Invisible Watermarking for Image Data Protection in Sensor Network Environments

Sungshin Women's University (Seoul, South Korea)
Seo-Yi Kim, Na-Eun Park, Il-Gu Lee
sykim.cse@gmail.com

성신여자대학교
SUNGSHIN WOMEN'S UNIVERSITY

Author

Seo-Yi Kim | Presenter

2020.03~2023.08
Sungshin Women's University, Seoul, South Korea
B.S. in Convergence Security Engineering

2023.09~2025.02
Sungshin Women's University, Seoul, South Korea
M.S. in Future Convergence Technology Engineering

2025.9~
Sungshin Women's University, Seoul, South Korea
Ph.D in Convergence Security Engineering

[Achievement] https://sites.google.com/view/cselabseo-yikim/%ED%99%88

[Contact] sykim.cse@gmail.com / 220257078@sungshin.ac.kr

Background

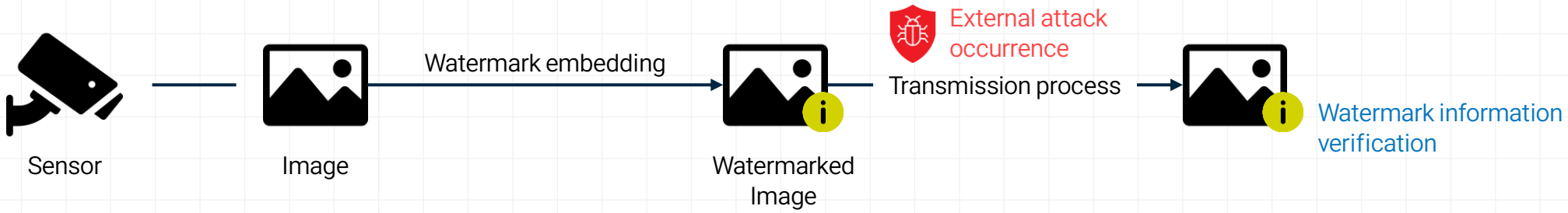
Background

If images captured by sensors are tampered with,

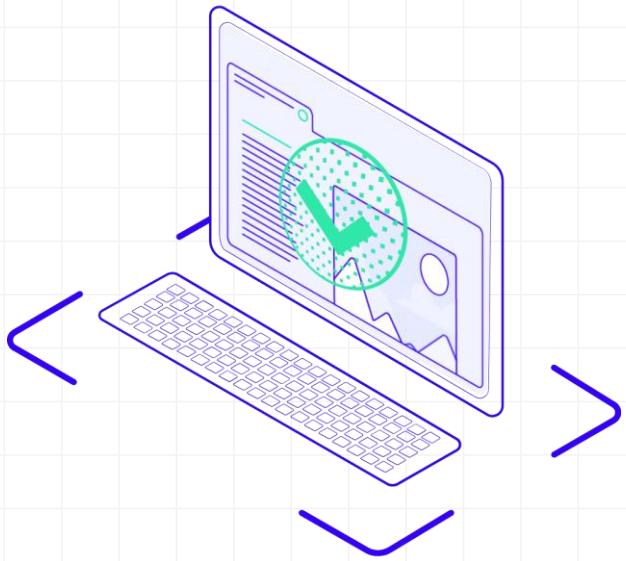
- serious security incidents can occur
- false positives / false negatives may result

Solution: Digital watermarking

- Invisibly embed identifiable information into the original image
- Enable tampering detection and source tracing



Background



Essential elements of digital watermarking

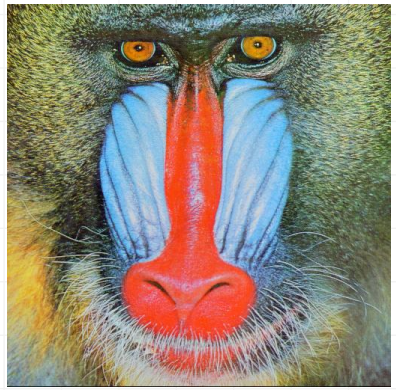
- Protecting the quality of the host image – Imperceptibility
- Ensuring strong resistance to external modifications – Robustness

Features of the proposed watermarking method

- An imperceptible watermarking scheme combining three-level DWT and SVD for image copyright protection
- Repeated watermark embedding across multiple frequency components
  - Error correction capability even when parts are damaged
- Robustness against various signal distortion techniques
  - Improved watermark extraction performance compared to conventional methods

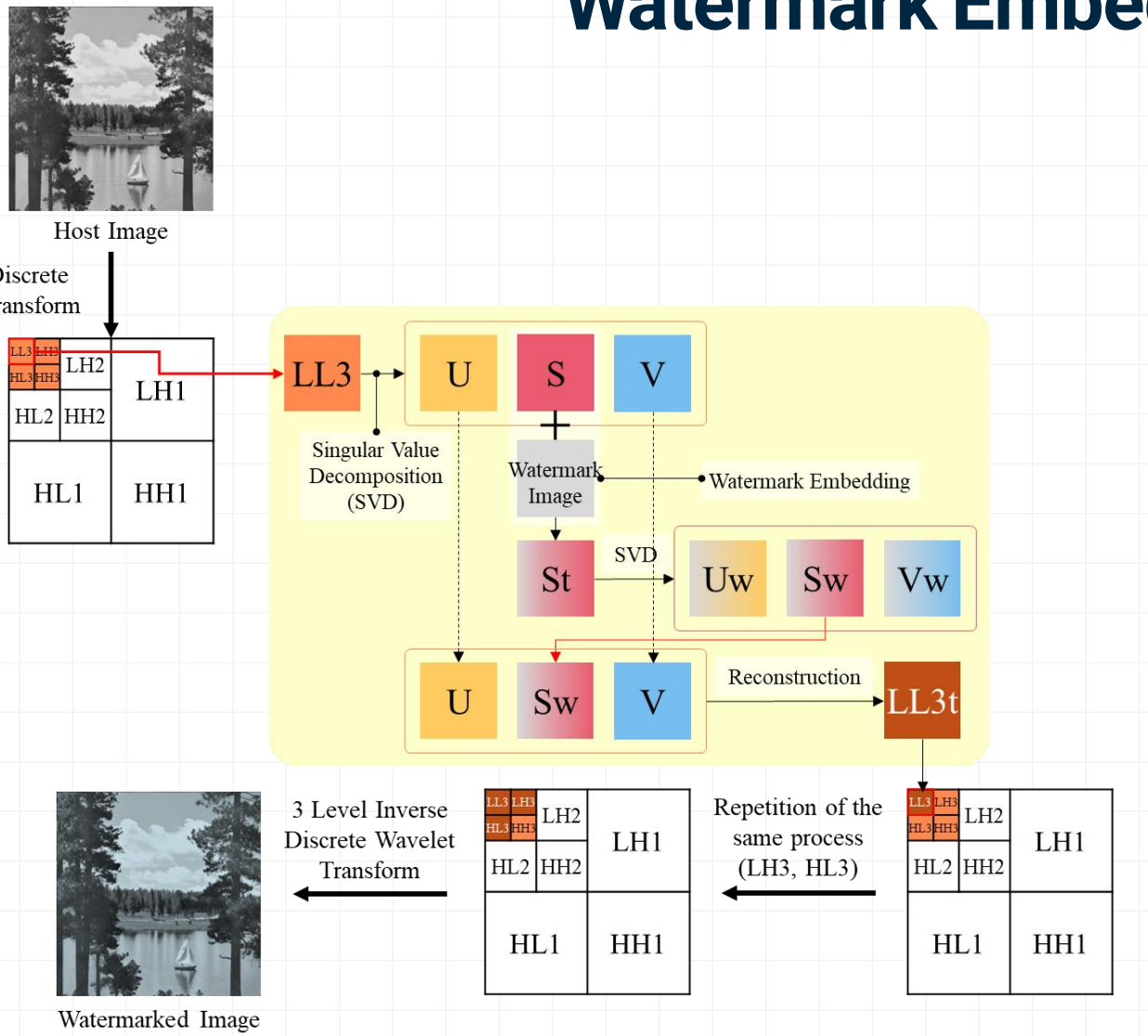
Image Frequency

- Gradual brightness changes with large patterns or smooth curves, and prominent structures
- Few image details with minimal edges or sharp transitions
  - ⇨ Images rich in low-frequency components
- Contain key features easily recognizable by humans, representing the overall shape or structure of the image



- Rapid brightness changes containing image details and textures
- Emphasize fine features such as edges and complex patterns
  - ⇨ Images rich in high-frequency components
- Overall structure is preserved even when high-frequency components change

Watermark Embedding



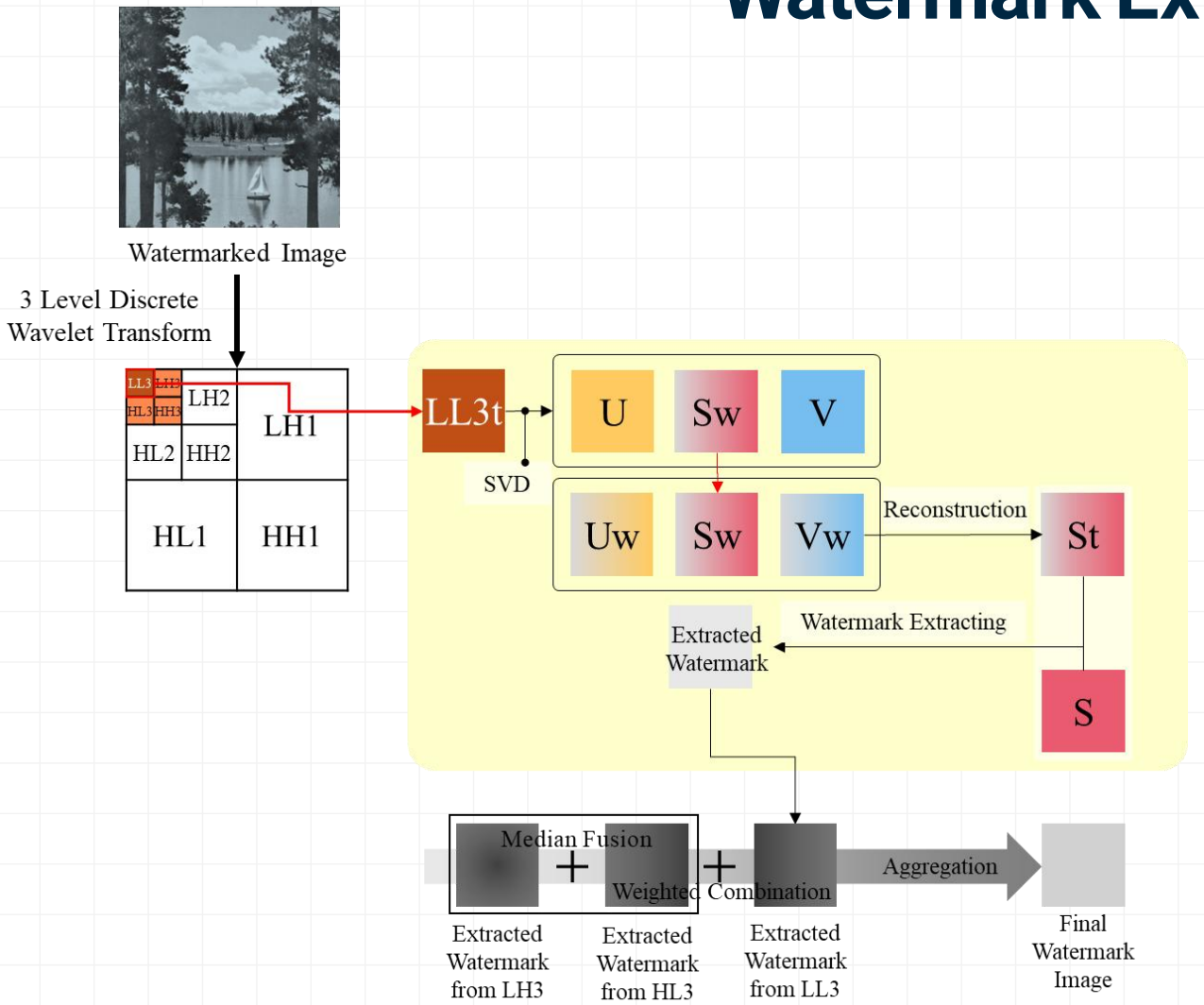
Watermark Embedding Process

1. Apply 3-level DWT to the host image
2. Perform SVD on the low-frequency band (LL3)
3. Embed the watermark image into the singular values (S)
4. Perform SVD on the singular values containing the watermark (St)
5. Use the obtained singular values (Sw) to perform inverse SVD

   ⇨ Reconstruct the low-frequency band (LL3t) with the embedded watermark
6. Replace the original LL3 with the watermarked LL3 (LL3t)
7. Repeat steps 2 – 6 for LH3 and HL3
8. Perform 3-level IDWT to restore the host image

   ⇨ Watermarked image construction completed

Watermark Extraction



Watermark Extraction Process

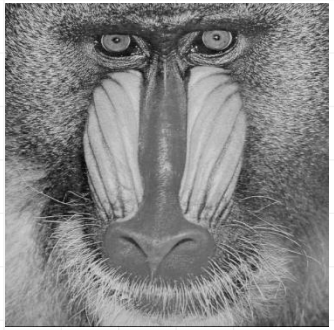
1. Perform 3-level DWT on the watermarked image
2. Perform SVD on the low-frequency band (LL3) ⇨ Extract LL3t
3. Extract singular values (Sw), then perform inverse SVD to reconstruct the singular values containing the watermark (St)
4. Extract the watermark image from the singular values containing the watermark (St)
5. Repeat steps 2 – 4 for LH3 (LH3t) and HL3 (HL3t)
6. Watermark reconstruction
   a. Apply Median Fusion to the watermarks extracted from LH3 and HL3 ⇨ Combine into a single watermark
   b. Perform Weighted Combination on the watermark obtained from step 1 and the watermark extracted from LL3
   c. Restore the final watermark

Experiment setting

Host Image

- 512x512 / PNG

Peppers.png



Mandrill.png

Watermark Image

- 64x64 / PNG

Watermark.png

Signal Distortion Attack

- Noise Attack
  - Gaussian Noise
  - Salt&Pepper
  - Sparkle Noise
- Compression Attack
  - JPEG Compression
  - JPEG2000 Compression
- Filtering Attack
  - Blurring Attack
  - Low-pass Filtering

Attack Parameters and Attack Intensity

Attack type	Attack	Parameter	Attack intensity (level)				
			1	2	3	4	5
Noise Attack	Gaussian noise	Variance	0.001	0.005	0.01	0.05	0.1
	Salt and pepper	Density	0.01	0.03	0.05	0.1	0.2
	Sparkle noise	Probability	0.01	0.03	0.05	0.1	0.2
Compression Attack	JPEG compression	Quality factor	90	70	50	30	10
	JPEG2000 compression	Quality factor	90	70	50	30	10
Filtering Attack	Blurring attack	Kernel size	3	5	7	9	11
	Low-frequency Filtering	Kernel size	3	5	7	9	11

Experiments List

- Image quality comparison with repeated watermark embedding
- Comparative analysis of watermarking performance according to embedding strength

Experiment 1

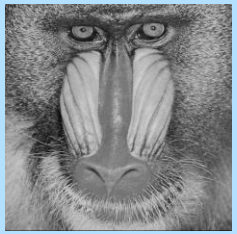
Image quality comparison with repeated watermark embedding

- Embed the watermark only into the LL3 component (1 time)
- Embed the watermark into the LL3, LH3, and HL3 components (3 times)
- Watermark embedding strength: a = 0.1
- Signal distortion attack strength: 3 levels

Image quality comparison

Single embedding

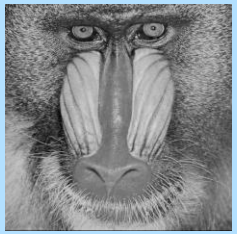
- PSNR: 55.12dB
- SSIM: 0.99



- PSNR: 53.70dB
- SSIM: 0.99

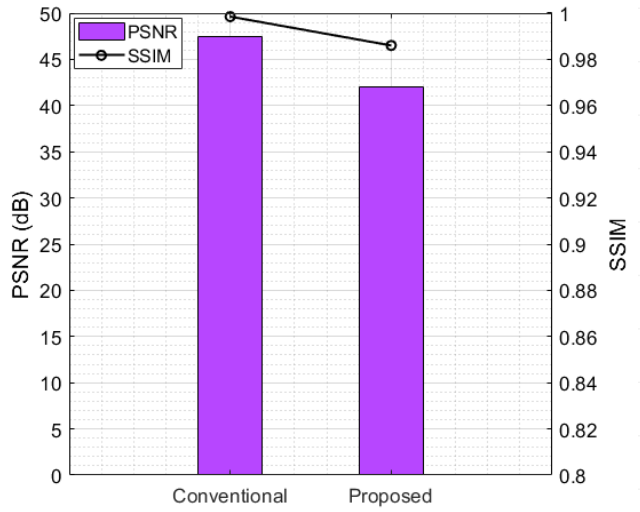
Triple embedding

- PSNR: 42.01dB
- SSIM: 0.98

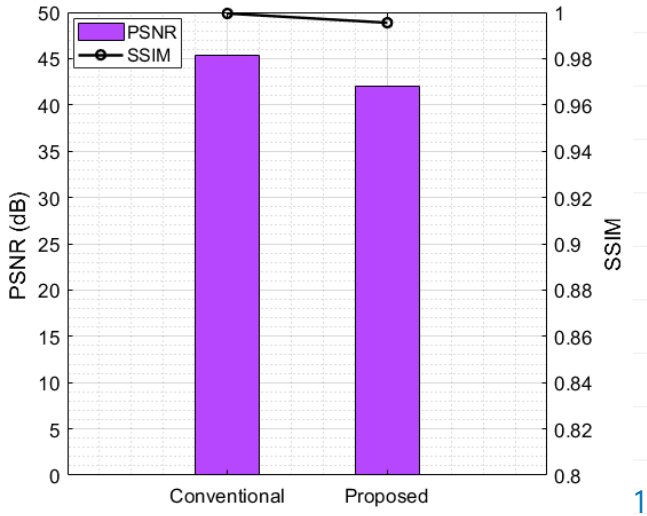


- PSNR: 42.04dB
- SSIM: 0.99

Peppers



Mandrill



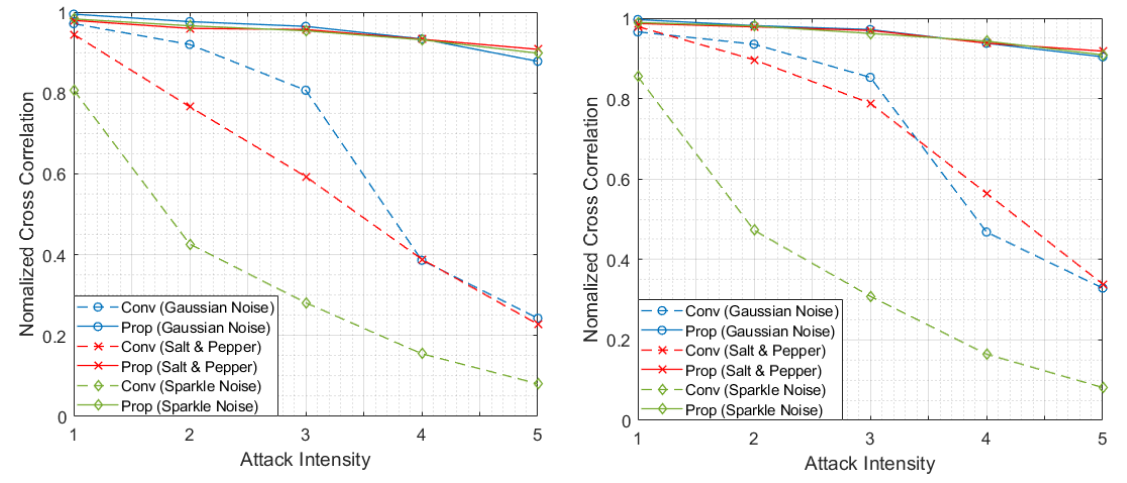
Experiment 2

Comparative analysis of watermarking performance according to embedding strength

- Watermark embedding strength: a = 0.1
- Signal distortion attack strength: 1~5 levels

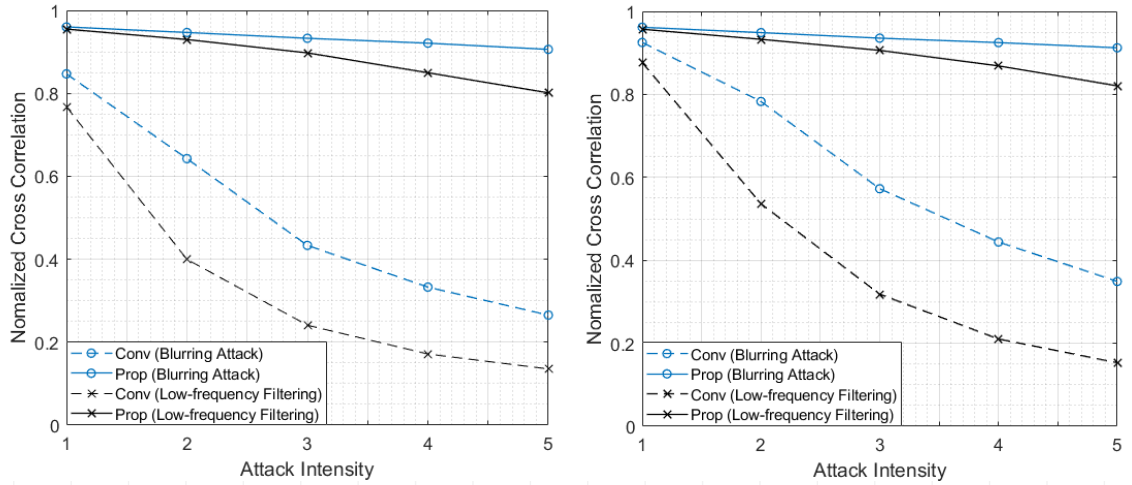
Extraction performance comparison (NCC)

Noise Attack – Gaussian noise, Salt&Pepper, Sparkle noise



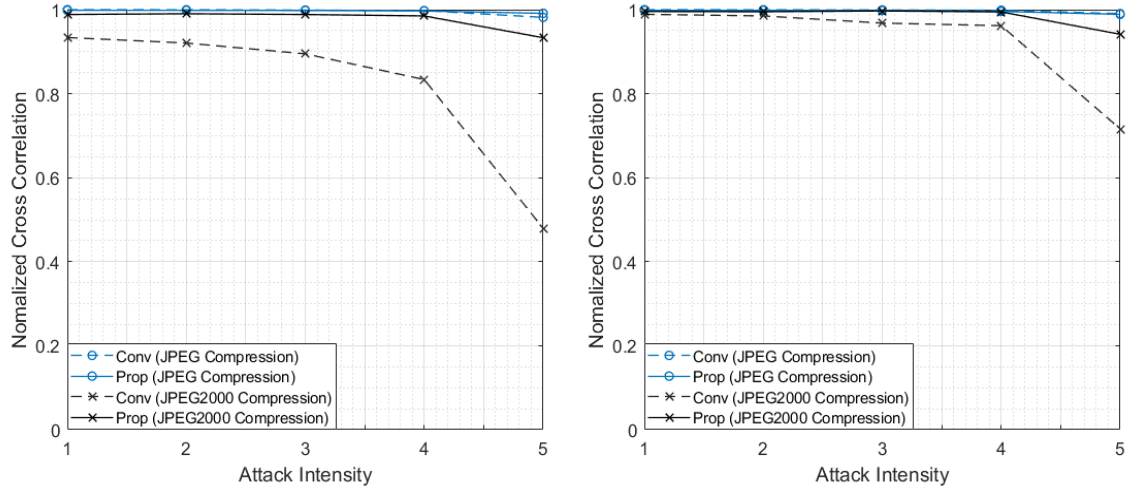
Peppers Mandrill

Filtering Attack – Blurring attack, Low-pass Filtering



Peppers Mandrill

Compression Attack – JPEG, JPEG2000 Compression



Peppers Mandrill

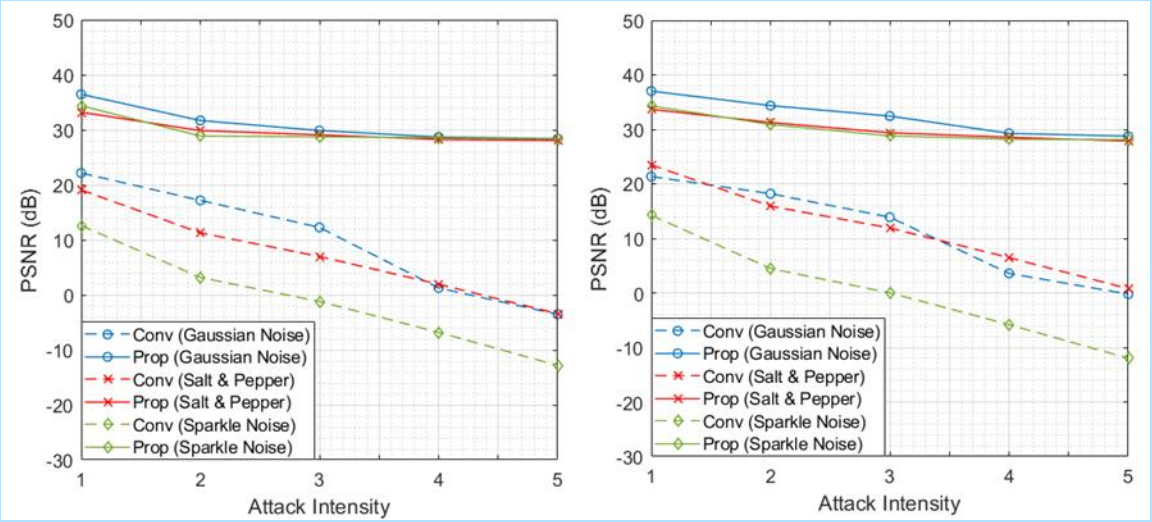
Experiment 2

Comparative analysis of watermarking performance according to embedding strength

- Watermark embedding strength: a = 0.1
- Signal distortion attack strength: 1~5 levels

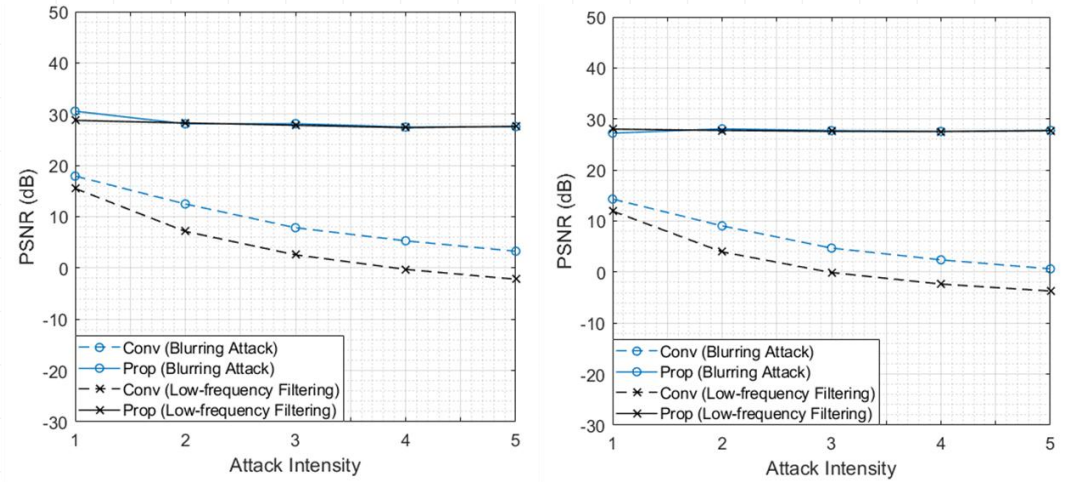
Extraction performance comparison (PSNR)

Noise Attack – Gaussian noise, Salt&Pepper, Sparkle noise



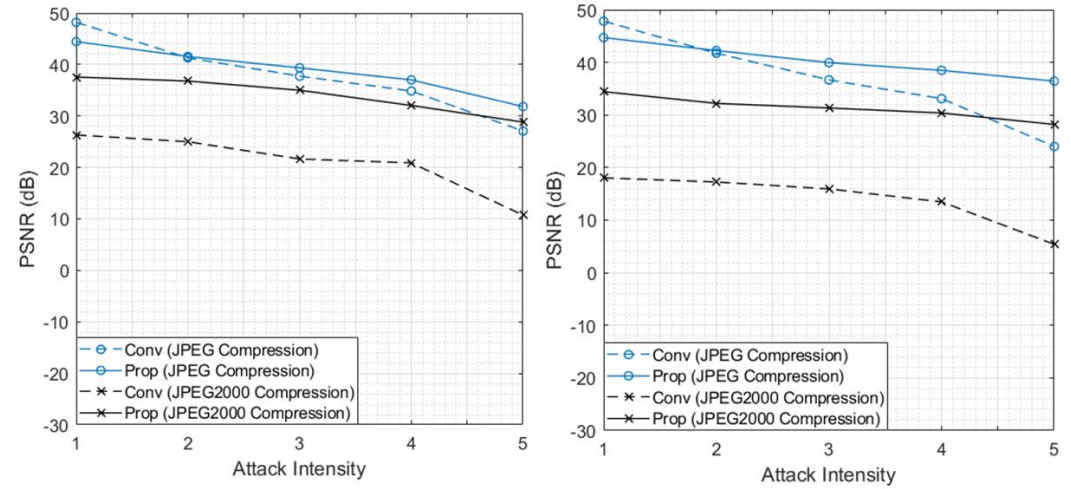
Peppers Mandrill

Filtering Attack – Blurring attack, Low-pass Filtering



Peppers Mandrill

Compression Attack – JPEG, JPEG2000 Compression



Peppers Mandrill

Conclusion

Propose a digital image watermarking method with strong robustness against external modifications and excellent imperceptibility

- Watermarking scheme combining three-level DWT and SVD
- Repeated embedding of singular value-based watermark into low-frequency (LL3) and selected high-frequency (LH3, HL3) components
- Implements a structure that complementarily restores damaged signals
- Robustness against various signal distortion techniques
- Improved watermark extraction performance compared to conventional methods

Expected Effects

- High practicality and applicability for digital content protectionEffective use in areas where imperceptibility and reliability are critical (e.g., copyright protection, data authentication)

Future Work

- Current research does not address color images
- For color images, all channels of RGB or YCbCr should be considered

Thank you

Sungshin Women's University
Seo-Yi Kim, Na-Eun Park, Il-Gu Lee
sykim.cse@gmail.com

성신여자대학교
SUNGSHIN WOMEN'S UNIVERSITY