Image Reversible Visual Transformation Based on MSB Replacement and Histogram Bin Mapping

Hao-Tian Wu
School of Computer Science and Engineering, South China University of Technology, Guangzhou, GD 510006, P. R. China
E-mail: wuht@scut.edu.cn

Shaohua Tang
School of Computer Science and Engineering, South China University of Technology, Guangzhou, GD 510006, P. R. China
E-mail: csshtang@scut.edu.cn

Jean-Luc Dugelay
Department of Digital Security
EURECOM
Campus SophiaTech, F-06410 Biot, Sophia Antipolis, France
E-mail: jld@eurecom.fr

***Abstract*—An image reversible transformation method is proposed for secret image transmission and privacy protection. With the proposed method, the visual content of a secret image is changed to mimic a target image while the secret image can be recovered from the transformed image. Different from the previous methods that divide the secret image into blocks, our method processes the secret image as a whole so that no block artifact will be caused. Firstly, the most significant bit (MSB) plane of the secret image is replaced and then a process called histogram bin mapping is conducted. The replaced MSB plane and histogram bin mapping information are further hidden into the transformed image. Via reversible data hiding, the secret image can be exactly recovered by extracting the hidden data and reversing the transformation process. The experimental results show that the visual content of secret images can be semantically changed, while almost all of the test images were successfully recovered from the corresponding transformed images.**

Keywords*—*Reversible data hiding*; *visual transformation*; *MSB replacement*; *histograms*; *bin mapping

I. Introduction

Recently, reversible visual transformation (RVT) has been proposed for secret image transmission and privacy protection in [1]-[5]. Different from image scrambling (e.g. [6]), steganography (e.g. [7]-[10]) and integrity verification (e.g. [11]-[14]), RVT was proposed to intentionally change image visual content for camouflage.

The technique of RVT is firstly in [1], where a secret image divided into fragments called tile images. The tile images are re-arranged and modified to create a mosaic image to mimic a target image. By adopting the reversible data hiding (RDH) method in [15] to hide the required information into the mosaic image, the secret image can be recovered when needed. However, one drawback of the method in [1] is that the target image should be selected from a large database to create a sufficiently similar mosaic image. This problem was addressed in [2], where both of the secret image and target image are divided into non-overlapping blocks of the same size. By sorting the blocks according to standard deviation of pixels in them, the color transformation in [16] is adopted to change the color characteristics of a secret block. The mean and standard deviation of a target block are further inherited by the corresponding secret block for visual transformation. However, real numbers are involved in the transformation and need to be converted into integers. Due to the truncation errors, the secret image can only be nearly recovered with the information hidden in the transformed image.

Based on the color transformation in [2], an improved method was proposed in [3] for image camouflage. More specifically, the transformation is simplified by shifting the pixel values in a block with a pre-defined value. The shift amplitudes of all blocks, the overflow/underflow information, rotation information and block indices, are embedded into the transformed image so that reversibility can be achieved. As the information of block indices has been reduced by using the clustering approach, smaller blocks can be generated in [3] to obtain the camouflage images of better quality. Furthermore, the transformation method proposed in [3] was also applied to generate the visually "encrypted" images in [4]. In [5], the original image is reversibly processed according to the transition probability matrix to mimic the target image.

As the methods in [1]-[5] all divide the secret images into blocks, the block effects are more or less introduced into the visually transformed images. Not only are visual distortions caused by the block effects, but the block-based transformation may be easily detected by image forensic [17]-[19] and steganalysis [20] algorithms. So it is worth to study how to perform RVT in a way other than in [1]-[5]. Different from dividing the secret image into blocks, a new RVT method is proposed in this paper for image camouflage by processing the image as a whole based on RDH (e.g., [21]-[35]).

The flowchart of the proposed RVT method is illustrated in Fig. 1. At first, the original secret image is transformed to mimic the target image by performing the most significant bit (MSB) replacement. To conceal the content, a histogram modification called bin mapping is further conducted to generate the intermediate transformed image. Meanwhile, the information that can be used to reverse the transformation is recorded, including the replaced MSB plane and the bin mapping information. Since the correlations between the neighboring pixels may be largely destroyed, those RDH methods (e.g. [22]-[31]) are not applicable for high-capacity embedding. Instead, the histogram-based method in [32] is adopted so that the side information can be hidden for the majority of test images. The experimental results have shown that the reversibility of visual

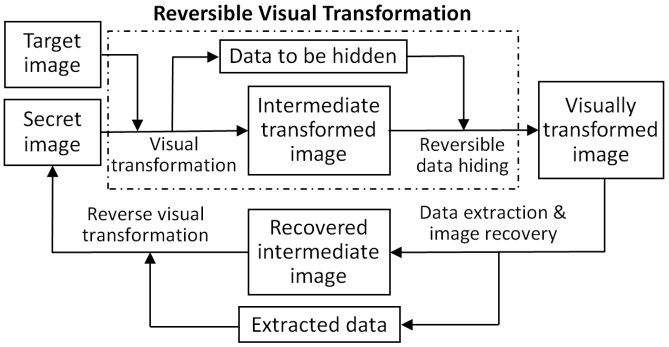


Fig. 1. Flowchart of the proposed reversible visual transformation method based on reversible data hiding.

transformation can be achieved with the proposed method by processing the secret image as a whole.

The rest of this paper is organized as follows. In Section II, we will introduce a new RVT method to conceal the secret image content by the processing it as a whole. The performance of the proposed method is analyzed in Section III. Finally, the concluding remarks are drawn in Section IV.

II. Proposed Reversible Visual Transformation Method

In this section, a RVT method is proposed for image camouflage. As illustrated in Fig. 1, the proposed reversible visual transformation consists of two phases, i.e., visual transformation and reversible data hiding. Accordingly, recovering the secret image from the visually transformed image consists of data extraction and reverse transformation.

A. Visual Transformation According to Target Image

To mimic the target image, the most significant part of the secret image is chosen to be modified. For this reason, the most significant bit (MSB) plane of a secret image is replaced by the MSB plane or a binary image obtained from the target image. To recover the secret image, the original MSB plane is compressed in a lossless way (e.g., by the JBIG2 compression standard [36]) and recorded as part of side information.

In addition to the MSB replacement, further modification is needed to blur the detail information. A simple but efficient histogram modification called bin mapping is performed. For a gray-level image, the histogram is firstly calculated. To maintain the updated MSBs during the histogram modification, the bin mapping is conducted by dividing the histogram into two intervals, i.e., $[0, 127]$ and $[128, 255]$. For a bin value that falls into one interval, it will be mapped within the same interval. Moreover, the histogram bins in each interval are sorted according to their heights. For an 8-bit pixel value p, which bin ranks the i-th in its interval, the following operation is conducted to modify the pixel value by

$$p' = \lfloor \frac{p}{128} \rfloor \times 128 + 63 + sign(i\%2 - 1) \times \lfloor \frac{i}{2} \rfloor \quad (1)$$

where $\lfloor \cdot \rfloor$ represents the floor function, $sign(i\%2 - 1) = 1$ when $i\%2 = 1$, and $sign(i\%2 - 1) = -1$ when $i\%2 = 0$. After applying Eq. (1) to every pixel in the MSB-replaced image, the highest bins are mapping around the center of each group. Since the difference between p and p' is within the range of $[-127, 127]$, it can be exactly represented with 8 bits (i.e., 1 byte) while there is no need to record the value of i. In total, at most 256 bytes are required to record the mapping of all histogram bins in the MSB-replaced image. The bin mapping information, together with the compressed bitstream of the original MSB plane, should be recorded to be hidden into the intermediate transformed image in the next phase.

B. RDH with the Method in [32]

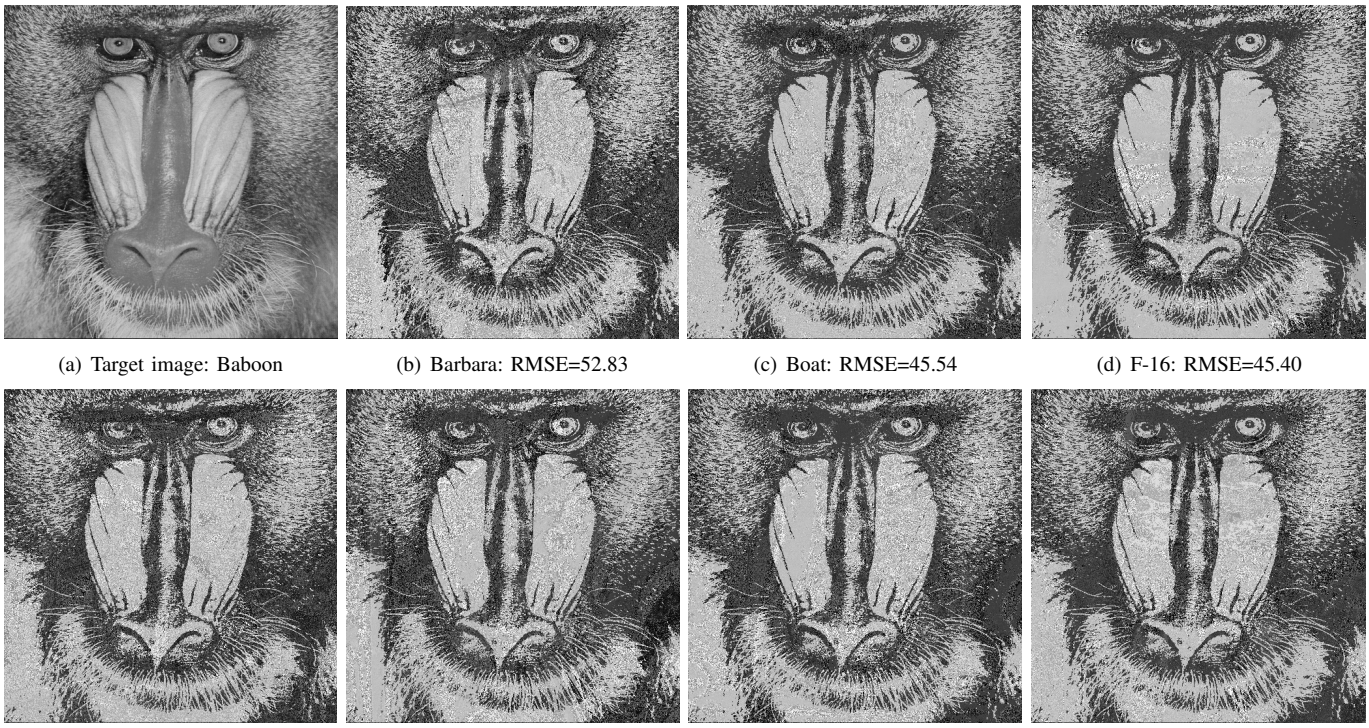
After MSB replacement and bin mapping, the second phase is to hide the recorded data into the intermediate transformed image. As the bin mapping has been conducted by applying Eq. (1) to every pixel, the correlations between the neighboring pixels are largely destroyed so that those RDH methods utilizing the correlations can hardly be adopted. To cope with this issue, a histogram-based RDH method is adopted, in which the correlations between the neighboring pixels are not utilized. Interested readers may refer to [32] for the detailed implementation of the RDH method proposed in it.

There are two parts of the recorded data to be hidden into the intermediate transformed image, i.e., the original MSB plane (after lossless compression) and the bin mapping information. The amount of the first part increases with image size and is much more than the amount of the second part for large images (e.g., 512×512). Since the bin mapping information can be represented by no more than 256 bytes, it is hidden by directly applying the RDH method in [32] to the intermediate transformed image in the **first round of embedding**.

After that, the bitstream of the compressed MSB plane is hidden in succession. In the **second round of embedding**, the RDH method [32] is also adopted but the image histogram is calculated excluding the MSB to keep the MSB plane unchanged. So the histogram bins are with the values from 0 to 127. That means that a pixel value $i \in [0, 127]$ and another pixel value $i + 128$ are counted in the same histogram bin. By applying the bin mapping specified in Eq. (1) to every pixel in the MSB-replaced image, the embedding capacity of adopting [32] can be increased. Different from the case that the image histogram consists of 256 bins, at most 32 pairs of bins can be used for data embedding because the histogram consists of 128 bins. At last, the visually transformed image is generated after two rounds of data embedding.

C. Recovering the Original Secret Image

To recover the secret image, two rounds of data extraction need to be conducted. Firstly, the histogram of the visually transformed image is calculated excluding the MSB so that the bitstream of the compressed MSB plane can be extracted. Meanwhile, the image before the second round of data embedding is blindly recovered. Then the histogram of the newly-recovered image is calculated so that the bin mapping information can be obtained. Since data hiding is reversible,



(a) Target image: Baboon (b) Barbara: RMSE=52.83 (c) Boat: RMSE=45.54 (d) F-16: RMSE=45.40

(e) Goldhill: RMSE=49.21 (f) Lena: RMSE=51.49 (g) Peppers: RMSE=51.90 (h) Sailboat: RMSE=48.53

Fig. 2. The target image "Baboon", and seven images transformed from the other test images with the proposed RVT method.

TABLE I. Visual Transformation of 8 USC-SIPI Images

Test image	Side information (bytes)		Embedding capacity (bytes)			Blind Self-recovery
	MSB plane	Bin mapping	First round	Second round	Pure data	
Lena	4749	256	416	5358	769	Yes
Boat	6307	245	1390	6598	1436	Yes
Barbara	6878	241	728	7165	774	Yes
F-16	3230	256	1311	3977	1508	Yes
Goldhill	6362	237	800	6543	744	Yes
Peppers	3524	256	398	3871	489	Yes
Sailboat	4700	256	767	5057	868	Yes
Baboon	16108	256	133	4529	-11702	No

the intermediate transformed image is obtained after the second round of data extraction. With the extracted bin mapping information, the original position of every histogram bin is known so that every bin can be moved back. Then the bitstream of MSB plane is decompressed and written back so that the secret image can be eventually recovered.

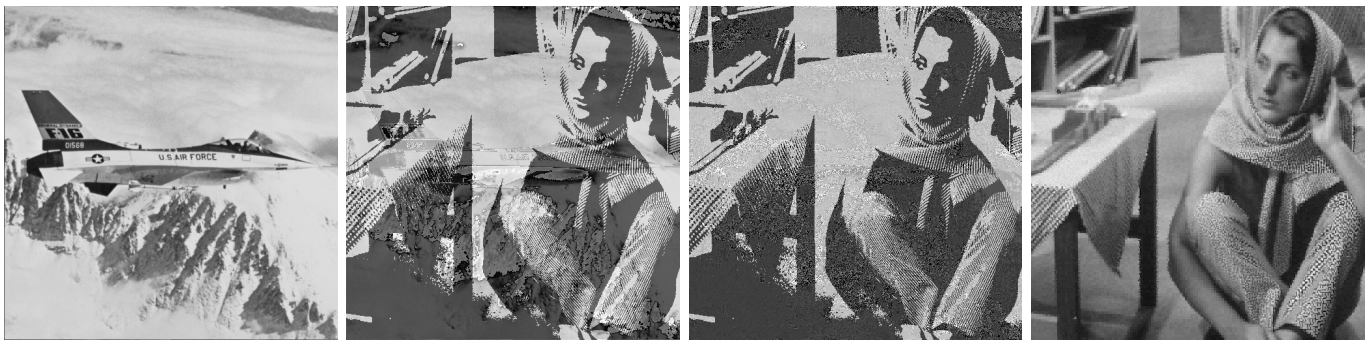
III. Experimental Results

In the experiments, eight USC-SIPI gray-level images with the size of 512×512 were used. Among them, "Baboon" and "Barbara" were chosen as the target images, respectively. For most of the test images, all of the side information was hidden into the transformed image. Only for the high-textured image "Baboon", the reversibility was not achieved due to the insufficient embedding capacity compared with the side information. As shown in Table I, additional data were hidden into the transformed images except "Baboon". For some test images, the amount of bin mapping information was less than 256 bytes because some gray levels were absent in the MSB-replaced images. To measure the difference between the transformed image and the target image, the root mean square error (RMSE) between them was calculated.

In Fig. 2, the target image "Baboon" and seven visually transformed images are shown. Although the corresponding RMSE was high, the visual content of each secret image was semantically changed. To further demonstrate the performance, six secret images to be camouflaged, the ones after MSB replacement, and the ones after visual transformation are shown in Fig. 3 and Fig. 4 by choosing "Barbara" as the target image, respectively. It can be seen in the second column of Fig. 3 and Fig. 4 that the contour of secret images can still be noticed after MSB replacement, indicating that the MSB replacement itself cannot conceal the visual content. By applying the operation in Eq. (1) to every pixel value, the visual content was largely blurred to conceal the image details. Compared with the images transformed by the method in [3] as shown in the right column, no block effect was caused by the proposed method. In the cases as shown in Fig. 2, Fig. 3 and Fig. 4, the same target image was chosen to illustrate the impact of secret images on the visually transformed ones. Despite that the secret images were different, all of the transformed images looked similar to each other.

Although the transformed images were visually different

(a) Secret image: Lena (b) MSB-replaced: RMSE=49.16 (c) Transformed image: RMSE=49.31 (d) Transformed image by Method [3]



(e) Secret image: F-16 (f) MSB-replaced: RMSE=43.59 (g) Transformed image: RMSE=42.69 (h) Transformed image by Method [3]

(i) Secret image: Boat (j) MSB-replaced: RMSE=52.36 (k) Transformed image: RMSE=42.90 (l) Transformed image by Method [3]

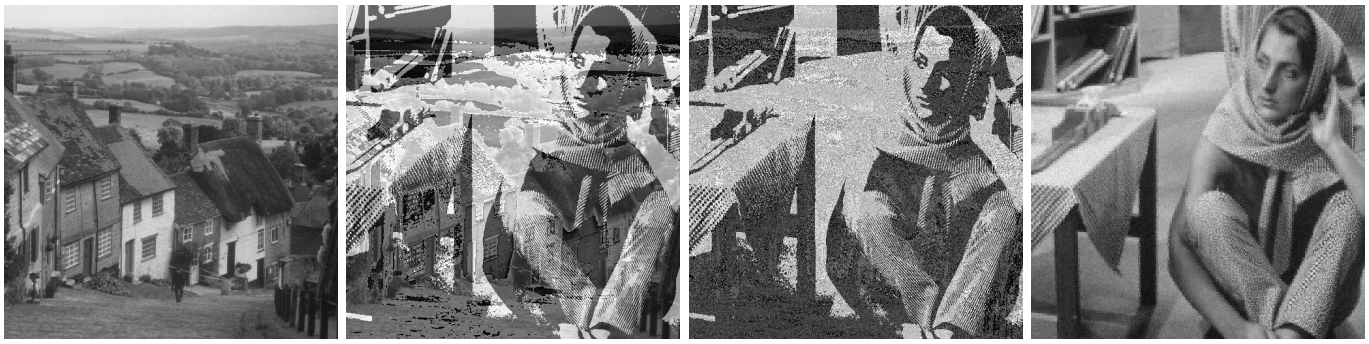
Fig. 3. The secret images (left column), MSB-replaced images (second column) and visually transformed images (third column) with the proposed method and the images transformed with the method [3] (right column) by choosing "Barbara" as the target image, respectively.

from natural images, the secret content can be protected. The security of the proposed RVT method relies on the order of scanning pixels in applying the method in [32] for RDH. Although the transformed images were different from the natural images, the computations for recovering the secret images will exponentially increase with the pixel number without knowing the correct order. Since the target image can be arbitrarily chosen, collusion attack can be avoided by using a different target image for each secret image.

IV. Concluding Remarks

We have proposed an image reversible visual transformation method for secret transmission and privacy protection. By replacing the most significant bit plane and performing the modification called histogram bin mapping, the secret image can be visually changed to mimic an arbitrary target image. By embedding the necessary information into the transformed image based on RDH, the transformation can be reversed to recover the original secret image.

Different from the image transformation methods in [1]-[5], the secret image is processed as a whole in our proposed method so that no block artifact is caused. The experimental results have shown that most test images can be reversibly transformed. Besides improving the visual quality of the transformed image, how to increase the embedding capacity for the high-textured images will be studied in future.



(a) Secret image: Goldhill (b) MSB-replaced: RMSE=48.90 (c) Transformed image: RMSE=47.36 (d) Transformed image by Method [3]

(e) Secret image: Peppers (f) MSB-replaced: RMSE=47.93 (g) Transformed image: RMSE=49.64 (h) Transformed image by Method [3]

(i) Secret image: Sailboat (j) MSB-replaced: RMSE=43.43 (k) Transformed image: RMSE=45.70 (l) Transformed image by Method [3]

Fig. 4. The secret images (left column), MSB-replaced images (second column) and visually transformed images (third column) with the proposed method and the images transformed with the method [3] (right column) by choosing "Barbara" as the target image, respectively.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their insightful comments and valuable suggestions to improve the paper quality. This work was supported by Natural Science Foundation of China (No. 61772208, 61632013), Natural Science Foundation of Jiangsu Province of China (No. BK20151131), and SCUT Fundamental Research Funds for the Central Universities of China (No. 2017MS038).

REFERENCES

[1] I. J. Lai and W. H. Tsai, "Secret-fragment-visible mosaic image - A new computer art and its application to information hiding," *IEEE Trans. Inf. Forens. Secur.*, Vol. 6, No. 3, pp. 936-945, Sep. 2011.

[2] Y. L. Lee and W. H. Tsai, "A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations," *IEEE Trans. Circuits Syst. Video Technol.*, Vol. 24, No. 4, pp. 695-703, Apr. 2014.

[3] D. Hou, W. Zhang, and N. Yu, "Image camouflage by reversible image transformation," *J. Vis. Commun. Image R.*, Vol. 40(A), pp. 225-236, Oct. 2016.

[4] W. Zhang, H. Wang, D. Hou, and N. Yu, "Reversible data hiding in encrypted images by reversible image transformation," *IEEE Trans. Multimedia*, Vol. 18, No. 8, pp. 1469-1479, Aug. 2016.

[5] D. Hou, W. Zhang, Z. Zhan, R. Jiang, Y. Yang, and N. Yu, "Reversible image processing via reversible data hiding," *Proc. IEEE International Workshop on Digital Signal Processing*, pp. 427-431, 2016.

[6] C. Li, D. Lin, and J. Lü, "Cryptanalyzing an Image-Scrambling Encryption Algorithm of Pixel Bits," *IEEE Trans. Multimedia*, Vol. 24, No. 3, pp. 64-71, Aug. 2017.

[7] B. Li, S. Tan, M. Wang, and J. Huang, "Investigation on Cost Assignment

in Spatial Image Steganography," *IEEE Trans. Inf. Forens. Secur.*, Vol. 9, No. 8, pp. 1264-1277, 2014.

[8] L. Guo, J. Ni, W. Su, C. Tang, and Y. Q. Shi, "Using Statistical Image Model for JPEG Steganography: Uniform Embedding Revisited," *IEEE Trans. Inf. Forens. Secur.*, Vol. 10, No. 12, pp. 2669-2680, 2015.

[9] X. Liao, Z. Qin, and L. Ding, "Data Embedding in Digital Images using Critical Functions," *Signal Processing: Image Communication*, Vol. 58, pp. 146-156, Oct. 2017.

[10] H. T. Wu, J. L. Dugelay, and Y. M. Cheung, "A Data Mapping Method for Steganography and Its Application to Images," *Proc. the 10th Information Hiding Workshop*, LNCS 5284, pp. 236-250, May, 2008.

[11] H. T. Wu and Y. M. Cheung, "Public Authentication of 3D Mesh Models," *Proc. the 2006 IEEE / WIC / ACM International Conference on Web Intelligence*, pp. 940-946, 2006.

[12] H. T. Wu and Y. M. Cheung, "A High-Capacity Data Hiding Method for Polygonal Meshes," *Proc. the 8th Information Hiding Workshop*, LNCS 4437, pp. 188-200, July, 2006.

[13] Y. M. Cheung and H. T. Wu, "A sequential quantization strategy for data embedding and integrity verification," *IEEE Trans. Circ. Syst. Video Technol.*, Vol. 17, No. 8, pp. 1007-1016, Aug. 2007.

[14] H. T. Wu and J. L. Dugelay, "Reversible Watermarking of 3D Mesh Models by Prediction-error Expansion," *Proc. IEEE International Workshop on Multimedia Signal Processing*, pp. 797-802, 2008.

[15] D. Coltuc and J. M. Chassery, "Very fast watermarking by reversible contrast mapping," *IEEE Signal Processing Letters*, Vol. 14, No. 4, pp. 255-258, Apr. 2007.

[16] E. Reinhard, M. Ashikhmin, B. Gooch, and P. Shirley, "Color transfer between images," *IEEE Comput. Graph. Appl.*, Vol. 21, No. 5, pp. 34-41, Sep.-Oct. 2001

[17] T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of JPEG artifacts," *IEEE Trans. Inf. Foren. Sec.*, Vol. 7, No. 3, pp. 1003-1017, 2012.

[18] W. Wang, J. Dong, and T. Tan, "Exploring DCT coefficient quantization effect for image tampering localization," *Proc. the 2011 IEEE International Workshop on Information Forensics and Security*, 2011.

[19] J. Yang, J. Xie, G. Zhu, S. Kwong, and Y. Q. Shi, "An effective method for detecting double JPEG compression with the same quantization matrix," *IEEE Trans. Inf. Foren. Sec.*, Vol. 9, No. 11, pp. 1933-1942, 2014.

[20] H. T. Wu, Y. Liu, J. Huang, and X. Yang, "Improved steganalysis algorithm against motion vector based video steganography," *Proc. the 21st IEEE International Conference on Image Processing*, pp. 5512-5516, 2014.

[21] Y. Q. Shi, X. Li, X. Zhang, H. T. Wu, and B. Ma "Reversible data hiding: Advances in the past two decades," *IEEE Access.*, Vol. 4, pp. 3210-3237, 2016.

[22] 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.*, Vol. 19, No. 7, pp. 989-999, Jul. 2009.

[23] Y. Hu, H. K. Lee, and J. Li, "DE-based reversible data hiding with improved overflow location map," *IEEE Trans. Circuits Syst. Video Technol.*, Vol. 19, No. 2, pp. 250-260, Feb. 2009.

[24] H. T. Wu and Y. M. Cheung, "Reversible watermarking by modulation and security enhancement," *IEEE Trans. Instrum. Meas.*, Vol. 59, No. 1, pp. 221-228, Jan. 2010.

[25] 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, Jan. 2011.

[26] H. T. Wu and J. Huang, "Reversible image watermarking on prediction error by efficient histogram modification," *Signal Processing*, Vol. 92, No. 12, pp. 3000-3009, Dec. 2012.

[27] 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, Dec. 2013.

[28] I. C. Dragoi and D. Coltuc, "On local prediction based reversible watermarking," *IEEE Trans. Image Process.*, Vol. 24, No. 4, pp. 1244-1246, Apr. 2015.

[29] X. Li, W. Zhang, X. Gui, and B. Yang, "Efficient reversible data hiding based on multiple histograms modification," *IEEE Trans. Inf. Foren. Sec.*, Vol. 10, No. 9, pp. 2016-2027, Sep. 2015.

[30] I. C. Dragoi and D. Coltuc, "Adaptive Pairing Reversible Watermarking," *IEEE Trans. Image Process.*, Vol. 25, No. 5, pp. 2420-2422, 2016.

[31] J. Wang, J. Ni, X. Zhang, and Y. Q. Shi, "Rate and Distortion Optimization for Reversible Data Hiding Using Multiple Histogram Shifting," *IEEE Trans. Cybern.*, Vol. 47, No. 2, pp. 315-326, Feb. 2017.

[32] H. T. Wu, J. L. Dugelay, and Y. Q. Shi, "Reversible image data hiding with contrast enhancement," *IEEE Signal Process. Lett.*, Vol.22, No.1, pp. 81-85, Jan. 2015.

[33] H. T. Wu, J. Huang, and Y. Q. Shi, "A reversible data hiding method with contrast enhancement for medical images," *J. Vis. Commun. Image R.*, Vol. 31, pp. 146-153, 2015.

[34] H. T. Wu, Y. M. Cheung, and J. Huang, "Reversible data hiding in paillier cryptosystem," *J. Vis. Commun. Image R.*, Vol. 40, pp. 765-771, 2016.

[35] H. T. Wu, S. Tang, J. Huang, and Y. Q. Shi, "A novel reversible data hiding method with image contrast enhancement," *Signal Processing: Image Communication*, Vol. 62, pp. 64-73, Mar. 2018.

[36] P. G. Howard, F. Kossentini, B. Martins, S. Forchhammer, and W. J. Rucklidge, "The emerging JBIG2 standard," *IEEE Trans. Circuits Syst. Video Technol.*, Vol.8, No.7, pp. 838-848, Jul. 1998.