Multimed Tools Appl
DOI 10.1007/s11042-017-4565-5

Which gray level should be given the smallest cost for adaptive steganography?

Yao Wei[1,2] · Weiming Zhang[1] · Weihai Li[1,2] · Nenghai Yu[1,2] · Xi Sun[1,2]

Received: 9 September 2016 / Revised: 15 February 2017 / Accepted: 28 February 2017

Abstract Currently, the most successful approach to steganography in digital image is distortion-minimization framework, which reduces the steganographers' work to the design of distortion function with the aid of practical coding schemes. Previous distortion functions for spatial images are all position dependent, in which cost is determined by the relationships between neighboring pixels. Noticing that Gamma encoding is usually involved in image preprocessing in many cameras or image processing software, which causes some pixels to change greatly, we believe these pixels sensitive to Gamma encoding are more suitable for modification, because they are hard to model due to their large variations. Inspired by this idea, we proposed a position independent scheme, where the cost is only linked to the gray level. The effectiveness of our work is verified by extensive experimental results, which reveal an interesting relationship between steganographic costs and gray levels. The speed test shows that the speed of proposed scheme is very high thus suitable to be used in the real-time applications.

Keywords Steganography · Distortion function · Gamma encoding · Gray level

1 Introduction

Steganography is a technique for covert communication, aiming to hide secret messages into ordinary digital media without drawing suspicion [7, 17, 24]. Designing steganographic algorithms for various cover sources is challenging due to the fundamental lack

✉ Weiming Zhang
zhangwm@ustc.edu.cn

1 University of Science and Technology of China, Anhui, China

2 Key Laboratory of Electromagnetic Space Information, Chinese Academy of Sciences, Anhui, China

Published online: 09 March 2017

of accurate models. According to whether the original cover image pixels can be recovered or not after data extraction, current data hiding schemes can be classified into two categories, i.e., reversible data hiding [1, 21, 26, 27, 30, 31] and irreversible data hiding [5, 8, 10–14, 23]. Currently, the most successful approach for irreversible data hiding is the distortion-minimization (DM) [18] framework, which minimizes the statistical detectability by employing a coding scheme to minimize a well-defined distortion function [5, 8, 10–14, 23]. Such work gains popularity due to the fact that both optimal embedding simulator which operates on the theoretical rate-distortion bound and practical coding schemes which work close to the bound are available [6]. Therefore, the key of this framework is the design of the distortion function which is usually composed of a cost assigned to each cover pixel. In this work, we just focus on the seganographic schemes in spatial domain.

As summarized in [18], the philosophy behind all steganographic schemes in Spatial domain based on DM [18] framework can be generalized as following three principles:

1) ***Complexity-First Principle***.

This principle implies that the steganographer should modify the area of complicated texture with high priority, which is hard to model in steganalysis.

Nearly all steganographic schemes follow the Complexity-First Principle. The first example of this principle is HUGO [23]. The pixel distortion is defined by the changing amplitude of SPAM (subtractive pixel adjacency matrix) [22] features, which is generated by exploiting correlations between the predicted residuals of neighboring pixels [16, 22]. High costs are distributed to pixels, the modification of which leads to a greater deviation in feature vectors. Because the pixels in smooth areas can be accurately predicted, the modifications in such areas will be easily detected by steganalyzers. Therefore the embedding changes of HUGO will be gathered within textured regions.

Another two examples of the first principle are WOW [12] and UNIWARD [13]. WOW [12] assigns high costs to pixels with large directional residuals generated by a bank of directional high-pass filters. Larger directional residuals indicates high unpredictability thus high texture complexity. So WOW [12] mainly changes the pixels in textured regions. The distortion function is further simplified in UNIWARD [13]. Both algorithms have been shown to better resist steganalysis using rich models [9] than HUGO [23].

Sometimes the complexity first principle can be shown in a more implicit way. MG (multivariate Gaussian model) [10, 28, 29] models the cover pixels as a sequence of independent Gaussian random variables with unequal variances. The costs are obtained by minimizing KL (Kullback-Leibler) divergence between the statistical distributions of cover and stego images. Because the KL divergence is related to the local variance of cover elements, MG [10, 28, 29] implicitly follows the Complexity-First principle as well.

2) ***Spreading Principle***.

This principle requires that two neighboring elements should not differ greatly in costs. In other words, an element with high costs should spread its high costs to its neighbors, and vice versa. HILL [19] employed this principle to improve WOW [12], and Sedighi et al. [28] used it to improve MG [10].

3) ***Modification Direction Synchronizing (MDS)***.

Adopted in non-additive distortion model, this principle suggests that neighboring pixels changed in the same directions will introduce smaller costs. This principle is also called Modification Directions Clustering (MDC) in [20]. It was successfully exploited by Denemark et al. [4], Li et al. [20] and Zhang [32], which significantly improve the performance in resisting steganalysis.

On one hand, all of previous steganographic schemes are position dependent, where the cost of each pixel is determined by the relationship between that pixel and its neighbors. The magnitude of individual pixel value is never taken into account in the design of spatial domain schemes. However, in DCT domain schemes, the magnitude of cover element is a key consideration in design of distortion function. The DCT coefficients with larger absolute value should be given smaller costs [11]. Therefore, we may wonder which gray level should be given the smallest cost in spatial domain. In this paper, we proposed a scheme where the answer is given. The distortion function is only associated with the gray level of the pixel and the cost of each pixel is totally independent of the pixel relationship. Our study reveals an interesting relationship between steganographic costs and gray levels.

On the other hand, with the rapid rise of smart phone users, it's quite common for people to share images over the mobile platform which provides extensive covers for covert communication. As a result, it's important to apply steganographic algorithms to mobile platform. Traditional researchers usually only focus on the steganalysis security. However, time complexity and space complexity are also important considerations on mobile platform due to their limited computing resources and battery volume. For example, it would be intolerable if you have to spend a long time embedding the message into the image before sending it. Besides, longer time of sending message may arouse suspection.

The rest of the paper is structured as follows. Preliminaries of DM [18] framework is introduced in next section. The detail of our scheme is demonstrated in Section 3. The efficiency of our scheme is verified by experiments in Section 4. And the conclusion is given in Section 5.

2 Preliminaries

The cover sequence is denoted by $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, where x_i is an integer, such as the gray value of a pixel. In this paper, we consider the case of ternary embedding operation, which can be represented by $I_i = \{x_i - 1, x_i, x_i + 1\}$ for all i.

As is established in [6], the distortion introduced by changing $\mathbf{x}$ to $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ can be simply denoted by $D(\mathbf{x}, \mathbf{y}) = D(\mathbf{y})$ in view of the assumption that the cover $\mathbf{x}$ is fixed. If the embedding algorithm changes $\mathbf{x}$ to $\mathbf{y} \in \mathcal{Y}$ with modification probability $\pi(\mathbf{y}) = P(Y = \mathbf{y})$, the sender can send up to $H(\pi)$ bits of message on average with average distortion $E_\pi(D)$ such that

$$H(\pi) = -\sum_{\mathbf{y}\in\mathcal{Y}} \pi(\mathbf{y})\ log\ \pi(\mathbf{y}). \tag{1}$$

$$E_\pi(D) = \sum_{\mathbf{y}\in\mathcal{Y}} \pi(\mathbf{y}) D(\mathbf{y}). \tag{2}$$

For a given message length L, the aim to minimize the average distortion can be formulated as the following optimization problems:

$$\min_{\pi}\ E_\pi(D), \tag{3}$$

$$\text{subject to } H(\pi) = L. \tag{4}$$

Following the maximum entropy principle, the optimal π has a Gibbs distribution [6]:

$$\pi_\lambda(\mathbf{y}) = \frac{1}{Z(\lambda)} \exp(-\lambda D(\mathbf{y})). \tag{5}$$

where $Z(\lambda)$ is the normalizing factor such that

$$Z(\lambda) = \sum_{\mathbf{y}\in\mathcal{Y}} \exp(-\lambda D(\mathbf{y})). \tag{6}$$

The payload constraint (4) determines the scalar parameter $\lambda > 0$. In fact, as proven in [5], the entropy in (4) decreases monotonically with λ, thus for a given L in feasible region, λ can be fast determined by binary search.

Specially, the distortion introduced by changing $\mathbf{x}$ to $\mathbf{y}$ can be approximate to additive distortion when embedding operation on x_i's is independent of each other. And the distortion can be measured by $D(\mathbf{y}) = \sum_{i=1}^{n} \rho^{(i)}(y_i)$,where $\rho^{(i)}(y_i) \in \mathbb{R}$ is the cost of changing the ith cover element x_i to y_i $(y_i \in I_i, i = 1, 2, \ldots, n)$. In this case, the optimal π is given by

$$\pi(y_i) = \frac{\exp(-\lambda\rho^{(i)}(y_i))}{\sum_{y_i\in I_i} \exp(-\lambda\rho^{(i)}(y_i))}, \quad i = 1, 2, \ldots, n. \tag{7}$$

For additive distortion, practical coding methods such as STCs (Syndrome-Trellis Codes) [6] can approach the lower bound of average distortion (3).

3 Proposed scheme

In this section, we will explore the relationship between embedding costs of steganography and gray level in spatial domain via Gamma encoding.

3.1 Gamma encoding

Gamma encoding is the name of a nonlinear operation used to code and decode luminance or tristimulus values in video or still image systems [25]. In the simplest cases, it is defined by the following power-law expression:

$$g(x, \gamma) = \left(\frac{x}{255}\right)^{\gamma} \times 255, \ x \in [0, 255]. \tag{8}$$

where x donotes the gray level (pixel value) of the gray image.

Gamma encoding is commonly involved in image preprocessing in many cameras or image processing software. After Gamma encoding, pixels of different gray level vary in the changing extent. We believe that the pixels changed greatly after Gamma encoding may be suitable for modification, because these pixels are hard to model due to their large variations. Inspired by such idea, we proposed a distortion function, in which the pixels that vary largely after Gamma encoding will be assigned small costs.

3.2 Distortion function

We change the γ parameter in the vicinity of 1. The pixel that varies most greatly is assigned the smallest cost, so the distortion function is as follow:

$$\rho(x) = \frac{1}{|g(x, 1) - g(x, 1 + \Delta)|}, \ x \in [0, 255]. \tag{9}$$

Here for simplicity, we just let $\Delta = 0.001$.

The cost is defined for each gray level, so the distortion function is actually a map with 256 keys. The cost of each cover pixel is generated by looking up the map. In our algorithm, we use the double-layered version of STCs [6] for ± 1 embedding. We assume that the embedding distortion is independent of the direction, i.e., each pixel plus or minus 1 with the same cost.

The distortion curve appears as a parabola (Fig. 1). Next, we analyze which gray level has the smallest cost for steganography according to the distortion function (9).

Firstly, let $x = \frac{x}{255}$, so the input and output of Gamma encoding are scaled to [0,1]. Then (8) can be simplified as:

$$g(x, \gamma) = x^{\gamma}, \ \ x \in [0, 1]. \tag{10}$$

Secondly, take the derivative of γ:

$$\frac{\partial g(x, \gamma)}{\partial \gamma} = x^{\gamma} \times \ln x. \tag{11}$$

Let $\gamma = 1, \ h(x) = \frac{\partial g(x,\gamma)}{\partial \gamma}$, we can get:

$$h(x) = x \times \ln x. \tag{12}$$

According to the distortion function (9), the cost value is the reciprocal of $|h(x)|$. As $x \in [0, 1]$,

$$|h(x)| = -x \times \ln x. \tag{13}$$

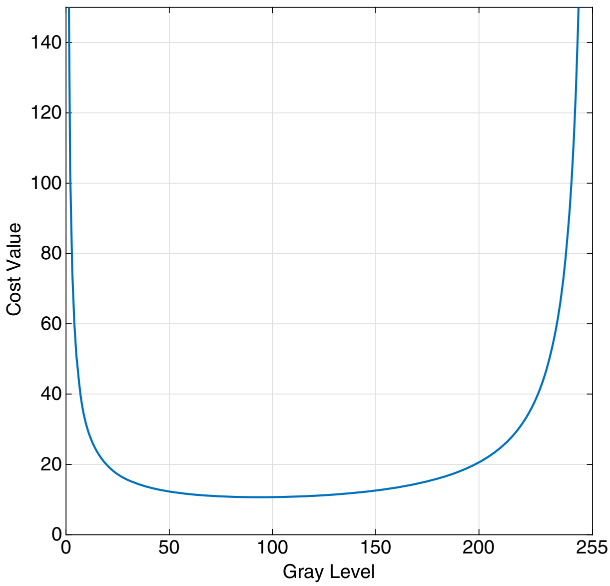


Fig. 1 Distribution of the pixel costs

Next, take the derivative of x:

$$\frac{\mathrm{d}|h(x)|}{\mathrm{d}x} = -(1 + \ln x). \tag{14}$$

By solve the equation $\frac{\mathrm{d}|h(x)|}{\mathrm{d}x} = 0$, we get:

$$x = \frac{1}{e}. \tag{15}$$

The cost value decreases monotonically with x when $x < \frac{255}{e}$ and increases monotonically when $x > \frac{255}{e}$. Consequently, the gray level that has the smallest cost is $x = \frac{255}{e} \approx 94$.

3.3 Time complexity

Because the STCs [6] encoding is commonly used in all adaptive schemes, we can omit the complexity of STCS [6] and focus on the distortion calculation. Since the distortion table is fixed, looking up the table at each pixel is the only operation, the whole complexity is O(kn), where n is the number of pixels and k is a constant factor. In SUNIWARD [13], totally three convolutions are used to calculate the residuals. Although the time complexity is still O(kn), the constant factor is much larger than that of proposed scheme. The time complexity of these two methods are further compared in the next experiment section.

4 Experiment

4.1 Discussion of the Δ parameter

In distortion function (9), Δ control the step of the gamma parameter offset from 1. We compare the testing error of different Δ in different embed ratio (Fig. 2) on BossBase ver 1.01

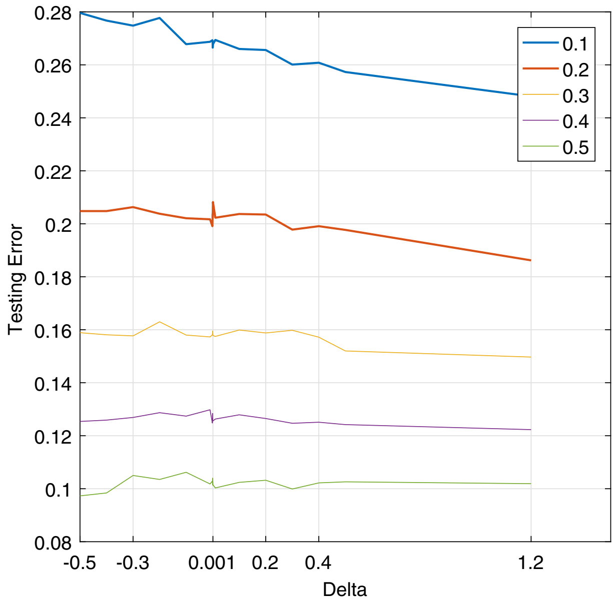
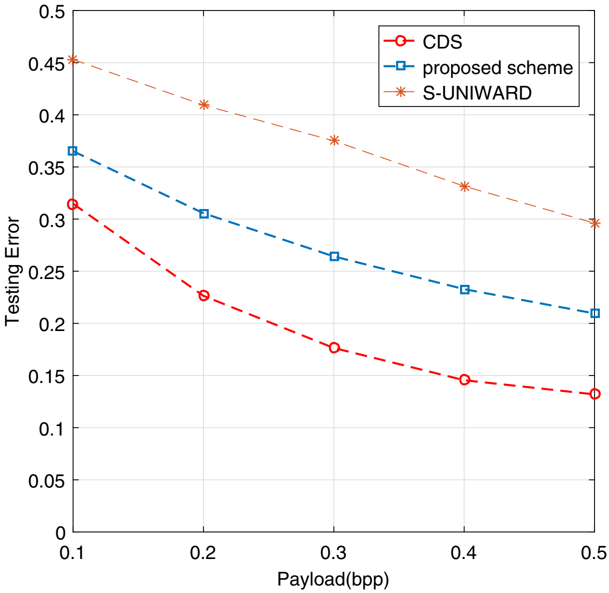
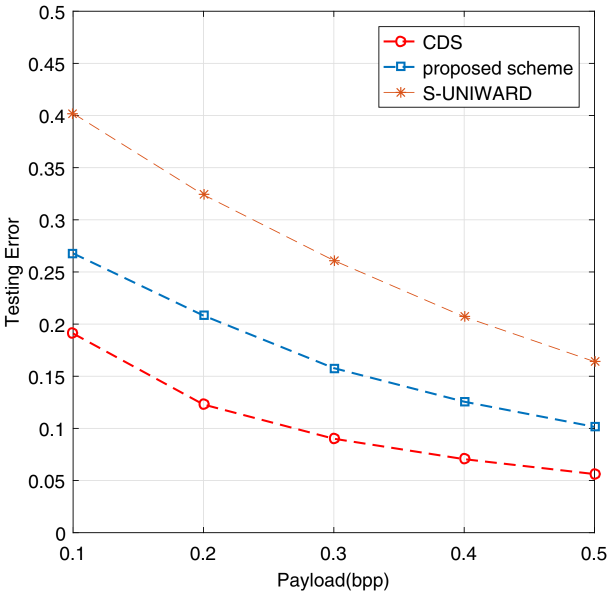


Fig. 2 Test error of different Δ in different embed ratio

[2] using SRM features. The result shows that changing the $\Delta = 0.001$ will not improve the test performance greatly, only small improvement will be obtained in ratio 0.1. So we will keep $\Delta = 0.001$.



(a) SPAM feature



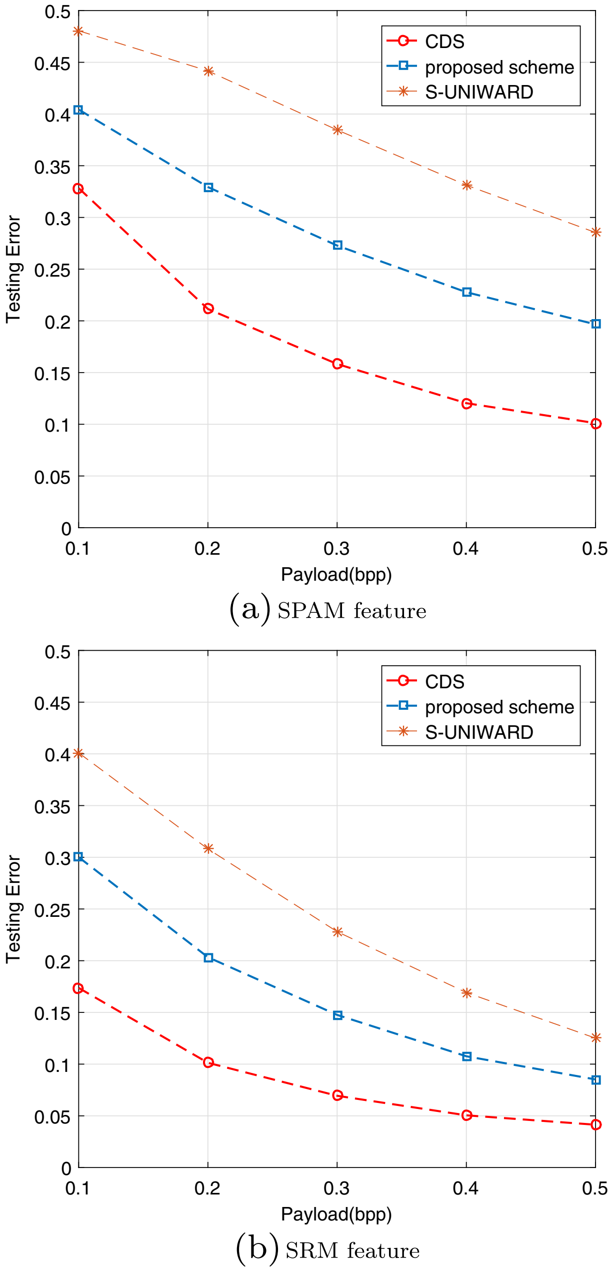
(b) SRM feature

Fig. 3 Comparion of proposed scheme and a constant distortion scheme (CDS), S-UNIWARD on BossBase ver 1.01 image database using SPAM feature and SRM feature

4.2 Testing error comparison

BossBase ver 1.01 [2] and BOWS2 database [3] each with 10000 gray-scale images of size 512 × 512 are used in experiment. The 686-D SPAM [22] and 32671-D SRM [9] are chosen as feature sets. Ensemble classifier [15] is used where Fisher linear discriminants are

Fig. 4 Comparion of proposed scheme and a constant distortion scheme (CDS), S-UNIWARD on BOWS2 image database using SPAM feature and SRM feature



chosen as base learners. For each image database, training set is composed of half random-selected cover images and their stego counterparts, while test set is composed of the rest half pairs. Testing error is used for evaluation, which is the average of the false positive rate and false negative rate. To verify proposed scheme, we compare it with the SUNIWARD [13], and a constant distortion scheme (CDS), in which the cost values of all pixels for every modification direction $(+1, -1)$ are all one. And the messages are also embedded using double-layered STCs [6].

From the experiment results shown in Figs. 3 and 4 (the detailed results are shown in Table 1), we can draw the following conclusions:

1. For BossBase database, the proposed scheme outweighs CDS by $\%5 - \%8$ for both SPAM and SRM feature.
2. For BOWS2 database, the proposed scheme outperforms CDS by $\%7 - \%11$ for SPAM feature. As for SRM feature, the proposed scheme outperforms CDS by $\%4 - \%12$, and the advantage of our scheme is more obvious for small payload.

The experiment shows that proposed scheme is not comparable to SUNIWARD [13], this is reasonable since our scheme only takes into account the gray value and SUNIWARD [13] exploits the pixel relationships. All experiments prove that there indeed exists correlation between gray levels and steganographic costs.

4.3 Speed comparison

In this section, we compare the distortion calculation speed between proposed scheme and SUNIWARD [13] on various size of images. The time spent on image IO and STCS [6] encoding is not taken into account. 100 pictures (4160*3120) from cellphone are used as image source. The original images are resized to various sizes of square image to create different image set. The result are show in Fig. 5. The test are run on matlab using single thread on a computer with I5-4570 3.2GHZ cpu.

In Fig. 5, the y axis is the average distortion calculation time used in each image in seconds while the x axis is the number of pixels. The time increases linearly with respect to number of pixels, which verifies the linear complexity. The slope of proposed scheme

Table 1 Steganalysis experiment result on different image set with different feature and algorithms

Image set	Feature	Algorithm	0.1	0.2	0.3	0.4	0.5
BOSS	SRM	CDS	0.191	0.1229	0.0901	0.0705	0.0562
		Proposed Scheme	0.2678	0.2082	0.1578	0.1256	0.1015
		SUNIWARD	0.408	0.331	0.259	0.211	0.165
	SPAM	CDS	0.3147	0.2264	0.1764	0.1455	0.1319
		Proposed scheme	0.3651	0.3056	0.2642	0.2328	0.2095
		SUNIWARD	0.453	0.4093	0.375	0.3315	0.2961
BOWS	SRM	CDS	0.1737	0.1013	0.0694	0.0505	0.0414
		Proposed scheme	0.3001	0.2034	0.1476	0.1076	0.0852
		SUNIWARD	0.401	0.3081	0.2281	0.1692	0.1251
	SPAM	CDS	0.3283	0.2115	0.1583	0.1204	0.1011
		Proposed scheme	0.4043	0.3294	0.2728	0.2277	0.1966
		SUNIWARD	0.4805	0.4417	0.3846	0.3312	0.2854

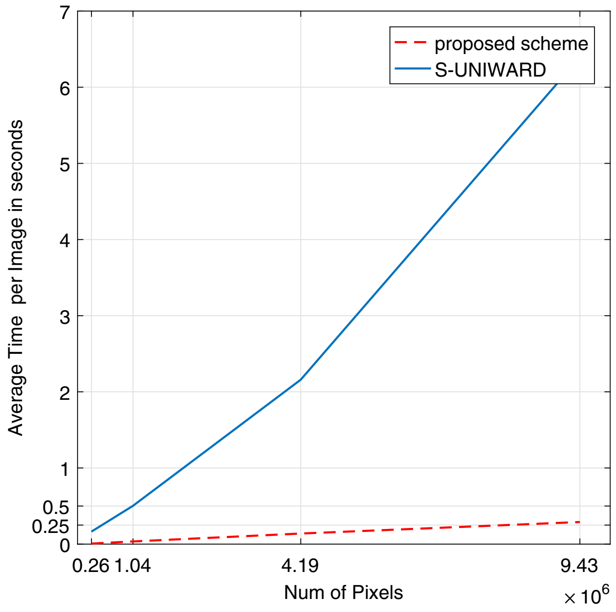


Fig. 5 Speed comparison between proposed scheme and SUNIWARD on different size of images

is much smaller than that of SUNIWARD [13], therefore, proposed scheme far outweighs SUNIWARD [13] in speed.

5 Conclusions

The most effective model for adaptive steganography is to embed messages while minimizing a carefully defined distortion function. In previous research, the design of all distortion function are position dependent, which exploits the relationships between neighbor pixels.

In this paper, we first pose a question: which gray level should be given the smallest cost in spatial domain? Then we proposed a novel scheme where the answer is given: the gray level that changes most greatly after the Gamma encoding should be assigned the smallest cost, which is approximately 94. The cost of each pixel is only linked to its gray level and independent of its position. In fact, the distortion metric is simply a map with 256 keys. The cost of each pixel is generated by looking up the map with gray level. So the metric is a universal distortion for all images. Because of its simplicity, compared to the prior position dependent scheme, on one hand, the algorithm enjoys low time complexity and is applicable for situation with high speed requirements. On the other hand, it can not be compared to other position dependent schemes for security. In spite of its security deficiency, our scheme reveals an interesting relationship between steganographic costs and gray levels.

However, the philosophy behind the proposed scheme remains unclear. One possible explanation is that Gamma encoding is usually involved in image preprocessing in many cameras or image processing software, which causes some pixels to change greatly naturally. Modifications of such pixels sensitive to Gamma encoding are hard to detect, because it's difficult to distinguish artificial modification from natural image preprocessing. But this explanation has not been verified yet. We leave this question open.

Our future work include finding the reasons behind the proposed scheme and combining this scheme with the position dependent schemes to improve security. Furthermore, more techniques in image preprocessing may be exploited to improve the current scheme.

Acknowledgements This work was supported in part by the Natural Science Foundation of China under Grant U1636201, 61572452.

References

1. Alattar AM (2004) Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans Image Process 13(8):1147–1156
2. Bas P, Filler T, Pevnỳ T (2011) break our steganographic system: the ins and outs of organizing boss. In: Information hiding. Springer, pp 59–70
3. Bas P, Furon T (2007) Bows2-original. http://bows2.ec-lille.fr/
4. Denemark T, Fridrich J (2015) Improving steganographic security by synchronizing the selection channel. In: Proceedings of the 3rd ACM workshop on information hiding and multimedia security. ACM, pp 5–14
5. Filler T, Fridrich J (2010) Gibbs construction in steganography. IEEE Trans Inf Forensic Secur 5(4):705–720
6. Filler T, Judas J, Fridrich J (2011) Minimizing additive distortion in steganography using syndrome-trellis codes. IEEE Trans Inf Forensic Secur 6(3):920–935
7. Fridrich J (2009) Steganography in digital media: principles, algorithms, and applications. Cambridge University Press
8. Fridrich J, Filler T (2007) Practical methods for minimizing embedding impact in steganography. In: Electronic imaging 2007. International Society for Optics and Photonics, pp 650,502–650,502
9. Fridrich J, Kodovskỳ J (2012) Rich models for steganalysis of digital images. IEEE Trans Inf Forensic Secur 7(3):868–882
10. Fridrich J, Kodovskỳ J (2013) Multivariate gaussian model for designing additive distortion for steganography. In: ICASSP, pp 2949–2953
11. Guo L, Ni J, Shi YQ (2012) An efficient jpeg steganographic scheme using uniform embedding. In: 2012 IEEE international workshop on information forensics and security (WIFS). IEEE, pp 169–174
12. Holub V, Fridrich J (2012) Designing steganographic distortion using directional filters. In: 2012 IEEE international workshop on information forensics and security (WIFS). IEEE, pp 234–239
13. Holub V, Fridrich J (2013) Digital image steganography using universal distortion. In: Proceedings of the first ACM workshop on information hiding and multimedia security. ACM, pp 59–68
14. Huang F, Huang J, Shi YQ (2012) New channel selection rule for jpeg steganography. IEEE Trans Inf Forensic Secur 7(4):1181–1191
15. Kodovskỳ J, Fridrich J, Holub V (2012) Ensemble classifiers for steganalysis of digital media. IEEE Trans Inf Forensic Secur 7(2):432–444
16. Kodovskỳ J, Pevnỳ T, Fridrich J (2010) Modern steganalysis can detect yass. In: IS&T/SPIE electronic imaging. International Society for Optics and Photonics, pp 754,102–754,102
17. Li B, He J, Huang J, Shi YQ (2011) A survey on image steganography and steganalysis. J Inf Hiding Multimed Signal Process 2(2):142–172
18. Li B, Tan S, Wang M, Huang J (2014) Investigation on cost assignment in spatial image steganography. IEEE Trans Inf Forensic Secur 9(8):1264–1277
19. Li B, Wang M, Huang J, Li X (2014) A new cost function for spatial image steganography. In: 2014 IEEE international conference on image processing (ICIP). IEEE, pp 4206–4210
20. Li B, Wang M, Li X, Tan S, Huang J (2015) A strategy of clustering modification directions in spatial image steganography. IEEE Trans Inf Forensic Secur 10(9):1905–1917
21. Ni Z, Shi YQ, Ansari N, Su W (2006) Reversible data hiding. IEEE Trans Circ Syst Video Technol 16(3):354–362
22. Pevnỳ T, Bas P, Fridrich J (2010) Steganalysis by subtractive pixel adjacency matrix. IEEE Trans Inf Forensic Secur 5(2):215–224
23. Pevnỳ T, Filler T, Bas P (2010) Using high-dimensional image models to perform highly undetectable steganography. In: Information hiding. Springer, pp 161–177
24. Pevnỳ T, Fridrich J (2008) Benchmarking for steganography. In: Information hiding. Springer, pp 251–267

25. Poynton CA (1998) Rehabilitation of gamma. In: Photonics west'98 electronic imaging. International Society for Optics and Photonics, pp 232–249
26. Qin C, Chang CC, Hsu TJ (2015) Reversible data hiding scheme based on exploiting modification direction with two steganographic images. Multimed Tools Appl 74(15):5861–5872
27. Qin C, Hu YC (2016) Reversible data hiding in vq index table with lossless coding and adaptive switching mechanism. Signal Process 129:48–55
28. Sedighi V, Cogranne R, Fridrich J (2016) Content-adaptive steganography by minimizing statistical detectability. IEEE Trans Inf Forensic Secur 11(2):221–234
29. Sedighi V, Fridrich J, Cogranne R (2015) Content-adaptive pentary steganography using the multivariate generalized gaussian cover model. In: IS&T/SPIE electronic imaging. International Society for Optics and Photonics, pp 94,090H–94,090H
30. Thodi DM, Rodríguez JJ (2007) Expansion embedding techniques for reversible watermarking. IEEE Trans Image Process 16(3):721–730
31. Tian J (2003) Reversible data embedding using a difference expansion. IEEE Trans Circ Systems Video Technol 13(8):890–896
32. Zhang W, Zhang Z, Zhang L, Li H, Yu N (2016) Decomposing joint distortion for adaptive steganography. IEEE Transactions on Circuits and Systems for Video Technology

Yao Wei master's degree. Yao Receive his bachelor's degree in Information Security, University of Science and Technology of China. His main research interests focus on information security, information hiding.

Weiming Zhang received his B.S. degree and PH.D. degree in 1999 and 2005 respectively from Information Engineering University, Zhengzhou, China. Currently, he is an professor with the School of Information Science and Technology, University of Science and Technology of China. His research interests include information hiding, multimedia security, and privacy-preserving data searching and analysis. He has published more than 80 papers in journals and conferences including IEEE Trans. Information Theory, IEEE Trans. Image ProcessingIEEE Trans. Inf. Foren. and Sec., and Information Hiding.

Weihai Li received his Ph.D. in Electromagnetic Field and Microwave Technology from University of Sience and Technology of China (USTC) in 2003. Now He works in the School of Information Science and Technology of USTC as a faculty. Dr. Li lead a research team of Digital Media Analysis in the Group of Information Processing Centor. His team is investigating technologies of media forensics, media content protection and analysis, remote sensing image processing, and etc. Dr. Li is a member of IEEE(Institute of Electrical and Electronic Engineers), ACM(Association for Computing Machinery), CCF(China Computer Federation), and CACR(Chinese Association for Cryptologic Research).

Nenghai Yu born in 1964, is a professor, Ph.D. supervisor,the director of Information Processing Center of USTC, deputy director of academic committee of School of Information Science and Technology,director of multimedia and communication lab, deputy director of Ministry of Education-Microsoft Key Laboratory of Multimedia Computing and Communications(2004–2010), the standing member of council of Image and Graphics Society of China,a member of Expert Committee of Cloud Computing of Chinese Institute of Electronics, member of Expert Committee of IP Applications and Value-added Telecommunications Technology of Chinese Institute of Communications,and a member of Expert Committee of Multimedia Safety of Division of Communications of Chinese Institute of Electronics. He was a visiting scholar in Institute of Production Technology, Faculty of Engineering, University of Tokyo, in 1999 and did cooperative research as the senior visiting scholar in Dept. of Electrical Engineering, Columbia University, from Apr. to Oct. 2008.

Xi Sun master's degree. Sun Receive his bachelor's degree in Physics, University of Science and Technology of China. His main research interests focus on information security, information hiding.