



DCT(Discrete Cosine Transform)

- 영상을 주파수 영역으로 변환하는 방법
- 신호를 코사인 함수의 합으로 표현한다.



DCT 수식

Discrete Cosine Transform

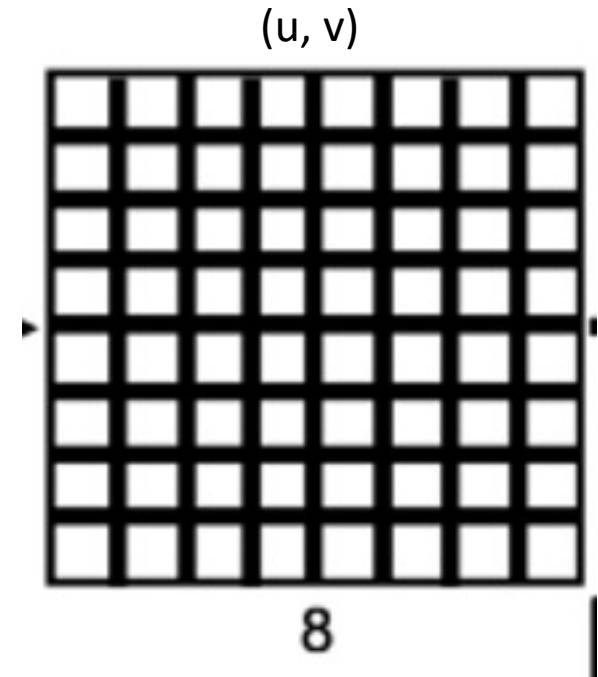
- The forward equation, for image A, is

$$b(u, v) = \frac{2}{N} C(u) C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} a(x, y) \cos\left(\frac{\pi u(2x+1)}{2N}\right) \cos\left(\frac{\pi v(2y+1)}{2N}\right)$$

- The inverse equation, for image B, is

$$a(x, y) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} C(u) C(v) b(u, v) \cos\left(\frac{\pi u(2x+1)}{2N}\right) \cos\left(\frac{\pi v(2y+1)}{2N}\right)$$

• Here $C(u) = \begin{cases} \frac{1}{\sqrt{2}} & \text{if } u = 0 \\ 1 & \text{otherwise} \end{cases}$



워터마크 삽입 방식

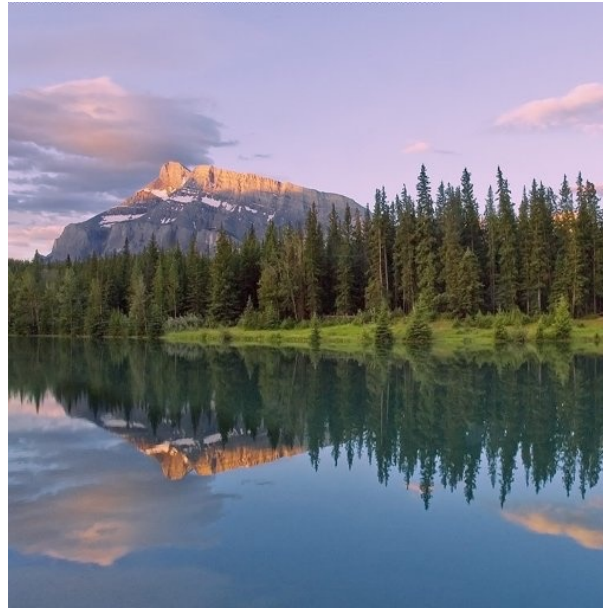
- 시도했던 구현 방식
 - 텍스트를 RGB의 고주파 영역에 삽입 → 픽셀 값의 작은 변화에도 워터마크가 손실
 - 이미지를 RGB의 고주파 영역에 삽입 → 고주파 성분을 강하게 지우는 압축 공격에 취약
- 최종 구현 방식
 - 난수 기반 삽입과 다수결 복구 방식 → 강인성을 강화
 - RGB 영역이 아닌 YCrCb의 Y 영역에 삽입하여 공격을 당하더라도 손상이 적도록 강화
 - numCopies 횟수만큼 중복 삽입하고 다수결 투표 기반 추출을 통해 작은 변화에도 잘 추출할 수 있도록 강화
 - 고주파 대역의 랜덤 위치에 삽입하여 보안 강화

워터마크 삽입 결과

- numCopies = 5, strength = 30



lena.jpg
DCT: 48.48 dB
DWT: 41.90 dB



landscape.jpg
DCT: 48.51 dB
DWT: 42.02 dB



IU.jpg
DCT: 48.54 dB
DWT: 42.18 dB

워터마크 공격 테스트

- Gaussian Noise, JPEG 압축, 가시성 워터마크 삽입 테스트를 진행
- 공격 후 워터마크를 추출했을 때 텍스트의 변화, PSNR 값 변화 평가
- numCopies = 3, 5
- strength = 10, 30, 50
- Gaussian Noise 표준편차: 1, 10, 50
- JPEG 압축 품질: 70, 80, 90
- 가시성 워터마크 투명도: 30%

워터마크 공격 테스트

- Gaussian Noise, JPEG 압축, 가시성 워터마크 삽입 후 이미지



Gaussian Noise(10)
32.90 dB

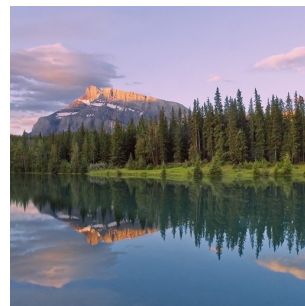
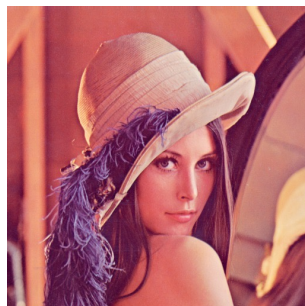


JPEG 압축(80)
39.71 dB



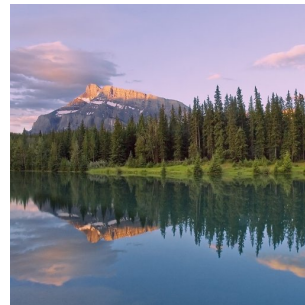
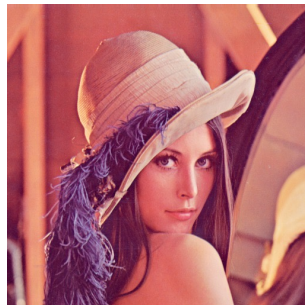
가시성 워터마크
28.23 dB

numCopies = 3, strength = 10



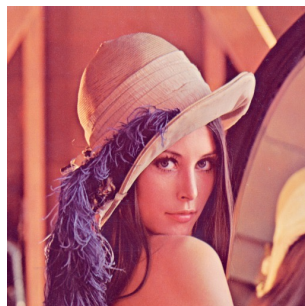
	lena.jpg	landscape.jpg	IU.jpg
노이즈(1)	DCT: X / 54.10 dB DWT: O / 52.55 dB	DCT: X / 53.97 dB DWT: O / 52.56 dB	DCT: X / 54.26 dB DWT: O / 52.56 dB
노이즈(10)	DCT: X / 35.93 dB DWT: X / 32.90 dB	DCT: X / 35.92 dB DWT: O / 32.93 dB	DCT: X / 35.98 dB DWT: O / 32.97 dB
노이즈(50)	DCT: X / 22.98 dB DWT: X / 19.24 dB	DCT: X / 23.03 dB DWT: X / 19.92 dB	DCT: X / 22.03 dB DWT: X / 19.98 dB
JPEG 압축(70)	DCT: X / 41.12 dB DWT: X / 38.89 dB	DCT: X / 38.31 dB DWT: X / 38.27 dB	DCT: X / 36.95 dB DWT: X / 36.87 dB
JPEG 압축(80)	DCT: X / 43.21 dB DWT: X / 40.16 dB	DCT: X / 45.00 dB DWT: X / 44.58 dB	DCT: X / 37.83 dB DWT: X / 37.84 dB
JPEG 압축(90)	DCT: X / 47.17 dB DWT: X / 46.20 dB	DCT: X / 47.31 dB DWT: X / 46.72 dB	DCT: X / 50.53 dB DWT: X / 49.14 dB
가시성 워터마크	DCT: X / 28.22 dB DWT: O / 28.23 dB	DCT: X / 27.09 dB DWT: O / 27.09 dB	DCT: X / 26.96 dB DWT: O / 26.97 dB

numCopies = 3, strength = 30



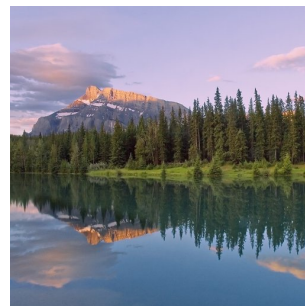
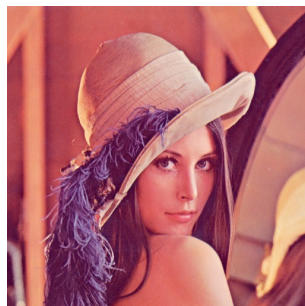
	lena.jpg	landscape.jpg	IU.jpg
노이즈(1)	DCT: X / 49.35 dB DWT: O / 52.56 dB	DCT: X / 49.33 dB DWT: O / 52.56 dB	DCT: X / 49.43 dB DWT: O / 52.56 dB
노이즈(10)	DCT: X / 35.80 dB DWT: O / 32.90 dB	DCT: O / 35.79 dB DWT: O / 32.93 dB	DCT: X / 35.85 dB DWT: O / 32.97 dB
노이즈(50)	DCT: X / 22.08 dB DWT: O / 19.24 dB	DCT: X / 23.03 dB DWT: O / 19.92 dB	DCT: X / 22.93 dB DWT: X / 19.98 dB
JPEG 압축(70)	DCT: O / 40.73 dB DWT: X / 37.95 dB	DCT: O / 38.09 dB DWT: X / 37.57 dB	DCT: X / 36.79 dB DWT: X / 36.40 dB
JPEG 압축(80)	DCT: X / 42.57 dB DWT: O / 39.21 dB	DCT: O / 44.06 dB DWT: O / 42.23 dB	DCT: X / 37.65 dB DWT: O / 37.49 dB
JPEG 압축(90)	DCT: O / 45.70 dB DWT: O / 45.24 dB	DCT: O / 45.79 dB DWT: O / 45.75 dB	DCT: X / 47.76 dB DWT: O / 47.42 dB
가시성 워터마크	DCT: X / 28.20 dB DWT: O / 28.23 dB	DCT: X / 27.08 dB DWT: O / 27.09 dB	DCT: X / 26.95 dB DWT: O / 26.97 dB

numCopies = 3, strength = 50



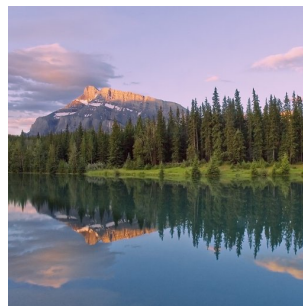
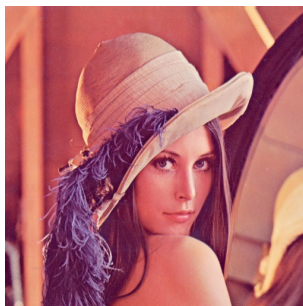
	lena.jpg	landscape.jpg	IU.jpg
노이즈(1)	DCT: X / 45.77 dB DWT: O / 52.55 dB	DCT: X / 45.60 dB DWT: O / 52.56 dB	DCT: X / 46.65 dB DWT: O / 52.56 dB
노이즈(10)	DCT: X / 35.57 dB DWT: O / 32.90 dB	DCT: O / 35.54 dB DWT: O / 32.93 dB	DCT: X / 35.59 dB DWT: O / 32.97 dB
노이즈(50)	DCT: O / 22.07 dB DWT: O / 19.25 dB	DCT: O / 23.01 dB DWT: O / 19.93 dB	DCT: X / 21.91 dB DWT: O / 19.98 dB
JPEG 압축(70)	DCT: O / 39.95 dB DWT: O / 37.02 dB	DCT: O / 37.66 dB DWT: O / 36.82 dB	DCT: X / 36.48 dB DWT: O / 35.96 dB
JPEG 압축(80)	DCT: X / 41.52 dB DWT: O / 38.84 dB	DCT: O / 42.67 dB DWT: O / 41.56 dB	DCT: X / 37.27 dB DWT: O / 37.31 dB
JPEG 압축(90)	DCT: O / 43.68 dB DWT: O / 45.17 dB	DCT: O / 43.73 dB DWT: O / 45.77 dB	DCT: X / 44.86 dB DWT: O / 47.41 dB
가시성 워터마크	DCT: X / 28.16 dB DWT: O / 28.23 dB	DCT: O / 27.05 dB DWT: O / 27.09 dB	DCT: X / 26.92 dB DWT: O / 26.97 dB

numCopies = 5, strength = 10



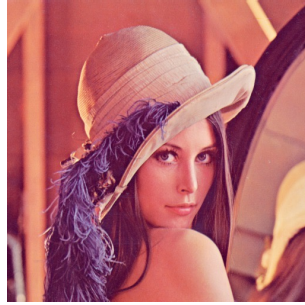
	lena.jpg	landscape.jpg	IU.jpg
노이즈(1)	DCT: X / 53.48 dB DWT: O / 52.55 dB	DCT: X / 53.40 dB DWT: O / 52.56 dB	DCT: X / 53.65 dB DWT: O / 52.56 dB
노이즈(10)	DCT: X / 35.92 dB DWT: O / 32.90 dB	DCT: X / 35.91 dB DWT: O / 32.93 dB	DCT: X / 35.97 dB DWT: O / 32.97 dB
노이즈(50)	DCT: X / 22.09 dB DWT: X / 19.24 dB	DCT: X / 23.03 dB DWT: X / 19.92 dB	DCT: X / 22.93 dB DWT: X / 19.98 dB
JPEG 압축(70)	DCT: X / 41.10 dB DWT: X / 38.79 dB	DCT: X / 38.29 dB DWT: X / 38.23 dB	DCT: X / 36.94 dB DWT: X / 36.82 dB
JPEG 압축(80)	DCT: X / 43.15 dB DWT: X / 40.04 dB	DCT: X / 44.91 dB DWT: X / 44.25 dB	DCT: X / 37.81 dB DWT: X / 37.82 dB
JPEG 압축(90)	DCT: X / 47.04 dB DWT: X / 45.76 dB	DCT: X / 47.18 dB DWT: X / 46.29 dB	DCT: X / 50.30 dB DWT: X / 48.30 dB
가시성 워터마크	DCT: X / 28.22 dB DWT: O / 28.23 dB	DCT: X / 27.10 dB DWT: O / 27.09 dB	DCT: X / 26.96 dB DWT: O / 26.97 dB

numCopies = 5, strength = 30



	lena.jpg	landscape.jpg	IU.jpg
노이즈(1)	DCT: X / 47.74 dB DWT: O / 52.56 dB	DCT: O / 47.72 dB DWT: O / 52.56 dB	DCT: O / 47.80 dB DWT: O / 52.56 dB
노이즈(10)	DCT: X / 35.72 dB DWT: O / 32.90 dB	DCT: X / 35.71 dB DWT: O / 32.93 dB	DCT: O / 35.77 dB DWT: O / 32.97 dB
노이즈(50)	DCT: X / 22.08 dB DWT: O / 19.24 dB	DCT: X / 23.02 dB DWT: O / 19.92 dB	DCT: X / 22.92 dB DWT: O / 19.98 dB
JPEG 압축(70)	DCT: X / 40.49 dB DWT: X / 37.37 dB	DCT: O / 37.96 dB DWT: X / 37.13 dB	DCT: X / 36.68 dB DWT: X / 36.07 dB
JPEG 압축(80)	DCT: X / 42.16 dB DWT: O / 38.64 dB	DCT: O / 43.51 dB DWT: O / 41.11 dB	DCT: O / 37.52 dB DWT: O / 37.26 dB
JPEG 압축(90)	DCT: X / 44.91 dB DWT: O / 44.46 dB	DCT: O / 44.99 dB DWT: O / 44.97 dB	DCT: O / 46.57 dB DWT: O / 46.20 dB
가시성 워터마크	DCT: X / 28.19 dB DWT: O / 28.23 dB	DCT: X / 27.07 dB DWT: O / 27.09 dB	DCT: O / 26.94 dB DWT: O / 26.97 dB

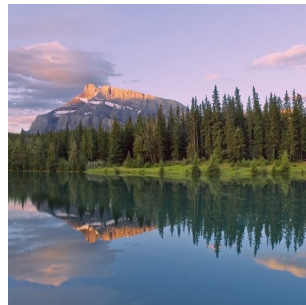
numCopies = 5, strength = 50



	lena.jpg	landscape.jpg	IU.jpg
노이즈(1)	DCT: O / 43.75 dB DWT: O / 52.55 dB	DCT: O / 43.72 dB DWT: O / 52.56 dB	DCT: O / 43.78 dB DWT: O / 52.56 dB
노이즈(10)	DCT: O / 35.33 dB DWT: O / 32.90 dB	DCT: O / 35.32 dB DWT: O / 32.93 dB	DCT: O / 35.37 dB DWT: O / 32.97 dB
노이즈(50)	DCT: O / 22.06 dB DWT: O / 19.25 dB	DCT: O / 23.00 dB DWT: O / 19.93 dB	DCT: O / 22.90 dB DWT: O / 19.98 dB
JPEG 압축(70)	DCT: X / 39.35 dB DWT: O / 36.14 dB	DCT: O / 37.30 dB DWT: O / 36.11 dB	DCT: X / 36.21 dB DWT: O / 35.44 dB
JPEG 압축(80)	DCT: O / 40.70 dB DWT: O / 38.14 dB	DCT: O / 41.63 dB DWT: O / 40.34 dB	DCT: O / 36.95 dB DWT: O / 37.00 dB
JPEG 압축(90)	DCT: X / 42.36 dB DWT: O / 44.35 dB	DCT: O / 42.40 dB DWT: O / 45.02 dB	DCT: O / 43.24 dB DWT: O / 46.20 dB
가시성 워터마크	DCT: X / 28.13 dB DWT: O / 28.23 dB	DCT: X / 27.02 dB DWT: O / 27.09 dB	DCT: O / 26.89 dB DWT: O / 26.96 dB

테스트 결과 종합

numCopies / strength



	lena.jpg	landscape.jpg	IU.jpg
노이즈(1)	DCT: 5 / 50 DWT: 3 / 10	DCT: 5 / 30 DWT: 3 / 10	DCT: 5 / 30 DWT: 3 / 10
노이즈(10)	DCT: 5 / 50 DWT: 5 / 10	DCT: 3 / 30 DWT: 3 / 10	DCT: 5 / 30 DWT: 3 / 10
노이즈(50)	DCT: 3 / 50 DWT: 3 / 30	DCT: 3 / 50 DWT: 3 / 30	DCT: 5 / 50 DWT: 3 / 50
JPEG 압축(70)	DCT: 3 / 30 DWT: 3 / 50	DCT: 3 / 30 DWT: 3 / 50	DCT: 5 / 50 DWT: 3 / 50
JPEG 압축(80)	DCT: 5 / 50 DWT: 3 / 30	DCT: 3 / 30 DWT: 3 / 30	DCT: 5 / 30 DWT: 3 / 30
JPEG 압축(90)	DCT: 3 / 30 DWT: 3 / 30	DCT: 3 / 30 DWT: 3 / 30	DCT: 5 / 30 DWT: 3 / 30
가시성 워터마크	DCT: X DWT: 3 / 10	DCT: X DWT: 3 / 10	DCT: 5 / 30 DWT: 3 / 10


테스트 결과 종합

- 사용하는 영상에 따라 결과가 달라진다.
- 워터마크를 여러 곳에 반복 저장할수록(numCopies ↑) 방어 성공률이 증가한다.
- 강도가 낮으면 시각적으로 눈에 덜 띄지만, 공격에는 더 취약하다.
- 공격에 대한 완전한 방어는 안되지만 파라미터를 조정하는 것에 따라 일정 정도까지는 방어할 수 있다.

한계 및 개선점

- 한계
 - 이미지의 픽셀 값의 위치를 바꾸는 Crop, Rotation 공격에는 취약하다.
 - 입력할 수 있는 최대 문자열 길이가 존재한다.
- 개선점
 - 파라미터를 adaptive하게 바꿔주는 방식
 - 비트열 대신 이미지 같이 워터마크를 다른 방식으로 표현

팀원 역할

- 최진우: DCT 변환 구현
 - 이정현: DWT 변환 구현
 - 공통: 워터마크 삽입 알고리즘, 공격 테스트
- 
- A large, solid orange triangle is positioned in the bottom-left corner of the slide, pointing towards the bottom-right.

참고 자료

- DWT, DCT 구현 코드는 아래 사이트를 참고하였습니다.
 - DWT: <https://github.com/ms4935/Forensic-Watermarking-program-for-image/blob/master/DWT.cpp>
 - DCT: <https://mynameisoh.tistory.com/30>
- 공격 테스트는 Opencv C++에서 제공하는 함수를 사용하였으며 나머지 워터마크 삽입 알고리즘은 직접 구현하였습니다.

Q&A