*Mathematical Biosciences and Engineering*

Mathematical Biosciences and Engineering, 16(4): 2322–2333
DOI: 10.3934/mbe.2019116
Received: 02 January 2019
Accepted: 04 March 2019
Published: 15 March 2019

http://www.aimspress.com/journal/MBE

*Research article*

# Steganography in beautified images

**Liyun Liu, Zichi Wang, Zhenxing Qian*， Xinpeng Zhang and Guorui Feng**

The authors are with School of Communication and Information Engineering, Shanghai University, Shanghai, 200444, P. R. China.

* **Correspondence:** E-mail: zxqian@shu.edu.cn.

**Abstract:** Existing distortion functions in steganography which achieved high undetectability are designed for unprocessed natural image. Nowadays, a large number of images are filtered before transmitting for the sake of beautification. In this situation, existing distortion functions should be improved to fit the properties of these beautified images. This paper proposes a distortion function optimization method for steganography on beautified images. Given an unprocessed image, a popular image beautification software is employed to produce two similar beautified images. One of them is used for embedding and the other one is employed as reference. Guided by the reference, existing distortion functions are improved by distinguishing the embedding costs for ±1 embedding. After embedding, the stego image is closer to the reference, which results in a higher undetectability against steganalysis. Experimental results also proved the increasing of undetectability when examined by modern steganalytic tools.

**Keywords:** steganography; filter image; distortion function.

## 1. Introduction

Steganography aims to transmit data secretly through digital media without drawing suspicion by slightly modifying cover data [1–4]. On the contrary, steganalysis is a technology to detect the secret transmission by analyzing the suspicious media. Therefore, the capability of resisting steganalysis is crucial to achieve steganography. Early steganographic methods try to increase the undetectability by decreasing the quantity of embedding changes [5–7]. However, it is not enough to guarantee the security performance since the strong correlation in natural image. Currently, the most effective steganography scheme is the STC (Syndrome Trellis Coding) based embedding [8], which is a practical approach to achieve minimal additive distortion between cover and stego image with a user-defined distortion function. Where the distortion function assigns a embedding cost for each cover element. In this framework, a well-designed distortion function is the critical factor [9]. There are numbers of typical distortion functions for spatial images [10–13] or JPEG images [14–18]. In this paper, we discuss JPEG steganography since JPEG is the most popular image format. A distortion function for JPEG steganography assigns embedding costs for all DCT coefficients. These embedding costs are used to quantify the effects when modifying the DCT coefficients. Combining with STC, the minimal cost embedding can be achieved.

However, existing distortion functions which achieved high undetectability are designed for unprocessed natural images. Nowadays, various of applications for image filtering in mobile or computer are widely used in order to beautify images. The pursuit of beauty has become so demanding that few people willing to put unpolished pictures [19–23] on public. Figure 1 shows an image of data set ImageNet [24] and its beautified versions in several different styles. Comparing with original version, the beautified image seems more beautiful.

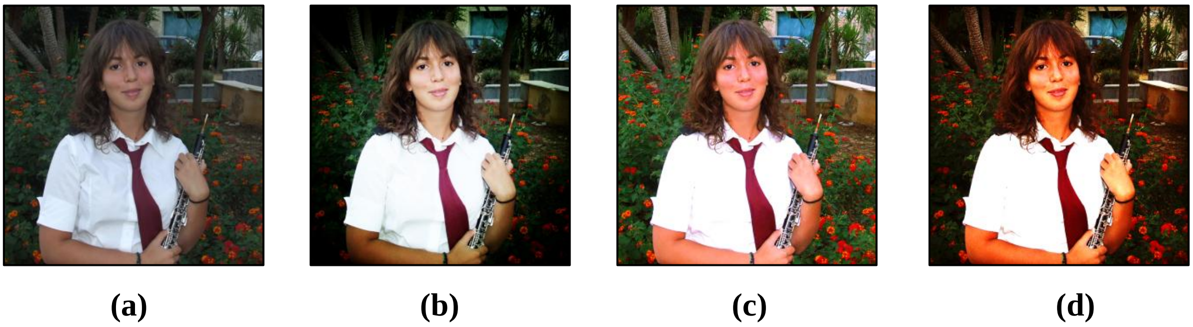


**Figure 1.** Performance of image beautification(a) original image, (b) beautified image in LOMO style, (c) beautified image in freshness style, (d) beautified image in sweet style.

In addition, from the initial simple whitening to local details now, companies have developed many beautification softwares with convenient grooming process to attract more users, e.g. “BeautyCam” [25], “CAMERA360” [26] and “TianTianPiTu” [27]. As a result, a large number of images are filtered before transmitting for the sake of beautification. That means that people are willing to transmit pictures in a public platform after been beautified. In this situation, existing distortion functions should be improved to fit the properties of the beautified images.

This paper proposes a distortion function optimization method for beautified images. We use a popular image beautification software to beautify a given image twice to produce two similar beautified images. One beautified image is used to guide the embedding made on the other one. Specifically, existing distortion functions are improved by distinguishing the embedding costs for ±1 embedding. Experimental results show that the undetectability of existing distortion functions for JPEG steganography is improved using the proposed method.

## 2. Proposed method

The flowchart of the proposed method is illustrated in Figure 2. Given an unprocessed natural image, a popular image beautification software is executed twice to produce two similar beautified images. One of them is used as cover, the other one is employed as reference. An existing STC based steganographic method is employed on the cover image to obtain a initial distortion function. Guided by the reference image, the embedding costs assigned by the initial distortion function are adjusted to achieve higher undetectability. The details are as follows.

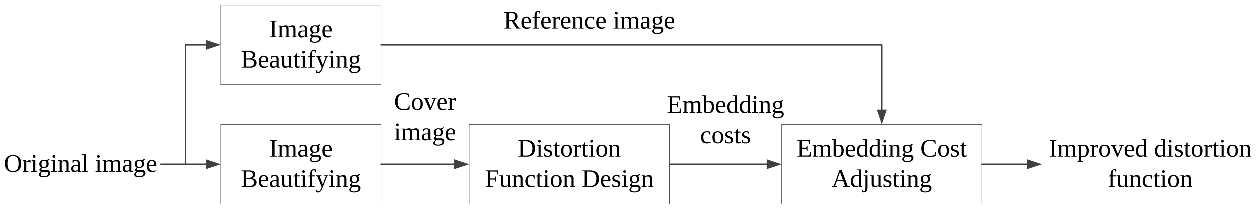


**Figure 2.** The proposed framework for distortion function optimization.

### *2.1. Reference and cover image generation*

The image beautification software “BeautyCam” is employed to produce beautified images. “BeautyCam” is a popular app which provides kinds of filter effect styles e. g. LOMO(Lomography), sweet etc. Filter effect can be achieved by adjusting the weights of RGB channels and some special operations.

For example, in LOMO style, the pixels in red channel are manipulated using Equation (1).

$$y=\frac{1}{1+e^{-\frac{x-0.5}{s}}} \tag{1}$$

where $x\in[0,255]$ is the value of a pixel, $s\in[0,1]$ is a constant to decide the degree of transformed color, and $y$ is the obtained pixel. Then a hole map is produced and multiply with the obtained image. To produce the hole map, a gray image with a white circle inside with the same input image size is created firstly. Meanwhile, a blur filter function is used to get a smooth effect [28].

However, it is difficult to know the details of image beautification in "BeautyCam" since it is a commercial software. For this reason, we treat it as a black box. In the software “BeautyCam”, a opacity value $\beta$ of the filter effect can be determined by a user, $1\% \le \beta \le 100\%$. Given an image, different but similar beautified images can be produced with different values of $\beta$.

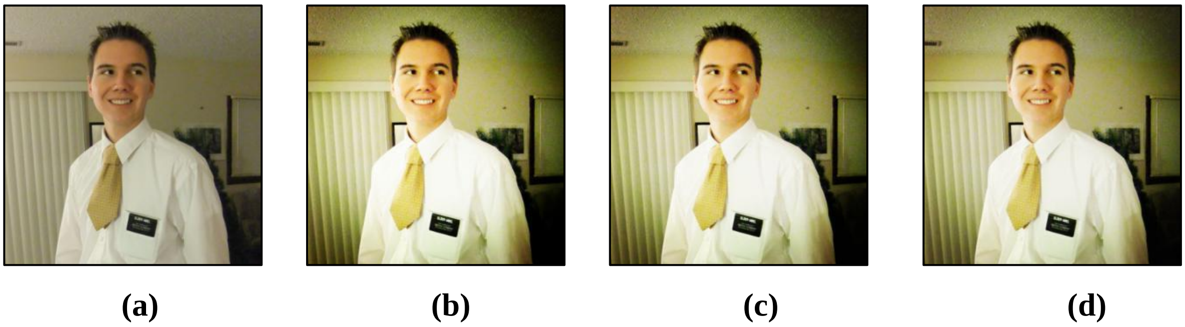


**Figure 3.** Image beautification with different parameters (a) original image, (b) LOMO style with $\beta$ = 100%, (c) LOMO style with $\beta$ = 90%, (d) LOMO style with $\beta$ = 80%.

As shown in Figure 3, an unprocessed natural image is beautified in LOMO style with $\beta$=100%, 90%, and 80% respectively. We can see that the three beautified images are similar in spite of different $\beta$. In the proposed method, we produce the cover and reference images using two slightly different $\beta$. The suitable value of $\beta$ will be discussed in subsection 2.3.

### *2.2. Embedding cost setting*

For an unprocessed color-scale JPEG image $\mathbf{X}_o$ sized $M \times N$, two similar beautified images $\mathbf{X}_c$ and $\mathbf{X}_r$ are produced using the image beautification software "BeautyCam". Then $\mathbf{X}_c$ is used for embedding and $\mathbf{X}_r$ is used as reference. For a color-scale JPEG image, there are three channels in total: Y, Cb, Cr. We choose the Y channel for embedding since it is the main ingredient of a image and also sized $M \times N$. Denote the $(i, j)$th quantized DCT coefficient in Y channel as $y(i, j)$, the +1 and –1 embedding costs assigned for $y(i, j)$ as $\rho_+(i, j)$ and $\rho_-(i, j)$ respectively, where $i \in \{1, 2, \ldots, M\}$, $j \in \{1, 2, \ldots, N\}$

In most steganographic methods based on STC, $\rho_+(i, j)=\rho_-(i, j)$, that means the embedding costs for +1 and –1 modification are equal. As we discovered in [29], this equivalence is unreasonable. Inspired by this, an existing distortion function is improved by distinguishing the embedding costs for ±1 embedding. To distinguishing ±1 embedding costs, $\mathbf{X}_r$ is used as reference to guide the embedding made on $\mathbf{X}_c$.

Denote the $(i, j)$th quantized DCT coefficient in Y channel of $\mathbf{X}_c$ and $\mathbf{X}_r$ as $y_c(i, j)$ and $y_r(i, j)$ respectively, we improve the embedding costs assigned for $y_c(i, j)$ according to $y_r(i, j)$. The residuals $\mathbf{R} = \{r(i, j)\}$ between $\mathbf{X}_c$ and $\mathbf{X}_r$ are calculated using Equation (2).

$$r(i, j) = y_r(i, j) - y_c(i, j) \tag{2}$$

Let the improved embedding costs for ±1 embedding be $\tilde{\rho}_+(i, j)$ and $\tilde{\rho}_-(i, j)$ respectively. Guided by the residuals $r(i, j)$, the initial embedding costs $\rho_+(i, j)$ and $\rho_-(i, j)$ assigned by one of the existing distortion functions is improved by Equations (3) and (4).

$$\tilde{\rho}_+(i, j) = f_+\left(\rho_+(i, j), r(i, j)\right) \tag{3}$$

$$\tilde{\rho}_-(i, j) = f_-\left(\rho_-(i, j), r(i, j)\right) \tag{4}$$

The two functions $f_+(\cdot)$ and $f_-(\cdot)$ are used to adjust the initial embedding costs $\rho_+(i, j)$ and $\rho_-(i, j)$ with the help of $r(i,j)$. The purpose of this adjustment is to shorten the difference of the two beautified images as far as possible. In this way, the stego beautified image is closer to the reference image, which results in a higher undetectability against steganalysis. According to this, the function functions $f_+(\cdot)$ and $f_-(\cdot)$ can be defined as,

$$f_+(\xi_1, \xi_2) = \begin{cases} \alpha \cdot \xi_1 & , \text{ if } \xi_2 > 0 \\ \xi_1 & , \text{ if } \xi_2 \le 0 \end{cases} \tag{5}$$

$$f_-(\xi_1,\xi_2)=\begin{cases}\alpha\cdot\xi_1 & , \text{ if } \xi_2<0\\ \xi_1 & , \text{ if } \xi_2\geq 0\end{cases} \tag{6}$$

where parameter $\alpha\in[0,1]$ is used to decide the extent of modification. By using Equations (5) and (6), the distortion functions are modified towards reference image. Therefore, the stego beautified image is closer to the reference image. A large α means ρ(i, j) is modified by a small amplitude, and vice versa. The improved embedding costs are the same with the initial versions if and only if $\alpha$=1. The value of $\alpha$ will be discussed in next subsection.

With embedding costs $\tilde{\rho}_+(i,j)$ and $\tilde{\rho}_-(i,j)$, the popular STC framework is employed for data embedding, which achieves minimal additive distortion between cover and stego image with given embedding costs. For data extraction, the secret data **m** can be directly extracted from stego elements **s** by a matrix computation using the following Equation,

$$\mathbf{m} = \mathbf{Hs} \tag{7}$$

where **H** is a low density parity-check matrix determined by the embedding speed, the embedding efficiency and the payload.

### *2.3. Parameters determination*

To find the best values of $\alpha$ and $\beta$, some experiments are carried out. We choose 1000 images from ImageNet to construct the datasets of original image. The 1000 images are cropped into 512 × 512 and compressed into JPEG with quality factor QF = 75 respectively. We choose LOMO style with the opacity $\beta$ = 100% to generate cover image. Reference image is constructed with the same filter effect but different $\beta$ is set as 90%, 80%, 70%, 60% respectively. The initial embedding costs are obtained using the popular JPEG steganographic methods JUNIWARD and UERD, and the payload is set as 0.5 bpnzac (bit per non-zero AC coefficient). The parameter $\alpha\in[0,1]$ which is used to adjust embedding costs is set as {0.1, 0.2, 0.3, … ,1}.

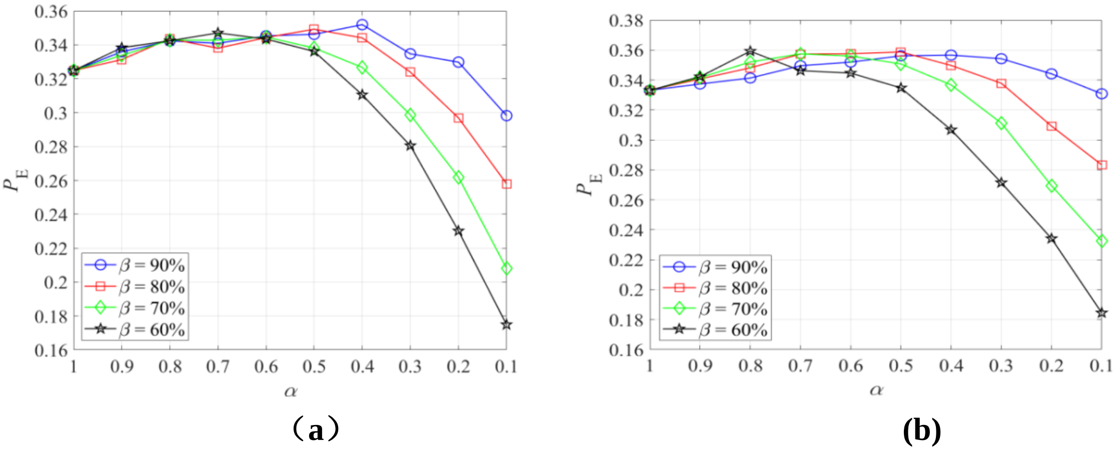


**Figure 4.** Detection error of DCTR with ensemble classifier for LOMO style and QF = 75 with (a) JUNIWARD, (b) UERD, and payload 0.5 bpnzac.

The detection error $P_E$ of steganalytic feature set DCTR [30] with ensemble classifier [31] is shown in Figure 4. It can be seen that the variations between $P_E$ and the values of $\alpha$ and $\beta$ perform similar tendency for different cases. On the whole, the optimal value of $\alpha$ to modify cost value is around 0.4 and the optimal value of $\beta$ to choose opacity is 90%. Therefore, the values of $\alpha$ and $\beta$ are determined as 0.4 and 90% respectively in the proposed method.

## 3. Experimental results

To verify the proposed method, we have conducted many experiments to hide secret data. We first setup the experimental environments using the popular database. Then we provide the results of undetectability using the proposed method.

### *3.1. Experiment setup*

The image dataset employed in our experiments is ImageNet which contains more than ten million uncompressed color-scale images.

The first 5000 images are cropped into 512 × 512 and compressed into JPEG with quality factor QF = 75 and QF = 95 respectively. Then all the 10000 JPEG images are used as the original images as described in section 2. To produce the cover images and the corresponding reference images, three styles LOMO, freshness, and sweet of filter effect for image beautification are employed. Figure 5 shows an image of ImageNet and its beautified versions in the employed three styles.

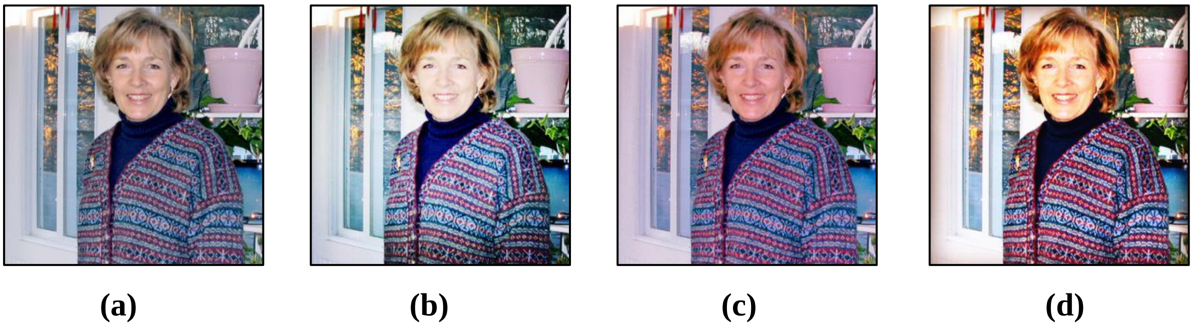


**Figure 5.** Example of image beautification(a) original image, (b) LOMO style, (c) freshness style, (d) sweet style.

In this way, 60000 JPEG images are obtained. As shown in Table 1, there are 5000 cover images for each style and quality factor. Likewise, 5000 corresponding reference images also produced for each style and quality factor respectively.

To verify the effectiveness of the proposed method, the popular JPEG steganographic methods JUNIWARD and UERD are used as benchmark. All embedding tasks are done by the STC framework. We set the payloads as 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, and 0.7 bpnzac, respectively.

For steganalysis, the popular feature sets ccJRM [32] and DCTR and are employed in our experiments. The ensemble classifier is used to measure the property of feature sets. In detail, half of the cover and stego feature sets are used as the training sets while the remaining half are used as testing sets. The criterion to evaluate the performance of feature sets is the minimal total error $P_E$

under equal priors achieved on the testing sets:

$$P_E = \min_{P_{FA}} \left( \frac{P_{\mathrm{FA}} + P_{MD}}{2} \right) \tag{8}$$

where $P_{\mathrm{FA}}$ is the false alarm rate and $P_{\mathrm{MD}}$ is the missed detection rate. The performance is evaluated using the average value of $P_{\mathrm{E}}$ over 10 random tests.

**Table 1.** Structure of cover and reference images.

| | | LOMO | sweet | freshness |
|---|---|---|---|---|
| QF = 75 | Cover images | 5000 | 5000 | 5000 |
| | Reference images | 5000 | 5000 | 5000 |
| QF = 95 | Cover images | 5000 | 5000 | 5000 |
| | Reference images | 5000 | 5000 | 5000 |

*3.2. Image quality*

The distortion between cover and stego is important for security of steganography. The key step in our approach is to construct an appropriate reference image. Figure 6 shows the images produced during steganography with the proposed method.

Figure 6(a) shows a JPEG image compressed by QF = 95, which is used as the original image **X**o. After beautified with styles LOMO using opacity $\beta$ = 100% and $\beta$ = 90% respectively, the obtained cover and reference image **X**c and **X**r are shown in Figure 6(b) and Figure 6(c) respectively. With the guidance of **X**r, **X**c is embedded with payload 0.5 bpnzac. The corresponding stego image is shown in Figure 6(d).

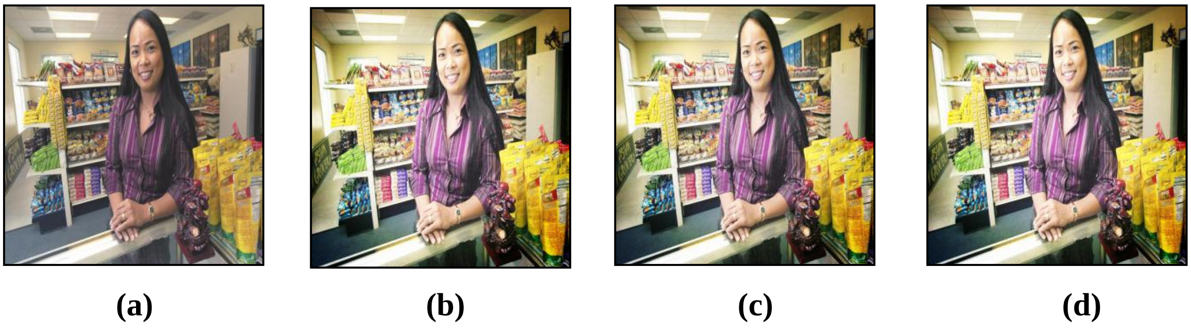


**Figure 6.** Images produced during steganography with the proposed method (a)original image, (b)cover image, (c)reference image, (d) stego image.

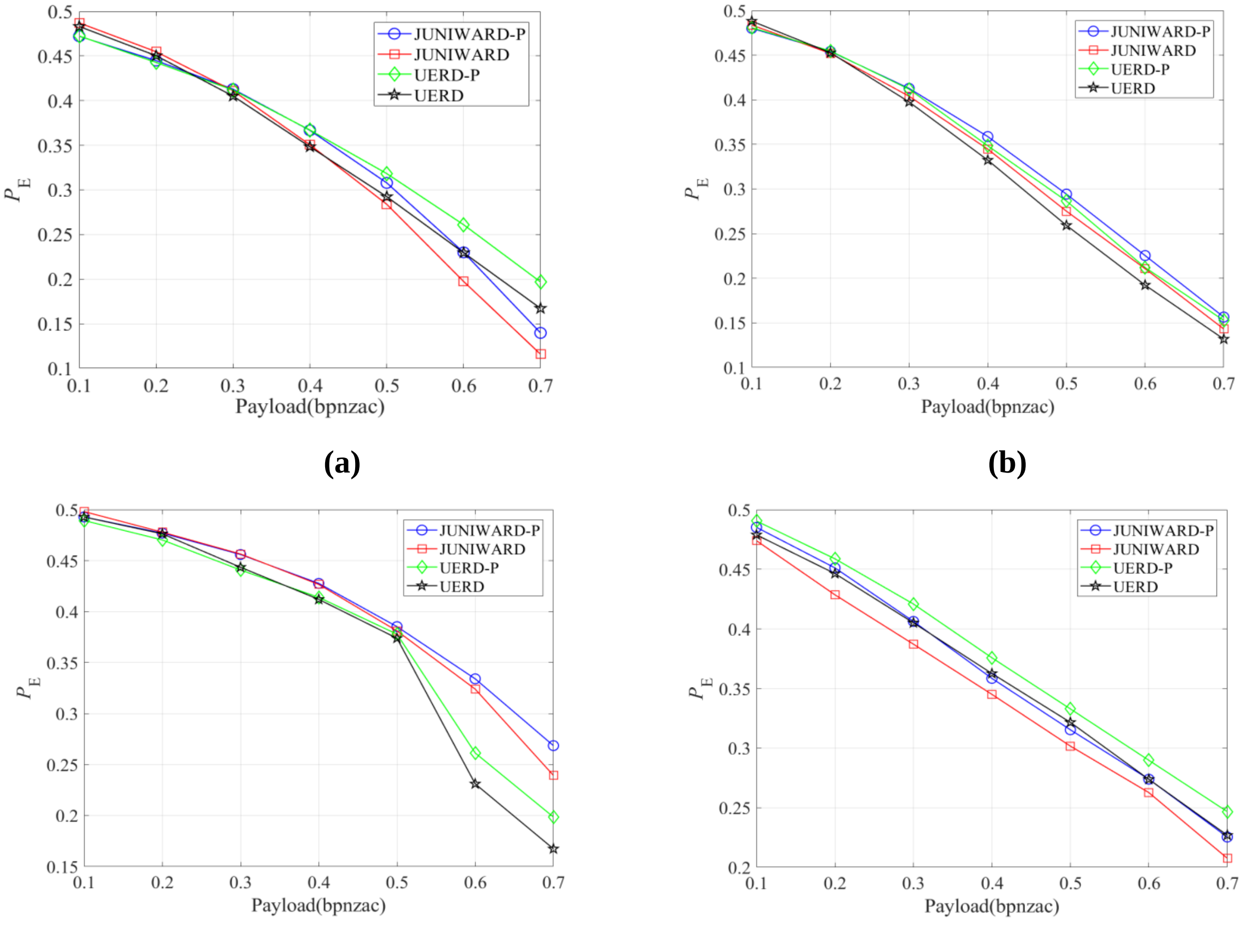
It is clear that the reference image is similar to cover image. Therefore, it is reasonable to modify cover image towards the reference image. In addition, stego image is also close to the cover. That means the stego image preserves good quality.

### *3.3 Undetectability against steganalysis*

Since the proposed method improves the distortion function, we name the improved versions of JUNIWARD and UERD as “JUNIWARD-P”, and “UERD-P” respectively. Figure 7 ~ Figure 9 show the undetectability comparisons of these methods against ccJRM and DCTR with quality factor 75 and 95 for three different beautification styles LOMO, sweet, and freshness.

The results in Figure 7 ~ Figure 9 indicate that the undetectability of all steganographic methods for JPEG steganography are improved for most cases by using the proposed method, especially for the cases of large payload. In practical application, embedding with large payload is more meaningful to transmit secret data.

For style LOMO, as shown in Figure 7, although the performance is slightly decreased for low payload, the $P_E$ of JUNIWARD can be improved by 3.26 % when payload is 0.6 bpnzac with DCTR for QF = 75, and 3.14 % with ccJRM for QF = 75.



**(a)**

**(b)**

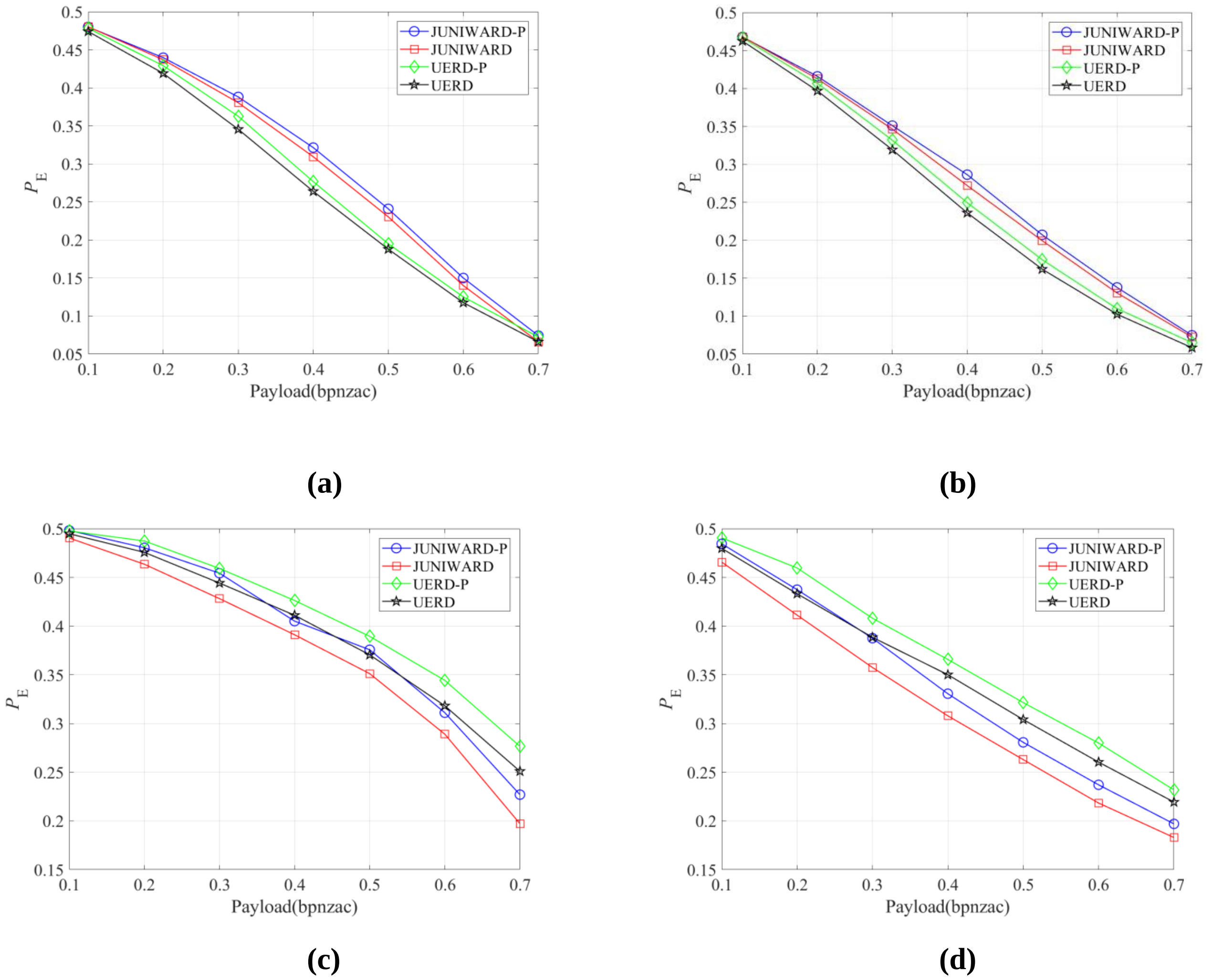
**(c)**

**(d)**

**Figure 7.** Comparisons of JUNIWARD, UERD and the improved versions against ccJRM and DCTR with QF = 75 and 95 for style LOMO (a) against DCTR with QF = 75, (b) against ccJRM with QF = 75, (c) against DCTR with QF = 95, (d) against ccJRM with QF = 95.

For style freshness, as shown in Figure 8, the improvement is 2.40 % when payload is 0.7 bpnzac with DCTR for QF = 95.

Figure 9 shows the results for style sweet, when payload is 0.5 bpnza with DCTR for JUNIWARD, the $P_E$ improved from 0.4188 to 0.4735. However, for QF = 75, the performance is only improved at the large payload.



(a)

(b)

(c)

(d)

**Figure 8.** Comparisons of JUNIWARD, UERD and the improved versions against ccJRM and DCTR with QF = 75 and 95 for style freshness(a) against DCTR with QF = 75, (b) against ccJRM with QF = 75, (c) against DCTR with QF = 95, (d) against ccJRM with QF = 95.

## 4. Conclusion

This paper proposes a universal method to improve the distortion functions in steganography for beautified images. Given an unprocessed natural image, the image beautification operation is executed twice to produce two similar beautified images. One is used for embedding and the other one for guidance. With this guidance, distortion functions are improved by distinguishing the embedding costs for ±1 embedding. Experimental results show that the proposed method is effective. For further study, it is significant to embedding data in the process of image beautification.

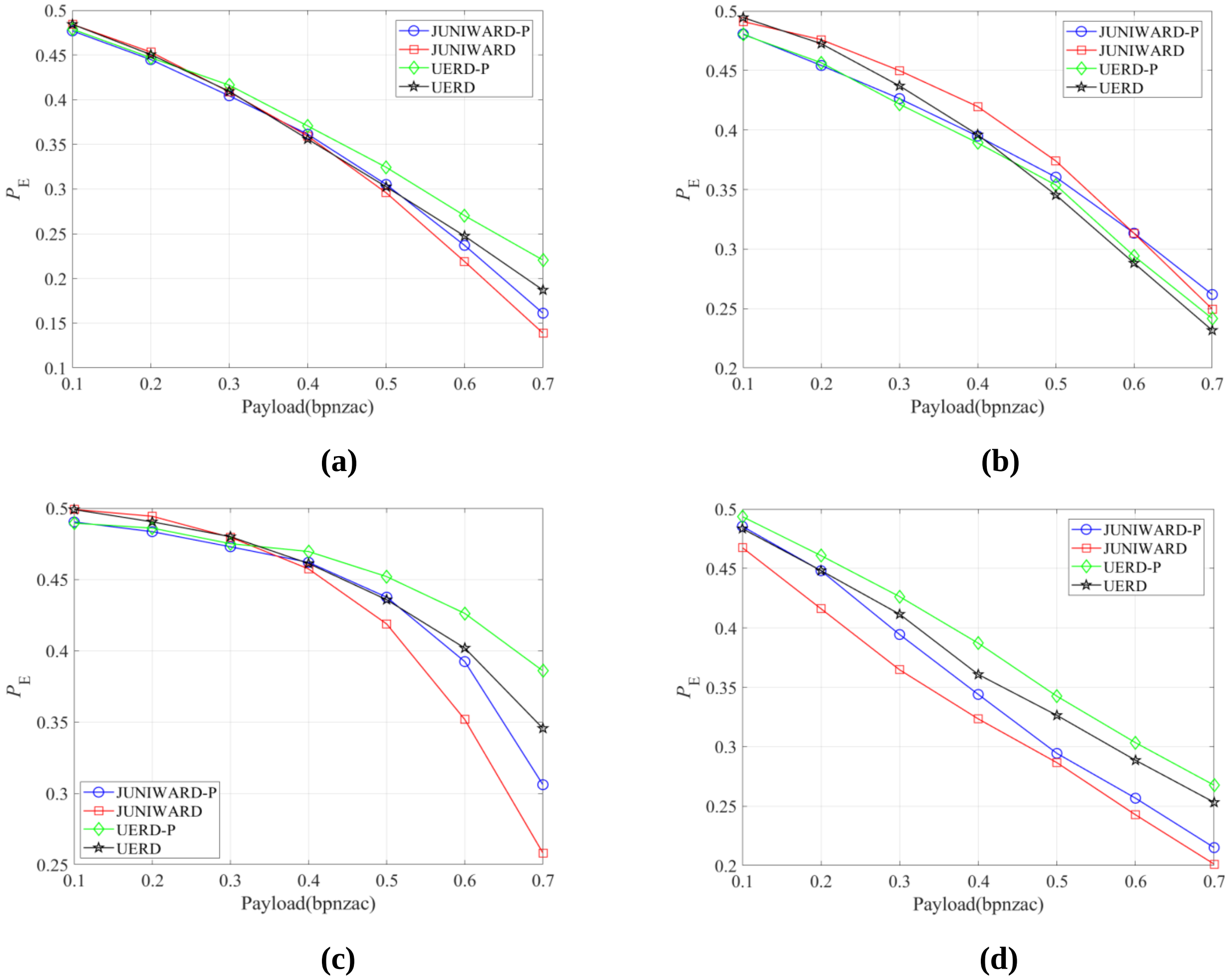


**Figure 9.** Comparisons of JUNIWARD, UERD and the improved versions against ccJRM and DCTR with QF = 75 and 95 for style sweet (a) against DCTR with QF = 75, (b) against ccJRM with QF = 75, (c) against DCTR with QF = 95, (d) against ccJRM with QF = 95.

## Acknowledgments

This work was supported by the Natural Science Foundation of China (U1736213, 61572308, U1636206, 61103181, U1636206, 61373151, and 61525203), and the Shanghai Excellent Academic Leader Plan (16XD14012 00).

## Conflict of interest

All authors declare no conflicts of interest in this paper.

## References

1. B. Li, S. Tan and M. Wang, et al., Investigation on cost assignment in spatial image steganography, *IEEE. TIFS.*, **9** (2014), 1264–1277.

2. Y. Ma, X. Luo and X. Li, et al., Selection of rich model steganalysis features based on decision rough set α-Positive region reduction, *IEEE. TCSVT.*, (2018), In press.
3. Y. Zhang, C. Qin and W. Zhang, et al., On the fault-tolerant performance for a class of robust image steganography, *J. Sigpro.*, **146** (2018), 99–111.
4. S. Li and X. Zhang, Towards construction based data hiding: from secrets to fingerprint images, *IEEE. TIP*., **28** (2019), 1482–1497.
5. J.Frdrich and D. Soukal, Matrix embedding for large payloads, *IEEE. TIFS.*, **1**(2006), 390–395.
6. X. Zhang and S. Wang, Efficient steganographic embedding by exploiting modification direction, *IEEE. LCOMM.*, **10** (2016), 781–783.
7. W. Zhang, X. Zhang and S. Wang, Maximizing steganographic embedding efficiency by combining hamming codes and wet paper codes, *Proc. IH2008, Santa Barbara, CA, USA*, (2008), 60–71.
8. T. Filler, J.Judas and J. Fridrich, Minimizing additive distortion in steganography using syndrome-trellis codes, *IEEE. TIFS.*, **6** (2011), 920–935.
9. X. Luo, X. Song and X. Li, et al., Steganalysis of HUGO steganography based on parameter recognition of syndrome-trellis-codes, *MTAP*., **75** (2016), 13557–13583.
10. T. Pevný, T. Filler and P. Bas, Using high-dimensional image models to perform highly undetectable steganography, *Proc. IH2008, Calgary, Canada,* (2010), 161–177.
11. V. Holub and J. Fridrich, Designing steganographic distortion using directional filters, *Proc. IEEE. WIFS., Binghamton, NY, USA*, (2012), 234–239.
12. B Li, M. Wang, and J. Huang, et al., A new cost function for spatial image steganography, *Proc. IEEE. ICIP., Paris, France*, (2014), 4206–4210.
13. V. Sedighi, J. Fridrich and R. Cogranne, Content-adaptive pentary steganography using the multivariate generalized gaussian cover model, *Proc. SOP., San Francisco, California, USA*, (2015), 94090H–94090H–13.
14. V. Holub and J. Fridrich, Digital image steganography using universal distortion, *Proc. ACM IH&MMS., New York, NY, USA*, (2013), 59–68.
15. L. J. Guo, J. Q. Ni and Y. Q. Shi, uniform embedding for efficient JPEG steganography, *IEEE. TIFS.*, **9** (2014), 814–825.
16. L. J. Guo, J. Q. Ni and W. K. Su, et al., Using statistical image model for JPEG steganography: Uniform Embedding Revisited, *IEEE. TIFS.*, **10** (2015), 2669–2680.
17. Z. Wang, X. Zhang and Z. Yin, Hybrid distortion function for JPEG steganography, *JEI.*, **25** (2016), 050501.
18. Z. Wang, Z. Qian and X. Zhang, et al., On improving distortion functions for JPEG steganography, *IEEE Access*, **6** (2018), 74917–74930.
19. C. Qin, C. Chang and Y. Chiu, A novel joint data-hiding and compression scheme based on SMVQ and image inpainting, *IEEE. TIP*., **23** (2014), 969–978.
20. Z. Qian, H. Zhou and X. Zhang, et al., Separable reversible data hiding in encrypted JPEG bitstreams, *IEEE. TDSC*., **15** (2018), 1055–1067.
21. Z. Qian and X. Zhang, Reversible data hiding in encrypted image with distributed source encoding, *IEEE. TCSVT.*, **26** (2016), 636–646.
22. Z. Qian, X. Zhang and S. Wang, Reversible data hiding in encrypted JPEG bitstream, *IEEE. TMM.*, **16** (2014), 1486–1491.

23. C. Qin, W. Zhang and F. Cao, et al., Separable reversible data hiding in encrypted images via adaptive embedding strategy with block selection, *J. Sigpro.*, **153** (2018), 09–122.
24. J. Deng, W. Dong and R. Socher, et al., ImageNet: A large-scale hierarchical image satabase, *IEEE CVPR.*, (2009), 248–255.
25. Beautification softwares "BeautyCam", *Meitu Company, Fujian, China*, 2018, Available from: https://mt.meipai.com/.
26. Beautification softwares "CAMERA360", *Chengdu Pinguo technology co. LTD, Chengdu, China*, 2015, Available from: http://www.camera360.com/.
27. Beautification softwares "TianTianPiTu", *Tencent Company, Shenzhen, China*, 2014, Available from: https://tu.qq.com/.
28. P. Joshi, D. M. Esciriva and V. Godoy, Opencv By example, *Penerbit Packt Publishing Ltd*, (2016), 87–92.
29. Z. Wang, J. Lv and Q. Wei, et al., Distortion function for spatial image steganography based on the polarity of embedding change, *Proc. IWDW., Beijing, China*, (2016), 487–493.
30. V. Holub and J. Fridrich, Low complexity features for JPEG steganalysis using undecimated DCT, *IEEE. TIFS.*,**10** (2014), 219–228.
31. J. Kodovsky, J. Fridrich and V. Holub, Ensemble classifiers for steganalysis of digital media, *IEEE. TIFS.*, **7** (2012), 432–444.
32. J. Kodovsky and J. Fridrich, Steganalysis of JPEG images using rich models, *Proc. ISOP., San Francisco, CA, USA*, (2012), 83030A–83030A–13.