# Defining Cost Functions for Adaptive Steganography at the Microscale

Kejiang Chen, Weiming Zhang, Hang Zhou, Nenghai Yu
CAS Key Laboratory of Electromagnetic Space Information
University of Science and Technology of China, Hefei, China
Email: chenkj@mail.ustc.edu.cn, zhangwm@ustc.edu.cn
zh2991@mail.ustc.edu.cn, ynh@ustc.edu.cn

Guorui Feng
School of Communication and Information Engineering
Shanghai University, Shanghai, China
Email: grfeng@shu.edu.cn

***Abstract*—In the framework of minimizing embedding distortion steganography, the definition of cost function almost determines the security of the method. Generally speaking, texture areas would be assigned low cost, while smooth areas with high cost. However, the prior methods are still not precise enough to capture image details. In this paper, we present a novel scheme of defining cost function for adaptive steganography at the microscale. The proposed scheme is designed by using a "microscope" to highlight fine details in an image so that distortion definition can be more refined. Experiments show that by adopting our scheme, the current steganographic methods (WOW, UNIWARD, HILL) will achieve better performances on resisting the state-of-the-art steganalysis.**

## I. Introduction

Steganography is the art of hiding messages in objects without drawing suspicion from steganalysis [1], [2]. Currently, the vast majority of work on steganography has focused on digital images. With the purpose of minimizing statistical detectability, modern steganography can be formulated as a source coding problem that minimizes embedding distortion [3]. Syndrome-trellis codes (STCs) provide a general methodology for embedding while minimizing an arbitrary additive distortion function with a performance near the theoretical bound [4].

As for content-adaptive steganography, how to define the cost function becomes one of the most important research issues. Taking into account of Adversary's attack method, the cost function of HUGO [5] is defined as the weighted sum of difference between feature vectors extracted from a cover image and its stego version in SPAM [6] feature space. In this way, pixels after modification which make the feature vectors vary widely will be assigned a higher cost. The embedding changes of HUGO will be made within texture regions and along edges. WOW [7] assigns low costs to pixels in regions that are easily modelable, while pixels in textural regions that are difficult to predict by directional filters have smaller costs. S-UNIWARD [8] has a slightly modified filter bank from WOW. S-UNIWARD and WOW have similar performance and they are more secure than HUGO. HILL [9] is realized by using a high-pass filter and two low-pass filters, making more embedding changes concentrated in textural areas. It outperforms S-UNIWARD under the detection by the powerful steganalysis which employs [10]. MiPOD [11] under a model-driven framework also has an empirical security. The generalized Gaussian function is utilized to model noise residuals of pixels. All these adaptive algorithms consider pixels independently and cluster the modifications in the texture areas.

The state-of-the-art methods have exploited pixels in texture areas for hiding information. By comparing the cover image and the corresponding distortion, we are able to find some pixels with high cost values inside texture areas. However, these areas are probably suitable for concealing data, and should be assigned with low costs. To some extent, the methods mentioned above are still not precise enough to capture image details. In this case, the cost function can be further developed.

We proposed a novel scheme of steganography which aims to create a fine distortion. With the help of a "Microscope", the texture regions can be highlighted so that we can capture fine details of images precisely. The processed image is called auxiliary image. Then we utilize existing steganography methods to define distortion on the auxiliary image. The defined distortion will be smoothed by a low-pass filter and assigned to the cover image. Finally, the information hiding would be well implemented by STCs. The algorithm, which is based on the above scheme, is called MS (Microscope) algorithm. We find that techniques in image enhancement such as unsharp masking (UM) [12] can act as the microscope. Experimental results show that the steganographic methods using the proposed scheme perform better than not using, in resisting steganalysis with both SRM and selection-channel-aware maxSRMd2 [13].

The rest of this paper is organized as follows. After introducing notations, we review the preliminaries and the scheme of minimizing additive distortion. In Section III we present a new stegonagraphic scheme which defines the distortion with the assistance of a microscope. Results of comparative experiments are elaborated in Section IV to demonstrate the effectiveness of the proposed scheme. Conclusion and future work are given in Section V.

978-1-5090-1138-4/16/$31.00 ©2016 IEEE

## II. Preliminaries and prior work

### A. Notations

Throughout the paper, matrices, vectors and sets are written in bold face. The cover image (of size $n_1 \times n_2$) is denoted by $\mathbf{X} = (x_{i,j})^{n_1 \times n_2}$, where the signal $x_{i,j}$ is an integer, such as the gray value of a pixel. $\mathbf{Y} = (x_{i,j})^{n_1 \times n_2}$ denotes the stego image. The embedding operation on $x_{i,j}$ is formulated by the range $I$. An embedding operation is called binary if $|I| = 2$ and ternary if $|I| = 3$ for all $i, j$. For example, the $\pm 1$ embedding operation is ternary embedding with $I_{i,j} = \{min(x_{i,j} - 1, 0), x_{i,j}, max(x_{i,j} + 1, 255)\}$, where "0" denotes no modification.

### B. Minimal Distortion Steganography

In the model established in [4], the distortion of modifying a pixel $x_{i,j}$ to $y_{i,j}$ can be simply denoted by $d_{i,j}(\mathbf{X}, y_{i,j})$. It's supposed that $d_{i,j}(\mathbf{X}, x_{i,j}) = 0$ and $d_{i,j}(\mathbf{X}, x_{i,j} - 1) = d_{i,j}(\mathbf{X}, x_{i,j} + 1) = d_{i,j} \in [0, \infty)$. The overall distortion of the image can be calculated as follows:

$$D(\mathbf{X}, \mathbf{Y}) = \sum_{i=1}^{n_1} \sum_{j=1}^{n_2} d_{i,j} |x_{i,j} - y_{i,j}|. \tag{1}$$

Denote $\pi(y_{i,j})$ as the probability of changing $x_{i,j}$ to $y_{i,j}$. For a given message length $m$, the sender wants to minimize the average distortion (1), one can simulate optimal embedding by assigning

$$\pi(y_{i,j}) = \frac{exp(-\lambda d_{i,j}(\mathbf{X}, y_{i,j}))}{\sum_{y_{i,j} \in I_{i,j}} exp(-\lambda d_{i,j}(\mathbf{X}, y_{i,j}))}, \tag{2}$$

where the scalar parameter $\lambda > 0$ determined by the payload constraint

$$m = \sum_{i=1}^{n_1} \sum_{j=1}^{n_2} \sum_{y_{i,j} \in I_{i,j}} \pi(y_{i,j}) \log \frac{1}{\pi(y_{i,j})}, \tag{3}$$

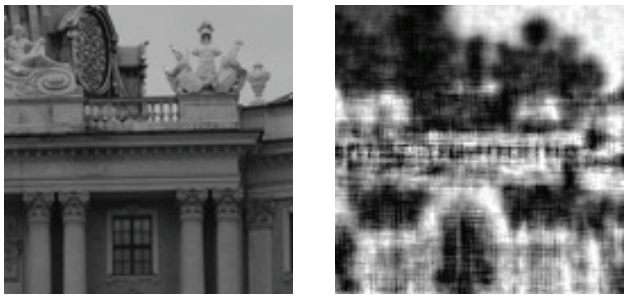
For additive distortion, there exist practical coding methods to embed messages, such as STCs [4], which can approach the performance of optimal embedding.

## III. Proposed method

### A. Motivation

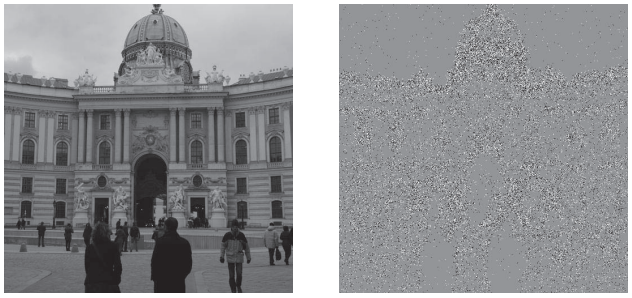
Generally speaking, content-adaptive steganography assigns low costs in texture regions while high costs in smooth areas. From this point of view, grasping the distribution of the texture areas in an image counts for a lot. By comparing the cover image and the corresponding distortion, we are able to find some pixels with high cost values inside texture areas. However, these areas are probably suitable for concealing data, and should be assigned with low costs. Furthermore, Fig. 2 (a) is the cover image and Fig. 2 (b) is the corresponding embedding changes. It is easy to find that there are some pixels modified in smooth areas, while the texture areas should have carried these message bits. These all indicate that the current steganographic methods do not capture fine detail of image well.

Fortunately, many methods in *image enhancement* do favor to search texture areas. On the basis of the techniques, we proposed a novel scheme of steganography, and it will be studied in detail in next section.



(a) (b)

Fig. 1: Image (a) is a part of 1013.pgm from Bossbase1.01 [14], and (b) is the corresponding modifying distortion defined by UNIWARD. The brightness in (b) is scaled and adjusted to [0,1], where 0 is the brightest (lowest distortion), and 1 is the darkest (highest distortion). There are some scattered bright elements inside the small dark regions in (b).



(a) (b)

Fig. 2: Cover image (a) is 1013.pgm from Bossbase1.01, and (b) is the corresponding embedding changes with a fixed payload 0.5 using UNIWARD. Note that embedding changes: +1 = white, -1 = black. We can find that there are some pixels changed in smooth areas.

### B. A novel framework for steganography

Since the current steganography cannot seize texture areas exactly, there is still a long way for us to improve the security of steganography. Just as mentioned in Section II, the additive distortion is the foundation of content-adaptive steganography. However, former distortion is not proper enough, which becomes severe in highly texture regions. So we attempt to design a new scheme to help steganographic algorithms locate the secure area more precisely. The proposed scheme can be implemented in five steps as shown in Fig. 3.

1) Magnify the cover image $\mathbf{X}$ so as to highlight fine details or to enhance details. The operation of enlarging images is not resizing but filtering. Many techniques of image process such as image sharpening can act as a "microscope". The processed image is called "auxiliary image", denoted by $\mathbf{X}'$.
2) Utilize distortion definition methods in existing steganography algorithm (WOW, UNIWARD, HILL, and etc.) to calculate the distortion $\mathbf{D}'$ on the auxiliary image $\mathbf{X}'$.
3) In order to spread the low costs of textural pixels to their neighbourhood, we employ a low-pass filter $\mathbf{L}$ to smooth the distortion $\mathbf{D}'$. For easy implementation, average filter

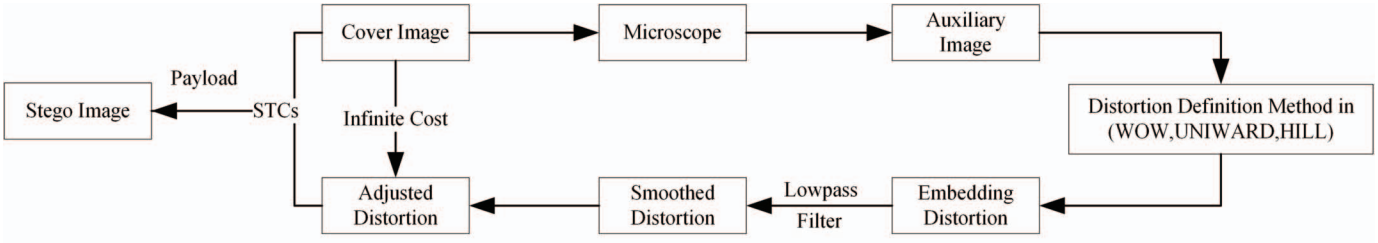



Fig. 3: The diagram of the proposed scheme using a "microscope".

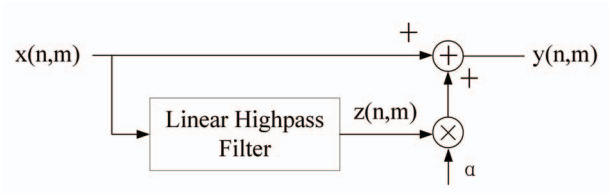



Fig. 4: Unsharp masking for image enhancement.

| | | |
|---|---|---|
| −1 | −1 | −1 |
| −1 | 8 | −1 |
| −1 | −1 | −1 |

Fig. 5: High-pass filter mask used to acquire a high-frequency image.

is adopted. We denote the smoothed distortion by $\mathbf{D}'_s$.

4) Assign the smooth distortion $\mathbf{D}'_s$ to the cover image $\mathbf{X}$. When it comes to the saturated pixels in the cover image $\mathbf{X}$, the distortion should be adjusted. There are essentially three options for pixel values at the boundary of the dynamic range as mentioned in [15]. Restricting the polarity of changes is adopted. If $x_{i,j} = 0$, then $d_{i,j}(\mathbf{X}, x_{i,j}-1) = \infty$; if $x_{i,j} = 255$, then $d_{i,j}(\mathbf{X}, x_{i,j}+1) = \infty$. The final distortion is denoted by $\mathbf{D}$.
5) With the help of STCs and distortion $\mathbf{D}$, steganography can be well implemented on the cover image $\mathbf{X}$.

The former embedding method adopting proposed scheme would be prefixed with "MS", such as MS-WOW, MS-UNIWARD and MS-HILL. In the scheme, performances of different microscopes vary greatly, so the selection of microscope is of great importance. We will discuss it in the next subsection.

### C. The selection of "Microscope"

The principal objective of "Microscope" is to highlight fine details in an image or to enhance details that have been blurred, either in error or as a natural effect of a particular method of image acquisition. Image enhancement is to the choice, such as edge enhancement, histogram equalization, unsharp masking and etc. Edge enhancement is an extremely common technique used to make images appear sharper. Histogram equalization performs its operation by remapping the gray levels of the image based on the probability distribution of the input gray levels. Unsharp masking (UM) is a widely used technique for improving the perceptual quality of an image by emphasizing its high-frequency components [16]. We conduct some contrast experiments, and find that unsharp masking is most suitable. To some degree, unsharp masking highlights fine details as well as maintains the original characteristics of the image.

In the linear UM algorithm [12], the enhanced image $y(n, m)$ is obtained from the input image $x(n, m)$ as

$$y(n, m) = x(n, m) + \alpha * z(n, m), \tag{4}$$

where $z(n, m)$ is the correction signal as the output of a high-pass filter and $\alpha$ is the positive scaling factor that controls the level of contrast enhancement achieved at the output. Base on the high-pass filter as shown in Fig. 5, $z(n, m)$ can be obtained by

$$\begin{aligned} z(n, m) =& 8x(n, m) - x(n-1, m-1) - x(n-1, m) \\ & - x(n-1, m+1) - x(n+1.m-1) - x(n+1, m) \\ & - x(n+1, m+1) - x(n, m-1) - x(n, m+1). \end{aligned} \tag{5}$$

The enhanced image are shown in Fig. 6. The enhanced image appears more acute than the original image as shown in Fig. 2(a) on account of having increased its details. There are hardly any pixels changed in the smooth area at the same embedding rate using MS-UNIWARD.

(a) (b)

Fig. 6: The enhanced image (a) is sharpened by UM algorithms. It's apparent that the enhanced image owns more details than the original image as shown in Fig. 2(a). (b) is the corresponding embedding changes of the original image with a fixed payload 0.5 using MS-UNIWARD. Note that embedding changes: +1 = white, -1 = black. We can find that there are very few pixels changed in the smooth area.

### D. Distortion Smoothness

With a microscope, we are able to seize the texture areas more precisely. We make a further enhancement of the algorithm by incorporating the Spreading Rule [17], so that the modifications will be clustered more accurately in the texture areas. Spreading rule indicates that the costs of modifying neighbouring elements should be similar, which has been successfully utilized in HILL by smoothing the distortion functions. Moderating costs (reducing high costs and increasing low costs) also helps defend against knowing attackers such as content-aware steganalysis [18]. In our scheme, we smooth the distortion $\mathbf{D}'$ of the auxiliary image by adopting a low-pass filter $\mathbf{L}$.

### E. Pseudo-code Procedure

To further clarify the scheme of steganography at the microscale, in Algorithm 1 we provide a pseudo-code that describes the implementation of information hiding and extraction.

**Algorithm 1** Microscope steganography

**Input:** A cover image $\mathbf{X}$ with $N$ pixels; $L$ bits of message $\mathbf{m}$ which determines the relative payload of target $\gamma = L/N$.
**Output:** The stego image $\mathbf{Y}$.

1: Sharpen the cover image $\mathbf{X}$ into auxiliary image $\mathbf{X}'$ using linear unsharp masking with scaling factor $\alpha$.
2: Utilize the distortion definition in existing steganography methods (WOW, UNIWARD, HILL, and etc.) to calculate the distortion $\mathbf{D}'$ on the auxiliary image $\mathbf{X}'$.
3: Acquire the smoothed distortion $\mathbf{D}'_s$ by smoothing the distortion $\mathbf{D}'$ with average filter.
4: Assign the distortion $\mathbf{D}'_s$ to the cover image $\mathbf{X}$. The distortion should be adjusted when it comes to saturated pixels in the cover image $\mathbf{X}$. If $x_{i,j} = 0$, then $d_{i,j}(\mathbf{X}, x_{i,j} - 1) = \infty$; if $x_{i,j} = 255$, then $d_{i,j}(\mathbf{X}, x_{i,j} + 1) = \infty$. The adjusted distortion will be the final distortion $\mathbf{D}$.
5: Embed $L$ bits of message $\mathbf{m}$ into cover image $\mathbf{X}$ with STCs according to the final distortion $\mathbf{D}$, and finally output the stego image $\mathbf{Y}$.

## IV. Experiment

### A. Setups

All experiments in this paper are carried out on BOSSbase 1.01 [14] containing 10,000 grayscale $512 \times 512$ images. The detectors are trained as binary classifiers implemented using the FLD ensemble with default settings. A separate classifier is trained for each embedding algorithm and payloads. The ensemble by default minimizes the total classification error probability under equal priors $P_{\mathrm{E}} = min_{P_{\mathrm{FA}}} \frac{1}{2}(P_{\mathrm{FA}} + P_{\mathrm{MD}})$, where $P_{\mathrm{FA}}$ and $P_{\mathrm{MD}}$ are the false-alarm probability and the missed-detection probability respectively. The ultimate security is qualified by average error rate $\overline{P}_{\mathrm{E}}$ averaged over ten 5000/5000 database splits, and larger $\overline{P}_{\mathrm{E}}$ means stronger security. The two feature sets used are SRM [10] and its selection-channel-aware

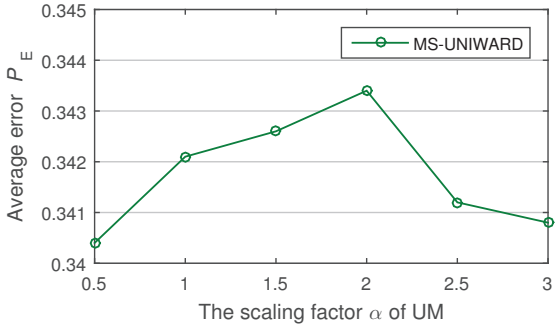



Fig. 7: Average detection error $\overline{P}_{\mathrm{E}}$ of MS-UNIWARD as a function of the scaling factor $\alpha$ using SRM.

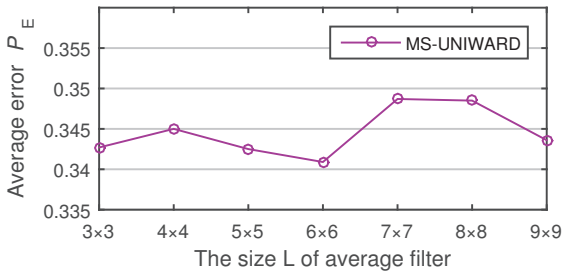



Fig. 8: Average detection error $\overline{P}_{\mathrm{E}}$ of MS-UNIWARD as a function of the average filter size $L$ using SRM.

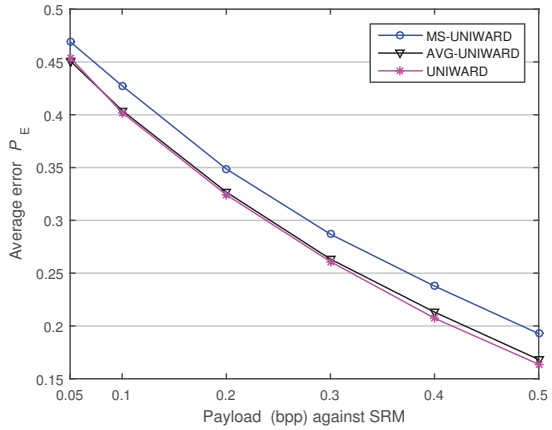



Fig. 9: Detection error for different embedding schemes when steganalyzing with SRM. Three schemes are UNIWARD, AVG-UNIWARD, MS-UNIWARD, respectively. The figure shows the effectiveness of the microscope (unsharp masking).

version maxSRMd2 [13]. As for maxSRMd2 ,the method we estimate embedding change probability is exactly the same as the proposed steganography method. All tested embedding algorithms are simulated at their corresponding payload-distortion bound for payloads $R \in \{0.05, 0.1, 0.2, 0.3, 0.4, 0.5\}$ bpp (bits per pixel).

### B. Determining the parameters of MS steganography

In the experiment, linear unsharp masking is adopted as the microscope, and average filter is implemented for distortion smoothness. As for MS-UNIWARD, first we explore the

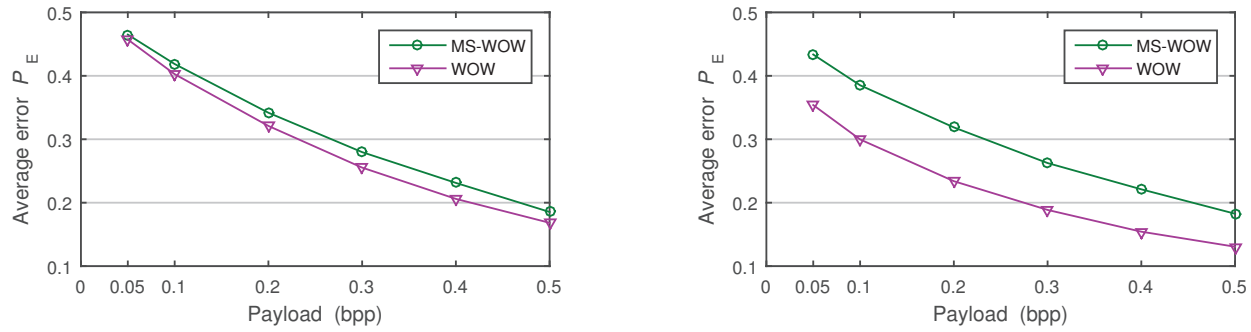



Fig. 10: Detection error for WOW and MS-WOW when steganalyzing with SRM (a) and maxSRMd2 (b).

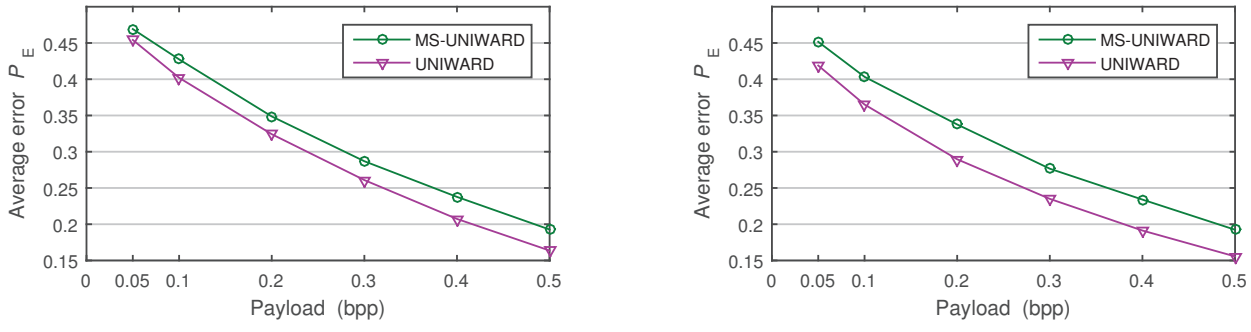



Fig. 11: Detection error for UNIWARD and MS-UNIWARD when steganalyzing with SRM (a) and maxSRMd2 (b).

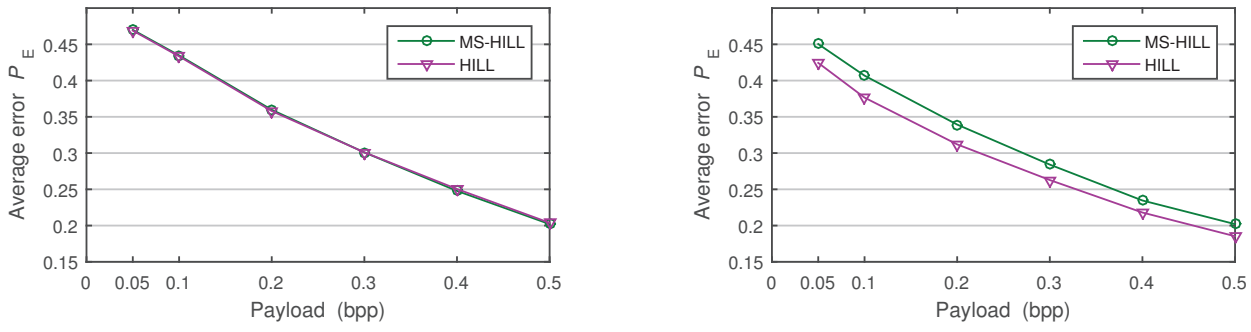



Fig. 12: Detection error for HILL and MS-HILL when steganalyzing with SRM (a) and maxSRMd2 (b).

TABLE I

DETECTABILITY IN TERMS OF $\overline{P}_E$ VERSUS EMBEDDED PAYLOAD SIZE IN BITS PER PIXEL (BPP) FOR PRIOR ART AND APPLIED TO OUR SCHEME ON BOSSBASE 1.01 USING THE FLD ENSEMBLE CLASSIFIER WITH TWO FEATURE SETS.

| Feature | Embedding Method | 0.05 | 0.1 | 0.2 | 0.3 | 0.4 | 0.5 |
|---|---|---|---|---|---|---|---|
| SRM | WOW | .4569 ± .0024 | .4035 ± .0021 | .3203 ± .0025 | .2556 ± .0030 | .2061 ± .0026 | .1680 ± .0027 |
| | MS-WOW | .4650 ± .0022 | .4186 ± .0032 | .3418 ± .0023 | .2797 ± .0024 | .2312 ± .0017 | .1854 ± .0018 |
| | UNIWARD | .4542 ± .0024 | .4021 ± .0024 | .3199 ± .0026 | .2574 ± .0017 | .2031 ± .0026 | .1640 ± .0025 |
| | MS-UNIWARD | .4692 ± .0015 | .4274 ± .0035 | .3487 ± .0031 | .2869 ± .0018 | .2377 ± .0031 | .1927 ± .0019 |
| | HILL | .4688 ± .0023 | .4340 ± .0034 | .3632 ± .0025 | .2996 ± .0023 | .2482 ± .0022 | .2038 ± .0017 |
| | MS-HILL | .4702 ± .0018 | .4347 ± .0032 | .3618 ± .0027 | .3009 ± .0029 | .2478 ± .0031 | .2023 ± .0021 |
| maxSRMd2 | WOW | .3546 ± .0022 | .3010 ± .0031 | .2341 ± .0025 | .1896 ± .0027 | .1553 ± .0031 | .1306 ± .0025 |
| | MS-WOW | .4336 ± .0013 | .3851 ± .0018 | .3187 ± .0021 | .2625 ± .0019 | .2211 ± .0017 | .1826 ± .0023 |
| | UNIWARD | .4189 ± .0024 | .3651 ± .0038 | .2896 ± .0028 | .2350 ± .0021 | .1913 ± .0026 | .1556 ± .0021 |
| | MS-UNIWARD | .4516 ± .0037 | .4033 ± .0024 | .3376 ± .0031 | .2766 ± .0024 | .2340 ± .0023 | .1924 ± .0037 |
| | HILL | .4244 ± .0023 | .3765 ± .0031 | .3120 ± .0029 | .2628 ± .0022 | .2180 ± .0025 | .1853 ± .0024 |
| | MS-HILL | .4504 ± .0025 | .4068 ± .0023 | .3393 ± .0032 | .2840 ± .0018 | .2388 ± .0028 | .2030 ± .0023 |

optimal value of scaling factor $\alpha$ of unshap masking. We set the size of average filter $L = 3 \times 3$ and keep it invariant. Fig. 7 shows the effect of different scaling factors $\alpha$ with a fixed payload of 0.2 bpp on empirical security. The result indicates that $\alpha = 2$ performs best. Since the scaling factor $\alpha$ has been set, an experiment is carried out to obtain the best filter size for $L$. The results are shown in Fig. 8. It is suggested that $L = 7 \times 7$ outperforms other sizes. Under the same experiment condition conducted in MS-WOW and MS-HILL, the optimal parameters are the same. In other words, the parameters ($\alpha = 2$, $L = 7 \times 7$) can serve as empirical parameters.

### C. The effectiveness of the microscope

We conduct some comparative experiments to investigate the effectiveness of the microscope in the MS algorithm. "AVG" represents the steganograpohy method with a single operation of average filter. Three steganography experiments (UNIWARD, AVG-UNIWARD, MS-UNIWARD) are carried out under the steganalytic feature set SRM. According to the results shown in Fig. 9, it is obvious that MS-UNIWARD performs far better than AVG-UNIWARD. It demonstrates that microscope in the algorithm contributes largely to the promotion of the performance.

### D. Application to prior methods

The proposed scheme is applied to the prior steganography methods. In this paper, WOW, UNIWARD and HILL are chosen as the steganography methods, for they are representative. The parameters of them have been discussed in the previous subsection. As shown in Fig. 10 and Fig. 11, MS-WOW performs better than WOW by about 1.0-2.5% steganalyzing with SRM and 5.0-8.5% steganalyzing with maxSRMd2. MS-UNIWARD performs better than UNIWARD by about 1.5-3.5% against SRM and 3.5-5.0% against maxSRMd2. It can be observed from Fig. 12 that MS-HILL and HILL have similar performances against SRM, while MS-HILL has an apparent improvement over HILL against maxSRMd2.

Table I shows the average total probability of error $\overline{P}_{\mathrm{E}}$ and its standard deviation for a range of payloads. Note that, the one using MS algorithm offers better security than not using. The experiment results mentioned above support the effectiveness of the proposed scheme.

## V. Conclusions

In this paper, we propose a new scheme which defines cost functions for adaptive steganography at the microscale. Before distortion definition, the cover image would be preprocessed with a microscope. Therefore, prior steganographic methods can seize the texture areas more precisely, so that the distortion can be defined further accurately. In our study, unsharp masking plays the role of the microscope. We also make a further enhancement of the MS algorithm incorporating the spreading rule by smoothing the embedding distortion on the auxiliary image. The experiment results verified that the proposed scheme does work.

Since image enhancement techniques vary greatly, we will try to explore the effectiveness of other methods. In addition, our work is discussed in additive distortion steganography, so we intend to generalize an extension of this work in non-additive distortion steganography in our future study.

## Acknowledgment

This work was supported in part by the Natural Science Foundation of China under Grant 61572452, Grant 61502007 and Grant 61373151, in part by the China Postdoctoral Science Foundation under Grant 2015M582015, and in part by the Strategic Priority Research Program of the Chinese Academy of Sciences under Grant XDA06030601.

## References

[1] T. Pevný and J. Fridrich, "Benchmarking for steganography," in *Information Hiding: 10th International Workshop*, pp. 251–267, Springer Berlin Heidelberg, 2008.

[2] J. Fridrich, *Steganography in digital media: principles, algorithms, and applications*. Cambridge University Press, 2009.

[3] J. Fridrich and T. Filler, "Practical methods for minimizing embedding impact in steganography," in *Electronic Imaging 2007*, pp. 650502–650502, International Society for Optics and Photonics, 2007.

[4] T. Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 920–935, 2011.

[5] T. Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 920–935, 2011.

[6] T. Pevny, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 215–224, 2010.

[7] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *2012 IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 234–239, IEEE, 2012.

[8] V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," *EURASIP Journal on Information Security*, vol. 2014, no. 1, pp. 1–13, 2014.

[9] B. Li, M. Wang, J. Huang, and X. Li, "A new cost function for spatial image steganography," in *2014 IEEE International Conference on Image Processing (ICIP)*, pp. 4206–4210, IEEE, 2014.

[10] J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 868–882, 2012.

[11] V. Sedighi, R. Cogranne, and J. Fridrich, "Content-adaptive steganography by minimizing statistical detectability," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 221–234, 2016.

[12] A. Polesel, G. Ramponi, V. J. Mathews, *et al.*, "Image enhancement via adaptive unsharp masking," *IEEE transactions on image processing*, vol. 9, no. 3, pp. 505–510, 2000.

[13] T. Denemark, V. Sedighi, V. Holub, R. Cogranne, and J. Fridrich, "Selection-channel-aware rich model for steganalysis of digital images," in *2014 IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 48–53, IEEE, 2014.

[14] P. Bas, T. Filler, and T. Pevnỳ, ""break our steganographic system" the ins and outs of organizing boss," in *International Workshop on Information Hiding*, pp. 59–70, Springer, 2011.

[15] V. Sedighi and J. Fridrich, "Effect of saturated pixels on security of steganographic schemes for digital images," in *2016 IEEE International Conference on Image Processing (ICIP)*, pp. 2747–2751, Sept 2016.

[16] R. C. Gonzalez and R. E. Woods, "Digital image processing," *Nueva Jersey*, 2008.

[17] B. Li, S. Tan, M. Wang, and J. Huang, "Investigation on cost assignment in spatial image steganography," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 8, pp. 1264–1277, 2014.

[18] A. D. Ker, T. Pevnỳ, and P. Bas, "Rethinking optimal embedding," in *Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security*, IH&MMSec'16, (New York, NY, USA), pp. 93–102, ACM, 2016.