Kaili QI, Minqing ZHANG, Fuqiang DI, Yongjun KONG, 2023. High capacity reversible data hiding in encrypted images based on adaptive quadtree partitioning and MSB prediction. *Frontiers of Information Technology & Electronic Engineering*, 24(8):1156-1168. https://doi.org/10.1631/FITEE.2200501

High capacity reversible data hiding in encrypted images based on adaptive quadtree partitioning and MSB prediction

Key words: Adaptive quadtree partitioning; Adaptive most significant bit (MSB) prediction; Reversible data hiding in encrypted images (RDH-EI); High embedding capacity

Corresponding author: Kaili QI
E-mail: 1804480181@qq.com
ORCID: https://orcid.org/0000-0002-0578-9819

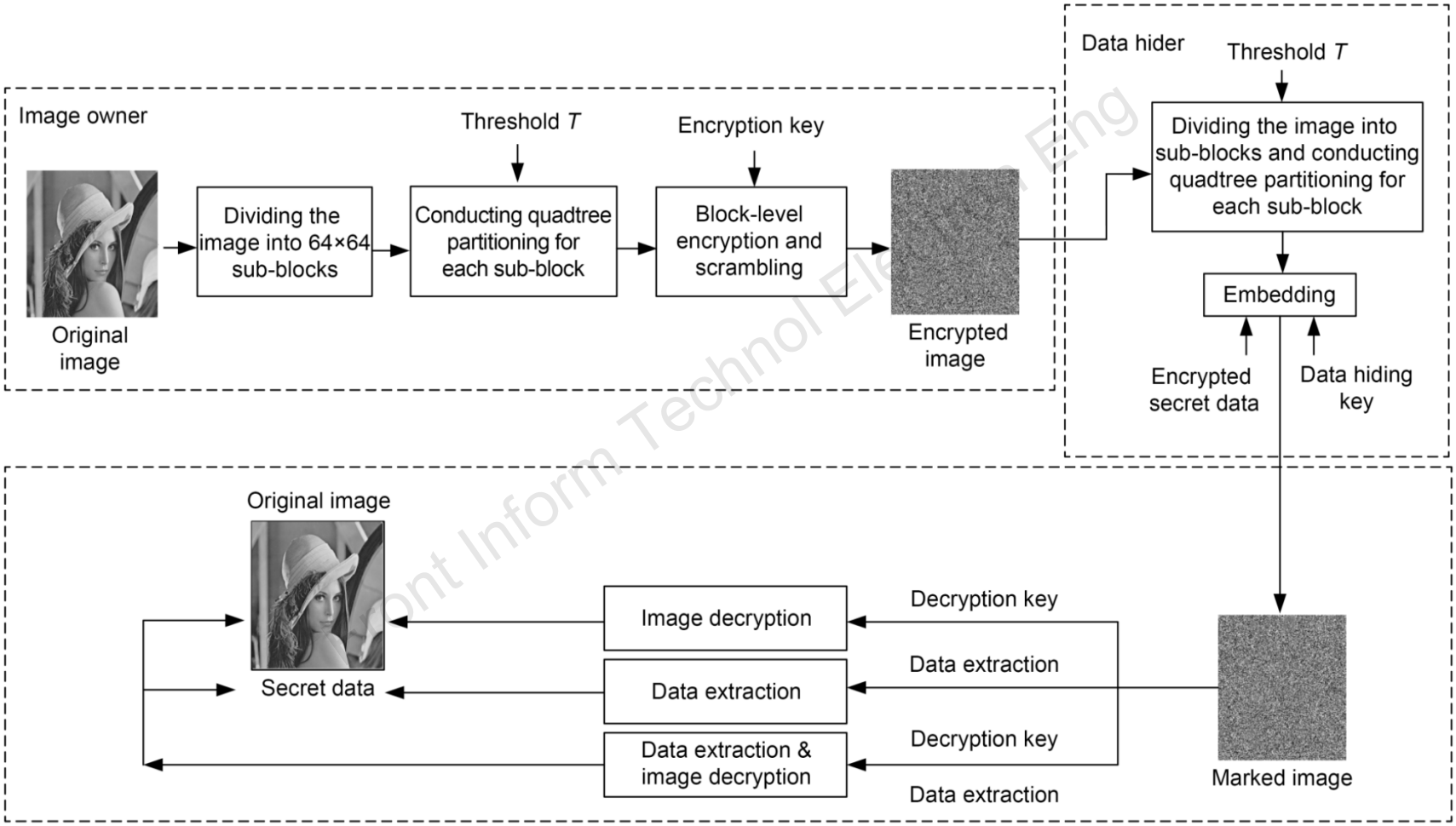
Motivation

- To ensure a high embedding rate and good image quality after data extraction and image restoration, Wang and He (2022) used the correlation between pixels and proposed a reversible information hiding scheme with a large capacity. However, the embedding capacity needs to be improved.
- To further improve the embedding capacity, in this paper we propose an improved scheme based on Wang and He (2022)’s method, and adopt adaptive quadtree partitioning according to the smoothness of the image to adaptively generate a number of blocks with different sizes.

Main idea

- According to the smoothness of the image, the image is partitioned into blocks based on adaptive quadtree partitioning, and then blocks of different sizes are encrypted and scrambled at the block level to resist the analysis of the encrypted images.
- In the data embedding stage, the adaptive most significant bit (MSB) prediction method proposed by Wang and He (2022) is improved by taking the upper-left pixel in the block as the target pixel, to predict other pixels to free up more embedding space. To the best of our knowledge, quadtree partitioning is first applied to RDH-EI.

Framework



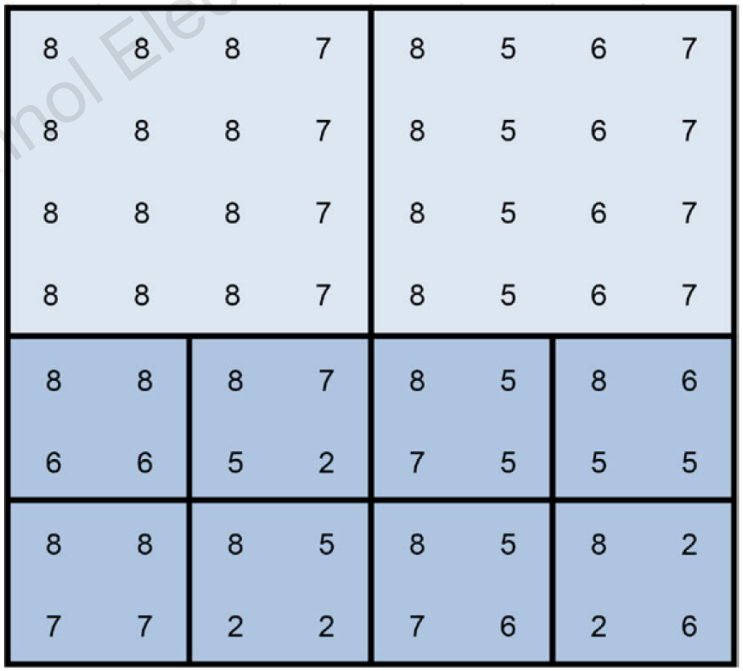
Algorithm framework and process

Method

1. Adaptive quadtree partitioning. If the condition of partitioning is met, the block will no longer be divided into four average blocks until a block of size 2×2 can no longer be partitioned.

162	162	162	161	162	157	163	161
162	162	162	161	162	157	163	161
162	162	162	161	162	157	163	161
162	162	162	161	162	157	163	161
162	162	162	161	162	157	163	161
164	164	158	155	161	159	159	160
160	160	163	158	160	162	159	156
159	159	155	157	158	159	156	157

(a)



(b)

Pixel values of the selected block (a) and the partitioning result (b)

Method

2. Image encryption. For the first encryption, encryption keys and a classic stream cipher are used to perform block-level encryption. For the second encryption, a number of 64×64 sub-blocks are first scrambled. Next, in each stage of quadtree partitioning scrambling, four same-level blocks of each 64×64 sub-block are scrambled according to the key of scrambling.

Method

3. Adaptive quadtree most significant bit (MSB) prediction. When the block size $a \times a$ is greater than 2×2, pixels of the block are reconstructed, first to arrange pixel *P* with eight bits, using the first three bits to arrange the minimum number of shared MSBs (MD), and then two bits are used to represent the size of the block (Dim).

255	255	255	255
254	254	255	255
255	253	255	254
255	255	255	253

11111111	10	101	11	11	11	10	10	11	11	11	01	11	10	11	11	11	01	nc

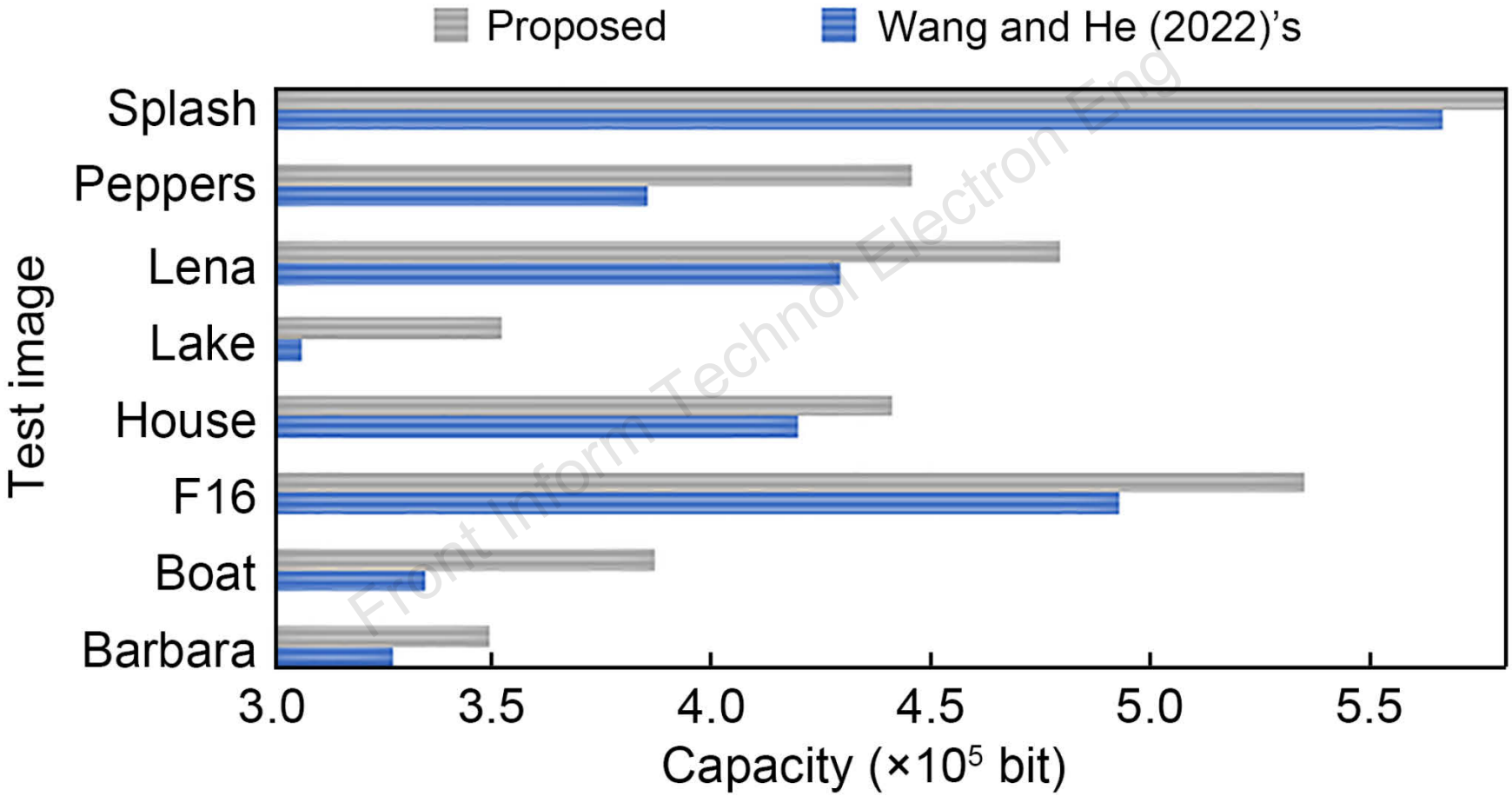
Pixel structure demonstration and pixel bit reconstruction of a 4×4 block

Method

4. Data hiding. After adaptive quadtree partitioning, the data hider performs adaptive MSB prediction for each size of the block to free up space for embedding the secret data.

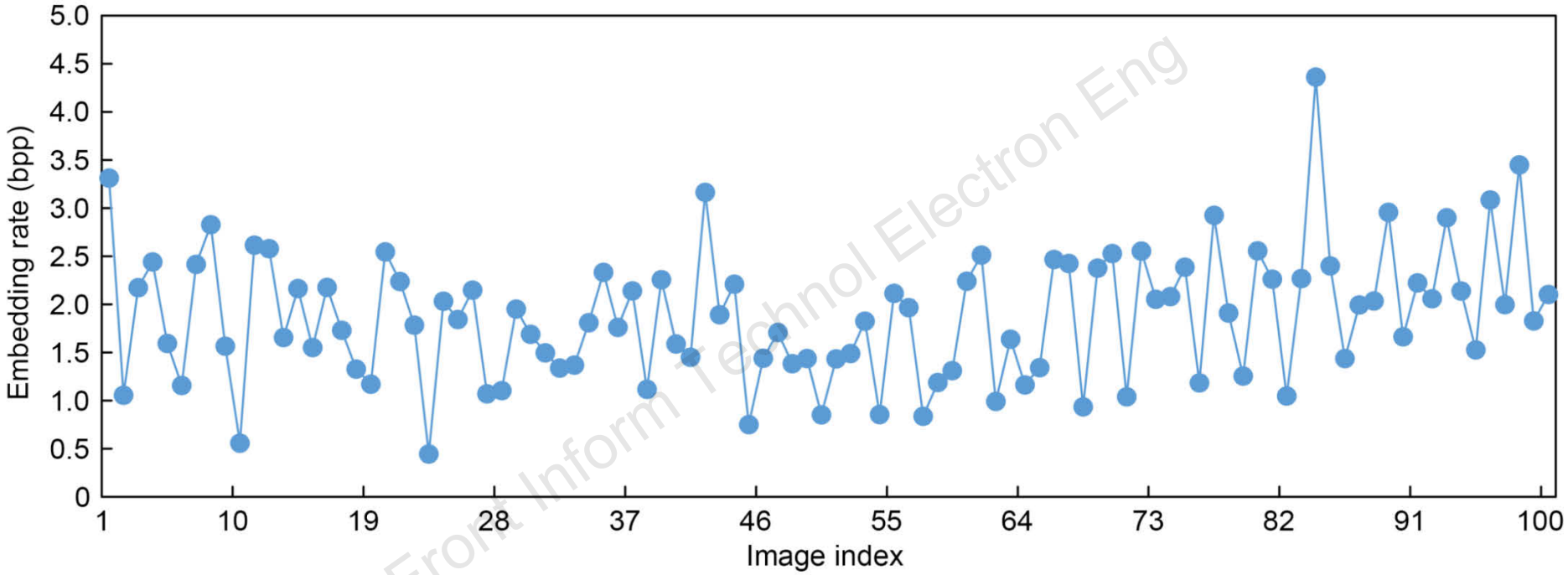
5. Data extraction and image restoration. The proposed method is truly separable. There are three types of receivers based on the type of key they hold, and receivers with different types of keys will recover different contents.

Major results



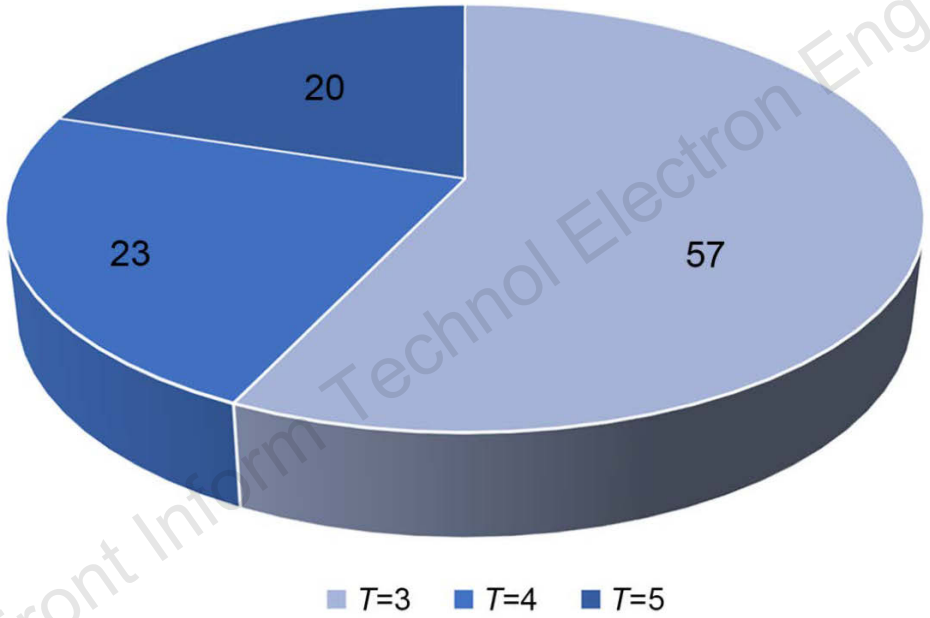
Comparison of the embedding capacity between the two schemes

Major results



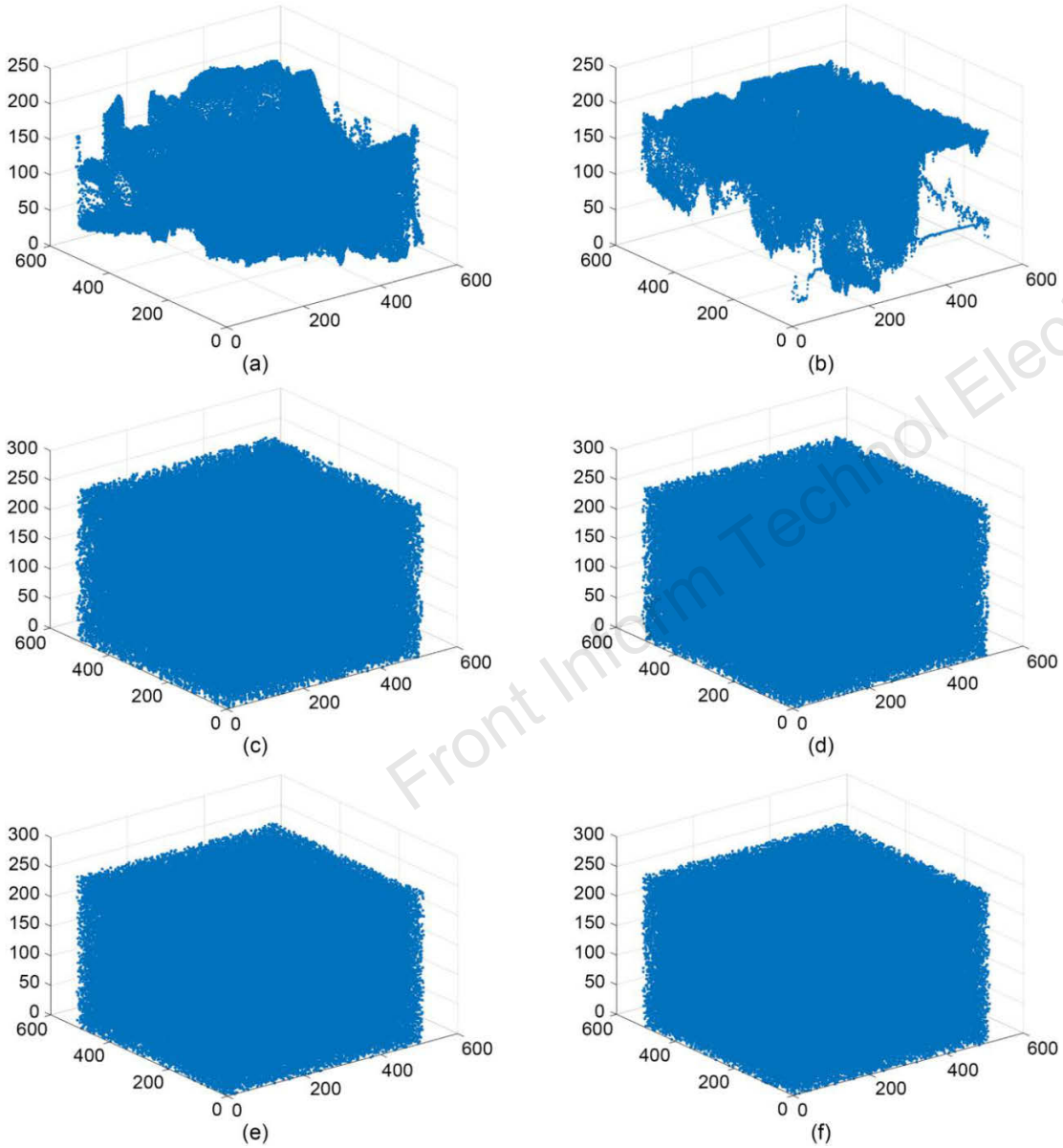
Embedding rate of the proposed method on 100 images randomly selected from the BOW-2 image database

Major results



Distribution diagram of the optimal parameter *T* in 100 randomly selected images

Major results



Scatter maps of different images: (a) original image of Lena; (b) original image of F16; (c) encrypted image of Lena; (d) encrypted image of F16; (e) marked encrypted image of Lena; (f) marked encrypted image of F16

Conclusions

- We adopt adaptive quadtree partitioning according to the threshold *T* and the smoothness of the image while ensuring reversibility to restore the original image. It can adaptively change the embedding capacity by adjusting *T.*
- Simulation results show that the proposed method is reversible and separable, and that its average embedding capacity is improved. For gray images with a size of 512×512, the average embedding capacity is increased by 25 565 bits.
- For images with smooth textures, the embedding capacity of our method is greatly improved compared with that of Wang and He (2022)’s method. In addition, our method has separability and reversibility, and thus is more practical than previous methods.