Journal of Information Hiding and Multimedia Signal Processing ©2018 ISSN 2073-4212
Ubiquitous International Volume **9**, Number **3**, May **2018**

Improved Reversible Data hiding based on Encrypted Signals with Public Key Cryptosystem

Ruiping Li

Modern Educational Technology Center
Henan Normal University
46 East of Construction Road, Xinxiang, 453007, China
liruiping@htu.edu.cn

Jing Zhang, Anqi Mao and Ming Li

College of Computer and Information Engineering
Henan Normal University
46 East of Construction Road, Xinxiang, 453007, China
15516532206@163.com; 947708436@qq.com; liming@htu.edu.cn

Received May, 2017; revised February, 2018

Abstract. *This work proposes an improved version of Chen et al.'s method, which is the first scheme of encrypted signal-based reversible data hiding with public key cryptosystem. The idea of pixel/unit pair division in the original scheme is abandoned. Each pixel/unit is designed to carry one bit of the additional data, and the payload is doubled compared with the original scheme. In addition, the quality of the obtained stego-image/signal is significantly higher due to the fact that the modification on the cover image/signal in data embedding procedure is very little. Analysis and experiments verified the superiority of the proposed method.*

Keywords: Reversible data hiding, Encrypted signal, Public key cryptosystem.

1. **Introduction.** Reversible data hiding possesses the property of categorical restoration of the host image after data extraction [1, 2, 3, 4, 5], this is important in some special applications such as medical imagery, military imagery and law forensics, for the cover image is too precious or too important to be damaged. However, in an open environment such as the cloud environment, the data hider as a third party is always untrusted. Therefore the image should be encrypted before for better privacy protection. Researches of reversible data hiding in encrypted images have been studied recently [6, 7, 8, 9, 10, 11, 12]. Some of them concentrate on embedding information into the partial unencrypted data of the images [6, 7], while others embed data directly into the fully encrypted images [8, 9, 10, 11, 12]. The flip-based method proposed by Zhang [8] can be considered as a classical method of reversible data hiding in the fully encrypted images, and it has been improved several times [9, 10, 11], but the core idea, i.e., the flip operation, did not changed, until the difference of pixels was further explored [12, 13, 14, 15] and the homomorphic encryption based method emerged [12, 15, 16].

In Chen et al.'s method [12], the image/signal is encrypted by the well-known Paillier homomorphic encryption, which is an RSA-based public key encryption. The security of it is under that of RSA strong assumption. Let $E(m)$ denote the cipher text of message m, then the addition homomorphic property of the used Paillier encryption can be described as:

$$E(m_1)E(m_2) = E(m_1 + m_2) \tag{1}$$

Before encryption, the image/signal is firstly divided into pixel/unit pairs, each of which consists of two adjacent pixels/units p_i and p_{i+1}. And each pixel/unit is divided into two parts: $p_i = x_i + y_i$, $x_i = 2\lfloor p_i/2 \rfloor$ and $y_i = p_i - x_i$. Thus, the pixel/unit pair is denoted by $\{x_i, y_i, x_{i+1}, y_{i+1}\}$, and the encrypted version is $\{E(x_i), E(y_i), E(x_{i+1}), E(y_{i+1})\}$ correspondingly.

To embed one bit into a pixel/unit pair, (2) and (3) are computed if the embedded bit is 0;

$$E(y_i') = E(2 + y_i - (y_{i+1} + 1)) = E(2)E(y_i)E(y_{i+1})^{-1}E(1)^{-1} \tag{2}$$

$$E(y_{i+1}') = E(2 + y_i + (y_{i+1} + 1)) = E(2)E(y_i)E(y_{i+1})E(1) \tag{3}$$

(4) and (5) are computed if the embedded bit is 1.

$$E(y_i') = E(2 + y_i + (y_{i+1} + 1)) = E(2)E(y_i)E(y_{i+1})E(1) \tag{4}$$

$$E(y_{i+1}') = E(2 + y_i - (y_{i+1} + 1)) = E(2)E(y_i)E(y_{i+1})^{-1}E(1)^{-1} \tag{5}$$

Then, $\{E(x_i), E(y_i), E(x_{i+1}), E(y_{i+1})\}$ is replaced with $\{E(x_i), E(y_i'), E(x_{i+1}), E(y_{i+1}')\}$ to finish data embedding.

The embedded data can be extracted directly from the encrypted stego-images, since there is a one-to-one mapping between $\{y_i, y_{i+1}\}$ and $\{y_i', y_{i+1}'\}$. Please refer to Table 2 in [12].

The embedded data can also be extracted from the decrypted stego-images. After decryption, the obtained pixel/unit pair is $\{x_i, y_i', x_{i+1}, y_{i+1}'\}$. By comparing the values of y_i' and y_{i+1}', the embedded bits can be extracted. If $y_i' < y_{i+1}'$, the embedded bit is 0, and y_i and y_{i+1} can be restored according to (6);

$$\begin{cases} y_i = \frac{y'_i + y'_{i+1} - 4}{2} \\ y_{i+1} = \frac{y'_{i+1} - y'_i - 2}{2} \end{cases} \tag{6}$$

else if $y_i' > y_{i+1}'$, the embedded bit is 1, and y_i and y_{i+1} can be restored according to (7).

$$\begin{cases} y_i = \frac{y'_i + y'_{i+1} - 4}{2} \\ y_{i+1} = \frac{y'_i - y'_{i+1} - 2}{2} \end{cases} \tag{7}$$

Finally, the image/signal can be reconstructed. For further details, please refer to [12]. It is noted that there exists some clerical errors in [12].

As claimed by the authors, [12] is the first to consider the encrypted signal-based reversible data hiding with public key cryptosystem. Although it has more payload and higher image/signal quality than other encrypted image-based reversible data hiding schemes, the performance can still be greatly improved by making some modifications on the original scheme.

2. **Improvements.** The points of improvements can be summarized as follows: 1) the idea of pixel/unit pair division is abandoned, but the partition of each pixel/unit is reserved; 2) the carrier for data embedding in each pixel/unit is changed from y_i to x_i; 3) the data embedding and extracting procedure is redesigned; 4) each pixel/unit is responsible for carrying one bit, and the payload is doubled compared with the original scheme; 5) the quality of the stego-images is significantly improved.

The process of the improved scheme is shown below:

Image/signal encryption: The provider deals with each pixel/unit of the image/signal respectively. Let a pixel/unit be p_i, where $p_i = x_i + y_i$, $x_i = 2\lfloor p_i/2 \rfloor$ and $y_i = p_i - x_i$. Clearly, x_i must be even. Then, x_i and y_i are encrypted using the public key of Paillier encryption to obtain the cipher text of p_i, i.e., $\{E(x_i), E(y_i)\}$. The security of the cryptosystem lies on the underlying Paillier encryption scheme used, which is the same as [12]. Additional data encryption: The same as that of [12].

Data embedding: Each bit of the encrypted additional data will be embedded into each pixel/unit of the image/signal by the data hider. The corresponding pixel/unit will be set as $\{E(x'_i), E(y_i)\}$. If the bit of the encrypted additional data to be embedded is 0, set $E(x'_i) = E(x_i)$; else if the bit is 1, $E(x'_i)$ is obtained by (8).

$$E(x'_i) = E(x_i + 1) = E(x_i)E(1) \tag{8}$$

Image/signal decryption: The receiver uses the secret key to decrypt the encrypted image/signal with embedded data to obtain the stego-image/signal where each pixel/unit is $p'_i = x'_i + y_i$, i.e., $\{x'_i, y_i\}$.

Data extraction and image/signal recovery: For each pixel/unit, if x'_i is even, indicating that (8) has not been performed on this pixel/unit, the extracted bit is 0, and p_i can be restored according to (9);

$$p_i = x_i + y_i = x'_i + y_i \tag{9}$$

else if x'_i is odd, indicating that (8) has been performed on this pixel/unit, the extracted bit is 1, and p_i can be restored according to (10).

$$p_i = x_i + y_i = x'_i - 1 + y_i \tag{10}$$

Finally, the image/signal can be recovered.

Additional data decryption: The same as that of [12].

3. **Analysis and experiments.** Image/signal quality and payload are two major issues in the area of data hiding. For quality, we consider images/signals with mean squared error (MSE) and peak signal-to-noise ratio (PSNR).

$$\mathrm{MSE} = \frac{1}{n}\sum_{k=1}^{n} (p_i - {p'}_i)^2 \tag{11}$$

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right) \tag{12}$$

where n is the number of total pixels/units. Since the encrypted additional data to be embedded is randomized, the probability of 0 appeared in the encrypted additional data is equal to that of 1 appeared, and (8) would be performed in about half the cases in the data embedding procedure. Hence, the expectation of MSE can be calculated from (13) when the payload is maximized.

$$\mathrm{MSE}_\varepsilon = \frac{1}{n}\sum_{k=1}^{n} (p_i - {p'}_i)^2 = \frac{1}{n}\sum_{k=1}^{n} (x_i - {x'}_i)^2 = \frac{(x_i - x_i)^2 + (x_i - (x_i + 1))^2}{2} = 0.5 \tag{13}$$

And the expectation of PSNR should be:

$$\mathrm{PSNR}_\varepsilon = 10\log_{10}\left(\frac{255^2}{0.5}\right) \approx 51.14 \tag{14}$$

The results show that the quality of the obtained stego-image/signal using the proposed method is significantly higher than that using the original method [12], where MSE_ε and $\mathrm{PSNR}_\varepsilon$ are 6.75 and 39.84 respectively.

In addition, the best payload is 1 bpp in the proposed method, which means that the data hider is able to embed one bit of the additional data into each pixel/unit. However, it is only 0.5 bpp in [12] due to the fact that at least two pixels/units can carry one bit.

The same as [12], we use images instead of signals in the experiments. Amount to 500 miscellaneous images obtained from both the USC-SIPI [17] and the ImageNet [18] image database are tested. In order to show the performance of the proposed method convincingly, the recent published schemes of reversible data hiding in encrypted images, i.e., [15] and [16], are also compared. Fig.1 shows the average PSNR versus payload using the proposed method, the original method [12], and the recent published schemes [15] and [16]. Clearly, the proposed method outperforms the other schemes in terms of either image quality or payload.

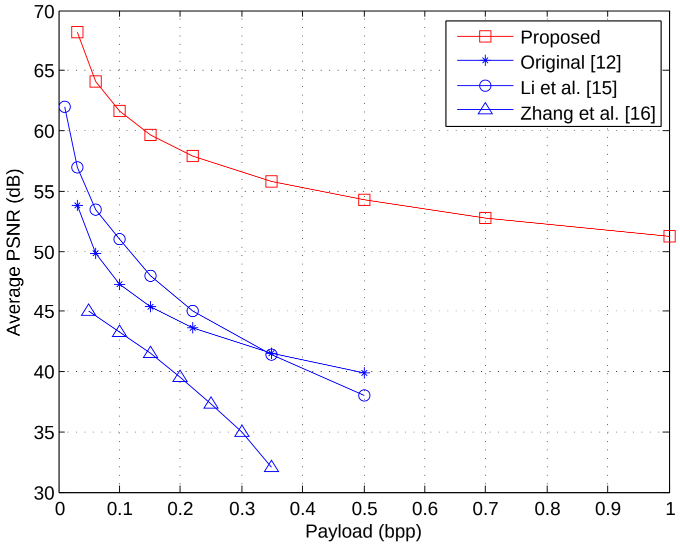

FIGURE 1. Average PSNR versus Payload.

4. **Conclusions.**

The first scheme of encrypted signal-based reversible data hiding with public key cryptosystem is improved in this letter. The idea of pixel/unit pair division is abandoned, and each pixel/unit could carry one bit of the encrypted additional data using the proposed data embedding method. The payload is doubled compared with the original scheme, and the quality of the obtained stego-image/signal is also significantly improved. Analysis and experiments verified the superiority of the proposed method.

Acknowledgment. This work is partially supported by the National Natural Science Foundation of China (Grant No. 61602158), the China Postdoctoral Science Foundation (Grant No. 2016M600030), the Science Foundation for the Excellent Youth Scholars of Henan Normal University (Grant No. YQ201607), and also by the PhD Scientific Research Foundation of Henan Normal University (Grant No. qd14134), and the Science Foundation for Young Scholars of Henan Normal University (Grant No. 2014QK20). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] J. Tian, Reversible data embedding using a difference expansion, *IEEE Trans. Circuits Syst. Video Technol.*, vol.13, no.8, pp.890–896, 2003.

[2] Z. Ni, Y.Q. Shi, N. Ansari, and W. Su, Reversible data hiding, *IEEE Trans. Circuits Syst. Video Technol.*, vol.16, no.8, pp.354–362, 2006.

[3] I. C. Dragoi, and D. Coltuc, Adaptive pairing reversible watermarking, *IEEE Trans. Image Process.*, vol.25, no.5, pp.2420–2422, 2016.

[4] B. Ou, X. Li, Y. Zhao, R. Ni, and Y. Q. Shi, Pairwise prediction-error expansion for efficient reversible data hiding, *IEEE Trans. image process.*, vol.22, no.12, pp.5010–5021, 2013.

[5] Z. Zhao, H. Luo, Z. M. Lu, and J. S. Pan, Reversible data hiding based on multilevel histogram modification and sequential recovery, *AEU-Int. J. Electron. Commun.*, vol.65, no.10, pp.814–826, 2011.

[6] S.G. Lian, Z.X. Liu, Z. Ren, and H.L. Wang, Commutative encryption and watermarking in video compression, *IEEE Trans. Circuits Syst. Video Technol.*, vol.17, no.6, pp.774–778, 2007.

[7] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F.G.B. De Natale, and A. Neri, A commutative digital image watermarking and encryption method in the tree structured haar transform domain, *Signal Process.-Image Commun.*, vol.26, no.1, pp.1–12, 2011.

[8] X. Zhang, Reversible data hiding in encrypted images, *IEEE Signal Process. Lett.*, vol.18, no.4, pp.255–258, 2011.

[9] W. Hong, T.S. Chen, and H.Y. Wu, An improved reversible data hiding in encrypted images using side match, *IEEE Signal Process. Lett.*, vol.19, no.4, pp.199–202, 2012.

[10] M. Li, D. Xiao, Z. Peng, and H. Nan, A modified reversible data hiding in encrypted images using random diffusion and accurate prediction, *ETRI J.*, vol.36, no.2, pp.325–328, 2014.

[11] M. Li, D. Xiao, A. Kulsoom, and Y. Zhang, Improved reversible data hiding for encrypted images using full embedding strategy, *Electron. Lett.*, vol.51, no.9, pp.690–691, 2015.

[12] Y.C. Chen, C.W. Shiu, and G. Horng, Encrypted signal-based reversible data hiding with public key cryptosystem, *J. Vis. Commun. Image R.*, vol.25, no.5, pp.1164–1170, 2014.

[13] X. Li, B. Yang, and T. Zeng, Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection, *IEEE Trans. Image Process.*, vol.20, no.12, pp.3524-3533, 2011.

[14] S. Weng, Y. Zhao, J.S. Pan, and R. Ni, Reversible watermarking based on invariability and adjustment on pixel pairs, *IEEE Signal Process. Lett.*, vol.15, pp.721-724, 2008.

[15] M. Li, D. Xiao, Y. Zhang, and H. Nan, Reversible data hiding in encrypted images using cross division and additive homomorphism, *Signal Process.-Image Commun.*, vol.39, pp.234–248, 2015.

[16] X. Zhang, J. Wang, Z. Wang, and H. Cheng, Lossless and reversible data hiding in encrypted images with public key cryptography, *IEEE Trans. Circuits Syst. Video Technol.*, vol.26, no.9, pp.1622–1631, 2016.

[17] USC-SIPI. http://sipi.usc.edu/database/, 2017 (accessed 19.10.17).

[18] ImageNet. http://www.image-net.org/, 2017 (accessed 19.10.17).