# REVERSIBLE DATA HIDING IN ENCRYPTED COLOR IMAGES BASED ON VACATING ROOM AFTER ENCRYPTION AND PIXEL PREDICTION

**Ioan Catalin Dragoi and Dinu Coltuc**

Electrical Engineering Department, Valahia University of Targoviste, Romania

## Introduction

A data hiding scheme developed for encrypted RGB images, derived from the work of Wu el al.*

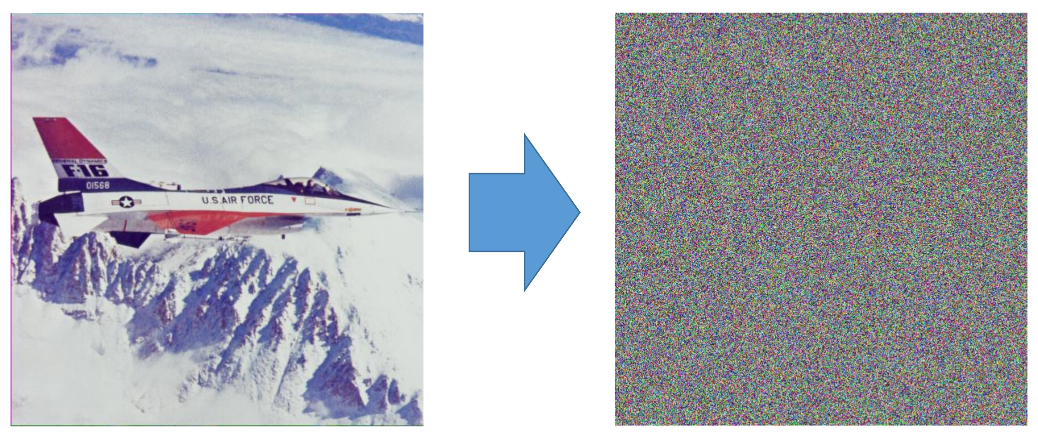
Original features:

- data insertion in R and B using G as a reference;
- mean based prediction;

## Encryption & Data insertion

**Encryption**:

- for each color channel, XOR with a pseudorandom sequence generated by an encryption key.



**Data insertion**:

- divide the encrypted R and B pixels into three sets:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| α | β | α | β | α | β | α | β |
| β | γ | β | γ | β | γ | β | γ |
| α | β | α | β | α | β | α | β |
| β | γ | β | γ | β | γ | β | γ |
| α | β | α | β | α | β | α | β |
| β | γ | β | γ | β | γ | β | γ |

- α pixels are processed in stage 1, β pixels in stage 2;
- select groups of pixels based on a data hiding key;
- embed bit $b$ by flipping the $t$ bit plane of a group (joint method)

$$P_t' = \begin{cases} \sim P_t, & if\ b = 1 \\ P_t, & if\ b = 0 \end{cases}$$

or replace the $t$ bit plane group parity value with $b$ (separate method).

## Decryption & Data extraction

**Decryption**:

- XOR with the bitstream sequence used for encryption.

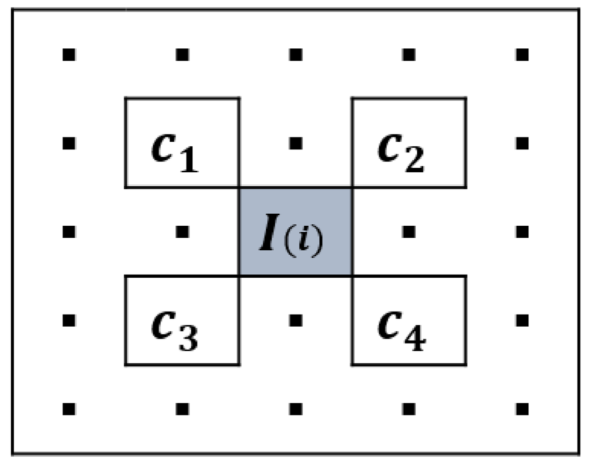
**Data extraction**:

- divide the pixels into α, β and γ;
- use the data hiding key to reform the α pixel groups;
- compute $U'$ and $V'$ using the decrypted image:

$$U' = R' - G$$
$$V' = B' - G$$

- flip the t bit plane of each α group, obtaining $R''$ and $G''$;
- compute $U''$ and $V''$ :

$$U'' = R'' - G$$
$$V'' = B'' - G$$

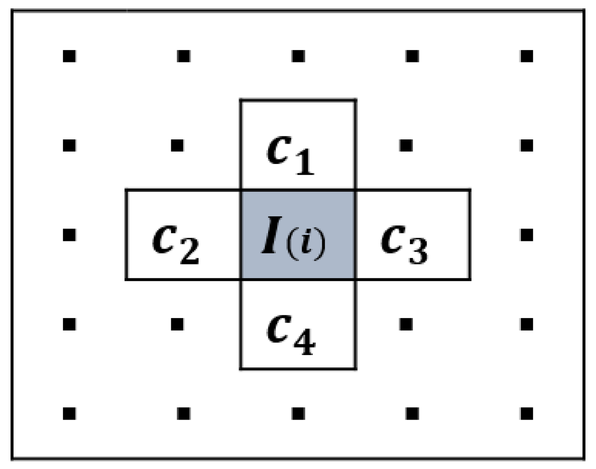


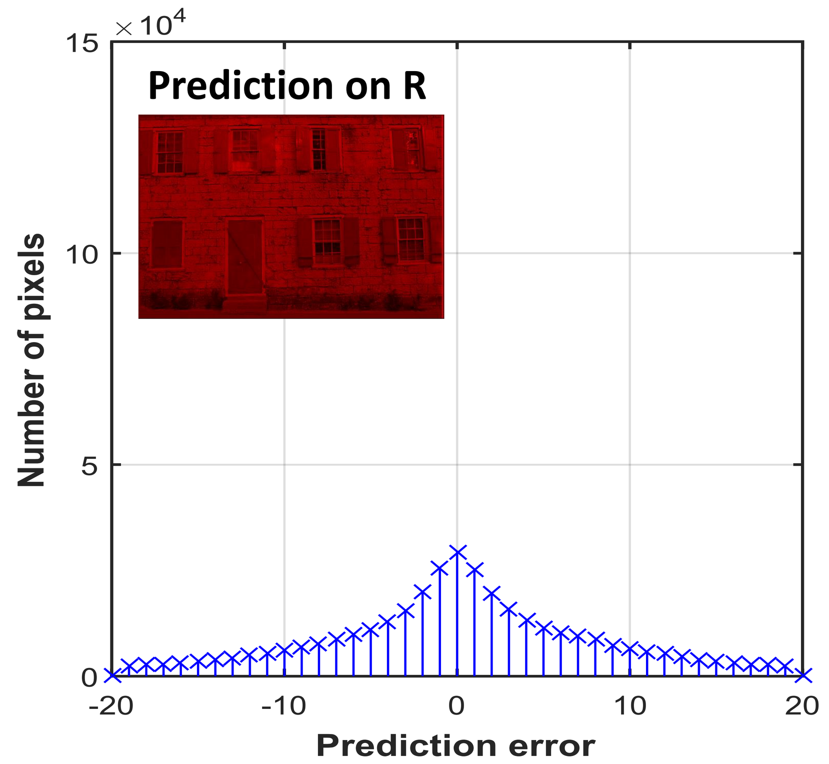
- predict the α pixels in $U$ and $V$ (based on the γ pixels):

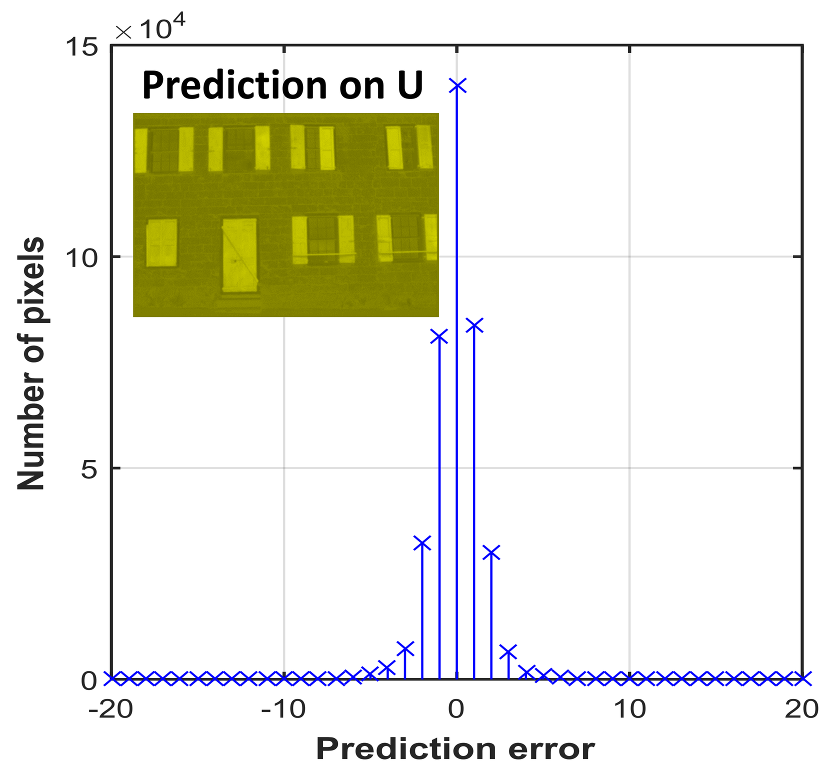
$$I_U = \frac{c_{U1}+c_{U2}+c_{U3}+c_{U4}}{4}$$

$$I_V = \frac{c_{V1}+c_{V2}+c_{V3}+c_{V4}}{4}$$

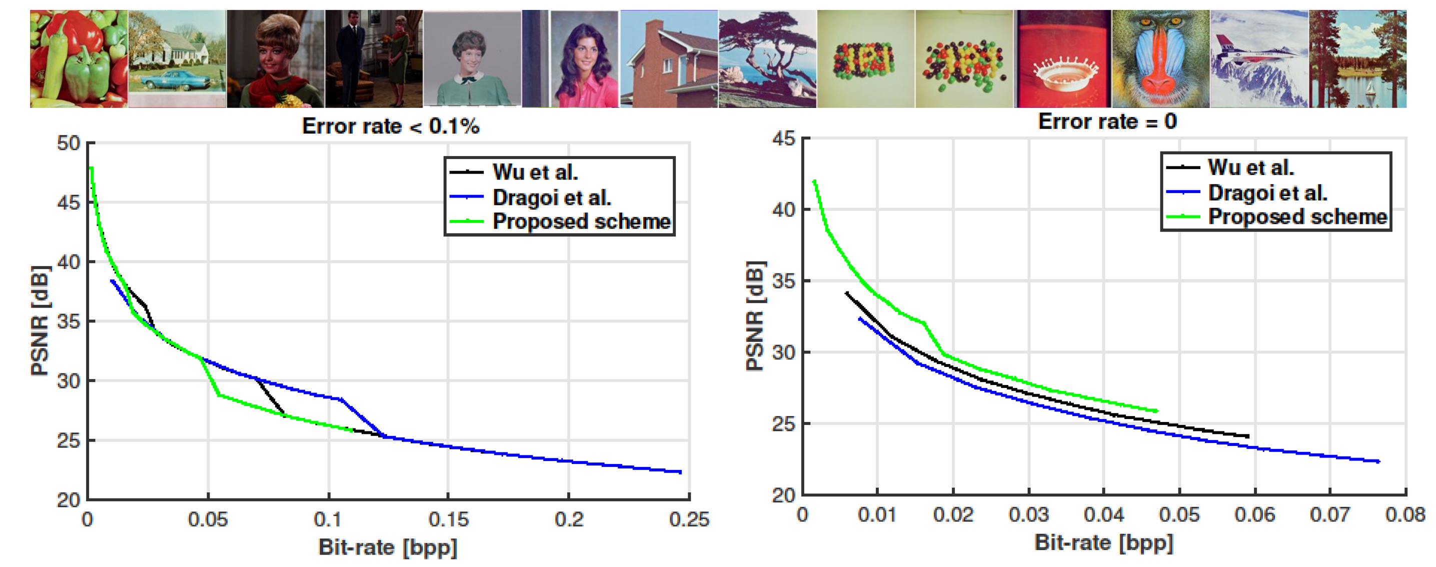
- for each group, select between U’ and U’’/ V’ and V’’;
- original pixels should have smaller prediction errors than their flipped counterparts;
- repeat the process for the β groups;

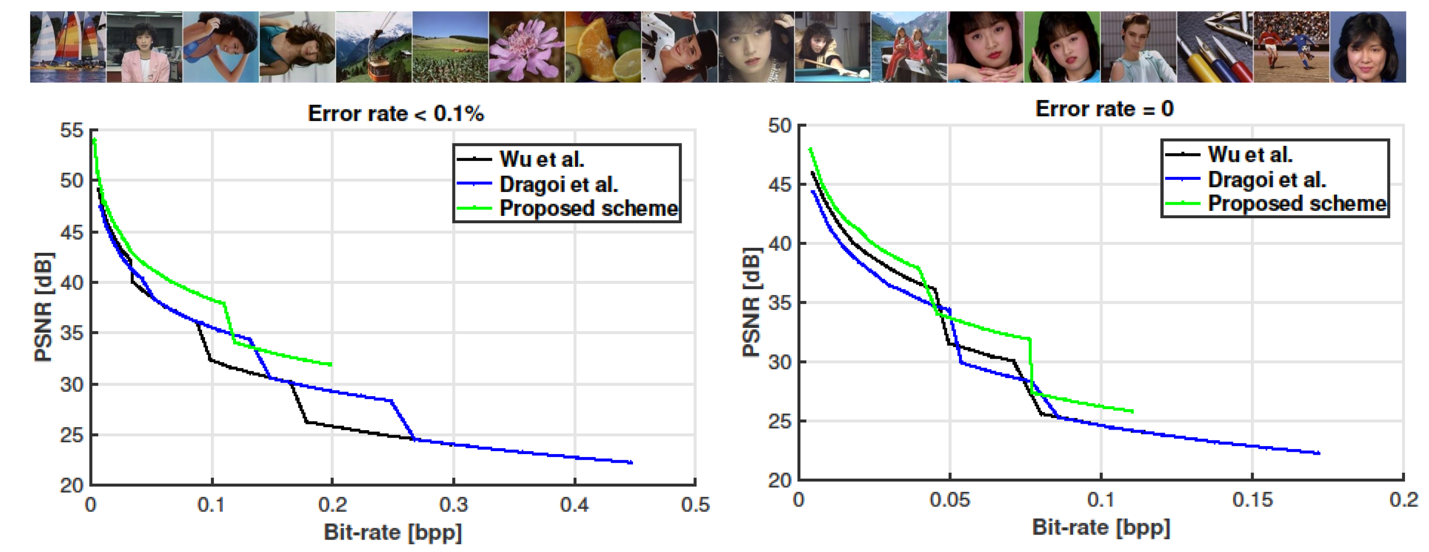


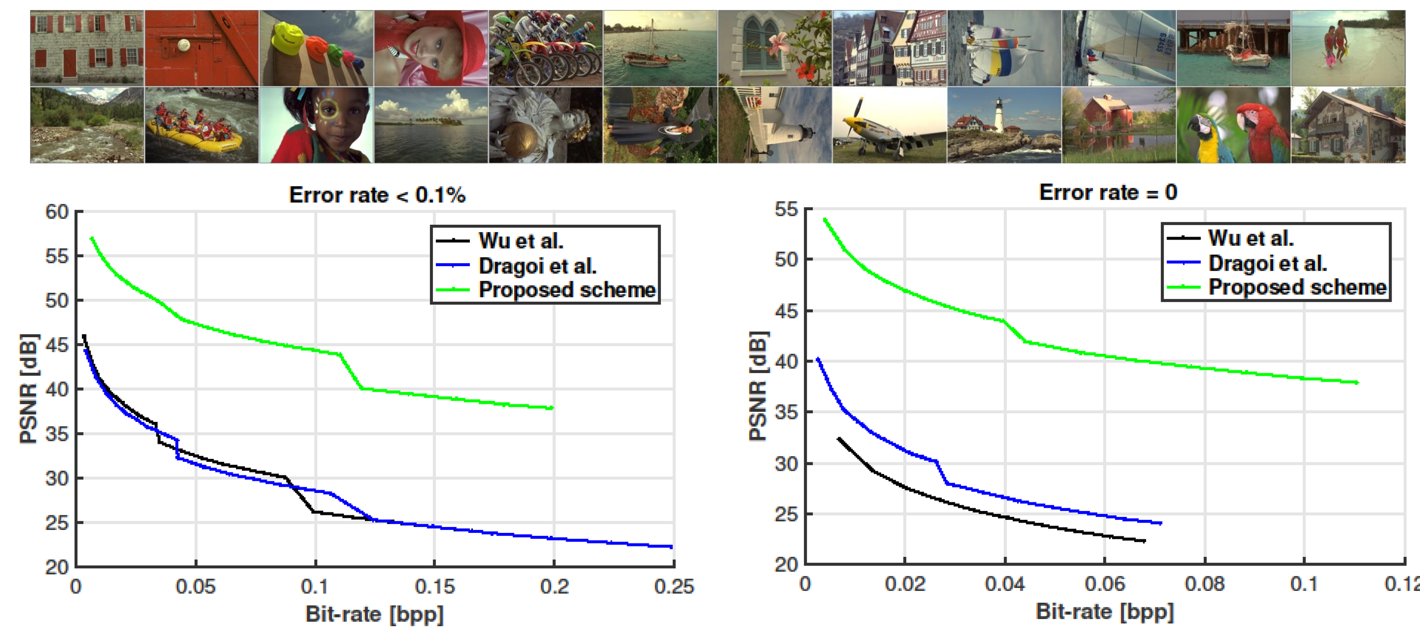



## Experimental Results




## Conclusions

- ✓ a more efficient data hiding scheme that exploits the correlation between color channel;
- ✓ negligible increase in complexity;
- ✓ significant gain in performance on the Kodak set.

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