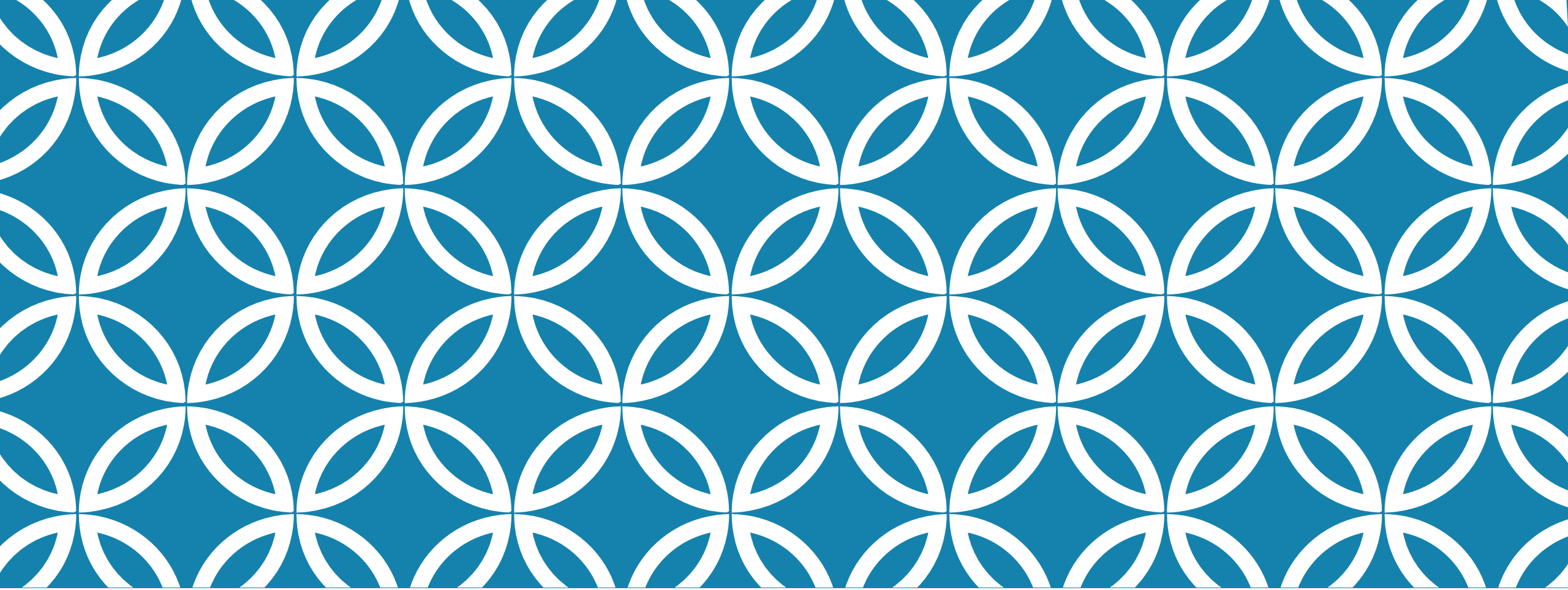


REVERSIBLE WATERMARKING/DATA HIDING

Chi Man Pun
University of Macau

Outline

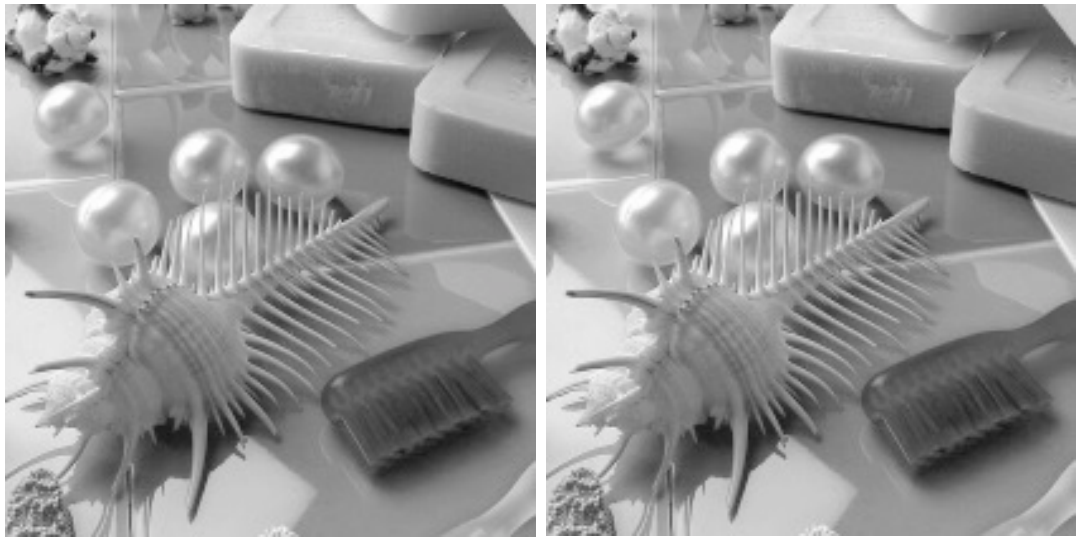
- Introduction of Reversible Watermarking / Data Hiding
- Proposed Reversible Watermarking / Data Hiding Based On Gradient Analysis
- Experimental Results
- Introduction of Reversible Data Hiding in Encrypted Images
- Proposed Reversible Image Reconstruction for Reversible Data Hiding in Encrypted Images
- Experimental Results
- Conclusion

Introduction

My dad has always been a stubborn and introvert guy. He has never been good at socialization. So he deosn't seem to have many friends or other kinds of social resources, which was crucial in the eyes of many people back in 1990s. Natrually he was expelled by his supervisor and lost his job when I was about 6. At that time almost anyone began to look down upon him and blame him for his "bad personality". He didn't argue and focused mainly on assisting me on my studies.

One thing is that he trained himself to be a nutriologist. He planned and made meals for me everyday to guarantee that I could eat well. By the way, I like my father's cooking, especially the pork stew, yummy. During my high school years, I always studied over night. His weekly menu helped me maitain a good condition.

Visible watermarking



(a) Original digital image (b) Watermarked image

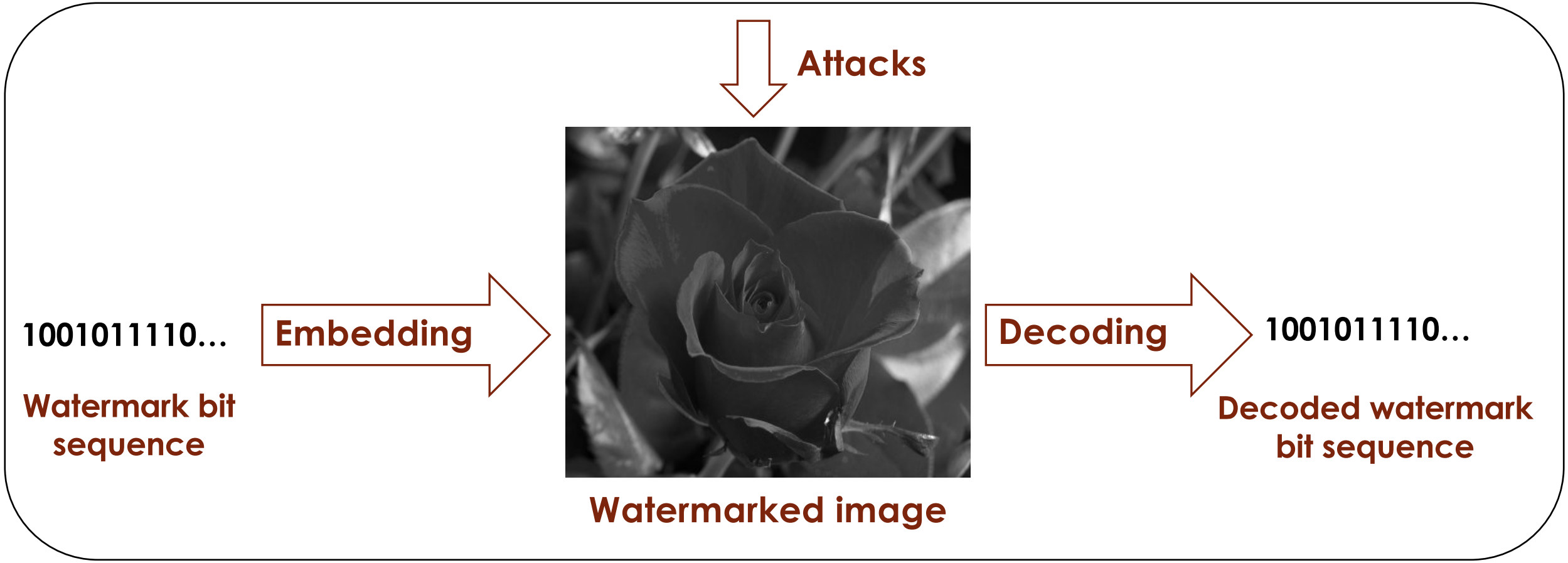
Invisible watermarking / Data Hiding

Introduction

The secret information could be a sequence of binary bits, a QR code, or a small picture logo. Such kind of information would be embedded into the host image through a specific watermarking algorithm, and the embedded secret information cannot be seen in the watermarked image domain.

Introduction

Robust Image Watermarking / Data Hiding



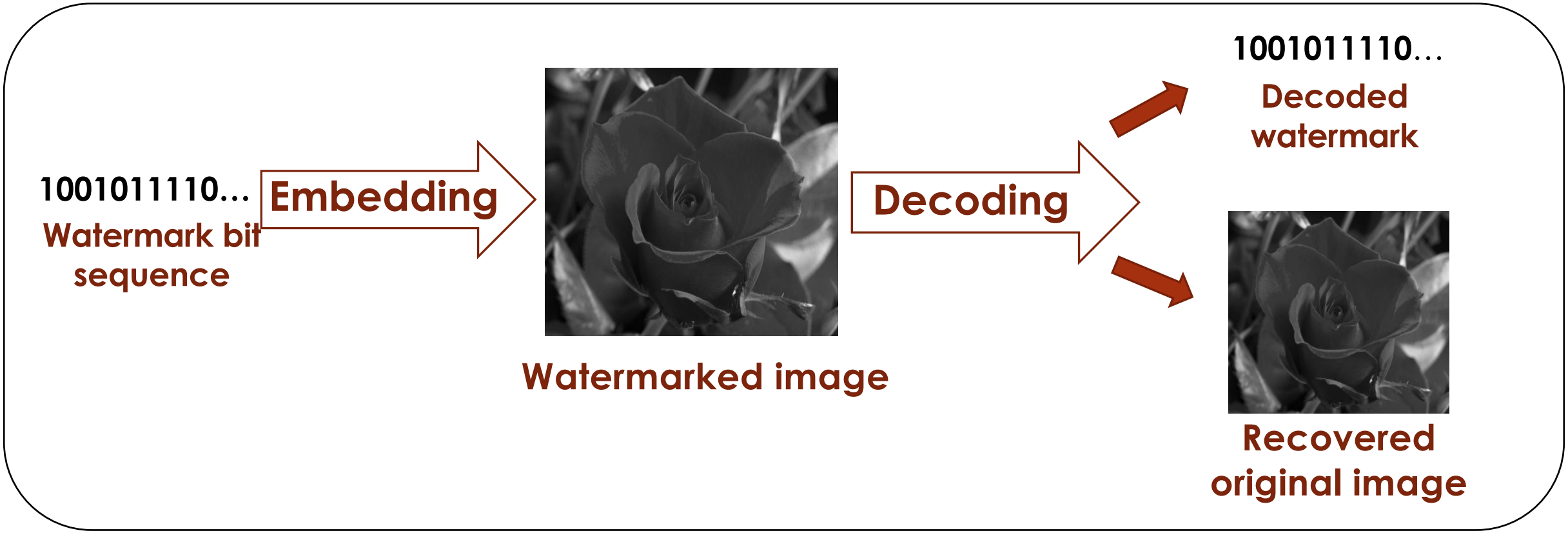
Robust Image Watermarking / Data Hiding

Properties:

- Imperceptibility means that the watermark should be perceptually invisible.
- Security means that the watermark should not be modified/removed by hackers.
- Robustness indicates the correctness of watermark extraction after undergoing different kinds of attacks.

Introduction

Reversible Image Watermarking / Data Hiding



Reversible Image Watermarking / Data Hiding

Properties:

- Imperceptibility means that the watermark should be perceptually invisible.
- Security means that the watermark should not be modified/removed by hackers.
- Reversibility indicates the ability of correct extraction of the embedded information and the recovery of the original host image.

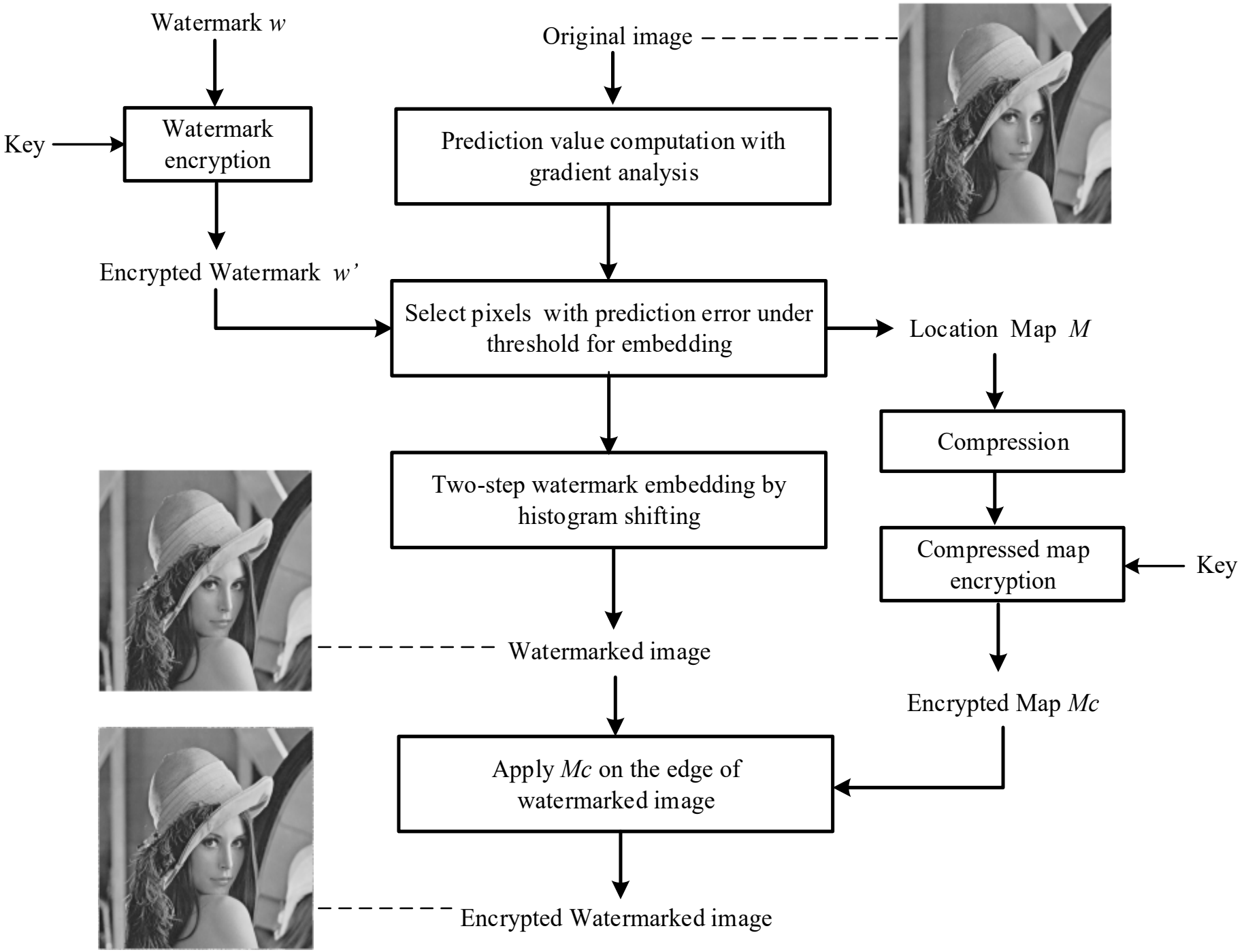
MOTIVATION

- Increasing content is created in digital form;
- Advent of internet / WWW;
- Current copyright laws is inadequate;
- Protect digital contents from illegal actions;
- Used for authentication, attachment of ownership and integrity control;
- Fields of law enforcement, military and medical systems.

Proposed Reversible Watermarking / Data Hiding Based On Gradient Analysis

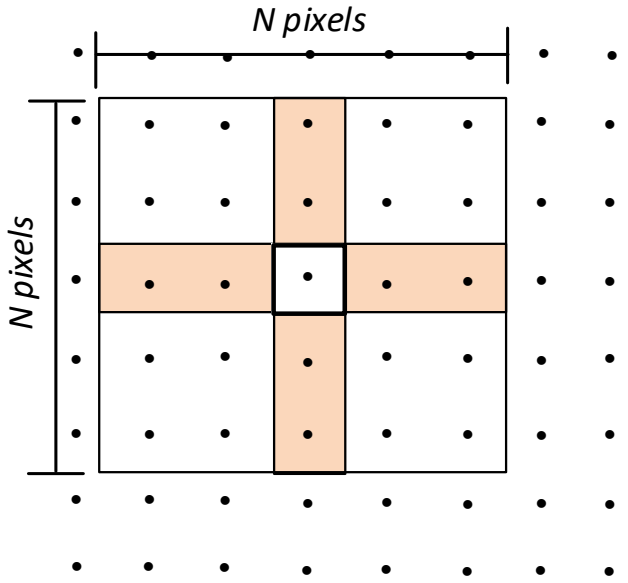
- Prediction value computation
- Watermark embedding based on prediction error expansion

Z. Jiang and **C.-M. Pun**, "Reversible Image Watermarking Using Prediction Value Computation with Gradient Analysis," *Proceedings of the 25th ACM Conference on Computer and Communications Security (CCS) Workshops*, 2018.


Watermark w
Key
Watermark encryption
Encrypted Watermark w'
Original image
Prediction value computation with gradient analysis
Select pixels with prediction error under threshold for embedding
Location Map M
Compression
Compressed map encryption
Key
Encrypted Map Mc
Two-step watermark embedding by histogram shifting
Watermarked image
Apply Mc on the edge of watermarked image
Encrypted Watermarked image

REVERSIBLE WATERMARKING METHOD BASED ON GRADIENT ANALYSIS

Prediction value computation



$N * N$ sliding window for p rediction value computation

$$x_{layern} = \frac{x_{i-(N-1)/2,j-(N-1)/2} + \ldots + x_{i+(N-1)/2,j+(N-1)/2}}{N^2 - 1}$$

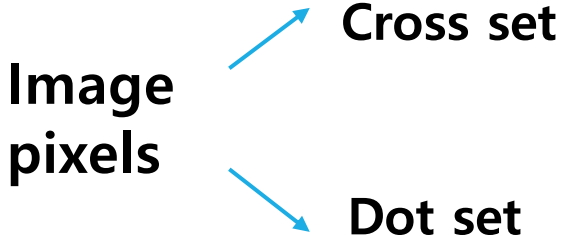
$$\bar{x} = Round\left(\frac{x_{layer1} + x_{layer2} + \ldots + x_{layern}}{n}\right)$$

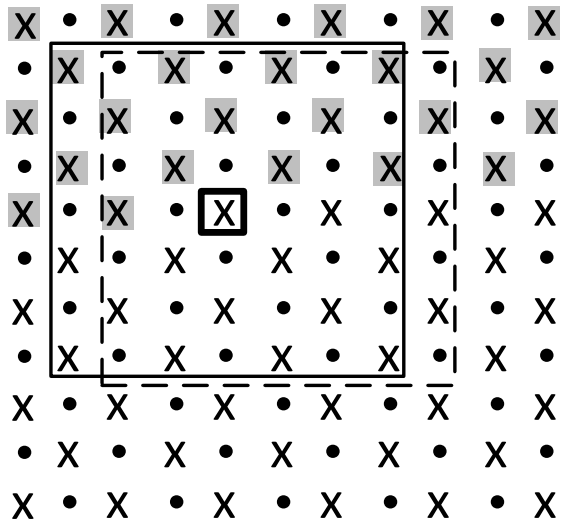
$$g_{i,j} = ac\tan\left(\frac{x_{i,i+1} - x_{i,j}}{x_{i+1,j} - x_{i,j}}\right)$$

$$\hat{x}_{i,j} = \begin{cases} \bar{x} & others \\ \dfrac{x_{i-(N-1)/2,j} + x_{i-(N-1)/2+1,j} + x_{i+(N-1)/2-1,j} + x_{i+(N-1)/2,j}}{N-1} & if\ there\ is\ horizontal\ edge \\ \dfrac{x_{i,j-(N-1)/2} + x_{i,j-(N-1)/2+1} + x_{i,j+(N-1)/2-1} + x_{i,j+(N-1)/2}}{N-1} & if\ there\ is\ vertical\ edge \end{cases}$$

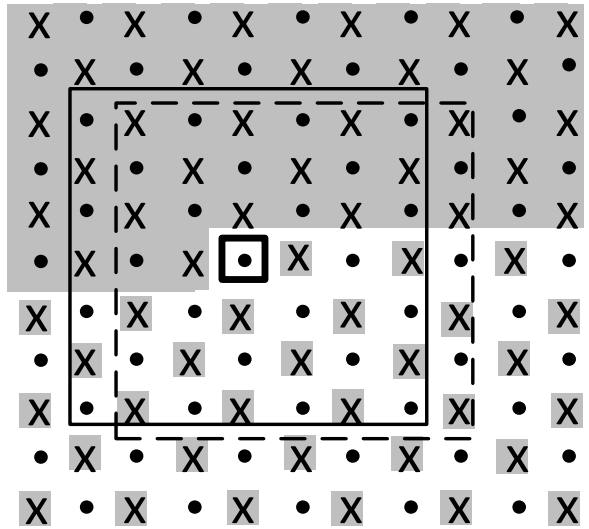
REVERSIBLE WATERMARKING METHOD BASED ON GRADIENT ANALYSIS

Two-step Embedding Process





(a) First embedding process



(b) Second embedding process

REVERSIBLE WATERMARKING METHOD BASED ON GRADIENT ANALYSIS

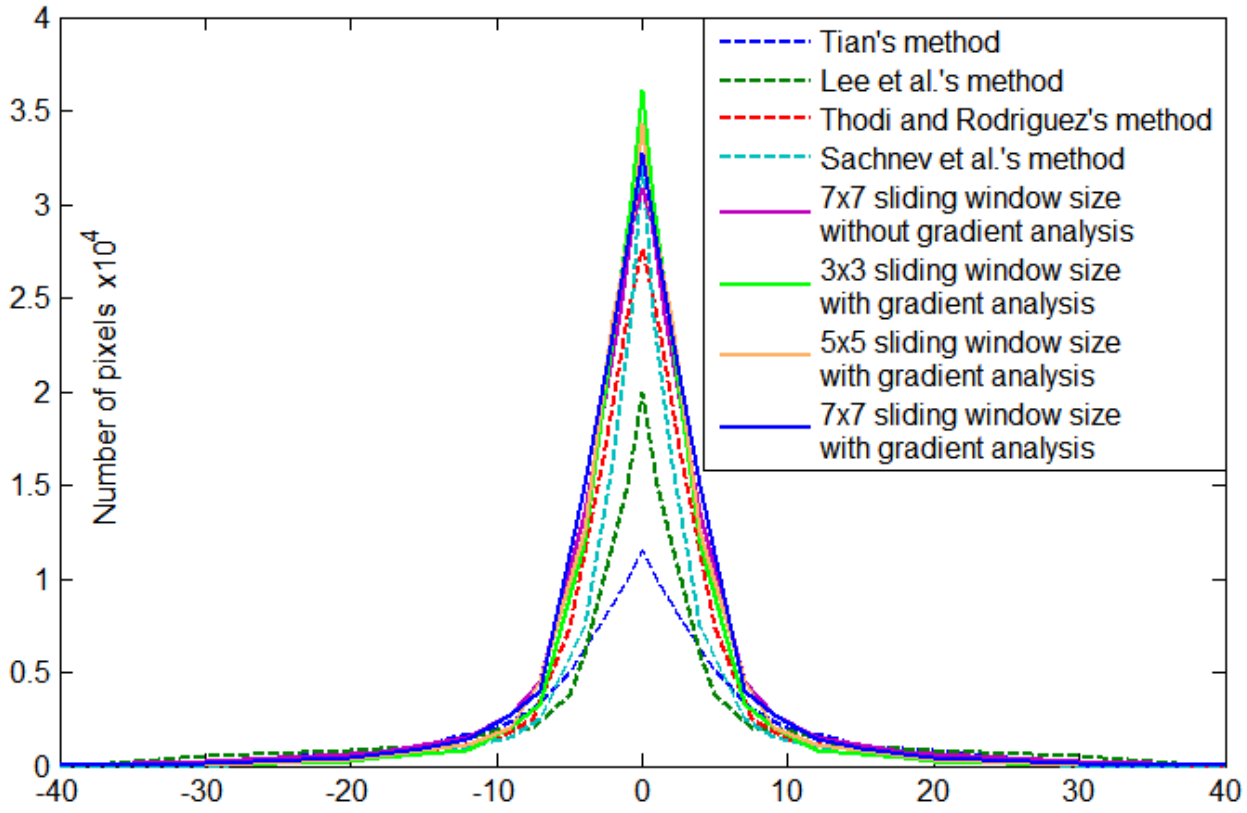
(a) without gradient analysis (b) with gradient analysis

Prediction error distributions

In these testing images, pixels with a prediction error above 5 are pictured using black dots, while those pixels whose prediction error was no greater than 5 are pictured using white dots.

More pixels with small prediction error

REVERSIBLE WATERMARKING METHOD BASED ON GRADIENT ANALYSIS



Prediction error distributions of proposed method and other methods

REVERSIBLE WATERMARKING METHOD BASED ON GRADIENT ANALYSIS

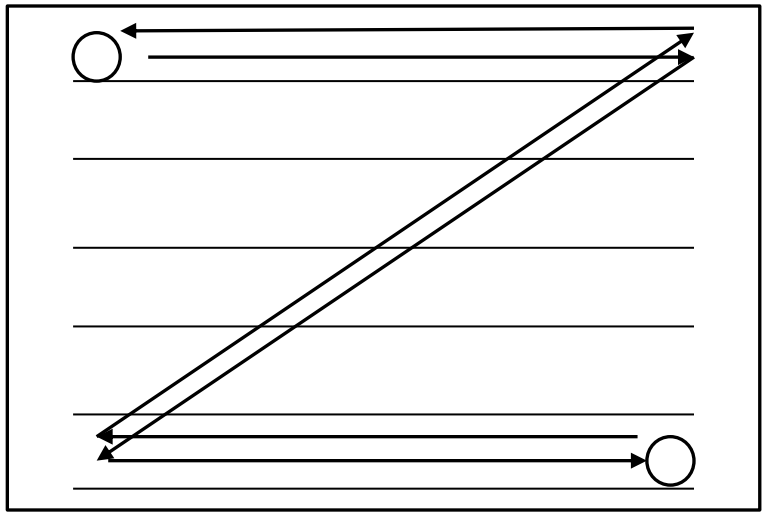
Reversible Watermark Embedding and Decoding

The watermark extraction and original pixel recovery should be processed in reverse order of the embedding process.

$$e_{i,j} = x_{i,j} - \hat{x}_{i,j}$$

$$E_{i,j} = 2 \cdot e_{i,j} + d$$

$$\begin{aligned} X_{i,j} &= \hat{x}_{i,j} + E_{i,j} \\ &= \hat{x}_{i,j} + 2 \cdot e_{i,j} + d \\ &= x_{i,j} + e_{i,j} + d \end{aligned}$$



$$E_{i,j} = X_{i,j} - \hat{x}_{i,j}$$

$$d = E_{i,j} \bmod 2$$

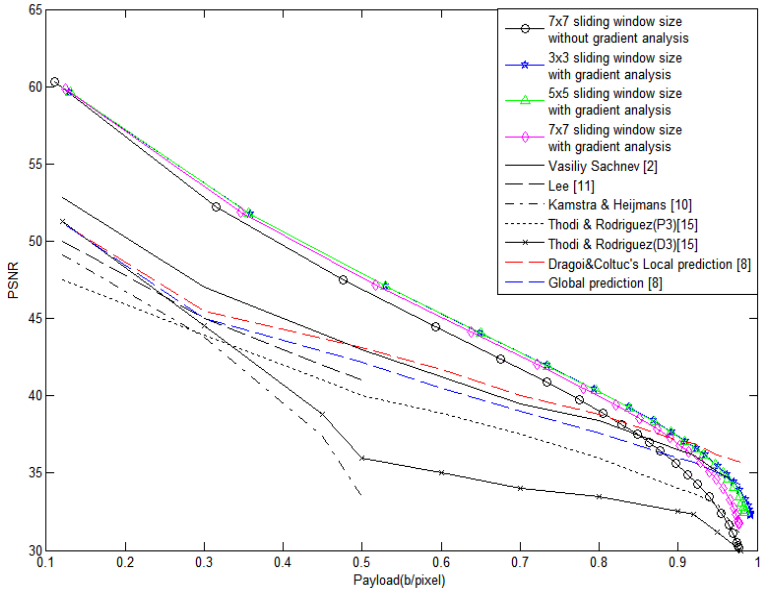
$$e_{i,j} = \left\lfloor \frac{E_{i,j}}{2} \right\rfloor$$

$$x_{i,j} = \hat{x}_{i,j} + e_{i,j}$$

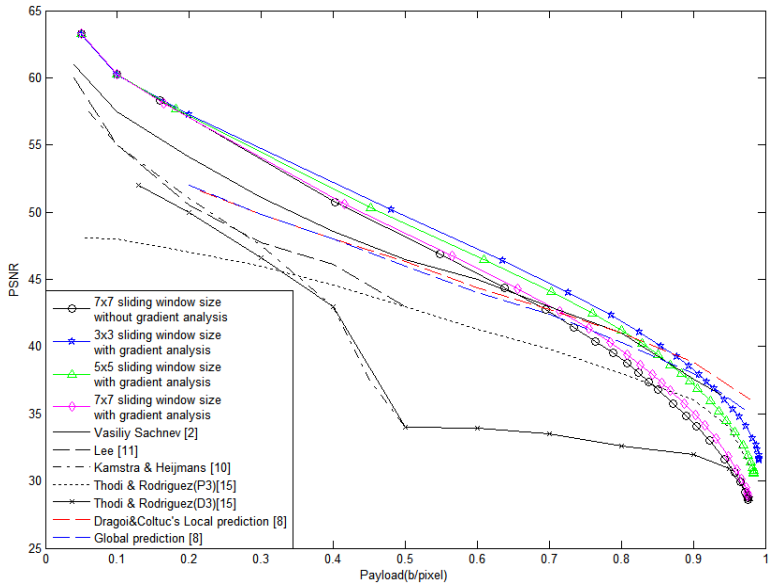
- ✓ Both of the watermark ***d*** and pixel information ***x(i,j)*** are embedded
- ✓ watermark ***d*** is decoded
- ✓ original pixel ***x(i,j)*** is recovered

Experimental Results

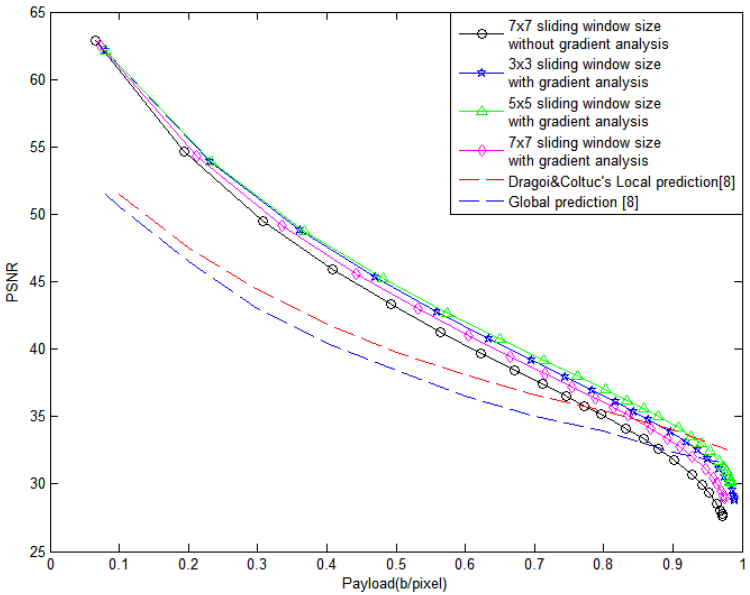
Results for Reversible Watermarking Method Based on Gradient Analysis



Lena



Jetplane



Boat

Image quality (PSNR) compared with other reversible watermarking methods

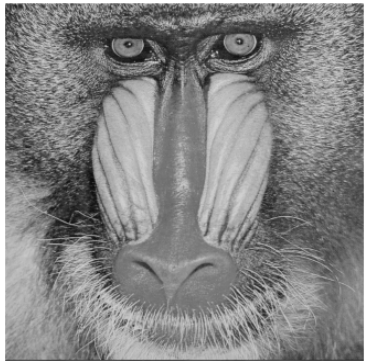
5x5 size sliding window
10,000 watermark bits

(a1) original image

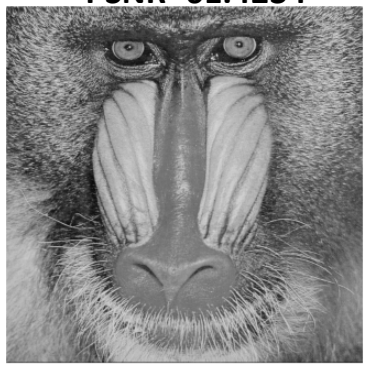
(a2) watermarked image
PSNR=61.4234

(b1) original image

(b2) watermarked image
PSNR=61.5728



(c1) original ima



(c2) watermarked image
PSNR=60.8011

(d1) original image

(d2) watermarked image
PSNR=60.7563

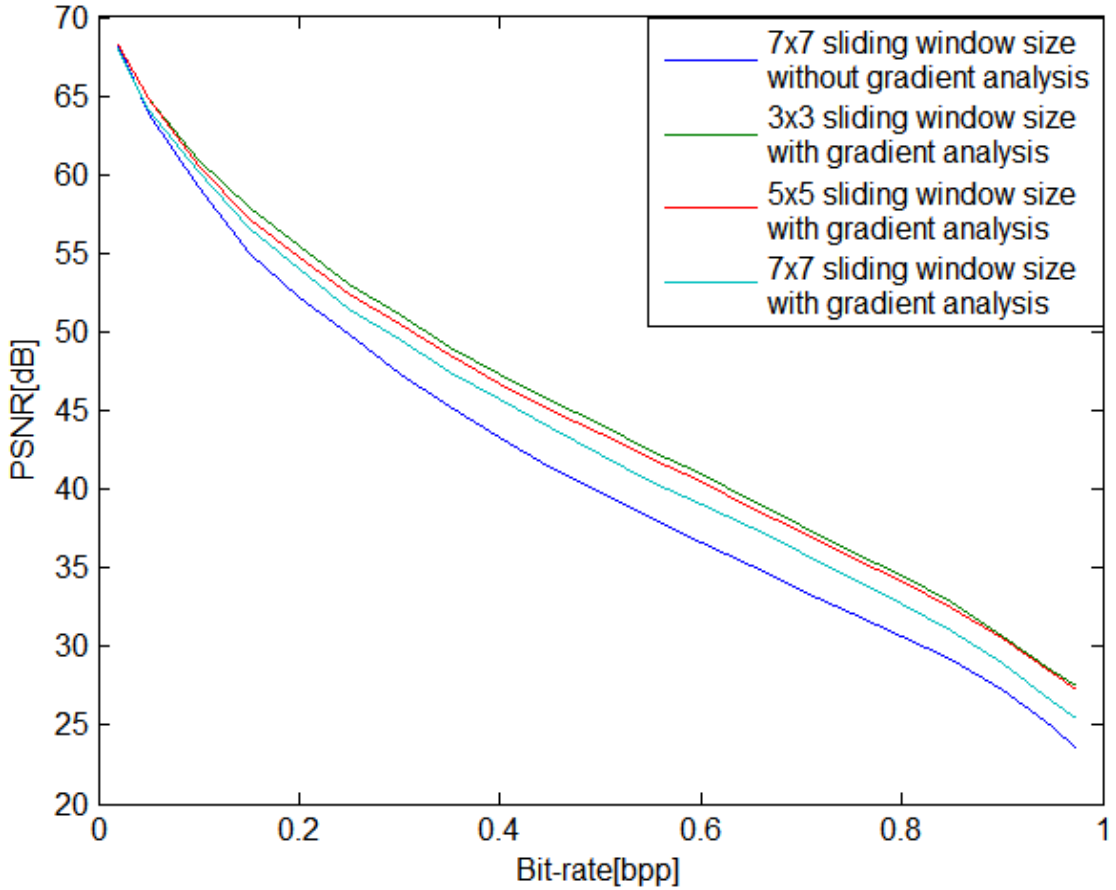
(e1) original image

(e2) watermarked image
PSNR=61.6829

(f1) original image

(f2) watermarked image
PSNR=61.0925

Results for Reversible Watermarking Method Based on Gradient Analysis



Average image quality under different embedding bit-rate

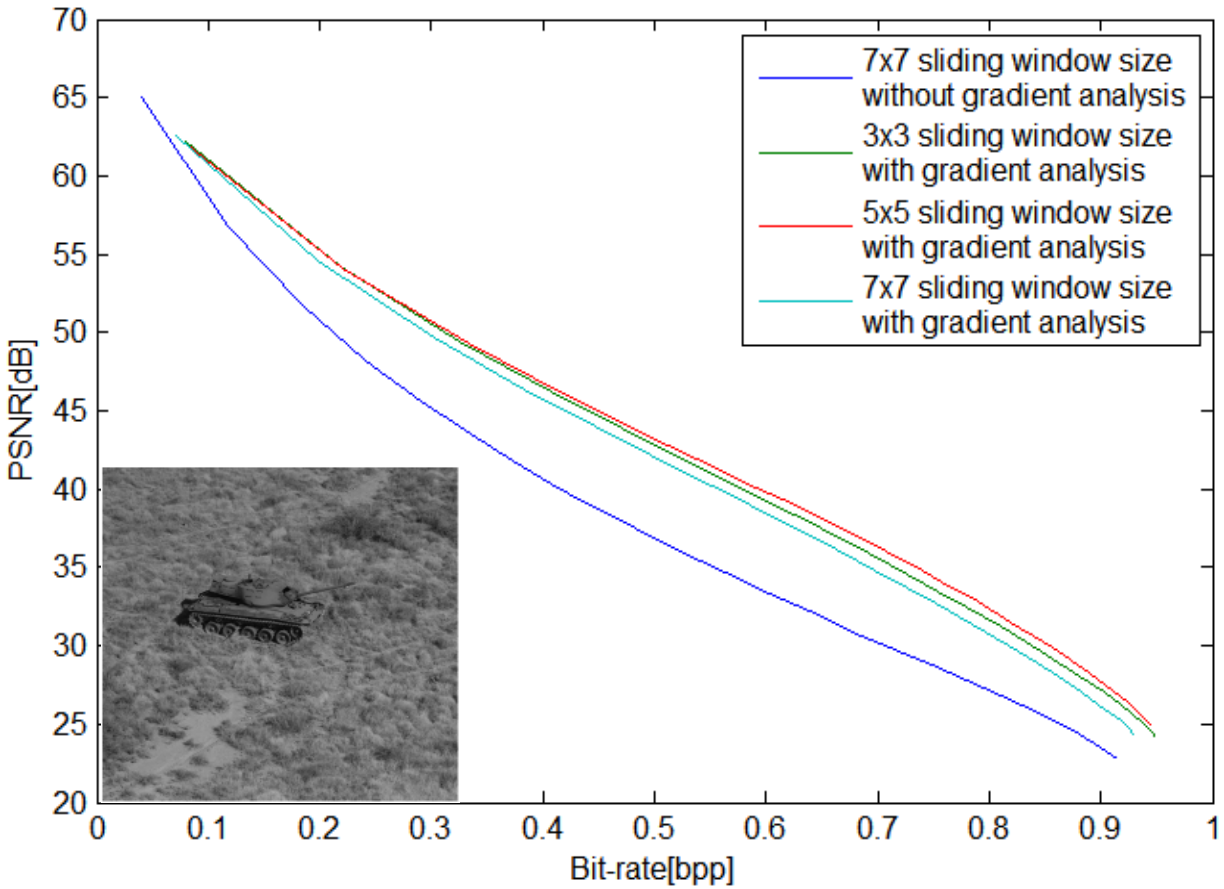
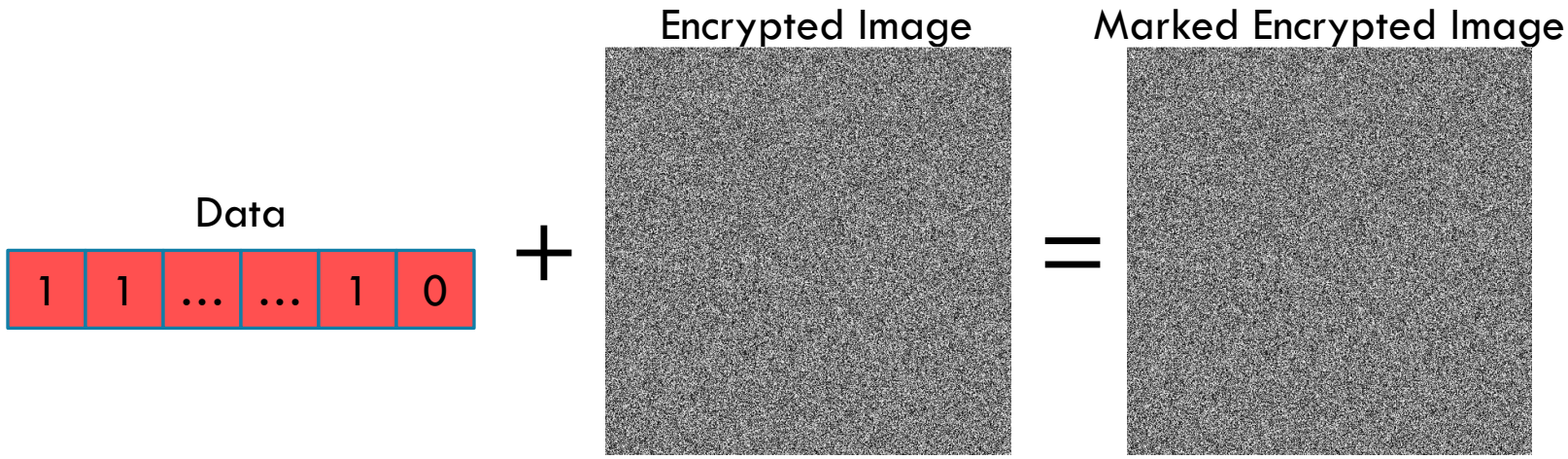


Image quality of ‘tank’ under different embedding bit-rate

REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES

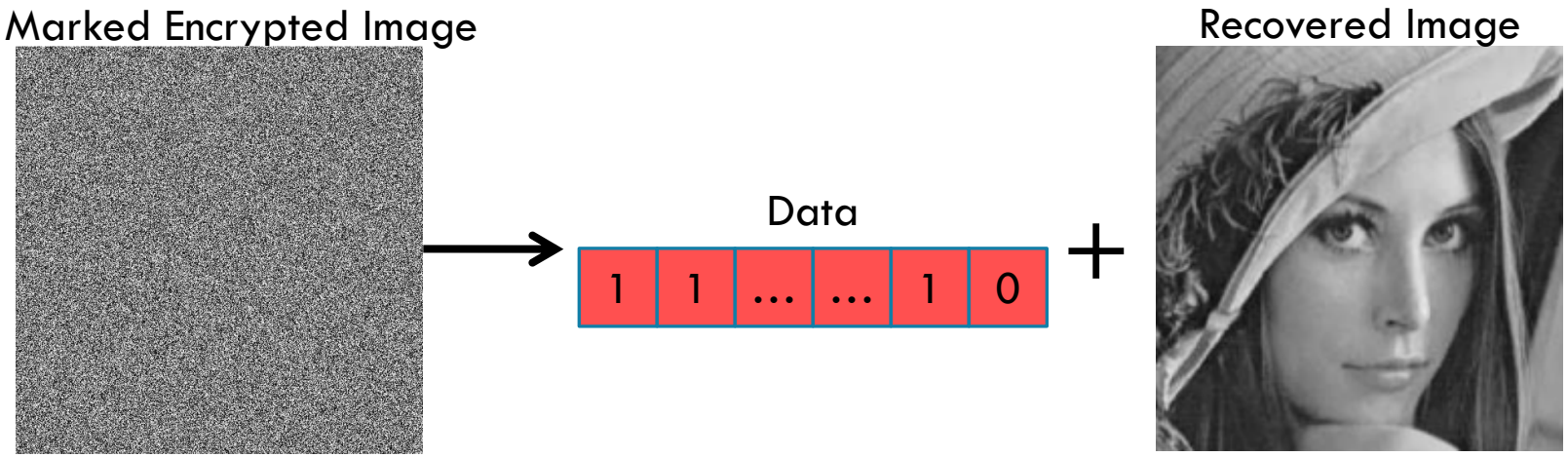
- What's reversible data hiding in encrypted images (RDHEI) ?
  - The object of RDH is an encrypted image.



Embedding process

REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES

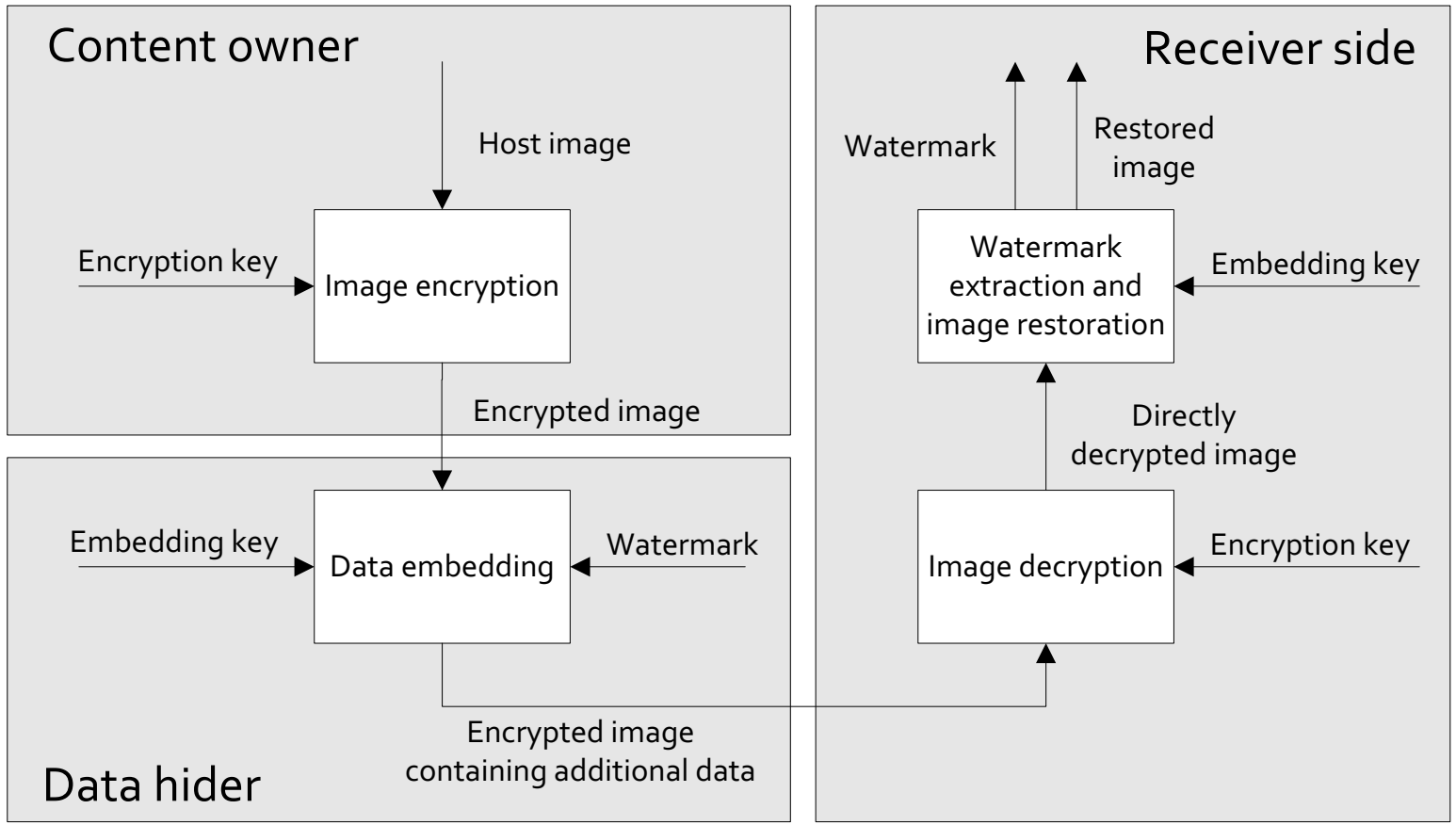
- What's reversible data hiding in encrypted images (RDHEI) ?
  - The object of RDH is an encrypted image.



The reversible process

REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES

- Image confidentiality and privacy protection
- Content owner encrypts host image
- Inferior assistant appends additional information
- Authorized party decrypt image and retrieve watermark



APPLICATIONS

- Medical image data center

A doctor wants to protect the privacy of his/her patient in a medical image. This can be realized by encryption.

A server of this center can embed some notations into the encrypted medical image to manage it. The server has been unable to know the content of the medical image.

CHALLENGES

- While obtaining a sufficiently smooth rearranged image, the amount of auxiliary data generated should not be too large;
- Ensuring the Security of Encrypted Images.

RELATED WORKS

- W. Zhang, H. Wang, D. Hou, and N. Yu, "Reversible data hiding in encrypted images by reversible image transformation," IEEE Trans. Multimedia, vol. 18, no. 8, pp. 1469-1479, Aug. 2016.

The original image is first transformed into an image similar to target image, and then traditional RDH algorithms can be employed to embed additional data into the transformed image

RELATED WORKS

- X. Cao, L. Du, X. Wei, D. Meng, and X. Guo, “High capacity reversible data hiding in encrypted images by patch-level sparse representation,” IEEE Trans. Cybernetics, vol. 46, no. 5, pp. 1132-1143, May. 2016.

A large vacated room is generated by using a patch-level sparse representation technique, and then after encryption the previously vacated room could be used to accommodate additional data.

RELATED WORKS

- S. Yi, and Y. Zhou, “Binary-block embedding for reversible data hiding in encrypted images”, Signal Process., Vol. 133, pp. 40-51, Apr. 2017.

The original image is first divided into blocks, and then classified into good group and bad group. Additional data is embedded by compressing the blocks in the good group.

RELATED WORKS

- C. Qin, W. Zhang, F. Cao, X. Zhang and C. -C. Chang, "Separable reversible data hiding in encrypted images via adaptive embedding strategy with block selection", Signal Process., Vol. 153, pp.109-122, Dec. 2018.

An analogues stream-cipher and block permutation method are used to encrypt blocks of the original image, then the encrypted blocks can be classified into smooth blocks and complex blocks, finally, additional data can be embedded by compressing LSBs of the smooth blocks.

RELATED WORKS

- Q. Li, B. Yan, H. Li, and N. Chen, “Separable reversible data hiding in encrypted images with improved security and capacity”, Multimed Tools Appl., Vol. 77, no. 23, pp.30749-30768, Dec. 2018.

A block permutation and a stream cipher combined encryption method is designed, bit replacement in prediction error is introduced to improve the embedding rate.

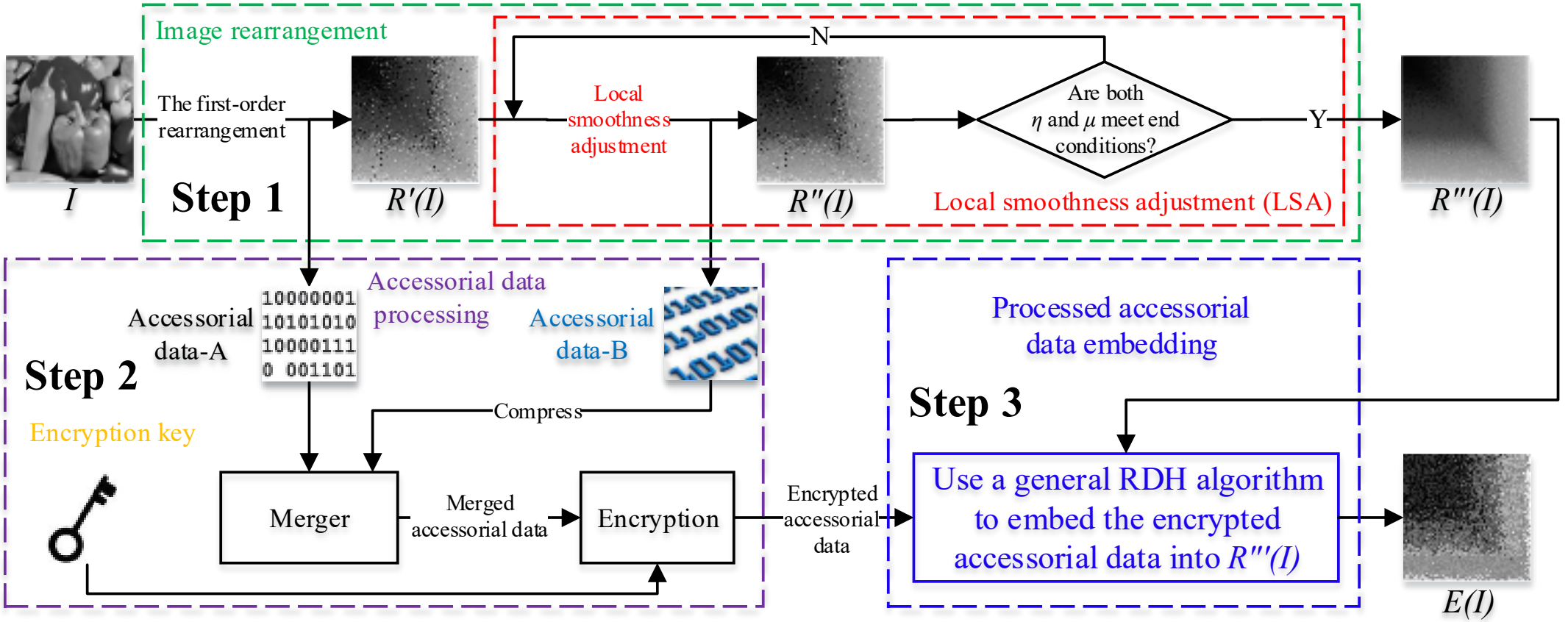
PROPOSED METHOD

– The main idea:

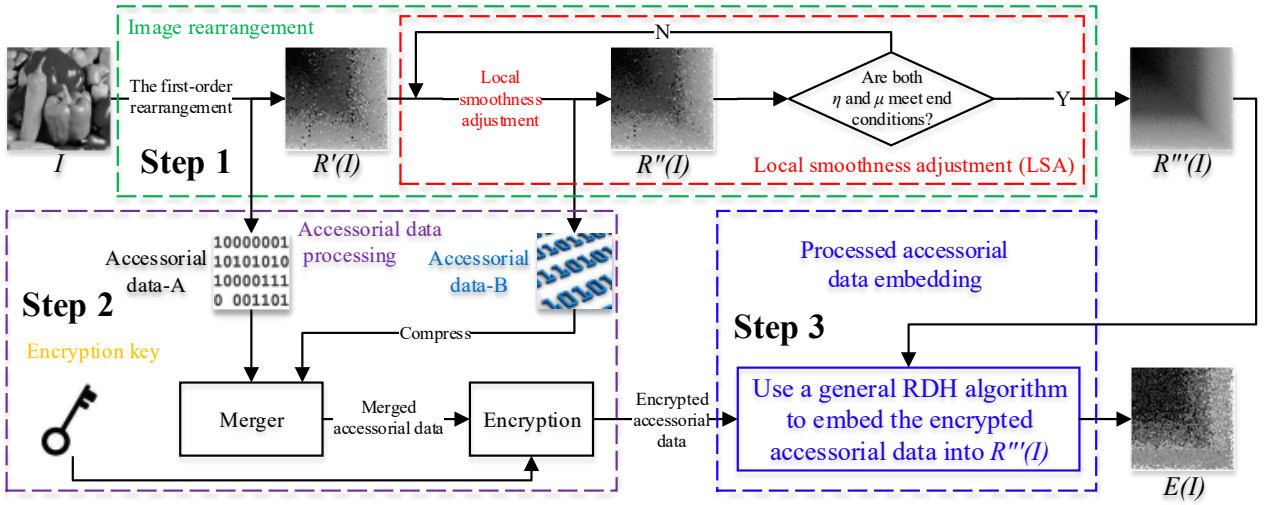
- We try to realize RDHEI framework by reversible image reconstruction (RIR).
- RIR rearranges the original image to construct a redundancy image and the meaningful information of the original image will become invisible at the same time.
- This rearranged image will be used as encrypted image, so RDH into this encrypted image becomes very easy and more additional data can be embedded.

PROPOSED METHOD

– The whole flowchart of RIR



PROPOSED METHOD

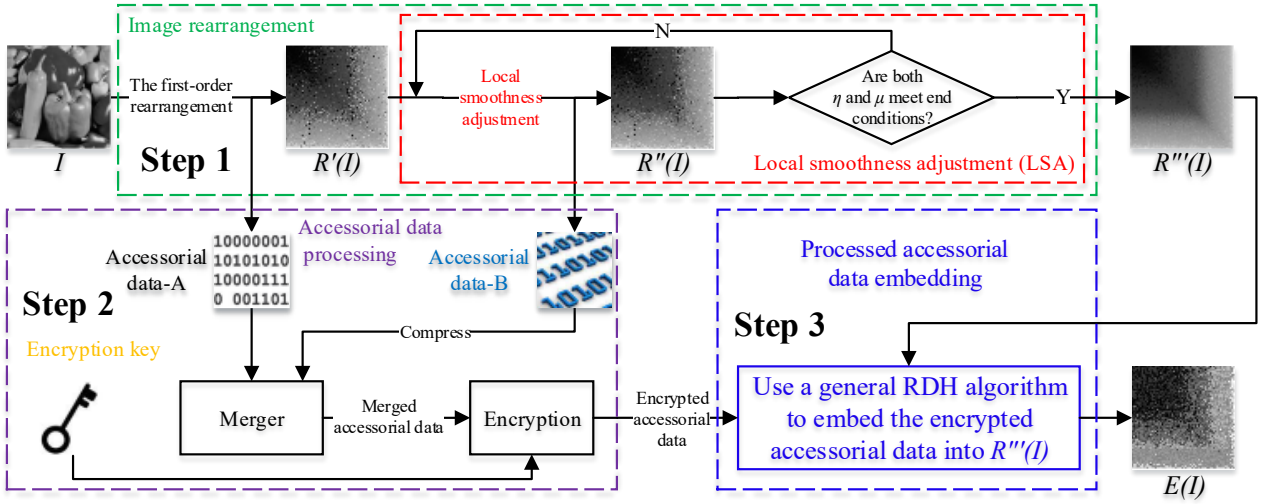


– Step 1- Image rearrangement

- This step includes two phases: the first-order rearrangement and local smoothness adjustment (LSA)*.
- The first-order rearrangement will try to make the whole image pixels distributed from small to large; however, in the output of this step, there are still large pixels distributed among small pixel and small pixels distributed among large pixel.
- In order to settle this problem, we design LSA mechanism, which adjusts the smooth extent of small regions.

*Z.-L. Liu and **C.-M. Pun**, "Reversible image reconstruction for reversible data hiding in encrypted images," *Signal Processing,* 161, pp. 50-62, 2019.

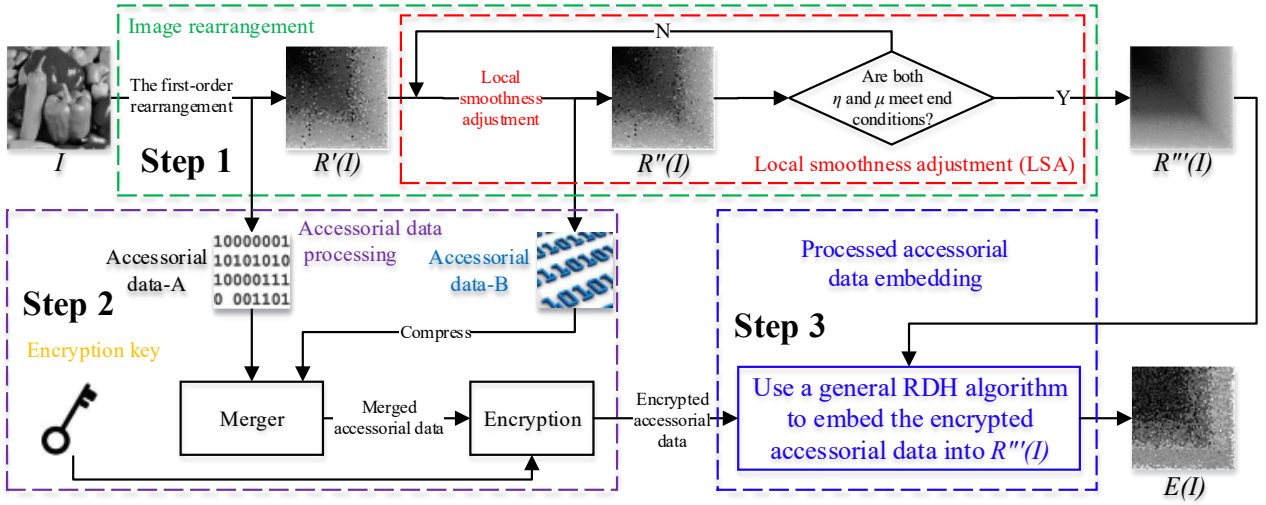
PROPOSED METHOD



– Step 2- Accessorial data processing

- Accessorial data is generated in RIR and used to losslessly recover I.
- This step will compress these accessorial data, merge them into a whole sequence and then encrypt the sequence to enhance security.

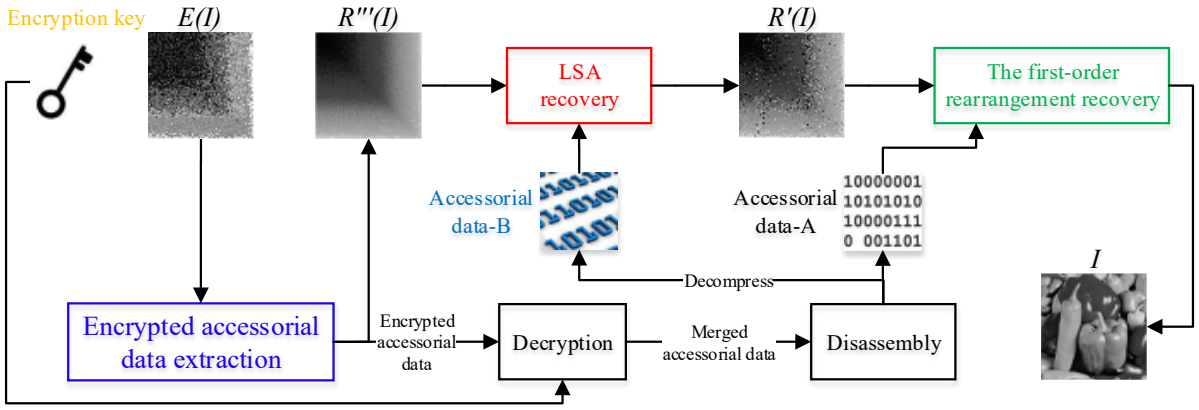
PROPOSED METHOD



– Step 3- Processed accessorial data embedding

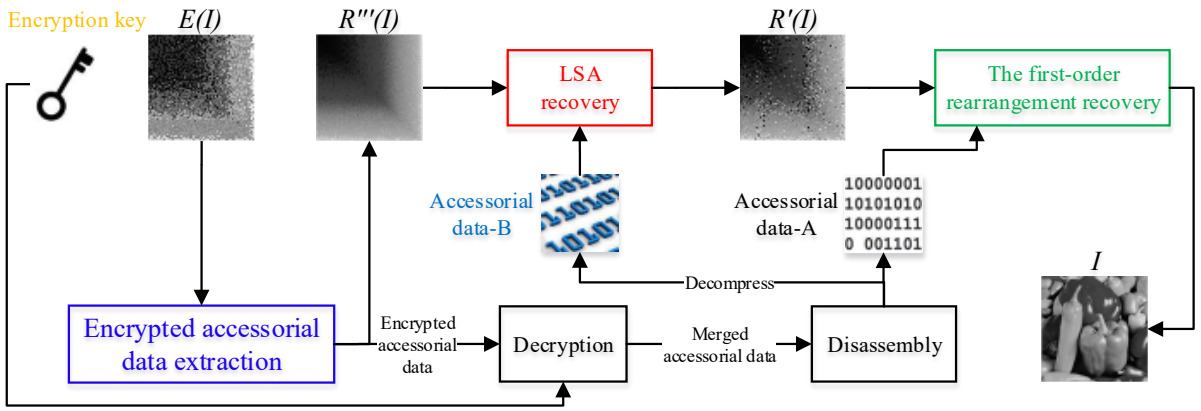
- The encrypted accessorial data (EAD) will be embedded into R'''(I) to generate the encrypted image E(I).
- Note that the process of EAD embedding can be realized by employing any general plaintext RDH algorithm.
- By doing all the above operations, the original image turns into an image that is meaningless but rich in redundancy, the privacy in the original image is also protected, and anyone, without encryption key, cannot access the content of the original image.

RECOVERY PROCESS OF RIR



- In order to recovery I from E(I), the authorized receiver first extracts encrypted accessorial data from E(I), and R'''(I) is generated at the same time.
- Secondly, she/he decrypts the encrypted accessorial data with the encryption key to get the merged accessorial data.

RECOVERY PROCESS OF RIR



- Thirdly, the authorized receiver decompresses the merged accessorial data (if necessary), and further disassembles the merged accessorial data into accessorial data-A and accessorial data-B.
- Fourthly, R'''(I) will be rearranged according to the records in accessorial data-B. Actually, this is the reverse process of LSA, and the final output of this step will be R'(I).
- Finally, I will be losslessly recovered by using accessorial data-A to restore R'(I).

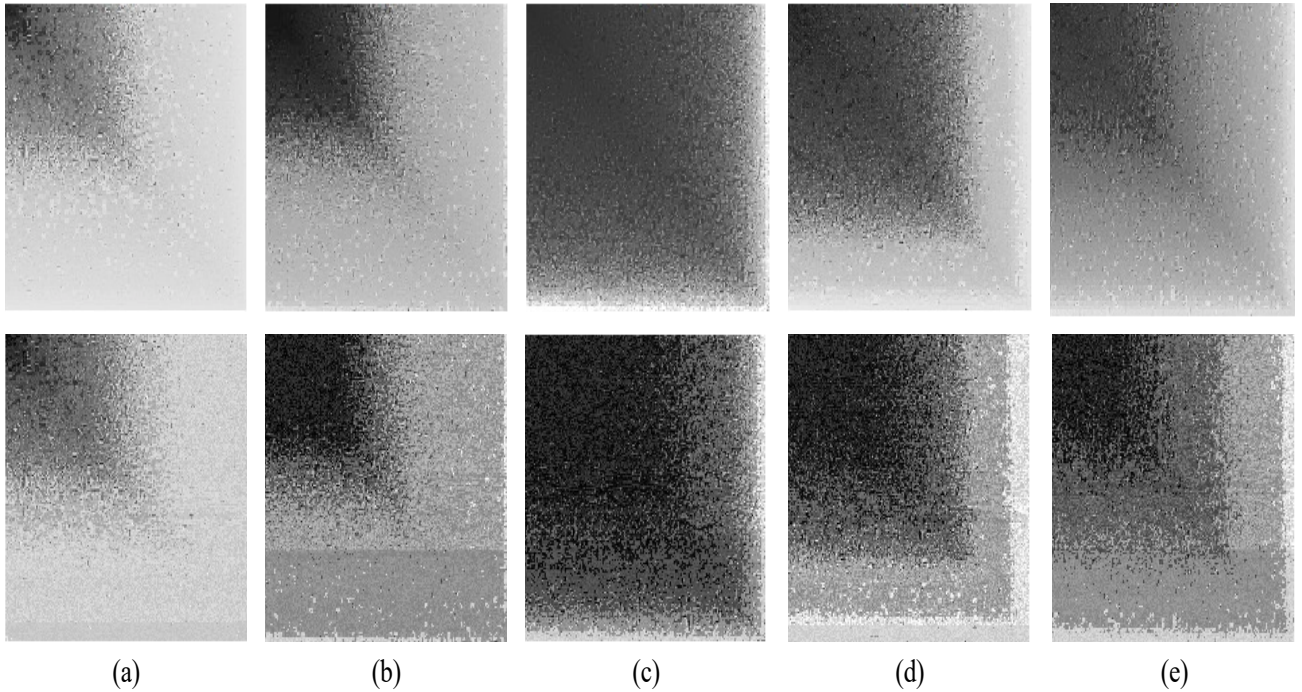
RESULTS

– Experiments of reversible image reconstruction

(a) (b) (c) (d)

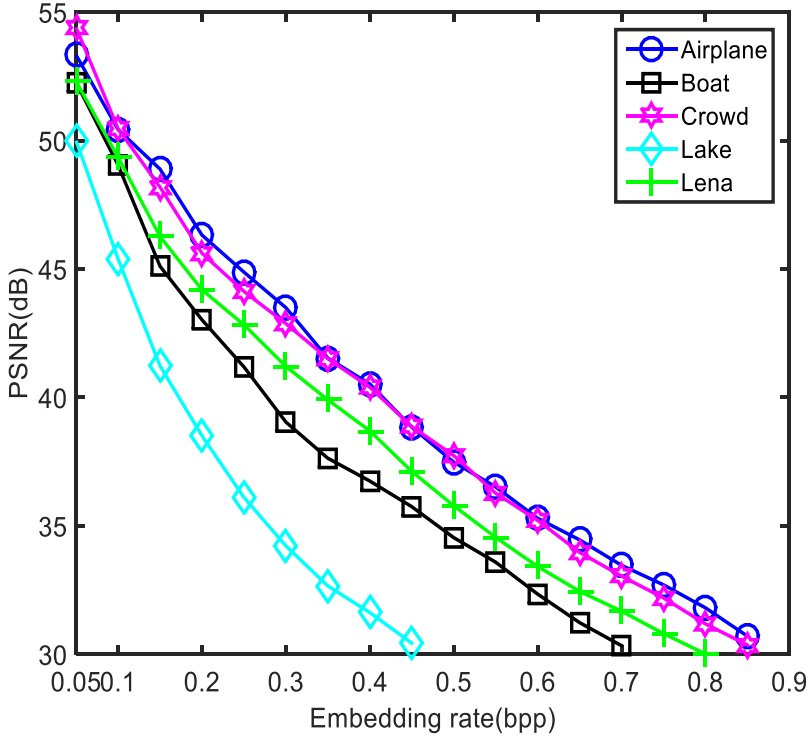
The overall process of RIR. (a) The original image. (b) The encrypted image. (c) The recovered image with right key. (d) The recovered image with wrong key.

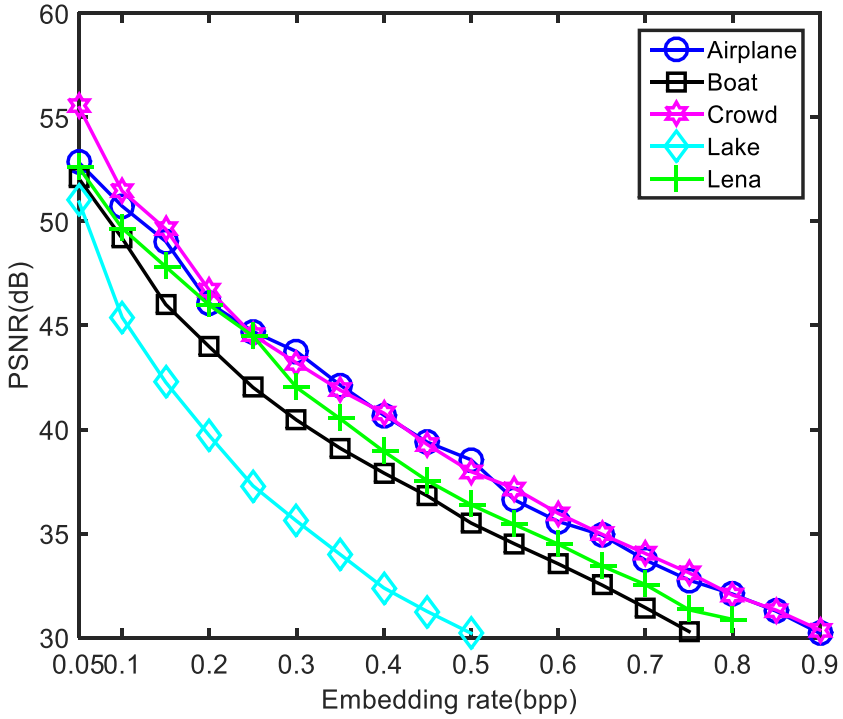
RESULTS



Results of testing RIR. (a) Airplane. (b) Boat. (c) Crowd. (d) Lake. (e) Lena. The first row is R'''(I) that generated in image rearrangement phase, the second row is the encrypted image that is outputted by RIR.

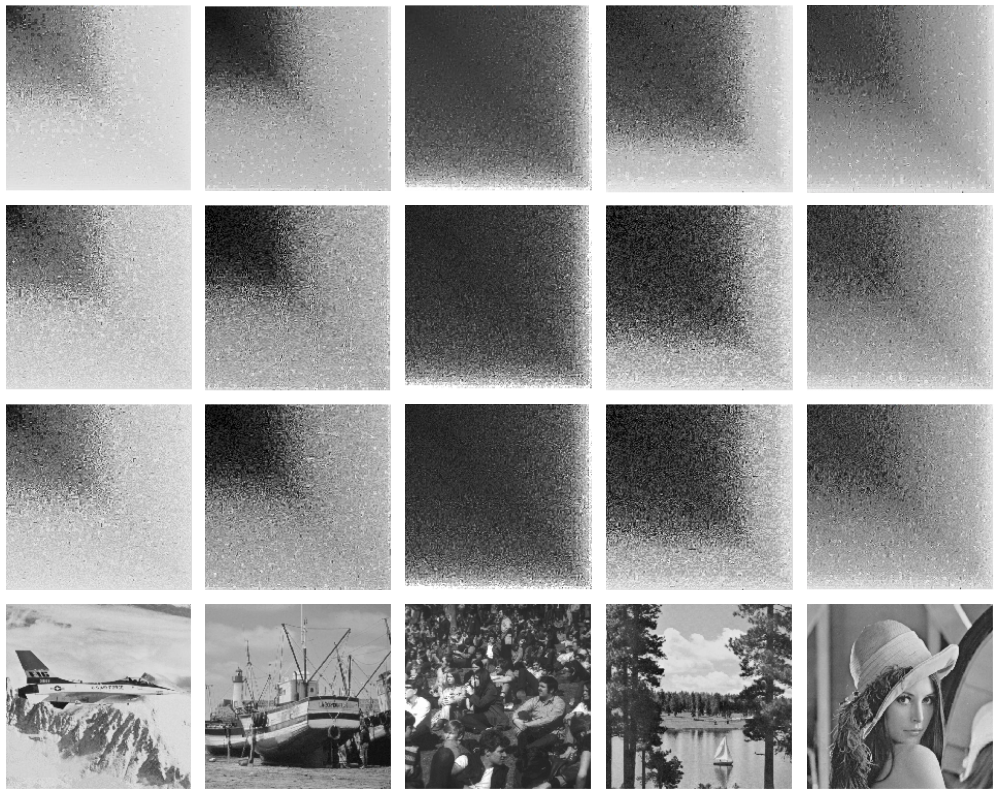
RESULTS





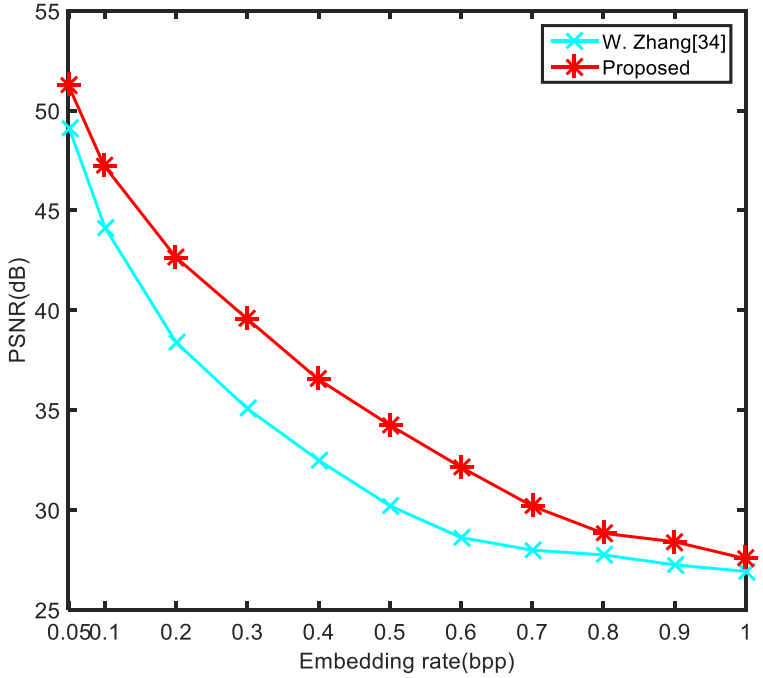
Results of individual test. (a) Results for (α, β) is set to (200, 20). (b) Results for (α, β) is set to (230, 23).

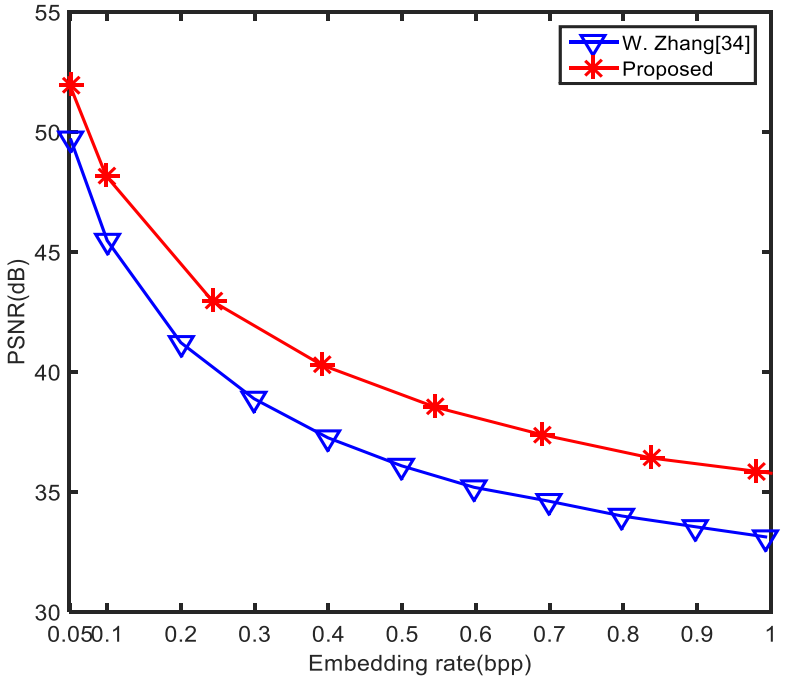
RESULTS



The encrypted image and the marked encrypted image. (a) Airplane. (b) Boat. (c) Crowd. (d) Lake. (e) Lena. The first row is the encrypted image, the second row is the marked encrypted image obtained when (α, β) is set to (200, 20), the third row is the marked encrypted image obtained when (α, β) is set to (230, 23), and the fourth row is the directly decrypted image when (α, β) is set to (230, 23). From left to right, embedding rates of the second row marked encrypted images respectively are 0.85 bpp, 0.7 bpp, 0.85 bpp, 0.45 bpp and 0.8 bpp; and 0.9 bpp, 0.75 bpp, 0.9 bpp, 0.5 bpp and 0.8 bpp for the third row.

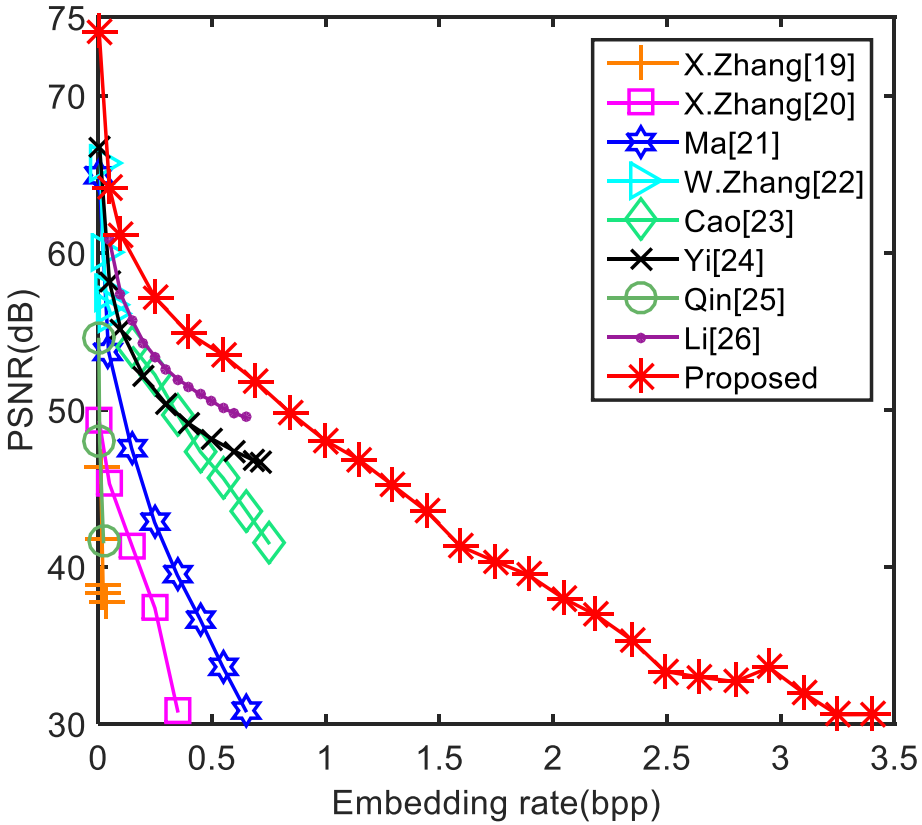
RESULTS





The average performance comparison between [34] and the proposed RIR based scheme. (a) RDH method [11] is employed to embed *EAD* and additional data. (b) RDH method [12] is employed to embed *EAD* and additional data.

RESULTS



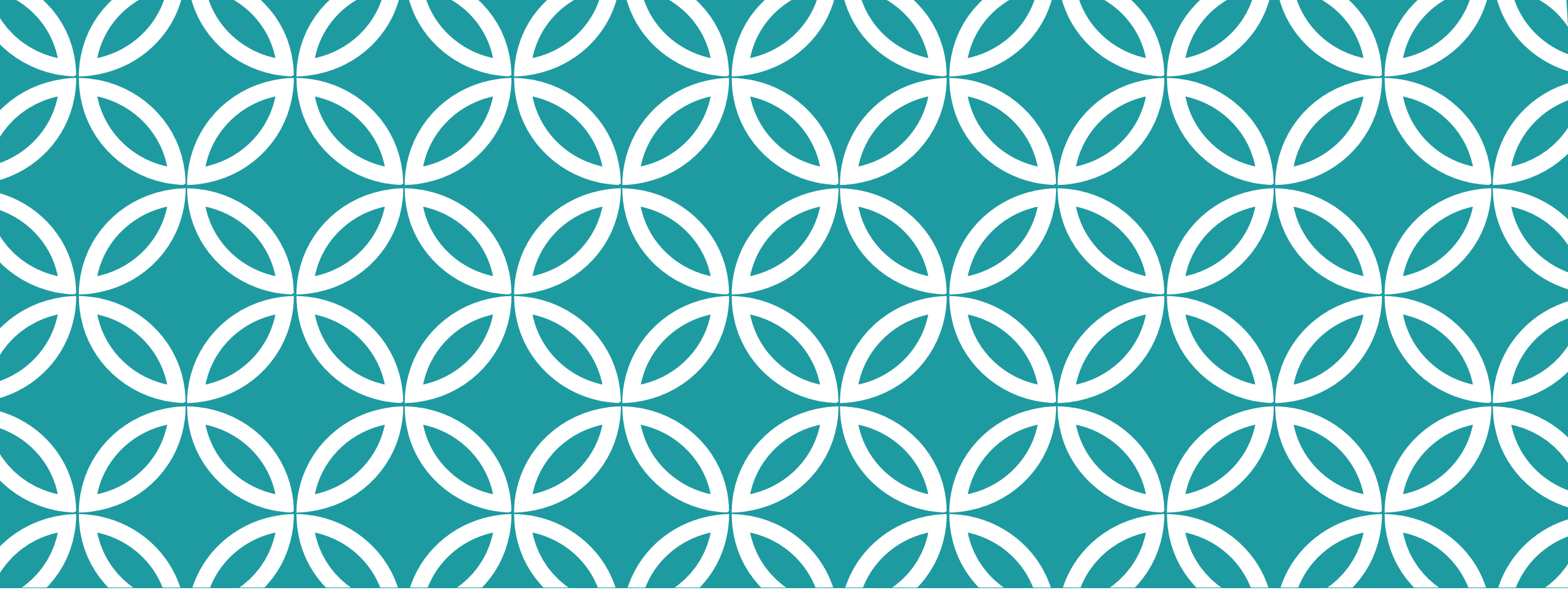
The average performance comparison between some previous RDHEI algorithms and the proposed RIR based scheme by employing RDH method in [27] to embed *EAD* and additional data.

CONCLUSION

- We plan to propose a novel framework by reversible image reconstruction (RIR), which means rearranging the original image to construct a redundancy image.
- By RIR, the original image will change into a meaningless rearranged image, and the privacy of the original image will be protected.
- Of course, the statistical characteristics of the rearranged image will be different from that of the original image.
- With using this rearranged image as an encrypted image, any general RDH algorithm for plain image can be employed to embed additional data, and a high performance can be expected.

PUBLICATIONS

- Z.-L. Liu and **C.-M. Pun**, "Reversible image reconstruction for reversible data hiding in encrypted images," *Signal Processing,* 161, pp. 50-62, 2019.
- Z.-L. Liu and **C.-M. Pun**, "Reversible data-hiding in encrypted images by redundant space transfer," *Information Sciences*, 433, pp. 188-203, 2018.
- Z. Jiang and **C.-M. Pun**, "Reversible Image Watermarking Using Prediction Value Computation with Gradient Analysis," *Proceedings of the 25th ACM Conference on Computer and Communications Security (CCS) Workshops*, 2018.



THE END! THANK YOU!