PPE-Based Reversible Data Hiding

Han-Zhou Wu
School of Inf. Science & Technology
Southwest Jiaotong University
Chengdu 611756, P. R. China
h.wu.phd@ieee.org

Hong-Xia Wang
School of Inf. Science & Technology
Southwest Jiaotong University
Chengdu 611756, P. R. China
hxwang@home.swjtu.edu.cn

Yun-Qing Shi
Department of ECE
New Jersey Institute of Technology
Newark, NJ 07102, United States
shi@njit.edu

ABSTRACT
We propose to utilize the prediction-error of prediction error (PPE) of a pixel to reversibly carry the secret data in this letter. In the proposed method, the pixels to be embedded are firstly predicted with their neighboring pixels to obtain the prediction errors (PEs). By exploiting the PEs of the neighboring pixels, the prediction of the PEs of the pixels to be embedded can be then determined. And, a sorting technique based on the local complexity of a pixel is used to collect the PPEs to generate an ordered PPE sequence so that, smaller PPEs will be processed first for data embedding. By reversibly shifting the PPE histogram (PPEH) with optimized parameters, the pixels corresponding to the altered PPEH bins can be finally modified to carry the entire secret data. Experimental results have implied that, the proposed algorithm can benefit from the prediction procedure, sorting technique as well as parameters selection, and therefore outperform some state-of-the-art works in terms of payload-distortion performance.

CCS Concepts
• **Computing methodologies** → Image processing;

Keywords
Reversible data hiding; prediction-error of prediction error (PPE); sorting; adaptive; watermarking.

1. MOTIVATION
The existing reversible data hiding (RDH) [1] algorithms, in most cases, predict the pixels with a well-designed predictor at first. Then, the secret bits are embedded in the resultant prediction-error histogram (PEH). The pixel prediction procedure is often required to well predict the pixels. Due to the spatial correlations between neighboring pixels, the existing methods often exploit the PE of a pixel to carry the secret data. In fact, there should also exist strong correlations between neighboring PEs. One evidence can be found in the prediction mechanism of modern video lossy compression. For example, in intra prediction, the prediction block for an intra 4 × 4 luma macroblock (consisting of 16 pixels) will be generated with nine possible prediction modes due to the spatial correlations between neighboring pixels. Then, in order to improve the coding efficiency, the prediction mode of a luma macroblock should be further predicted from the prediction modes of neighboring luma macroblocks since correlations also exist between the neighboring prediction modes. The success of steganalysis by modeling the differences between neighboring pixels with 1-order and 2-order Markov chains [2] also reveals that correlations exist between the neighboring PEs if we consider the differences as a kind of PEs.

IH&MMSec 2016, June 20–23, 2016, Vigo, Spain.
ACM 978-1-4503-4290-2/16/06.
http://dx.doi.org/10.1145/2909827.2933196

Therefore, we can actually adopt the prediction-error of prediction error (PPE) of a pixel to hide data. Based on this perspective, we propose a reliable PPE-based RDH method in this letter, in which the PPEs of the pixels to be embedded are firstly determined according to their neighboring pixels. To reduce the distortion for a required payload, the pixels are sorted by the local complexities. A pixel with a lower complexity will be preferentially embedded with a secret bit. By shifting the resultant PPE histogram (PPEH), the corresponding pixels can be finally altered to carry the secret data. Experiments have implied that, the proposed method can provide a good payload-distortion behavior.

2. ESSENTIALS OF PROPOSED METHOD
The proposed method uses grayscale images. The data embedding procedure mainly consists of four parts: the pixel prediction, the prediction of prediction error, the use of pixel sorting, and the data hiding in the image.

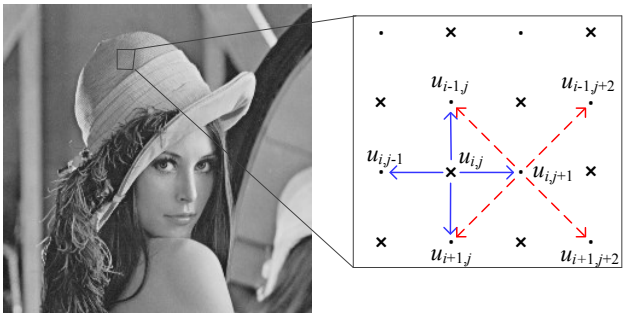


Figure 1: The pixel prediction pattern. The pixel $u_{i,j}$ will be predicted from its four neighbors in the dot set, and $u_{i,j+1}$ will be predicted from its four neighbors still in the dot set.

For pixel prediction, all pixels are divided into two sets: the cross set and dot set (see Fig. 1). The cross set is used for data hiding and dot set for pixel prediction. We use this rhombus pattern as it can maintain a good prediction performance [3]. It is noted that, one may use other efficient prediction patterns. We consider $u_{i,j}$ in Fig. 1 as an example. In Fig. 1, $u_{i,j}$ will be predicted from its four neighbors by using the interpolation operation [1]. The resultant prediction-error is computed as $e_{i,j} = u_{i,j} - u_{i,j}^{+}$, where $u_{i,j}^{+}$ is the prediction value. The prediction of $e_{i,j}$, denoted by $e_{i,j}'$, will be the average of the PEs of neighboring pixels in the dot set. As shown in Fig. 1, the neighbor $u_{i,j+1}$ will be predicted from four neighbors still in the dot set by using the interpolation operation. Therefore, we can finally obtain the PE of $e_{i,j}$, namely, $e_{i,j}^{+} = e_{i,j} - e_{i,j}'$.

In addition to the prediction of PEs, a pixel sorting technique, also called pixel selection, is used. The purpose is to put the PPEs in a decreasing order of the prediction accuracy so that smaller PPEs can be processed first, which benefits the embedding performance. Here, we refer the reader to [7] for a complete understanding.

After sorting, we collect a part of the PPEs with relatively smaller values to generate a PPEH. We choose two peak-zero bin-pairs (l_p, l_z) and (r_p, r_z) for data hiding. During data embedding, the PPEs in range $[l_z, l_p) \cup (r_p, r_z]$ are shifted to avoid ambiguous. For a PPE with a value of l_p or r_p, if the secret bit equals "0", the PPE will be kept unchanged; otherwise, it will be modified as (l_p-1) or (r_p+1). Thus, a marked PPEH can be generated and the used pixels can be finally modified with $\{\pm 1, 0\}$ operation to match the PPEH. This way, the marked image can be finally constructed.

It is noted that, there is no need that $h(l_p)+h(r_p)$ is maximal as long as $h(l_p)+h(r_p)$ is larger than the size of the required payload. Here, $h(x)$ denotes the frequency of the PPEH bin x. It is desirable that, the expected number of altered pixels is as small as possible in order to keep the distortion low as a larger number of modified pixels usually corresponds to a higher distortion. In applications, $|l_z|$ and $|r_z|$ are both small, indicating that, the computational cost to find the two peak-zero bin-pairs will be very low.

Furthermore, as altering a pixel may result in overflow/underflow problem, to ensure reversibility, the boundary pixels in the cross set should be shifted in advance and then recorded to produce a location map, which should be self-embedded with the secret data. Since the boundary pixels in nature images are relatively rare, the effect on the pure payload could be ignored.

Note that, since changes in the cross set will not affect the dot set, the dot set can be applied for data hiding after data hiding with the cross set. The advantage is that, when using only the cross set, pixels with larger PPEs have to be modified to carry the required payload; while, for the consecutive usage of the cross set and dot set, two set of sorted PPEs with smaller values can be used first, implying that, the required payload of each set is approximately half of that for data embedding only with the cross set, and thus could maintain a lower distortion. After the receiver acquires the marked image, he can completely extract the hidden data and recover the original image without loss. It can be performed with an inverse operation to the data hider side.

3. EXPERIMENTS AND DISCUSSION

We have implemented the proposed PPE-based RDH algorithm, and applied it to the standard testing images (sized 512×512, and 8-bit grayscale): Airplane, Lena, Baboon, and (Fishing) Boat. The payload-distortion performance was evaluated by comparing with Sachnev *et al*. [3], Hong *et al.* [4], Luo *et al*. [1], Li *et al*. [5], and Hsu *et al*. [6]. It is observed from Fig. 2 that, the proposed method outperforms these state-of-the-art works in terms of the payload-distortion performance. In future, there is still room for further improvement such as by designing a better predictor, better evaluating local complexities, or applying better data embedding operation. And, it is possible to apply the PPE for different cover media, and/or employ high-order prediction errors for data hiding.

4. ACKNOWLEDGMENT

This work was supported by the Chinese Scholarship Council (CSC) under the grant No. 201407000030, and partially supported by the National Natural Science Foundation of China (NSFC) under the grant No. U1536110.

5. REFERENCES

[1] L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong. Reversible image watermarking using interpolation technique. *IEEE Trans. Inf. Forensics Security*, 5(1): 187-193, Mar. 2010.

[2] T. Pevný, P. Bas, and J. Fridrich. Steganalysis by subtractive pixel adjacency matrix. *IEEE Trans. Inf. Forensics Security*, 5(2): 215-224, Jun. 2010.

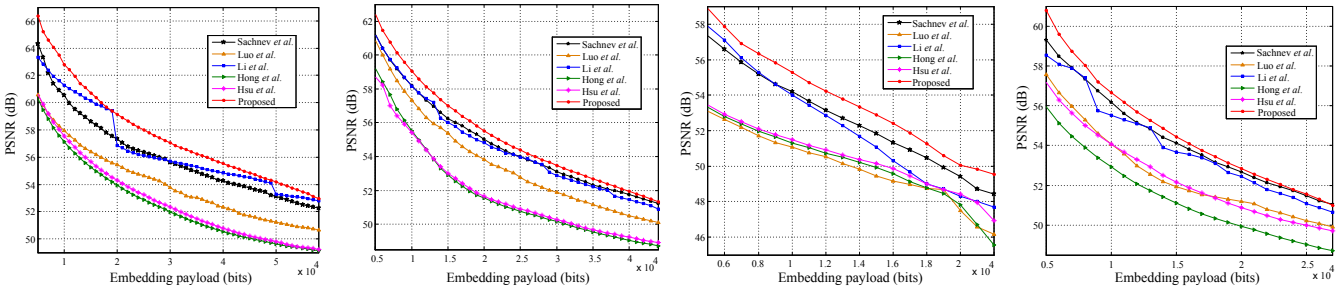
[3] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi. Reversible watermarking algorithm using sorting and prediction. *IEEE Trans. Circuits Syst. Video Technol.*, 19(7): 989-999, Jul. 2009.

[4] W. Hong, T. Chen, and C. Shiu. Reversible data hiding for high quality images using modification of prediction errors. *J. Syst. Softw.*, 82(11): 1833-1842, Nov. 2009.

[5] X. Li, B. Yang, and T. Zeng. Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection. *IEEE Trans. Image Process.*, 20(12): 3524-3533, Dec. 2011.

[6] F. Hsu, M. Wu, and S. Wang. Reversible data hiding using side-match predictions on steganographic images. *Multimed. Tools Appl.*, 67(3): 571-591, Dec. 2013.

[7] H. Wu, H. Wang, and Y. Shi. Prediction-error of prediction error (PPE)-based reversible data hiding. *arXiv:1604.04984*, Online Available, Apr. 2016.



(a) Airplane (b) Lena (c) Baboon (d) Boat

Figure 2: The payload-distortion performance comparison between the state-of-the-art methods of Sachnev *et al.* [3], Hong *et al.* [4], Luo *et al.* [1], Li *et al.* [5], Hsu *et al.* [6] and the proposed method.