Yongning GUO, Guodong SU, Zhiqiang YAO, Wang ZHOU, 2024. Reversible data hiding scheme for encrypted JPEG bitstreams using adaptive RZL rotation. *Frontiers of Information Technology & Electronic Engineering*, 25(10):1353-1369. https://doi.org/10.1631/FITEE.2300749

# Reversible data hiding scheme for encrypted JPEG bitstreams using adaptive RZL rotation



**Key words:** Joint Photographic Experts Group (JPEG); Reversible data hiding; Embedding capacity; File size preservation; Format compatibility

Corresponding author: Guodong SU
E-mail: gdsu@fpnu.edu.cn
ORCID: https://orcid.org/0000-0002-3050-7166

# Motivation

- Joint Photographic Experts Group (JPEG) is one of the most commonly used formats of lossy compression for digital images since it provides a considerable compression ratio and a satisfactory image quality. Considering compelling concerns about the invasion of privacy, research has been undertaken on how to develop an effective reversible data hiding (RDH) scheme for encrypted JPEG bitstreams, to provide security and privacy for both secret messages and valuable carriers.
- In the last decade, many schemes have been developed to achieve a good embedding capacity and secure privacy protection. However, it is also desired that these schemes can always ensure both format compatibility and file size preservation even when a legal operation is conducted, such as encryption or steganography.

# Main idea

- We propose an effective RDH scheme in encrypted JPEG bitstreams based on RZL (run size of zeros/level of a non-zero alternating current (AC) coefficient) rotation. First, an effective encryption algorithm is exploited to encipher JPEG bitstreams while keeping format compatibility and file size preservation well. Then, RZL pairs from a discrete cosine transform (DCT) block are parsed from received JPEG bitstreams and form an ordered sequence. Next, we construct a one-to-one mapping relationship between the secret messages and the ordered sequence, so that the secret messages can be simply embedded into the sequence of RZL pairs, rather than into the RZL pairs themselves.

# Framework

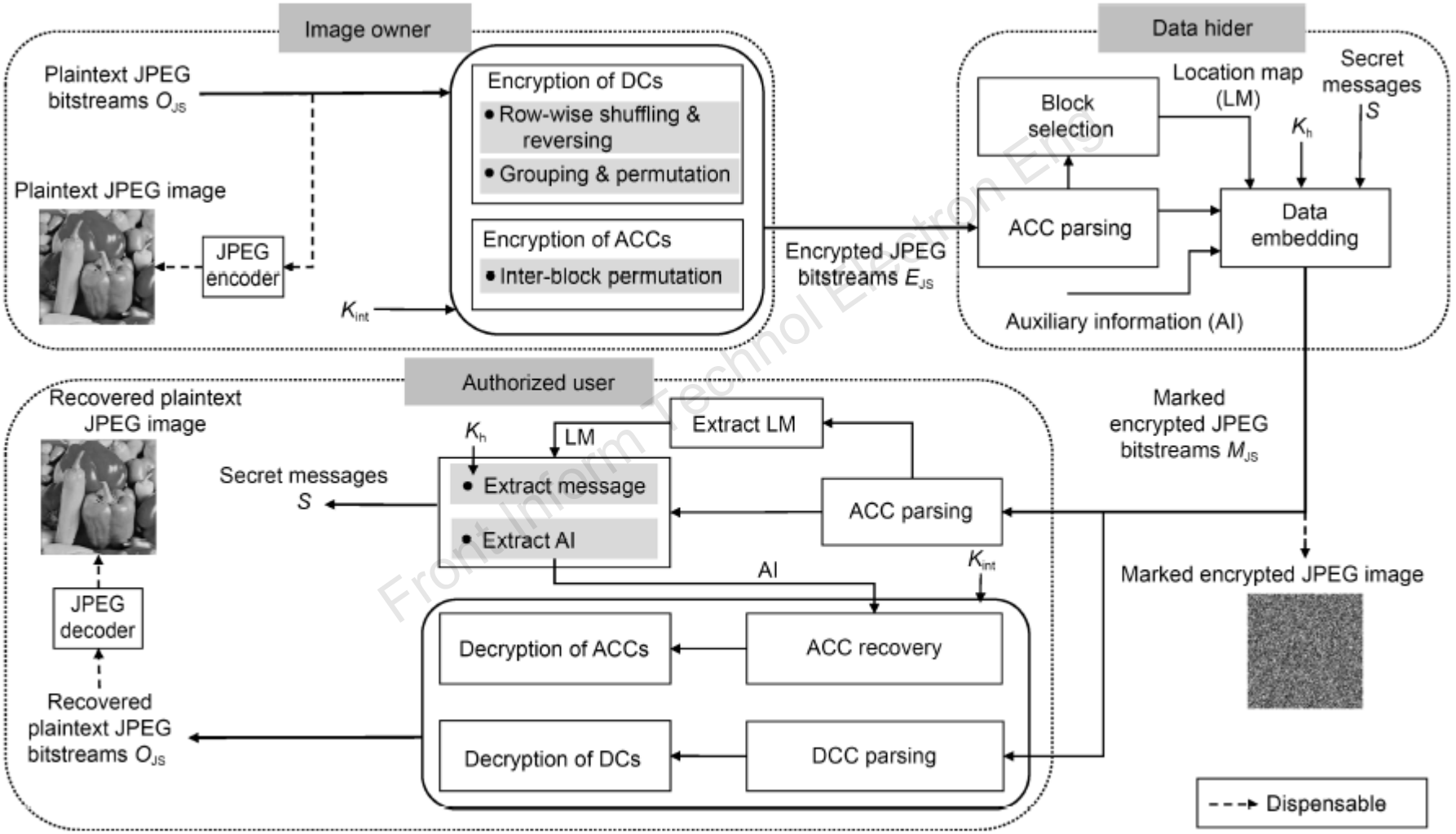


Fig. 2 Basic framework of the proposed scheme

# Method

The low frequency coefficients are larger in absolute magnitude when compared to the high frequency coefficients. Following this fact, an adaptive state mapping is defined and used to serve for concealing secret messages.

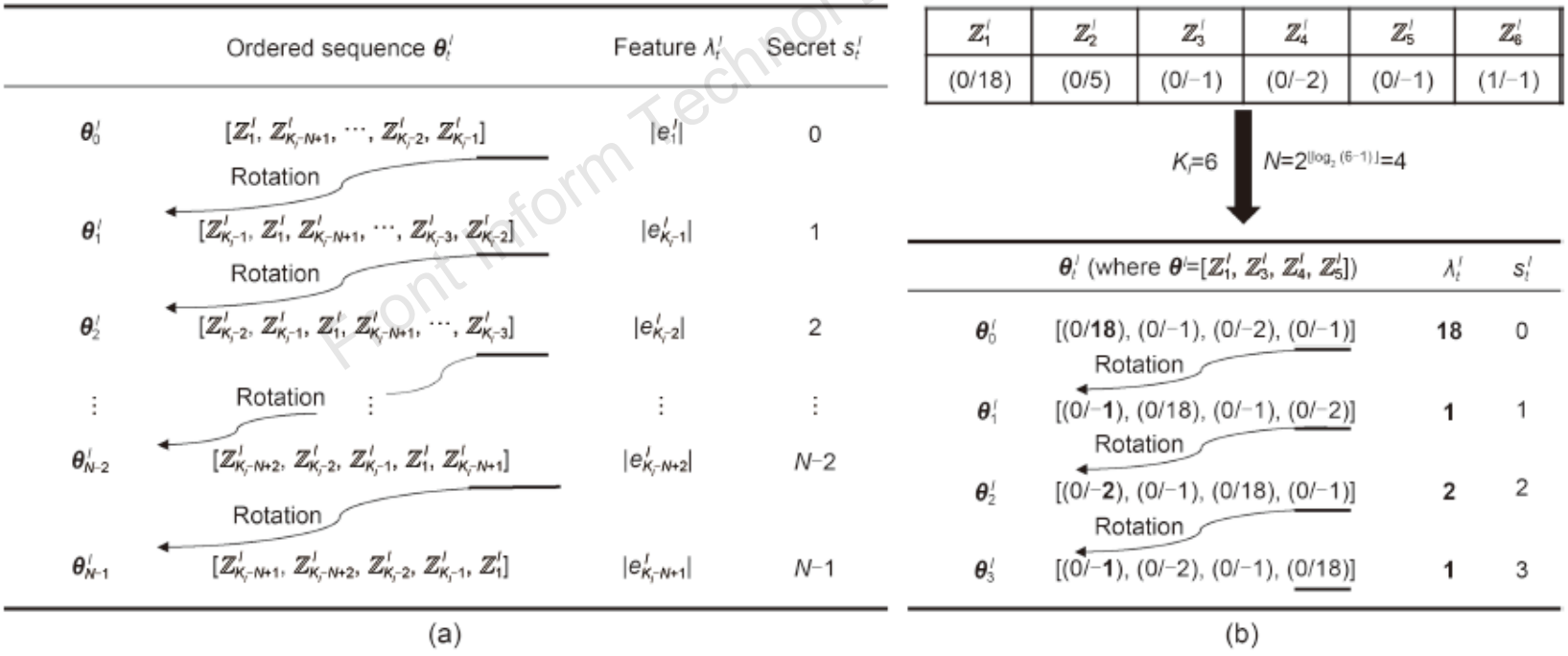


**Fig. 4 Adaptive state mapping definition (a) and an example of state mapping table for case in Fig. 3 (b)**

# Results

**Table 3 Average embedding capacity of the proposed scheme on images from four datasets**

| Dataset | Embedding capacity (bit) | | | | |
|---|---|---|---|---|---|
| | QF=50 | 60 | 70 | 80 | 90 |
| UCID (512×384) | 1392.58 | 1626.15 | 1913.57 | 2729.10 | 3712.60 |
| BossBase (512×512) | 1157.77 | 1338.23 | 1633.21 | 2518.61 | 3555.99 |
| BOWS-2 (512×512) | 1339.65 | 1569.36 | 1887.36 | 2825.24 | 3800.14 |
| CorelDraw (768×512) | 2152.70 | 2478.88 | 2795.10 | 4111.46 | 5718.03 |

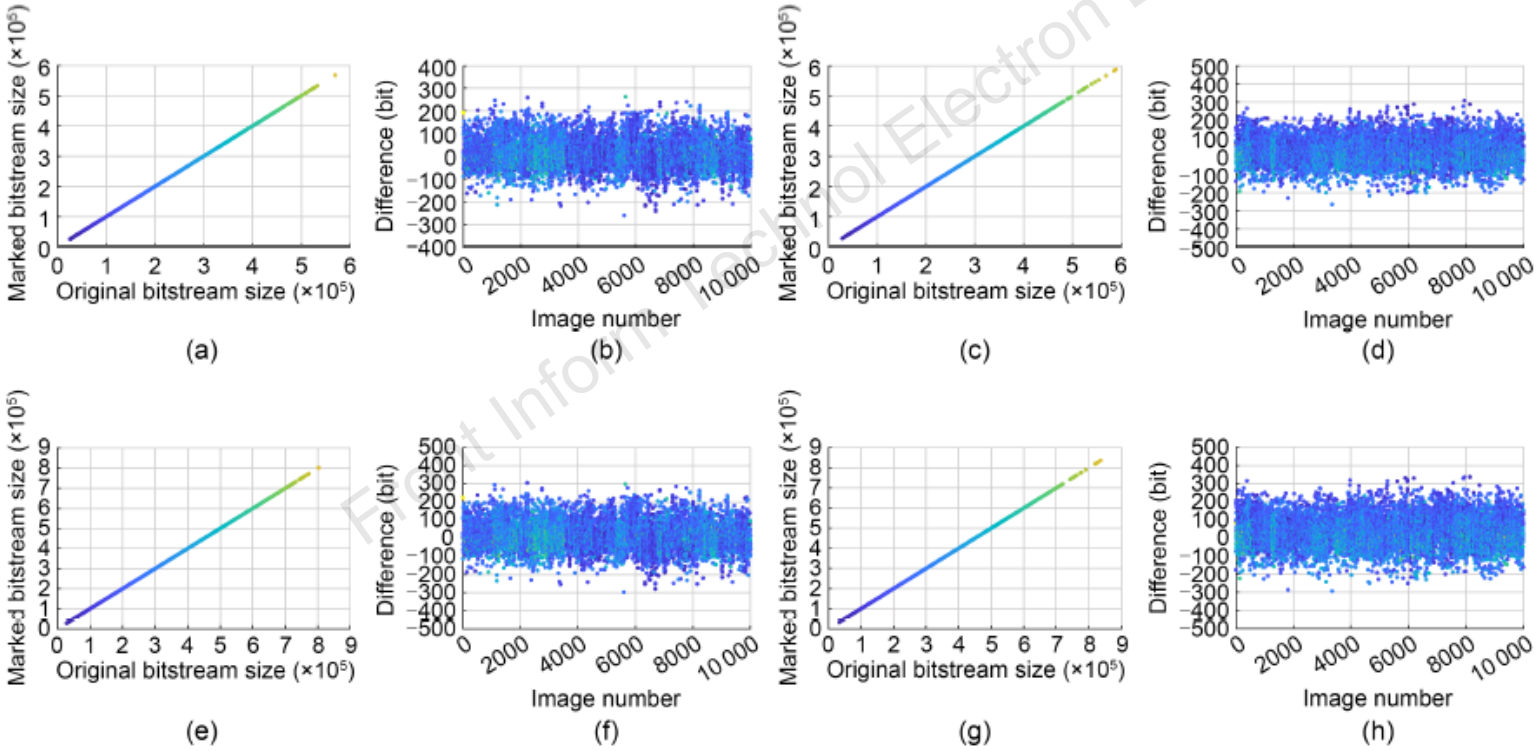




**Fig. 8 Illustrations of relationships of file size (bits) between the entropy encoded data of the original JPEG bitstreams and that of the marked encrypted JPEG bitstreams under various datasets and QFs: (a) distribution for BossBase under QF=60; (b) difference for BossBase under QF=60; (c) distribution for BOWS-2 under QF=60; (d) difference for BOWS-2 under QF=60; (e) distribution for BossBase under QF=80; (f) difference for BossBase under QF=80; (g) distribution for BOWS-2 under QF=80; (h) difference for BOWS-2 under QF=80**

# Conclusions

1. A novel RDH scheme in encrypted JPEG bitstreams toward RZL pairs is put forward. The comparisons of the experimental results showed that the proposed scheme had a superior performance, exceeding the performance of some state-of-the-art schemes

in terms of embedding capacity.

2. Meanwhile, the proposed RDH scheme in encrypted JPEG images is quite well compatible with the JPEG standard and effectively suppresses the file size increment.

3. Additionally, our RDH scheme in encrypted JPEG bitstreams has reversibility; that is, the secret messages can be extracted error-free and the original plaintext JPEG image can be recovered losslessly.

Yongning GUO is a full professor at the Fujian Polytechnic Normal University. His research interests include image processing and image encryption.

Guodong SU is an associate professor at the Fujian Polytechnic Normal University. His research interests include data hiding, deep learning, and watermarking.

Zhiqiang YAO is a full professor at the Fujian Normal University. His research interests include application security, big data security, and privacy protection.