Rebuttal: On the Security of Reversible Data Hiding in Encrypted Images by MSB Prediction

Pauline Puteaux, William Puech

Rebuttal: On the Security of Reversible Data Hiding in Encrypted Images by MSB Prediction

Pauline Puteaux, *Member, IEEE,* and William Puech, *Senior Member, IEEE*

***Abstract*—This rebuttal is a response to the correspondence [3] from Dragoi and Coltuc about the security flaws in our proposed approach, "Embedded Prediction Errors-based High Capacity Reversible Data Hiding (EPE-HCRDH) in encrypted images" published in IEEE Transactions on Information Forensics and Security in 2018 [4]. After providing an examination of the EPE-HCRDH approach, we detail several solutions that have already been proposed using state-of-the-art methods. Through visual security level analysis, we show that the very recent methods described are efficient to correct the security flaws.**

***Index Terms*—Image encryption, image security, reversible data hiding, MSB prediction.**

I. An examination of the EPE-HCRDH approach

Prior to the publication of our article in **2018**, to our knowledge, there were no methods of achieving a favourable trade-off between the payload in bits-per-pixel (*bpp*) and the quality of the reconstructed image in terms of PSNR or SSIM. Indeed, a high payload value would lead to a degradation of the reconstructed image's quality. Moreover, it should also be noted that almost all of the other state-of-the-art methods at the time, were based on Least Significant Bit (LSB) substitution and made little use of the redundancy between pixels in the clear domain to realize the data embedding of a secret message. In our proposed work [4], we have taken the opposing view by developing a Most Significant Bits (MSB) prediction-based reversible data hiding in encrypted images (RDHEI) method. In the EPE-HCRDH approach, the original image is encrypted without modification and information about the location of all pixels which cannot be correctly predicted is embedded by MSB substitution. In order to localize the prediction errors, flags of consecutive bits equal to 1 are used. With this information, the data hider can detect all the bits which can be marked and substitutes them with bits of a secret message. In this case, the payload is slightly lower than 1 *bpp*, but perfect reversibility is achieved. So, the proposed EPE-HCRDH approach provides a high payload with a little complexity. But as highlighted by Dragoi and Coltuc [3], the fact of using flags, so that the data hider can embed a secret message introduces security flaws in the method. In spite of this, the method has attracted the attention of many researchers, with 100 citations (according to Google Scholar on November 9, 2020) in several peer-reviewed journals of excellent reputation (IEEE Transactions on Circuits and Systems for Video Technology [1], IEEE Transactions on Multimedia [6], [9], [10], [12], IEEE Access [8], IEEE Transactions on Signal Processing, IEEE Transaction on Dependable and Secure Computing [11], ...). Today, we can say that high capacity RDHEI has become a hot topic.

II. Proposed improvements

Based on our method [4], many papers have suggested improvements. In **2018**, Puyang *et al.* first proposed an extension of the EPE-HCRDH approach [7]. They suggested using a more efficient predictor, and by doing so, this limits the number of prediction errors. In addition, they explained that the first and second MSB-planes could be used for data embedding. Thanks to the use of the second bit plane, a payload of 1.35 *bpp* on average is obtained. At the same time, starting from the MSB-plane, we suggested iteratively analyzing each bit-plane of an image to highlight the prediction errors before encryption and data embedding [5]. After decoding, the original image is perfectly reconstructed by using the information on error location and prediction in a similar way as in the EPE-HCRDH approach. Experimental results showed that the resulting payload is equal to 1.84 *bpp* on average. In **2019**, Yi *et al.* proposed a method based on labeling a parametric binary tree, where the spatial correlation between pixels in the clear domain is maintained in the domain encrypted within small blocks [10]. To realize the data embedding, the bits of a secret message are embedded by substitution by exploiting the spatial correlation between pixels. The authors reached a payload value in the order of 2 *bpp*. Wu *et al.* further improved this approach and obtained a payload of approximately 2.5 *bpp* on average [9]. In their method, Chen and Chang rearranged the MSB-planes by block [2]. This allows them to transform the MSB-planes of the original image into a binary sequence which can be compressed using extended range coding. Thanks to this rearrangement and compression, they can release a larger space for data embedding and the payload value is higher (payload > 1.5 *bpp*). During decoding, the embedded secret message can be extracted directly into the encrypted domain with the help of the data hiding key and the clear marked image can be obtained with the encryption key. Wu *et al.* designed a new RDHEI scheme based on bitplane partition [8]. After processing the self-embedding, the authors showed that a considerable part of the redundancy in the cover image is still preserved. Therefore, they used a MSB prediction method to finally obtain a payload value of 2.27 *bpp*. Still in 2019, Yin *et al.* proposed a high-capacity algorithm based on multi-MSB prediction and Huffman coding [12]. Multi-MSB of each pixel is adaptively predicted and marked by Huffman coding in the original. After encryption, the vacated space is used to embed additional data by multi-MSB substitution. Experimental results show that this method achieved a payload of more than 3 *bpp*. In **2020**, Chen *et al.* designed a multi-MSB compression to obtain a large embedding space including three strategies: iterative MSBs-inversion prediction, adjacent prediction plane XOR and block variable length coding [1]. This allows them to obtain a high payload value (> 1 *bpp*), whilst reducing the size of the marked encrypted image.

In order to **remove security flaws** and increase capacity, in 2020, we have also proposed a new recursive RDHEI method [6]. All the bit-planes of an image are processed recursively, from the most significant one to the least significant by combining error prediction, adaptation, encryption and embedding, as long as it is possible. Using the fact that pixels in the clear domain are highly correlated – MSB-planes are easy to predict – a large part of the bits of an image can be substituted by bits of a secret message. Contrary to [4], [5] and [7], there are no flags to highlight the prediction errors. Indeed, an adaptation of the bit-planes is performed in order to draw several specific configurations and a prediction error value list is built to make it possible to detect and correct all of the incorrectly predicted pixels during the decoding step. Moreover, this method **increases** both the payload value and the **security level** of the EPE-HCRDH approach, while allowing perfect reversibility.

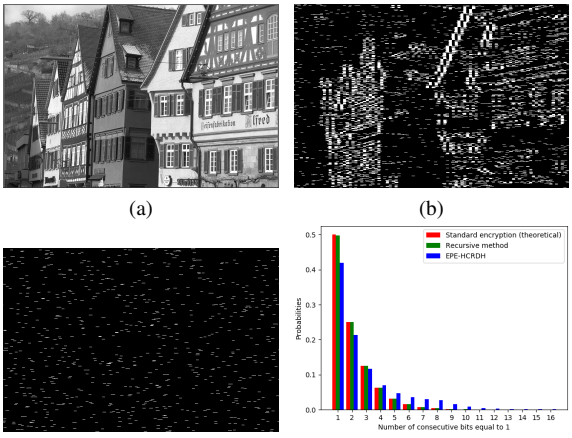
As highlighted by Dragoi and Coltuc [3], using the EPE-HCRDH approach in [4], each bit-plane is processed by sequences of 8 bits. So, there is a prediction error in a sequence, it is highlighted using two flags encoded by 8 bits each. Therefore, whatever the processed bit-plane, nearly 24 bits are lost and cannot be used for data embedding when a prediction error occurs. With our method proposed in [6], each bit-plane is processed bit by bit and if a prediction error occurs, its value is stored in a prediction error value list. Each prediction error value is encoded using $8 - k$ bits (with k the current bit-plane

P. Puteaux and W. Puech are with the Laboratoire d'Informatique, de Robotique et de Microlectronique de Montpellier, Centre National de la Recherche Scientifique, Univ. Montpellier, Montpellier 34095, France (e-mail: pauline.puteauxlirmm.fr; william.puechlirmm.fr).

index), because its value is in the range $\left[-(2^{6-k}+1),\ 2^{6-k}+1\right]$. As all bit-planes are processed and less bits are used to encode a prediction error as in [4], therefore the obtained payload is more significant. Using a predictor such as the Median Edge Detector, the number of prediction errors decreases. As a result, the payload is equal to 2.46 *bpp*, which indicates a gain of approximately 1.5 *bpp*.

III. Visual security level analysis

Fig. 1 illustrates a comparison between the **visual security level** of a marked encrypted image obtained with the EPE-HCRDH approach [4] and the recursive method proposed in [6]. In Fig. 1.a-c, we present the sequence maps of eight or more consecutive MSB equal to 1 on the marked encrypted image associated to the original *Kodim08* image (Fig. 1.a) using the EPE-HCRDH approach [4] (Fig. 1.b) and using the recursive method [6] (Fig. 1.c). Due to flags and error sequences, we can see that there are security flaws using the EPE-HCRDH approach [4], as presented by Dragoi and Coltuc [3]. Indeed, information related to the original image content (in particular, edges) can be identified in the marked encrypted domain. On the contrary, using the recursive method [6], there are only few sequences of eight or more consecutive MSB equal to 1 and they do not provide any information on the content of the original image.



(a) (b) (c) (d)

Fig. 1: **Visual security level** analysis: a) Original *Kodim08* image. Associated map of sequences of eight or more consecutive MSB equal to 1 on the marked encrypted image using: b) The EPE-HCRDH approach [4], c) The recursive method [6]. d) Distribution of sequences of consecutive MSB equal to 1 depending on their length: red) In an encrypted image (theoretical uniform pixel distribution), blue) In the marked encrypted image associated to (a) using the EPE-HCRDH approach [4], green) In the marked encrypted image associated to (a) using the recursive method [6].

Fig. 1.d illustrates the distribution of sequences of consecutive MSB (DSC MSB) equal to 1 as a function of their length. In red, we represent this associated to an encrypted image in the theoretical case, *i.e.* in case of "perfect" encryption considering the pixel distribution as uniform. In this case, the DSC MSB equal to 1 follows a Geometric law with parameter $p = 0.5$. In blue, we can see that the DSC MSB equal to 1 in the marked encrypted image using the EPE-HCRDH approach [4] does not follow this law. Indeed, the Kullback-Leibler divergence from this distribution to this obtained in case of "perfect" encryption is equal to 8×10^{-2}. This is consistent with the analysis of Dragoi and Coltuc [3] and highlights the security issues using EPE-HCRDH.

In green, we display the DSC MSB equal to 1 in the marked encrypted image using the recursive method [6]. With this approach [6], contrary to EPE-HCRDH-based approaches, the Kullback-Leibler divergence from this distribution to this obtained in case of "perfect" encryption is equal to 4×10^{-5}. This result ensures that using a reversible adaptation of the bitplanes instead of flags [6] allows us to **correct the security flaws** of the EPE-HCRDH approach [4].

IV. Conclusion

In conclusion, our paper [4] published in IEEE Transactions on Information Forensics and Security in 2018 – and in particular the EPE-HCRDH approach – has made it possible to launch the investigation into new methods for RDHEI. Despite the **security flaws** described by Dragoi and Coltuc [3], it is a precursor to a new philosophy of data embedding based on MSB prediction.

Since this paper has been published, several solutions have already been proposed in state-of-the-art approaches to **correct the security flaws** and to try to increase the payload. In particular, in 2020, we have shown that all the bitplanes of an encrypted image could be used to perform the embedding of a secret message, from MSB to LSB [6]. In contrast to the EPE-HCRDH approach, prediction errors are not highlighted using flags. Indeed, a reversible adaptation of the bitplanes is carried out to enable the detection and correction of prediction errors during the decoding phase. Therefore, the removal of these flags **increases the visual security level** of MSB prediction-based high-capacity RDHEI methods.

References

[1] F. Chen, Y. Yuan, H. He, M. Tian, and H.-M. Tai, "Multi-MSB compression based reversible data hiding scheme in encrypted images," *IEEE Transactions on Circuits and Systems for Video Technology*, pp. 1–1, 2020, DOI: 10.1109/TCSVT.2020.2992817.

[2] K. Chen and C.-C. Chang, "High-capacity reversible data hiding in encrypted images based on extended run-length coding and block-based MSB plane rearrangement," *Journal of Visual Communication and Image Representation*, vol. 58, pp. 334–344, 2019.

[3] I. C. Dragoi and D. Coltuc, "On the security of reversible data hiding in encrypted images by MSB prediction," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 187–189, 2020.

[4] P. Puteaux and W. Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 7, pp. 1670–1681, 2018.

[5] ——, "EPE-based huge-capacity reversible data hiding in encrypted images," in *IEEE Workshop on Information Forensics and Security (WIFS)*. IEEE, 2018, pp. 1–7.

[6] ——, "A recursive reversible data hiding in encrypted images method with a very high capacity," *IEEE Transactions on Multimedia*, pp. 1–1, 2020, DOI: 10.1109/TMM.2020.2985537.

[7] Y. Puyang, Z. Yin, and Z. Qian, "Reversible data hiding in encrypted images with two-MSB prediction," in *IEEE Workshop on Information Forensics and Security (WIFS)*. IEEE, 2018, pp. 1–7.

[8] H.-T. Wu, Z. Yang, Y.-M. Cheung, L. Xu, and S. Tang, "High-capacity reversible data hiding in encrypted images by bit plane partition and MSB prediction," *IEEE Access*, vol. 7, pp. 62 361–62 371, 2019.

[9] Y. Wu, Y. Xiang, Y. Guo, J. Tang, and Z. Yin, "An improved reversible data hiding in encrypted images using parametric binary tree labeling," *IEEE Transactions on Multimedia*, pp. 1–1, 2019, DOI: 10.1109/TMM.2019.2952979.

[10] S. Yi and Y. Zhou, "Separable and reversible data hiding in encrypted images using parametric binary tree labeling," *IEEE Transactions on Multimedia*, vol. 21, no. 1, pp. 51–64, 2019.

[11] Z. Yin, Y. Peng, and Y. Xiang, "Reversible data hiding in encrypted images based on pixel prediction and bit-plane compression," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2020, DOI: 10.1109/TDSC.2020.3019490.

[12] Z. Yin, Y. Xiang, and X. Zhang, "Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding," *IEEE Transactions on Multimedia*, vol. 22, no. 4, pp. 874–884, 2019.