UC San Diego

Image Tampering Detection Based on Steganographic Watermarking

Team 26
Peng Chen
Yifan Peng
Jianxiao Cai

ECE 253 Digital Image Processing | December 13, 2024

Problem Solving

Problem	Solution
 Weak robustness in watermarking embedding.	Add the robust watermark embedding scheme. 
 Desire for self-recovery of tampered images.	Develop an advanced self-recovery mechanism. 
 Inadequate metrics for evaluating performance.	Use better evaluation metrics for result assessment. 

Previous Method

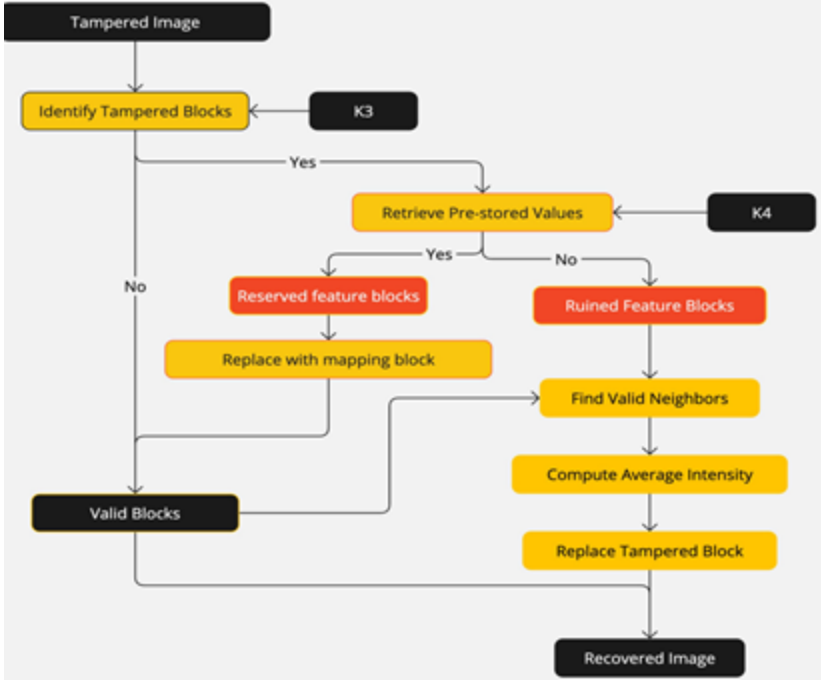
- **Previous Schemes:**
  - **Lu and Liao (2001)[1]:** Authentication and copyright protection; lacked security and restoration.
  - **Zhu et al.[2]:** Semi-fragile scheme; limited for high tampering.
  - **Zhang and Wang[3]:** Fragile, low visual quality (~28 dB); effective for tampering <3.2%.
  - **Singh and Agarwal[4]:** Robust, poor imperceptibility (<30 dB); tampering rate <50%.

- **Challenges and Limitations:**
  - Trade-offs between robustness, imperceptibility, and restoration.
  - Dependency on original host image (non-blind methods).
  - Limited performance under high tampering rates.

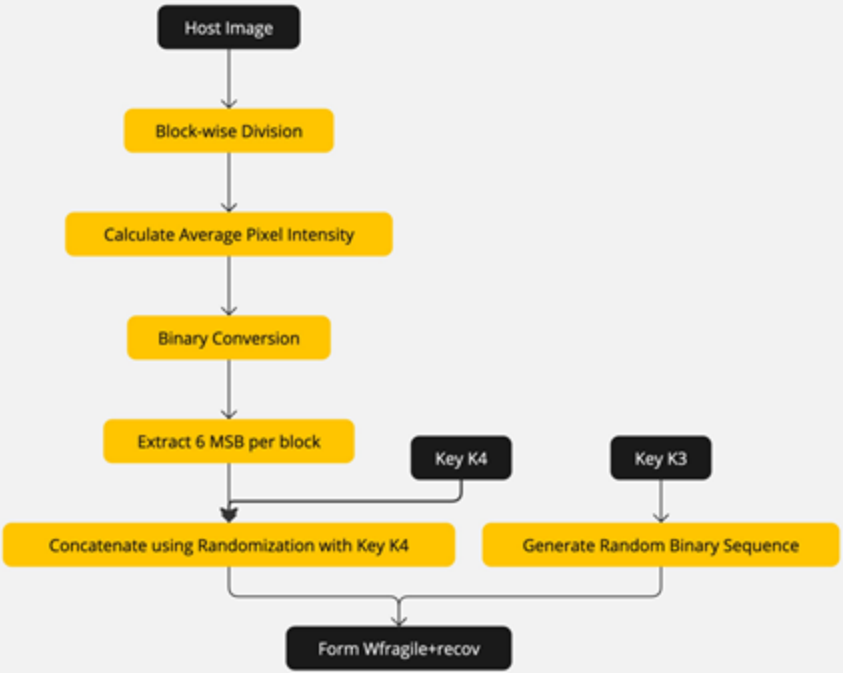
[1]S. Lu, H.Y. Liao, Multipurpose watermarking for image authentication and protection. IEEE Trans.Image Process. 10(10), 1579–1592 (2001)
[2]X. Zhu, A.T. Ho, P. Marziliano, A new semi-fragile image watermarking with robust tampering restoration using irregular sampling. Signal Process. Image Commun. 22(5), 515-528 (2007)
[3]X. Zhang, S. Wang, Fragile watermarking with error-free restoration capability. IEEE Trans. Multimed. 10(8), 1490–1499 (2008)
[4]P. Singh, S. Agarwal, A self recoverable dual watermarking scheme for copyright protection and integrity verification. Multimed. Tools Appl. 76(5), 6389–6428 (2017)

Proposed Method

- Fragile Watermark



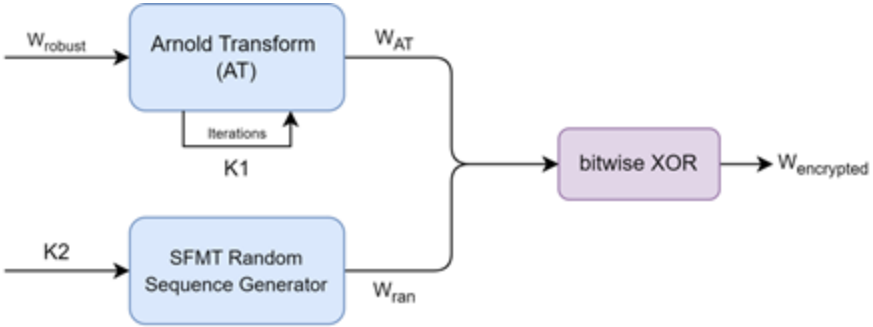
Preparation stage: block partitioning, padding, and watermark generation



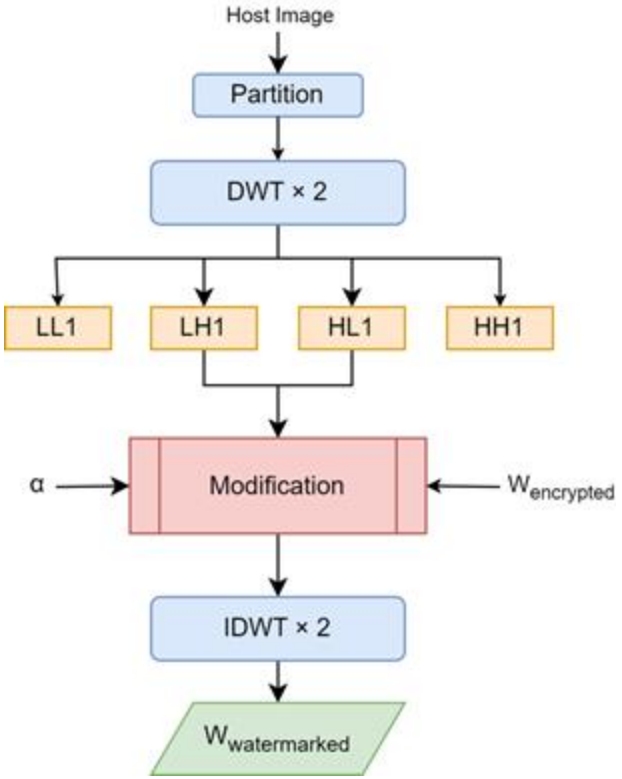
Recovery stage: reconstructing tampered regions using ANBA

Proposed System

- Robust Watermark



Preparation stage: encrypted to enhance security

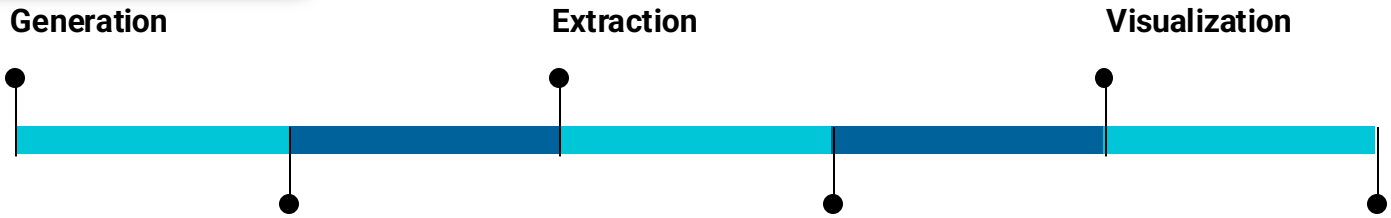


Embedding stage: DWT and IDWT

Results

- System Overview

Add robust watermark embedding mechanism to generate two kinds of watermark.

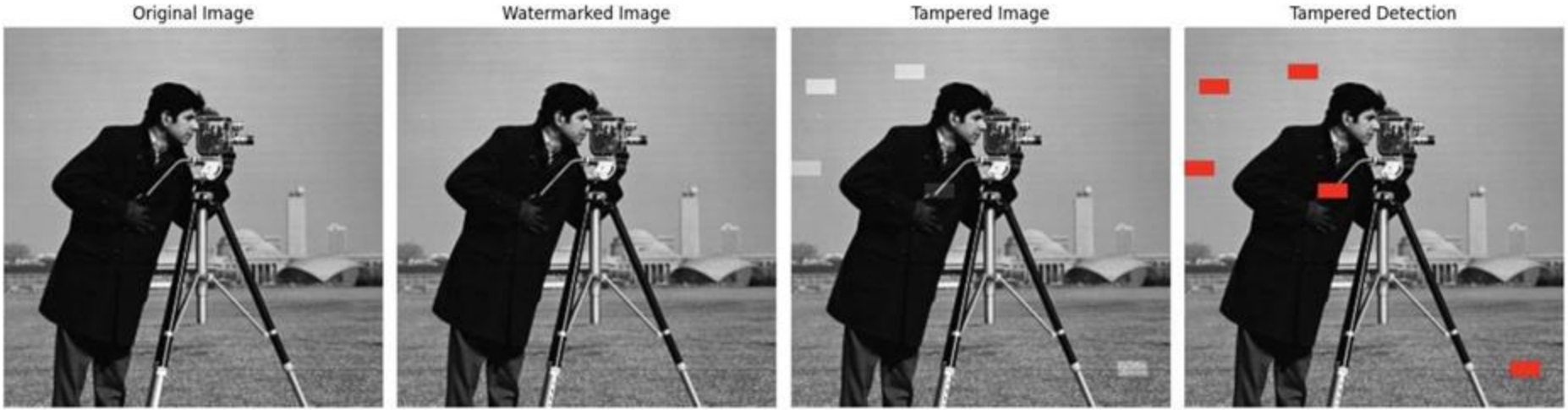


Reconstruct tampered regions using ANBA (Adaptive Neighborhood Block Averaging).

Assess an comprehensive system's performance in embedding, tampering detection, and recovery.

Results

- Watermark Embedding and Tampering Detection



Results

- Image Recovering

Tampered Image

Recovered Image

Results

- Performance Metrics

Image	PSNRwatermark	SSIMwatermark	BER	TDeff	PSNRrecovery	SSIMrecovery
1	38.92	0.9918	0.1170	93.32	35.69	0.9857
2	45.90	0.9963	0.0574	97.01	28.73	0.9815
3	45.92	0.9949	0.1945	93.07	42.03	0.9884
4	44.31	0.9966	0.2201	93.09	36.23	0.9818
5	45.90	0.9980	0.1795	93.06	35.93	0.9826
6	45.91	0.9962	0.1664	92.12	39.94	0.9860
7	45.89	0.9957	0.2205	94.26	36.59	0.9782
8	32.64	0.9637	0.1378	90.34	32.35	0.9589
9	30.75	0.9873	0.1319	92.31	38.56	0.9863
avg	**41.79**	**0.9912**	**0.1583**	**93.18**	**36.23**	**0.9810**

Performance Metrics

Results

- Comparison

Scheme	Watermarked Image Quality	Tamper Detection	Recovery Quality
Proposed Scheme	**PSNR: 41.79 dB SSIM: 0.9912**	**93.18%**	**PSNR: 36.23 dB SSIM: 0.9733 (Tampering Rate ≈ 20%)**
Singh & Agarwal(2021)[1]	PSNR: ≤30 dB	/	Limited to tampering rate <50%
Zhang & Wang(2008)[2]	PSNR: ~28 dB	/	Limited to tampering rate <3.2%
Ansari et al.(2021)[3]	PSNR: ~41 dB	99.80%	Significant recovery up to 80% tampering

Result Comparison

[1]P. Singh, S. Agarwal, A self recoverable dual watermarking scheme for copyright protection and integrity verification. Multimed. Tools Appl. 76(5), 6389–6428 (2017)
[2]X. Zhang, S. Wang, Fragile watermarking with error-free restoration capability. IEEE Trans. Multimed. 10(8), 1490–1499 (2008)
[3]I.A. Ansari, M. Pant, C.W. Ahn, SVD based fragile watermarking scheme for tamper localization and self-recovery. Int. J. Mach. Learn. Cybern. 7(6), 1225–1239 (2016)

Summary

- Addresses limitations of previous schemes.
- Outperforms existing methods in visual quality, robustness, and recovery.
- A balanced solution with imperceptibility, robustness, tamper detection and recovery quality.