REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES BASED ON RESERVING ROOM AFTER ENCRYPTION AND MULTIPLE PREDICTORS

Ioan Catalin Dragoi and Dinu Coltuc

Electrical Engineering Department, Valahia University of Targoviste, Romania

Email: catalin.dragoi@valahia.ro, dinu.coltuc@valahia.ro

Introduction

A refined version of our recent embedding scheme[1] based on the data hiding framework of Wu & Son[2].

Original features: data extraction based on multiple predictors, adaptive selection of predictors.

Encryption & Data insertion

Encryption

- exclusive-or with a pseudorandom bitstream sequence generated by the encryption key.

Data insertion

A	B	A	B	A	B
B	U	B	U	B	U
A	B	A	B	A	B
B	U	B	U	B	U
A	B	A	B	A	B

- divide the encrypted pixels into three sets (***A***, ***B*** and ***U***);
- distribute the pixels in ***A*** into groups based on an embedding key;
- select an image bit plane;
- insert the ***b*** data bit in a group of ***n*** pixels by bit-flipping the values from the ***t*** selected bit plane:

$$C_t'(i) = \begin{cases} \sim C_t(i) & \text{if } b = 1 \\ C_t(i) & \text{if } b = 0 \end{cases}, \text{ where } i \in \{1, 2, \dots, n\};$$

- the process is repeated for the ***B*** set.

[1] Dragoi et al., Improved Reversible Data Hiding in Encrypted Images Based on Reserving Room After Encryption and Pixel Prediction. 25th Eur. Conf. Signal. Process., 2017.

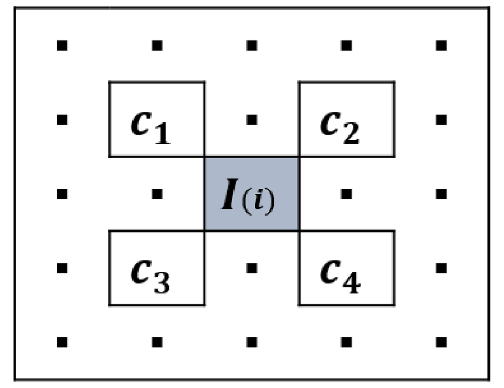
[2] Wu & Son, High-capacity reversible data hiding in encrypted images by prediction error. Signal Processing, 2014.

Decryption & Data extraction

Decryption

- exclusive-or with the bitstream sequence used for encryption.

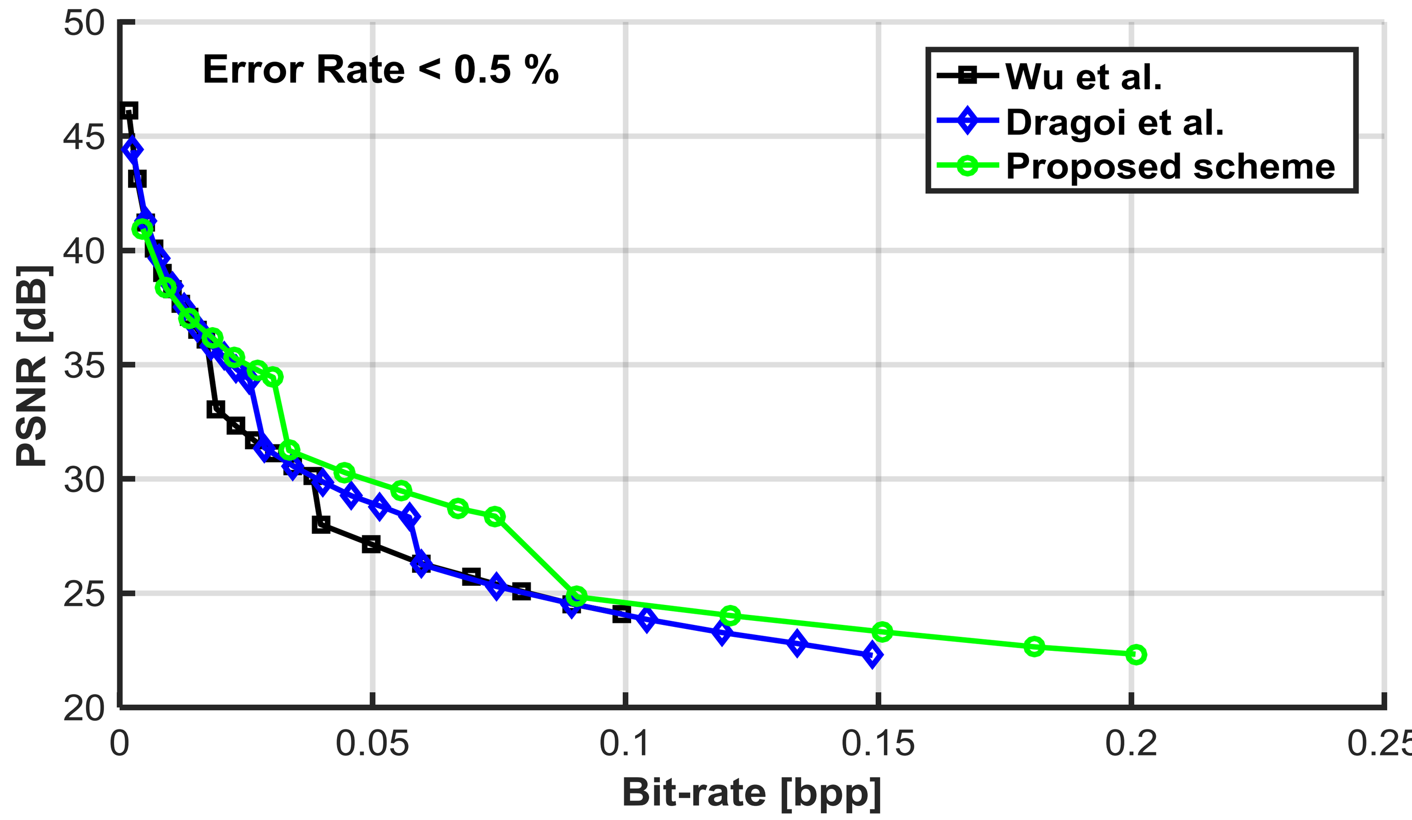
Data extraction

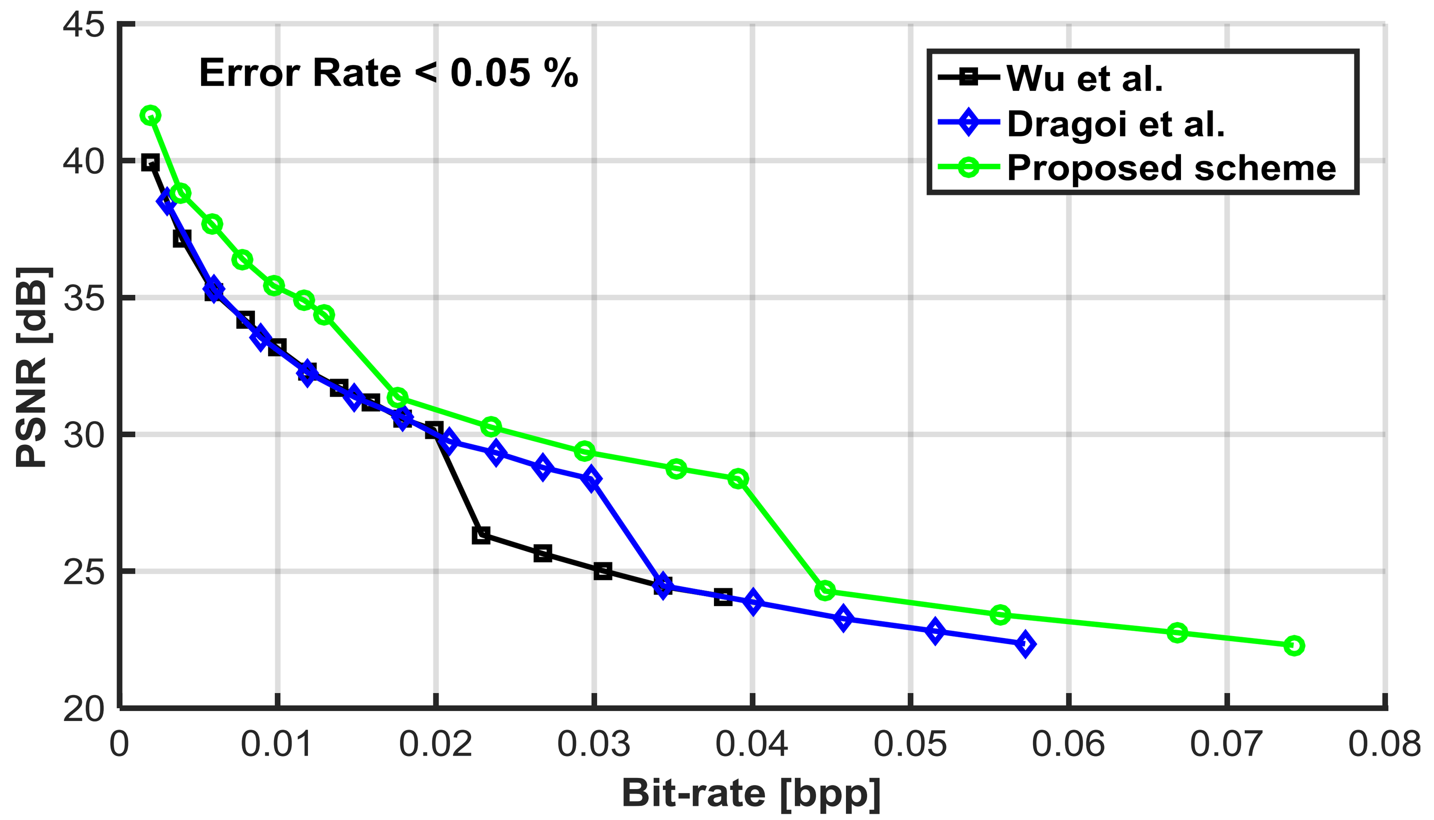


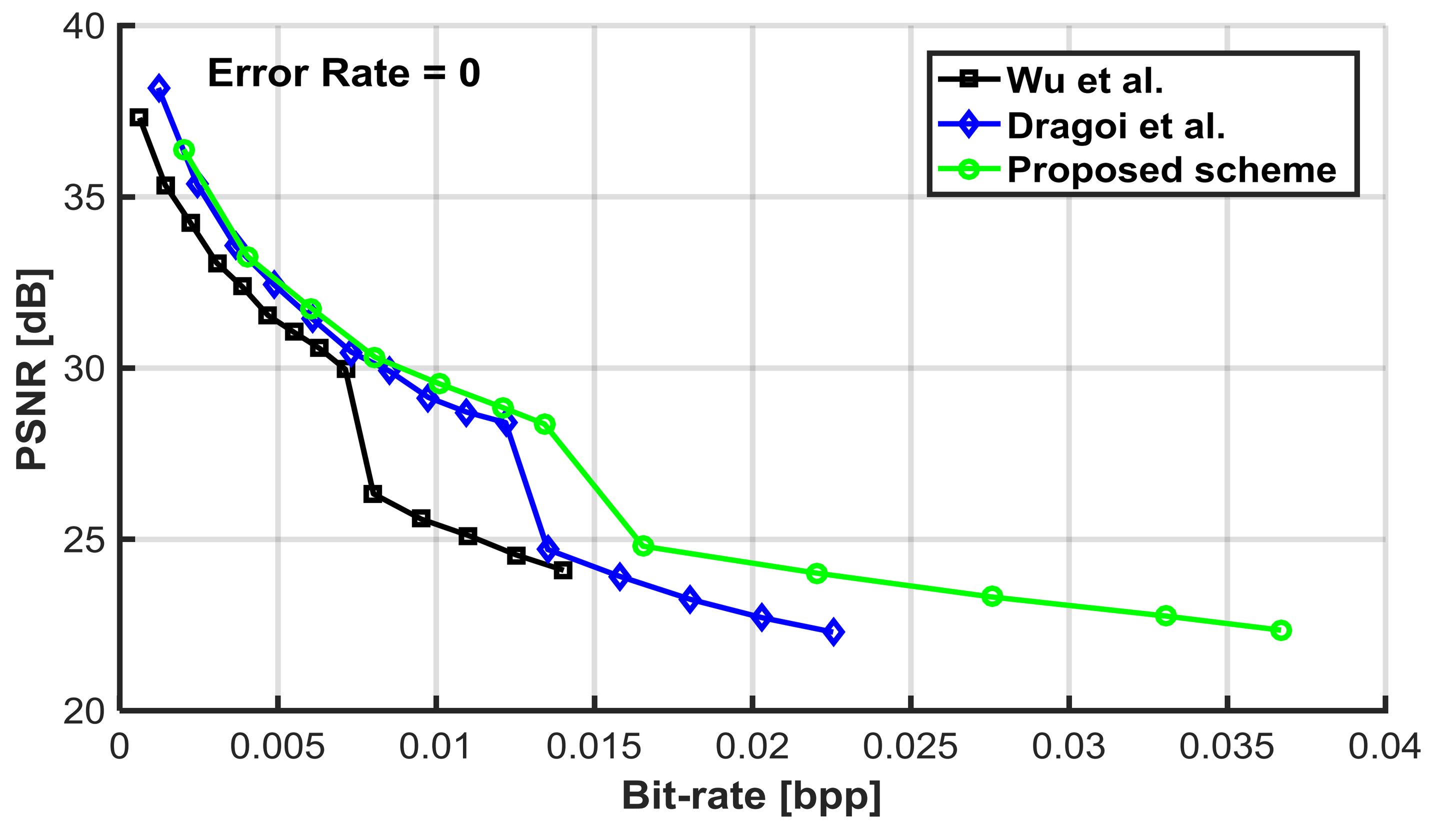
- divide the decrypted pixels into ***A***, ***B*** and ***U***;
- use the embedding key to distribute the pixels in ***A*** into groups;
- determine four predicted value for each pixel based on pixels from ***U***:
  - the average on the prediction context
    $\hat{I}_1 = \frac{c_1+c_2+c_3+c_4}{4}$
  - a weighted average based on vertical and horizontal gradients
    $\hat{I}_2 = \frac{(D_a+1)\frac{c_1+c_4}{2}+(D_b+1)\frac{c_2+c_3}{2}}{D_a+D_b+2}$, where $D_a = |c_2 - c_3|$ and $D_b = |c_1 - c_4|$
  - the median on the prediction context
    $\hat{I}_3 = \frac{c(2)+c(3)}{2}$, where $c(1) \le c(2) \le c(3) \le c(4)$
  - the midpoint (the average of the min and max values)
    $\hat{I}_4 = \frac{c(1)+c(4)}{2}$
- the algorithm evaluates if the current group had its ***t*** bit plane flipped;
- original pixels should have smaller prediction errors than their flipped counterparts;
- only the predictors that provide clear answers for the current group are used;
- the process is repeated for the pixels in ***B*** (they are predicted based on ***U*** and the restored ***A***).

Experimental Results

Average PSNR/bit-rate performance under different decoding error rates on 32 images (8 classic test images and the Kodak set).







Conclusions

- ✓ Outperforms both our previous approach and the data hiding scheme of Wu & Sun;
- ✓ Adaptive selection of multiple predictor → less decoding errors;
- ✓ Improved bit-rates for errorless decoding;
- ✓ Marginal increase in complexity.