Letters

Towards Robust Image Steganography

Jinyuan Tao, Sheng Li, Xinpeng Zhang, and Zichi Wang

***Abstract*— Posting images on social network platforms is happening everywhere and every single second. Thus, the communication channels offered by various social networks have a great potential for covert communication. However, images transmitted through such channels will usually be JPEG compressed, which fails most of the existing steganographic schemes. In this paper, we propose a novel image steganography framework that is robust for such channels. In particular, we first obtain the channel compressed version (i.e., the channel output) of the original image. Secret data is embedded into the channel compressed original image by using any of the existing JPEG steganographic schemes, which produces the stego-image after the channel transmission. To generate the corresponding image before the channel transmission (termed the intermediate image), we propose a coefficient adjustment scheme to slightly modify the original image based on the stego-image. The adjustment is done such that the channel compressed version of the intermediate image is exactly the same as the stego-image. Therefore, after the channel transmission, secret data can be extracted from the stego-image with 100% accuracy. Various experiments are conducted to show the effectiveness of the proposed framework for image steganography robust to JPEG compression.**

***Index Terms*— Steganography, robust, JPEG compression.**

I. Introduction

Data hiding is a technique of embedding secrets into the digital media imperceptibly, which can be categorized into watermarking and steganography according to different applications. Watermarking is the process of marking the digital media for copyright protection [1]–[3], while steganography is mainly developed for covert communication [4]–[10]. Different types of media data are considered in the literature for steganography including text [5], image [6], [7], audio [8] and video [9], where the image steganography is the most popular. The task of image steganography is to make tiny changes on the pixels either in the spatial domain or the transformed domain to carry sufficient secret information. Meanwhile, the statistical and visual features of the original image are preserved.

Early image steganographic methods adjust the value of the pixel (or coefficient) either by following a specific statistical model or reducing the modification caused by data embedding [11]–[15]. Westfeld [11] uniformly spread out the changes over all the Discrete Cosine Transformation (DCT) coefficients to resist the statistical attacks. In [13], the directions of modification are fully exploited to achieve high embedding efficiency. In [15], the DCT coefficients are categorized into four bands with different embedding rates. The stego-images generated by these schemes can be easily detected using modern steganalysis tools [16]. Recent works on image steganography focus on syndrome trellis coding (STC) based data embedding [17]–[20]. In these schemes, different distortion functions are designed to measure the distortion caused due to the data embedding. The STC seeks a solution to minimize such distortion, which achieves relatively good performance in terms of resisting the steganalysis tools.

Regardless the STC based or the non-STC based steganographic schemes, they focus on how to embed the secret such that no suspicions are caused by data embedding. The subtle changes of the pixels are not able to resist any post processing on the stego-images. The secrets can only be extracted when the communication channel is lossless. However, this is generally not the case for the images transmitted and stored in social network platforms, which will usually be JPEG compressed due to the limitation of storage and bandwidth. In such a case, all the aforementioned steganographic schemes cannot work because of the JPEG compression. With the social networks more and more popular, the corresponding communication channels become a useful resource for covert communication. To take advantage of such channels, it is necessary and urgent to develop image steganographic schemes that are robust to JPEG compression.

A few attempts have been conducted in the literature for designing such steganographic schemes [21], [22]. In these schemes, the Reed-Solomon error correction is applied to encode the secret data to improve the data extraction accuracy. While the data embedding is performed by modifying the quantized DCT coefficients of the original image. In [21], the strength of the modification is computed based on the corresponding DCT coefficients from a set of four neighboring blocks. In [22], the modification strength is obtained

Manuscript received June 2, 2018; revised September 30, 2018; accepted November 9, 2018. Date of publication November 13, 2018; date of current version February 5, 2019. This work was supported in part by the National Natural Science Foundation of China under Grant 61602294, Grant U1636206, Grant 61525203, and Grant 61472235, in part by the Shanghai Sailing Program under Grant 16YF1404100, in part by the Young Oriental Scholar under Shanghai Institutions of Higher Education, in part by the Shanghai Dawn Scholar Plan under Grant 14SG36, and in part by the Shanghai Excellent Academic Leader Plan under Grant 16XD1401200. This paper was recommended by Associate Editor A. K. Roy-Chowdhury. *(Corresponding author: Sheng Li.)*

J. Tao, X. Zhang, and Z. Wang are with the School of Communication and Information Engineering, Shanghai University, Shanghai 200444, China (e-mail: taojinyuanshu@163.com; wangzichi@shu.edu.cn; xzhang@shu.edu.cn).

S. Li is with the School of Computer Science, Shanghai Institute of Intelligent Electronics and Systems, Fudan University, Shanghai 201203, China(e-mail: lisheng@fudan.edu.cn).

Digital Object Identifier 10.1109/TCSVT.2018.2881118

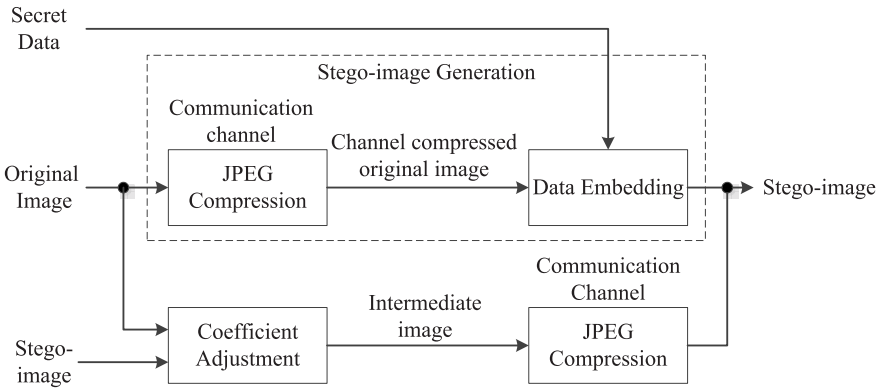

Fig. 1. The proposed framework for robust image steganography.

by dither modulation. These schemes are able to generate the stego-image with high data extraction accuracy as well as reasonably good non-detectability after the channel transmission.[1] However, they can not guarantee full recovery of the secret data even with the help of error correction codes. Meanwhile, the payload needs to be very low to ensure the non-detectability.

In this paper, we propose a novel image steganography framework that is able to resist the JPEG compression. Unlike the existing schemes, our framework does not require any error correction on the secret data, which guarantees the full recovery of the secret data from the stego-image. The main contributions are summarized as follows.

1) We propose a novel image steganography framework robust to JPEG compression, where any of the existing JPEG steganographic schemes can be adopted to generate the stego-image.
2) We propose a coefficient adjustment scheme to modify the original image based on the stego-image, so as to generate the corresponding image (with hidden data) before the channel transmission (termed as the intermediate image for simplicity).
3) We proof that we can always generate an intermediate image whose channel compressed version is exactly the same as the stego-image.
4) It is guaranteed that the secret data can be recovered from our stego-image with 100% accuracy, and high non-detectability can be achieved by using an advance JPEG steganographic scheme in our framework.

II. The Proposed Method

The flowchart of our proposed framework is illustrated in Fig. 1. Given an original image and the secret data to be hidden, our purpose is to generate an intermediate image whose channel compressed version is exactly the same as the stego-image. To this end, we first obtain the stego-image by data embedding on the channel compressed original image using any of the existing JPEG steganographic schemes. Then, we propose a coefficient adjustment scheme to produce the intermediate image based on the stego-image and the original image. This scheme ensures that the channel compressed version of the intermediate image is exactly the same as the stego-image.

[1]Unless otherwise stated, all the stego-images mentioned in the rest of this paper refer to the image with hidden data after the channel transmission.

A. Stego-Image Generation

Let's assume the quality factor of the JPEG compression of the communication channel is Q_c (within the range of $[1, 100]$), which can be obtained according to the image received from the output of the channel. Most of the time, the original image is already JPEG compressed, we denote the corresponding quality factor as Q_o. Given the quantized DCT coefficients of an original JPEG image, the communication channel first performs an inverse DCT quantization according to Q_o to estimate the original DCT coefficients, which are then quantized again according to Q_c. The quantized DCT coefficient located at (i, j) after the channel compression is computed as

$$C(i, j) = \text{round}\left[O(i, j)\frac{M_o(i, j)}{M_c(i, j)}\right], \tag{1}$$

where round$(\cdot)$ is the rounding operation, $O(i, j)$ is the quantized DCT coefficient of the original image at (i, j), $M_o(i, j)$ and $M_c(i, j)$ are the corresponding quantization steps at (i, j) for quality factors Q_o and Q_c, respectively. Once the channel compressed original image is available, we generate the stego-image by embedding the secret data into this image using any of the existing JPEG steganographic schemes. In our implementation, we adopt two popular JPEG steganographic schemes: the J-UNIWARD [18] and UERD [19], for the generation of stego-images. These schemes incorporate the STC framework with different distortion functions. The J-UNIWARD measures the distortion by a sum of relative changes between the original and stego images in the wavelet domain, the UERD computes the distortion by multiplying the quantization steps and the energy of the DCT block. Sometimes, the original image might be uncompressed. In such a case, we perform JPEG compression on the original image using $Q_o = 100$ to obtain an original JPEG image. Then, we obtain the channel compressed original image according to Q_c for generating the stego-image.

The stego-image is eventually the image received from the output of the communication channel for covert communication. Upon receiving the stego-image, the secret data can be extracted based on the data extraction of the JPEG steganographic scheme adopted in the framework.

B. Coefficient Adjustment

Now the question becomes to how to generate an intermediate image before the channel transmission such that its channel compressed version is exactly the stego-image. To do so, we propose in this section a coefficient adjustment scheme to generate the intermediate image based on the original image and the stego-image. The design of the scheme relies on the following lemma.

Lemma 1: Given the stego-image S and the original image O, we can always find a dithering map α to make the following equation hold

$$S(i,j) = \text{round}\left[I(i,j)\frac{M_o(i,j)}{M_c(i,j)}\right], \tag{2}$$

where

$$I(i,j) = O(i,j) + \alpha(i,j), \tag{3}$$

where $\alpha(i,j)$ is an integer.

Proof: Advanced JPEG steganographic schemes tend to modify each quantized DCT coefficient (i.e., $C(i,j)$) by a maximum of 1 or -1 [18], [19]. First of all, if $C(i,j) = S(i,j)$, then Eq. (2) always holds for $\alpha(i,j) = 0$. Now, let's consider the rest two cases including $S(i,j) = C(i,j)+1$ and $S(i,j) = C(i,j) - 1$. For simplicity, we denote

$$Z(i,j) = O(i,j)\frac{M_o(i,j)}{M_c(i,j)}. \tag{4}$$

If $S(i,j) = C(i,j) + 1$, then Eq. (2) is equivalent to

$$Z(i,j) + \alpha(i,j)\cdot\frac{M_o(i,j)}{M_c(i,j)} = C(i,j) + \lambda, \tag{5}$$

where $\lambda \in [0.5, 1.5)$. To make Eq. (5) hold, we have to find an integer $\alpha(i,j)$ to make the following inequality hold

$$\begin{aligned}[C(i,j) + 0.5 - Z(i,j)]\cdot\frac{M_c(i,j)}{M_o(i,j)} &\le \alpha(i,j) \\ &< [C(i,j) + 1.5 - Z(i,j)]\cdot\frac{M_c(i,j)}{M_o(i,j)}.\end{aligned} \tag{6}$$

The existence of $\alpha(i,j)$ depends on the distance between the upper bound and lower bound of the inequality (6), which is computed as

$$d = \frac{M_c(i,j)}{M_o(i,j)}. \tag{7}$$

In general, Q_c should be less than Q_o for the sake of storage saving. This means the quantization step $M_c(i,j)$ should be larger than $M_o(i,j)$. Therefore, d is always larger than 1 and we can always find an integer $\alpha(i,j)$ to make the inequality (6) hold, and Eq. (2) is held accordingly. If $Q_c > Q_o$, $M_c(i,j)$ will be less than $M_o(i,j)$. In such a case, we have $d < 1$ and the existence of $\alpha(i,j)$ is not guaranteed.

For the same token, we can also proof that there exists an integer $\alpha(i,j)$ to make Eq. (2) hold when $S(i,j) = C(i,j)-1$. Note that the range of λ becomes $[-1.5, 0.5)$ in such a case. ■

Given an original JPEG image, we adjust $O(i,j)$ by

$$I(i,j) = O(i,j) + \alpha(i,j), \tag{8}$$

where

$$\alpha(i,j) = \underset{x \text{ is an integer}}{\text{argmin}}\left|[O(i,j) + x]\cdot\frac{M_o(i,j)}{M_c(i,j)} - S(i,j)\right|. \tag{9}$$

After the adjustment, we are able to generate the intermediate image (which is a JPEG image) by using the same quantization table as the original JPEG image, where $I(i,j)$ is the quantized DCT coefficient. According to the lemma, we can always produce an intermediate image whose channel compressed version is exactly the same as the stego-image.

It should be noted that our proposed scheme is not robust when the coefficients of the intermediate image are changed by a middleman. In such a case, the channel compressed version of the intermediate image may not be exactly the same as the stego-image, which will result in incorrect data extraction.

III. Experimental Results and Discussions

Two databases are used in our experiment including the BOSSbass-1.01 [23] and UCID [24]. The BOSSbass-1.01 contains 10000 uncompressed grayscale images with the size of 512×512, and the UCID consists of 1338 uncompressed color images with the size of 512×384. These images are JPEG compressed using two quality factors including $Q_o = 100$ and $Q_o = 95$, which are severed as the original JPEG images. Thus, we build four JPEG image databases including the BOSSbass with $Q_o = 100$ and $Q_o = 95$, the UCID with $Q_o = 100$ and $Q_o = 95$. We consider two different communication channels with quality factors of $Q_c = 95$ and $Q_c = 75$.

A. Robustness

To evaluate the robustness of the proposed framework for image steganography, we randomly select 1000 images from the each of the JPEG image databases and consider the following two cases.

1) The JPEG images with $Q_o = 100$ are assumed to be transmitted in the communication channel with $Q_c = 95$.
2) The JPEG images with $Q_o = 95$ are assumed to be transmitted in the communication channel with $Q_c = 75$.

For each case, we perform the data embedding using our proposed framework to generate 1000 intermediate images, where the stego-images are generated using the J-UNIWARD and UERD at a specific payload from 0.05 to 0.5 bpnzac (bit per non zero AC coefficients). Let's denote our proposed framework with the use of J-UNIWARD and UERD as the J-UNIWARD-P and UERD-P, respectively. The average data extraction error rate (i.e., the percentage of wrongly extracted secret data bits) of the stego-images is given in Table I for

TABLE I

THE AVERAGE DATA EXTRACTION ERROR RATE OF THE STEGO-IMAGES AFTER THE CHANNEL TRANSMISSION (BOSSBASS/UCID)

Payload(bpnzac)		0.05	0.1	0.2	0.3	0.4	0.5
$Q_o = 100$ $Q_c = 95$	UERD	0.4962/0.4986	0.4985/0.5012	0.5007/0.5022	0.5002/0.4999	0.5024/0.5004	0.5008/0.4995
	UERD-P	**0/0**	**0/0**	**0/0**	**0/0**	**0/0**	**0/0**
	J-UNIWARD	0.4964/0.4987	0.5015/0.5011	0.5049/0.4995	0.4992/0.5013	0.4997/0.5005	0.4989/0.4989
	J-UNIWARD-P	**0/0**	**0/0**	**0/0**	**0/0**	**0/0**	**0/0**
$Q_o = 95$ $Q_c = 75$	UERD	0.5011/0.4996	0.5036/0.4989	0.4996/0.5020	0.5004/0.4997	0.502/0.5014	0.4984/0.4998
	UERD-P	**0/0**	**0/0**	**0/0**	**0/0**	**0/0**	**0/0**
	J-UNIWARD	0.5050/0.5022	0.4988/0.5026	0.5011/0.4993	0.4987/0.5003	0.5026/0.5008	0.4994/0.4988
	J-UNIWARD-P	**0/0**	**0/0**	**0/0**	**0/0**	**0/0**	**0/0**

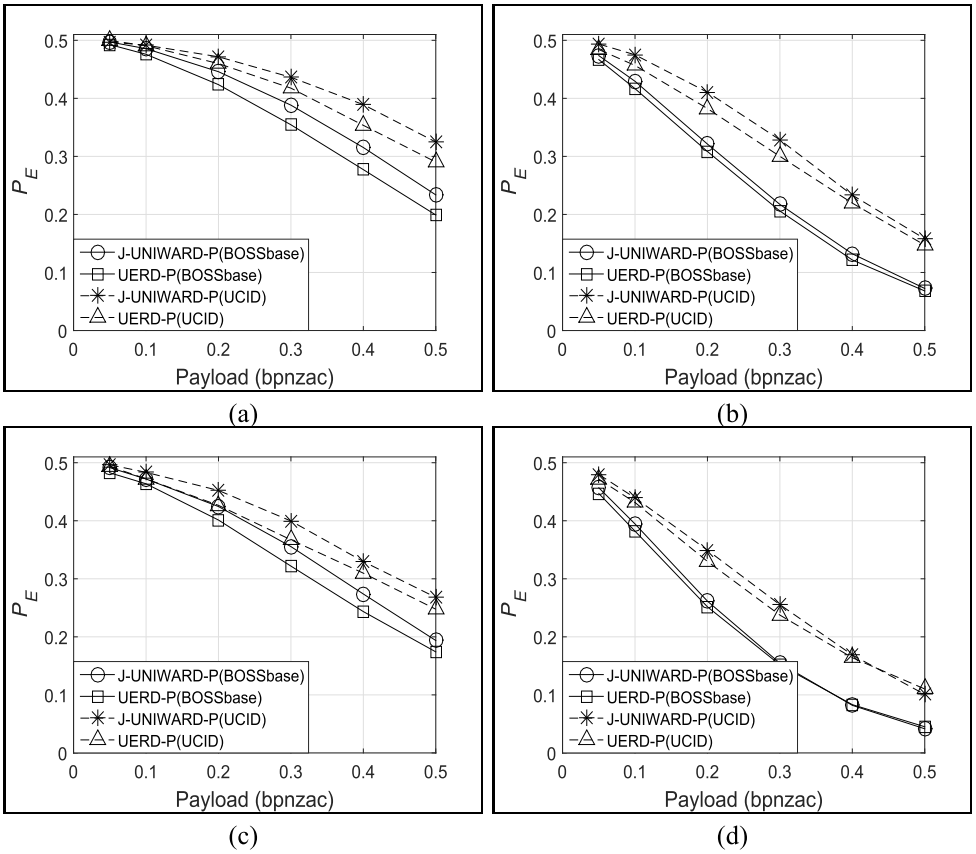

Fig. 2. The non-detectability of the stego-images after the channel transmission. (a) and (b): Non-detectability against the DCTR-8000D detector, with $Q_c = 95$ for (a) and $Q_c = 75$ for (b). (c) and (d): Non-detectability against the GFR-17000D detector, with $Q_c = 95$ for (c) and $Q_c = 75$ for (d).

different schemes, where the J-UNIWORD and UERD refer to the case that we use them to generate the stego-images before the channel transmission. As expected, by using our proposed framework, we can achieve 100% data extraction accuracy for the stego-images after the channel transmission. On the contrary, if we directly use the existing steganographic schemes to generate the stego-images before the channel transmission, we can not extract the secret at all after the channel transmission.

B. Non-Detectability

We adopt two popular feature sets to detect the existence of secret data in our stego-image, including the DCTR-8000D [25] and the GFR-17000D [26]. The ensemble classifier proposed in [27] is used for training and classification. For the BOSSbass/UCID with $Q_o = 100$, we conduct JPEG recompression using $Q_c = 95$ to produce 10000/1338 double JPEG compressed images, which are served as the cover images after the channel transmission. We then perform data embedding on the original JPEG images using our proposed framework to generate 10000/1338 stego-images with $Q_c = 95$. The same operation is also conducted on the BOSSbass/UCID with $Q_o = 95$ using $Q_c = 75$. For each JPEG image database, half of the double JPEG compressed images and half of the stego-images are used for training, while the rest are used for testing. Such process is repeated ten times (i.e., ten trials) to obtain an average classification error rate

$$P_E = \frac{1}{10}\sum_{i=1}^{10}\min_{\tau}\frac{1}{2}[P^i_{\text{fa}}(\tau) + P^i_{\text{md}}(\tau)], \tag{10}$$

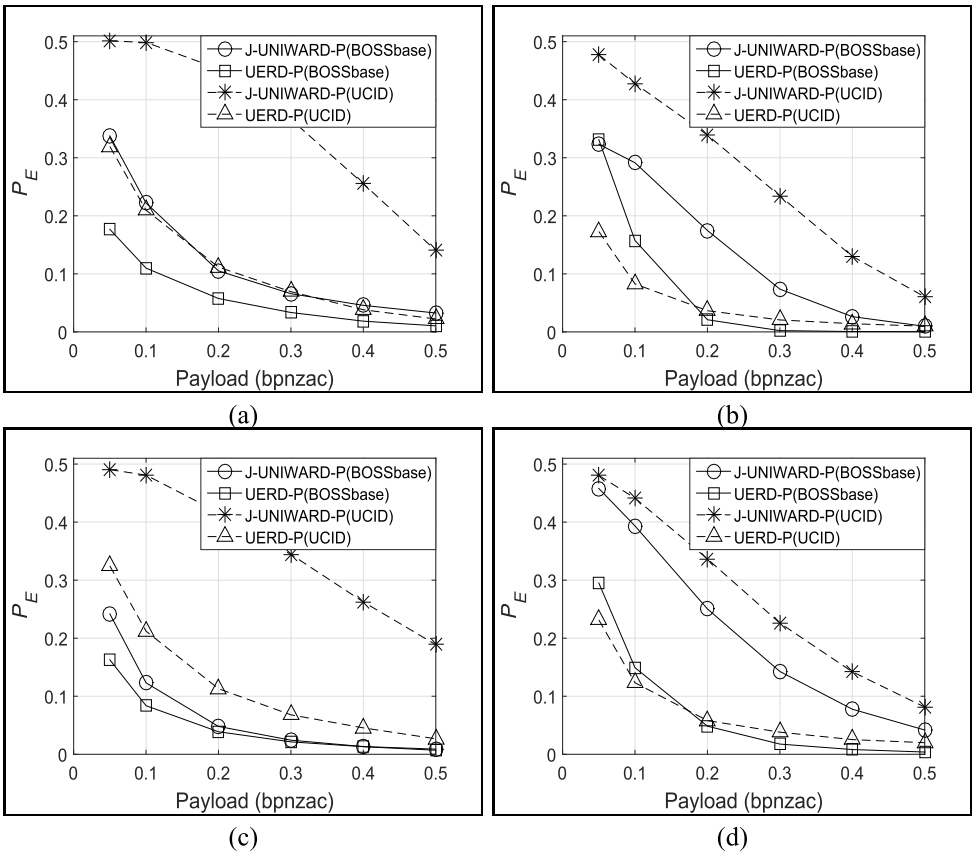

Fig. 3. The non-detectability of the intermediate images. (a) and (b): Non-detectability against the DCTR-8000D detector, with $Q_c = 95$ for (a) and $Q_c = 75$ for (b). (c) and (d): Non-detectability against the GFR-17000D detector, with $Q_c = 95$ for (c) and $Q_c = 75$ for (d).

where τ refers to the threshold of the ensemble classifier, P^i_{fa} and P^i_{md} are false alarm rate and missed detection rate of the ith trial. Fig. 2 shows the performance of the non-detectability of our stego-images, which is considerably good on both databases thanks to the advanced JPEG steganographic schemes adopted in our framework.

Sometimes, the communication channel may be monitored by service providers. In such a case, it is also necessary to evaluate the non-detectability of the intermediate images. For each JPEG image database, half of the original images and half of the intermediate images (corresponding to the stego-images generated before) are used for training the ensemble classifier, while the rest are adopted for testing. Fig. 3 shows the non-detectability of the intermediate images. It can be seen that the intermediate images do not perform as good as the stego-images. This is expected as the dithering strength of the original quantized DCT coefficients may be larger than 1 to produce an intermediate image (see Section II-B). We can also observe that, most of the time, the use of J-UNIWORD produces the intermediate images with much better non-detectability compared with using the UERD, especially on the UCID database.

Table II further gives the average PSNR of the intermediate images, where the column of payload zero reports the PSNR of the original images. It can be seen that, compared with the original images, the PSNR of the intermediate images is slightly reduced on both databases. In addition, the J-UNIWARD-P performs better than the UERD-P, especially on the BOSSbass-1.01.

C. Comparisons

We compare our framework with the schemes proposed in [21] and [22], all of which use the BOSSbass-1.01 for evaluation. Both of the two existing schemes use Reed-Solomon error correction to improve the data extraction accuracy. In terms of the non-detectability, only the performance of the stego-images after the channel transmission is reported in [21] and [22]. In [21], all the 10000 images in the database are used to generate 10000 stego-images, while the work in [22] only selects 2000 images to generate 2000 stego-images. Both of them randomly select half of the stego-images to train an ensemble classifier, while the rest are used for testing. We use all the 10000 images in the database and redo our experiment by following the same protocol. Fig. 4 shows the comparison among different schemes for the stego-images after the channel transmission, where the results of the two existing schemes are duplicated from [21] and [22]. The set of images selected for evaluating the performance of our scheme is not exactly the same as that selected in [21], because the selection is done randomly. This is generally not an issue since the P_E is shown to be a stable performance indicator for the ensemble classifier when sufficient images are used for training [27]. On the other hand, fewer training samples will lead to higher P_E when evaluating the non-detectability of a steganographic scheme

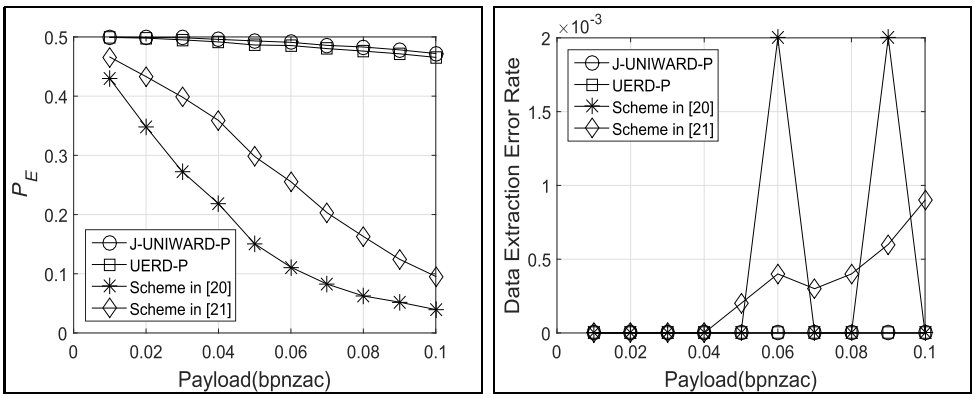

Fig. 4. The comparison among different robust image steganographic schemes at $Q_c = 75$. (a) Non-detectability (against the CCPEV548 detector [28]), (b) the data extraction error rate.

TABLE II
THE AVERAGE PSNR (db) OF THE INTERMEDIATE IMAGES (BOSSBASS/UCID)

Payload(bpnzac)		0	0.05	0.1	0.2	0.3	0.4	0.5
$Q_o = 100$	UERD-P	58.99/39.65	55.56/39.59	53.47/39.52	50.85/39.35	49.13/39.17	47.84/38.98	46.80/38.79
$Q_c = 95$	J-UNIWARD-P	58.99/39.65	58.59/39.65	58.11/39.64	57.18/39.63	56.28/39.61	55.39/39.59	54.51/39.57
$Q_o = 95$	UERD-P	46.33/37.87	46.13/37.64	45.85/37.38	45.10/36.86	44.16/36.35	43.09/35.88	41.96/35.43
$Q_c = 75$	J-UNIWARD-P	46.33/37.87	46.25/37.86	46.16/37.84	45.94/37.81	45.68/37.76	45.41/37.70	45.13/37.63

[29]. Therefore, the scheme in [22] should have lower P_E if all the images in the database are used for training and testing.

We can see from Fig. 4 that, regardless of using the J-UNIWORD or the UERD, the non-detectability of our stego-images is significantly better than those generated from the existing schemes. In addition, even with the help of error correction codes, the existing schemes can not guarantee 100% data extraction accuracy, especially when the payloads are high. On the contrary, our framework always guarantees the full recovery of the secret data regardless of the payloads.

D. Applications

Currently, our framework works under the condition that the operation of the channel contains only the JPEG compression. Such a condition is found to be satisfied in some internet forums. For example, in the forum with the address http://bbs.zhouzheng.net/index.php, an original JPEG image with a quality factor higher than 80 will be JPEG recompressed using a quality factor of 80 during the uploading. We upload 10 high quality daily JPEG images ($Q_o = 95$) with hidden data using our proposed scheme to this forum. As expected, all the messages can be perfectly extracted from the posted images.

IV. CONCLUSIONS

A novel framework for robust image steganography is proposed in this paper, which is able to resist the JPEG compression of the communication channel. In this framework, we first obtain the stego-image by embedding data into the channel compressed original image using any of the existing JPEG steganographic schemes. According to the stego-image, we propose a coefficient adjustment scheme to slightly modify the original image to produce an intermediate image. We proof that we can always generate an intermediate image whose channel compressed version is exactly the same as the stego-image. Therefore, it is guaranteed that the secret data can be recovered from our stego-image with 100% accuracy. Meanwhile, it is able to achieve high non-detectability when an advanced steganographic scheme is adopted in our framework.

REFERENCES

[1] M. Asikuzzaman and M. R. Pickering, "An overview of digital video watermarking," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 9, pp. 2131–2153, Sep. 2018.
[2] M. Asikuzzaman, M. J. Alam, A. J. Lambert, and M. R. Pickering, "Imperceptible and robust blind video watermarking using chrominance embedding: A set of approaches in the DT CWT domain," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 9, pp. 1502–1517, Sep. 2014.
[3] M. Asikuzzaman, M. J. Alam, A. J. Lambert, and M. R. Pickering, "Robust DT CWT-based DIBR 3D video watermarking using chrominance embedding," *IEEE Trans. Multimedia*, vol. 18, no. 9, pp. 1733–1748, Sep. 2016.
[4] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2009.
[5] T. Y. Liu and W. H. Tsai, "A new steganographic method for data hiding in microsoft word documents by a change tracking technique," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 1, pp. 24–30, Mar. 2007.
[6] B. Li, S. Tan, M. Wang, and J. Huang, "Investigation on cost assignment in spatial image steganography," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 8, pp. 1264–1277, Aug. 2014.
[7] C. Qin, C.-C. Chang, Y.-H. Huang, and L.-T. Liao, "An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 23, no. 7, pp. 1109–1118, Jul. 2013.
[8] Y. Huang, C. Liu, S. Tang, and S. Bai, "Steganography integration into a low-bit rate speech codec," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1865–1875, Dec. 2012.
[9] D. Xu, R. Wang, and Y. Q. Shi, "Data hiding in encrypted H.264/AVC video streams by codeword substitution," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 596–606, Apr. 2014.
[10] S. Li and X. Zhang, "Toward construction based data hiding: From secrets to fingerprint images," *IEEE Trans. Image Process.*, vol. 28, no. 3, pp. 1482–1497, Mar. 2019.

[11] A. Westfeld, "F5—A steganographic algorithm," in *Proc. Int. Workshop Inf. Hiding*. Berlin, Germany: Springer, 2001, pp. 289–302.
[12] P. Sallee, "Model-based steganography," in *Proc. Int. Workshop Digit. Watermarking*. Berlin, Germany: Springer, 2003, pp. 154–167.
[13] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Commun. Lett.*, vol. 10, no. 11, pp. 781–783, Nov. 2006.
[14] J. Fridrich and D. Soukal, "Matrix embedding for large payloads," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 3, pp. 390–395, Sep. 2006.
[15] H.-T. Wu and J. Huang, "Secure JPEG steganography by LSB^{+} matching and multi-band embedding," in *Proc. IEEE Int. Conf. Image Process.*, Sep. 2011, pp. 2737–2740.
[16] J. Fridrich and J. Kodovský, "Rich models for steganalysis of digital images," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 868–882, Jun. 2012.
[17] T. Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 920–935, Sep. 2011.
[18] V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," *EURASIP J. Inf. Secur.*, vol. 2014, no. 1, pp. 1–13, Dec. 2014.
[19] 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. Forensics Security*, vol. 10, no. 12, pp. 2669–2680, Dec. 2015.
[20] W. Zhang, Z. Zhang, L. Zhang, H. Li, and N. Yu, "Decomposing joint distortion for adaptive steganography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 27, no. 10, pp. 2274–2280, Oct. 2017.
[21] Y. Zhang, X. Luo, C. Yang, D. Ye, and F. Liu, "A framework of adaptive steganography resisting JPEG compression and detection," *Secur. Commun. Netw.*, vol. 9, no. 15, pp. 2957–2971, 2016.
[22] Y. Zhang, X. Zhu, C. Qin, C. Yang, and X. Luo, "Dither modulation based adaptive steganography resisting JPEG compression and statistic detection," *Multimedia Tools Appl.*, vol. 77, no. 14, pp. 17913–17935, 2017.
[23] P. Bas, T. Filler, and T. Pevný, "'Break our steganographic system': The ins and outs of organizing BOSS," *J. Amer. Statis. Assoc.*, vol. 96, no. 454, pp. 488–499, 2011.
[24] G. Schaefer, "UCID: An uncompressed color image database," *Proc. SPIE Electron. Imag. Storage Retr. Methods Appl. Multimedia*, vol. 5307, pp. 472–480, 2003.
[25] V. Holub and J. Fridrich, "Low-complexity features for JPEG steganalysis using undecimated DCT," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 219–228, Feb. 2015.
[26] X. Song, F. Liu, C. Yang, X. Luo, and Y. Zhang, "Steganalysis of adaptive JPEG steganography using 2D Gabor filters," in *Proc. ACM Workshop Inf. Hiding Multimedia Secur.*, 2015, pp. 15–23.
[27] J. Kodovský, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 432–444, Apr. 2012.
[28] J. Kodovský and J. Fridrich, "Calibration revisited," in *Proc. ACM Workshop Multimedia Secur.*, 2009, pp. 63–74.
[29] A. D. Ker, "A capacity result for batch steganography," *IEEE Signal Process. Lett.*, vol. 14, no. 8, pp. 525–528, Aug. 2007.