Improved Reversible Data Hiding in Encrypted Images based on Reserving Room After Encryption and Pixel Prediction

EUSIPCO2017

Ioan-Catalin Dragoi, Henri-George Coanda and Dinu Coltuc

Electrical Engineering Department, Valahia University of Targoviste, Romania

Introduction

Joint and separate vacating room after encryption reversible data hiding in encrypted images (RDH-EI) inspired by the Wu & Son scheme[1].

Original features: two stages of embedding, partition in 3 sets, median based prediction, error correction, data hiding by parity value flipping.

Proposed scheme

Encryption:
- XOR with a sequence generated by an encryption key.

Data hiding:
- divide encrypted pixels in sets A, B, U;
- select groups of pixels from A and B based on a data hiding key;

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

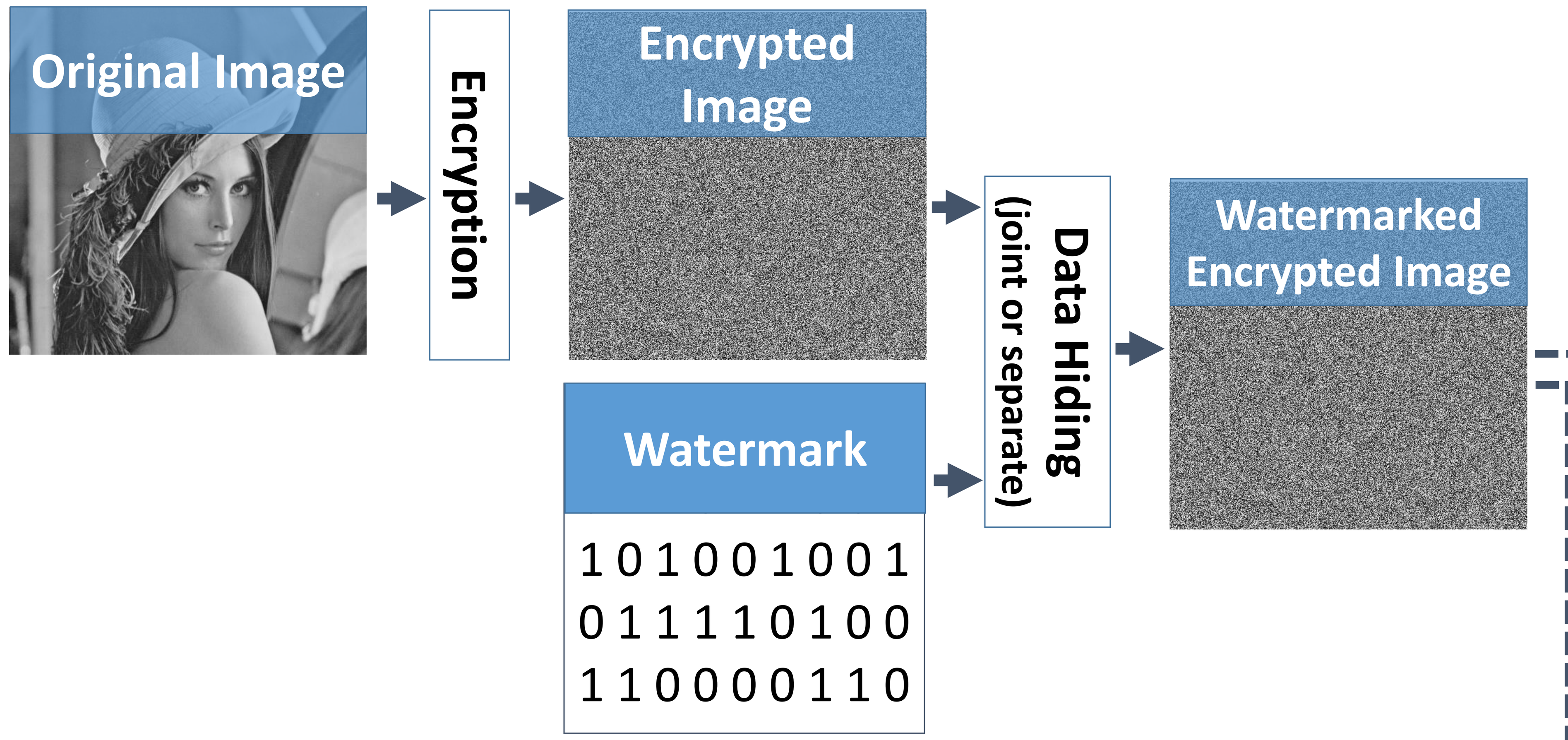
Joint method:
- add control bits for BCH[2] error correction;
- embed A in stage 1 and B in stage 2;
- embed bit b by flipping the t bit plane of the selected group:

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

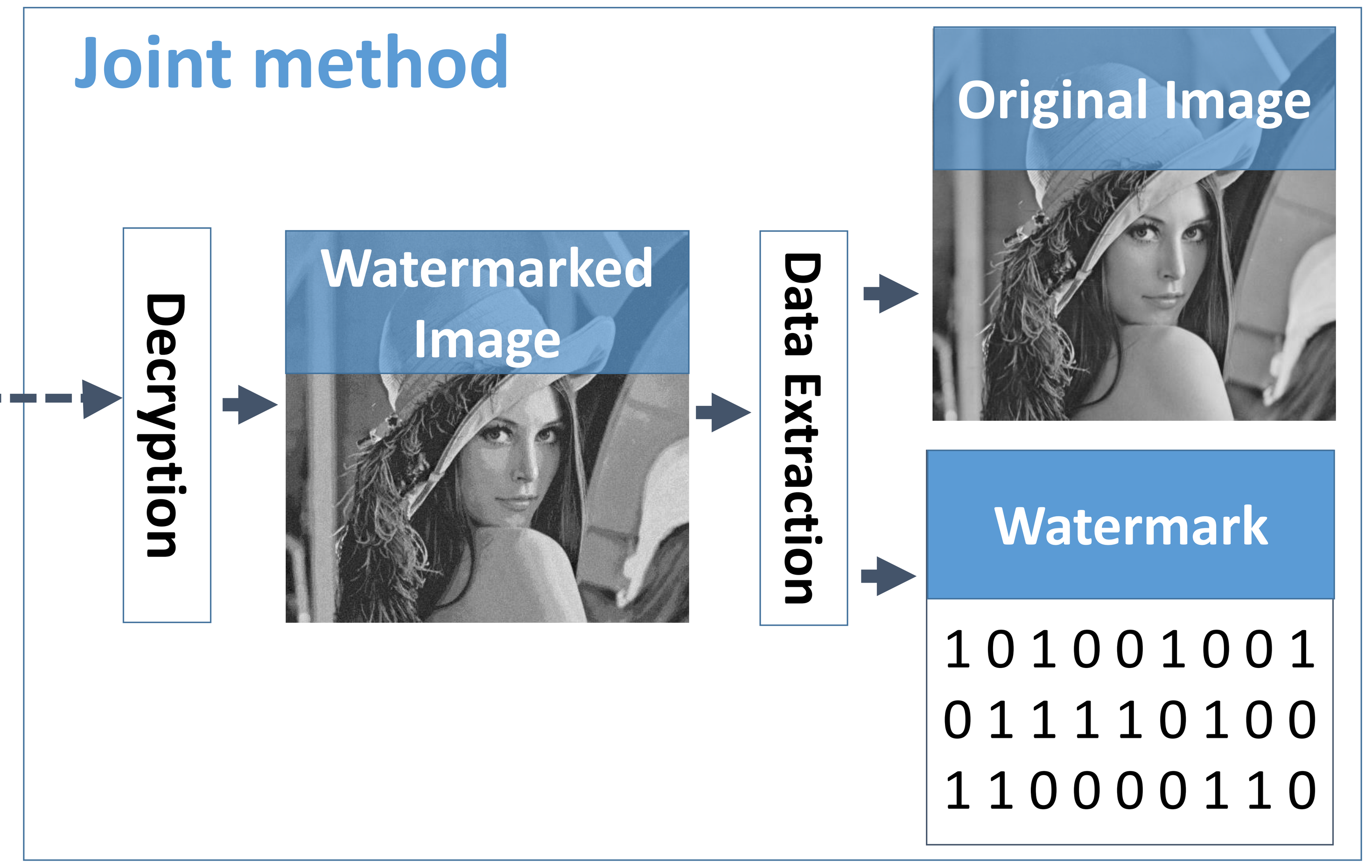
Separate method:
- replace the t bit plane parity value of the selected group with b (by maintaining or flipping the corresponding bits);
- the groups must contain an odd number of pixels.

Data extraction & image restoration:
- predict groups of A based on U and of B based on U and restored A;
- predicted values are used for bit flipping detection.

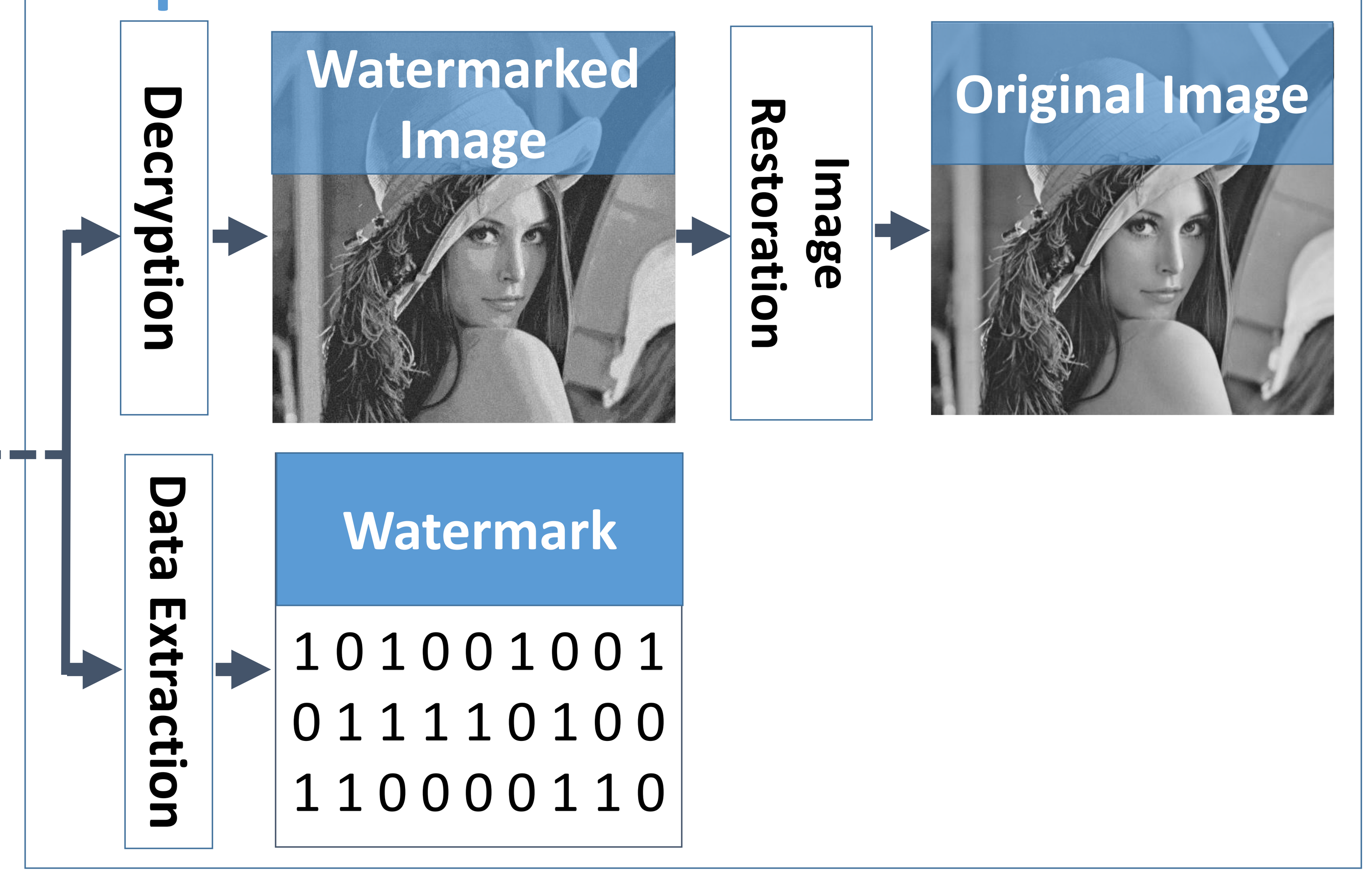
[1] Wu & Son, High-capacity reversible data hiding in encrypted images by prediction error. Signal Processing, 2014.
[2] Bose et al., On A Class of Error Correcting Binary Group Codes. Information and Control, vol. 3, 1960.



Joint method

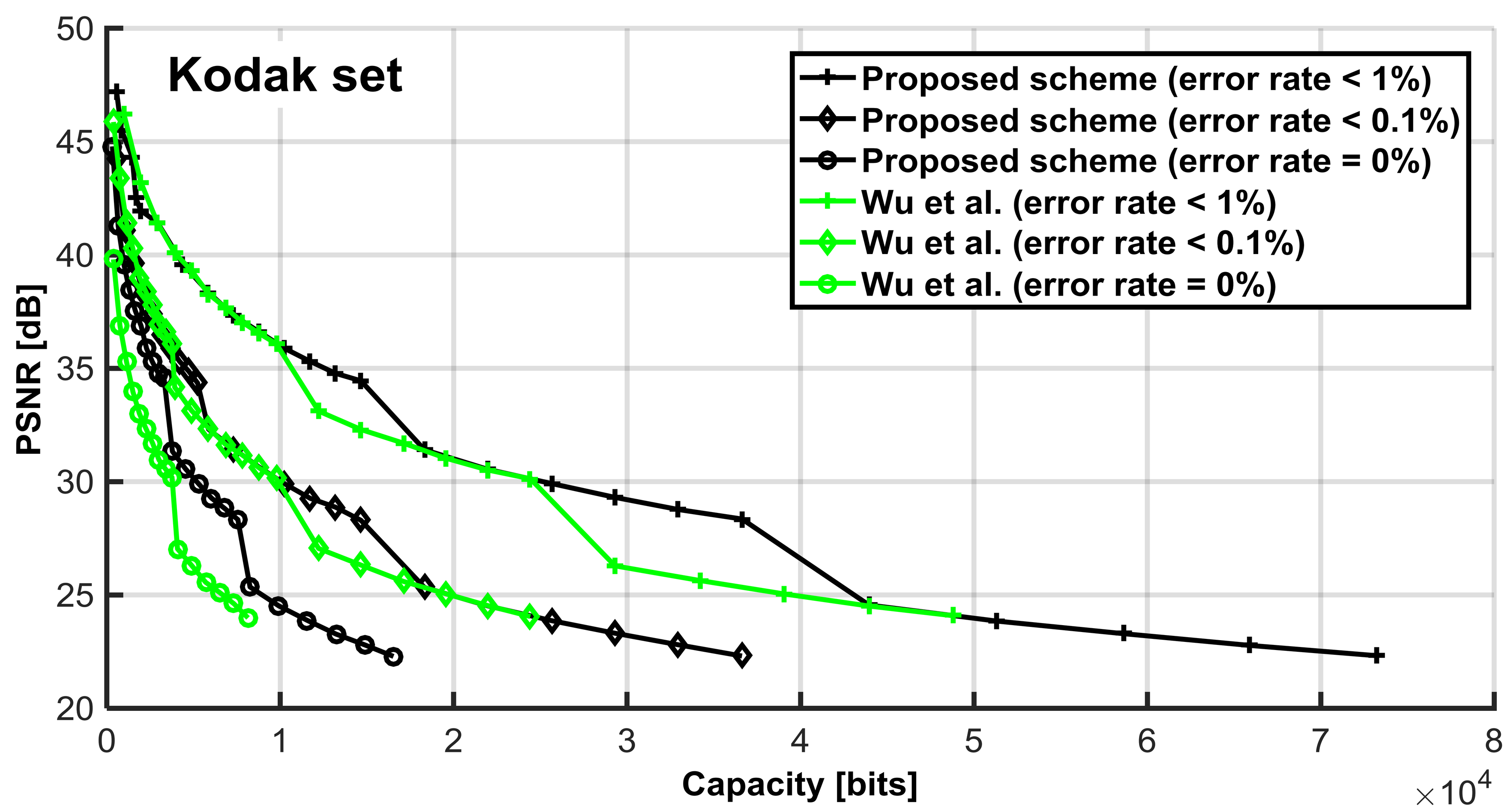


Separate method



Experimental Results

n	Wu et al. [8]	Proposed scheme							
		no coding	BCH (7,4)	BCH (15,7)	BCH (15,5)	BCH (31,21)	BCH (31,16)	BCH (31,11)	BCH (31,6)
5	39066	58299	33180	27042	19230	39390	29940	20490	11040
9	21703	32254	18300	14883	10545	21750	16500	11250	6000
13	15025	22237	12576	10207	7205	14946	11316	7686	4056
17	11490	16935	9544	7743	5445	11355	8580	5805	3030
22	9301	13651	7668	6210	4350	9150	6900	4650	2400
25	7813	11419	6396	5160	3600	7638	5748	3858	1968
29	6735	9802	5472	4411	3065	6525	4900	3275	1650
33	5919	8578	4768	3837	2655	5685	4260	2835	1410
37	5279	7618	4224	3382	2330	5055	3780	2505	1230
41	4764	6846	3780	3025	2075	4509	3364	2219	1074
45	4340	6210	3420	2731	1865	4110	3060	2010	960
49	4246	6069	3336	2668	1820	3984	2964	1944	924
53	3685	5227	2856	2269	1535	3417	2532	1647	762
57	3426	4839	2632	2094	1410	3165	2340	1515	690
61	3202	4503	2440	1933	1295	2934	2164	1394	624



Conclusions

- ✓ Outperforms the RDH-EI scheme of Wu & Sun;
- ✓ BCH codes → better tradeoff between capacity, watermarking distortions and decoding errors;
- ✓ image partition & two staged embedding → capacity improvement;
- ✓ Parity value flipping → distortion reduction.