J. Vis. Commun. Image R. 71 (2020) 102822

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

journal homepage: www.elsevier.com/locate/jvci

An embedding strategy on fusing multiple image features for data hiding in multiple images ☆

Junxue Yang [a], Xin Liao [a,b,*]

[a] College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China
[b] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

ARTICLE INFO

Article history:
Received 22 October 2019
Accepted 2 May 2020
Available online 29 May 2020

Keywords:
Multiple images steganography
Embedding strategy
Multiple image features
Image complexity
Steganographic capacity

ABSTRACT

Data hiding in multiple images has been a significant research direction in information security. How to reasonably design the embedding strategy to spread the payload among multiple images is still an open issue. In this paper, we propose an embedding strategy on fusing multiple features. We utilize the typical characteristic parameters of gray level co-occurrence matrix, the image entropy and the shape parameter to describe image complexity. Furthermore, we combine with the number of cover images, the number of cover images assigned to steganographer and the size of cover image to estimate the steganographic capacity of each image. The strategy is implemented together with some state-of-the-art single image steganographic algorithms. Experimental results demonstrate that the security performance of the proposed strategy is higher than that of the state-of-the-art embedding strategy against the blind universal pooled steganalysis.

1. Introduction

Steganography technology makes use of the redundancy of digital medias and the insensitivity of the human visual system to conceal secret information [1–4]. Although many kinds of digital medias can be used as steganographic covers, the digital image is optimal because of the higher popularity and availability. Recent years have seen a remarkable progress in steganography. Numerous modern and content-adaptive steganographic algorithms, such as WOW [5], S-UNIWARD [6], HILL [7] and MiPOD [8], has been proposed utilizing syndrome trellis codes [9]. However, existing image steganography is mostly based on single cover, which restricts the length of the payload and the security of steganography [10]. Moreover, with the rapid development of image data, the steganographer has massively available images. Therefore, multiple images steganography is more applicable to practical scenario. Currently, the research on multiple images steganography is separated into two major aspects, one is embedding strategy and another is steganographic capacity [11].

Ker [10] first postulated multiple images steganography in 2006. Simultaneously, it was proposed that the optimal choice of spreading payload is likely to embed into as few covers as possible. Later, based on the threshold measurement statistical method of the number of covers, Ker demonstrated the parameter and payment model of game theory, and designed two effective embedding strategies: spreading payload into the fewest number of covers, or equally spreading payload into all covers [12]. Due to the lack of practical pooled steganalyzer, the above embedding strategies are derived from some specific detection analysis in theory. Subsequently, the blind universal pooled steganalysis was designed [13], and the embedding strategy based on uniform payload distribution (UPD) was proposed in [14]. The embedding strategy UPD uniformly distributes payload into all cover images. In embedding strategy UPD, the only requirement is that each cover image's sub-payload cannot exceed its steganographic capacity. Otherwise, the cover image's sub-payload is set as its steganographic capacity. Then recalculate the average sub-payload for the remaining cover images. Based on the larger size and more equilibrated histogram priority rule, a universal embedding strategy for both spatial and JPEG domain was presented [15]. After that, Cogranne et al. obtained the optimal joint function by applying the statistical model for the single image detector's output, and then used it to test several practical embedding strategies [16].

After the existing embedding strategies have been analyzed, we find that most of embedding strategies are derived from specific detection analysis methods, and rarely associated with image features. To tackle with this problem, we propose an embedding strat-

☆ This paper has been recommended for acceptance by Zicheng Liu.
* Corresponding author.
E-mail address: xinliao@hnu.edu.cn (X. Liao).

https://doi.org/10.1016/j.jvcir.2020.102822
1047-3203/

egy on fusing multiple image features in this paper. In this strategy, multiple image features, the typical characteristic parameters of gray level co-occurrence matrix, the image entropy and the shape parameter, are employed to depict image complexity. Then when computing steganographic capacity, we consider not only the above image complexity, but also the number of images in the steganographic system and the number and size of images assigned to steganographer. Finally, the images with the highest capacity yet to be used are iteratively selected to embed payload, and the sub-payload for each selected image is equal to its estimated capacity. Experimental results show that the proposed strategy can obtain better security performance against the blind universal pooled steganalysis.

The rest of this paper is organized as follows. In Section 2, we propose an embedding strategy on fusing multiple features (FMF). And we progressively introduce the proposed strategy in terms of the depiction of image complexity, the estimation of steganographic capacity and payload distribution. After that, we give the corresponding design of our experiments and results in Section 3. Finally, we make a conclusion.

2. Proposed embedding strategy

In this section, a novel embedding strategy FMF is introduced based on multiple features. Firstly, we give the depiction of image complexity by fusing three kinds of image features. Then we present the computing method of steganographic capacity on the basis of some theories. Finally, we describe how to distribute the payload. Fig. 1 depicts the three steps of the embedding strategy FMF. For further details on each step is described as follows.

2.1. The depiction of image complexity

In multiple images steganography, to reduce the overall embedding distortion, steganographers usually keep the correlation among images according to image features, and embed payload into regions with higher complexity.

The image complexity can be described in many ways. We utilize the typical characteristic parameters of gray level co-occurrence matrix, the image entropy and the shape parameter to depict it.

The characteristic parameters: The gray level co-occurrence matrix is a significant method to depict the image texture feature. It describes the spatial distribution of gray value and image complexity. Its mathematical expression is

$$P(i,j,d,\theta) = \{(x,y),(x+d_x,y+d_y)|f(x,y) = i, f(x+d_x,y+d_y) = j\} \quad (1)$$

where $1 \leqslant x \leqslant m, 1 \leqslant y \leqslant n, m$ and n are the total number of pixels in x and y-axis directions, respectively. d_x, d_y denote the position offsets with directionality. θ value determines the direction in which the matrix is generated. Here, we set $d = 1, \theta = 0°$, $45°$, $90°$, $135°$.

In order to precisely describe the image texture feature, many parameters that can represent matrix conditions are derived from the gray level co-occurrence matrix. We select several typical parameters [17].

(1) *Contrast G*: Contrast [18] reflects the clarity of the image, difference in gray between adjacent pixel and the depth of the texture. It has a pivotal impact on the visual effects. High contrast is helpful for image definition and detail. Generally speaking, a high-contrast image is clearer and more eye-catching, and the image's texture complexity is greater. That is to say, contrast is in direct proportion to the image texture complexity $T, T \propto G$. Contrast can be obtained by using

$$G = \sum_{i=1}^{m}\sum_{j=1}^{n}[(i-j)^2 P(i,j,d,\theta)] \quad (2)$$

where G is contrast, the rest of symbols follow the same meaning as Eq. (1).

(2) *Energy J*: Energy [19] is the measure of the stability of the image texture's gray level change, which reflects the image gray level distribution uniformity and texture thickness. Large energy value indicates that the texture is a texture with stable regular variation, that is, the image texture complexity is inversely correlated with energy, $T \propto \frac{1}{J}$. Energy can be formulated as

$$J = \sum_{i=1}^{m}\sum_{j=1}^{n} P^2(i,j,d,\theta) \quad (3)$$

where J is energy, the rest of symbols follow the same meaning as Eq. (1).

(3) *Correlation Cov*: Correlation [20] reflects the consistency of image texture and is an effective indicator to measure the image texture complexity. Correlation can also be used to measure the similarity in the row or column directions of the elements of the gray level co-occurrence matrix. Its value reflects the local correlation of the image. When the correlation is higher, the image texture complexity is lower. Namely, the image texture complexity is inversely proportional to the correlation, $T \propto \frac{1}{Cov}$. Its compute equation is

$$Cov = \sum_{i=1}^{m}\sum_{j=1}^{n} \frac{i \times j \times P(i,j,d,\theta) - u_1 u_2}{d_1^2 d_2^2} \quad (4)$$

where u_1, u_2 are mean, and d_1^2, d_2^2 are variance, i.e.,

$$\begin{aligned} u_1 &= \sum_{i=1}^{m} i \sum_{j=1}^{n} P(i,j,d,\theta) \\ u_2 &= \sum_{j=1}^{n} j \sum_{i=1}^{m} P(i,j,d,\theta) \\ d_1^2 &= \sum_{i=1}^{m} (i-u_1)^2 \sum_{j=1}^{n} P(i,j,d,\theta) \\ d_2^2 &= \sum_{j=1}^{n} (j-u_2)^2 \sum_{i=1}^{m} P(i,j,d,\theta) \end{aligned} \quad (5)$$

Here, we select three typical parameters of gray level co-occurrence matrix to depict the image texture feature. Because the other two parameters except contrast are in inverse proportion

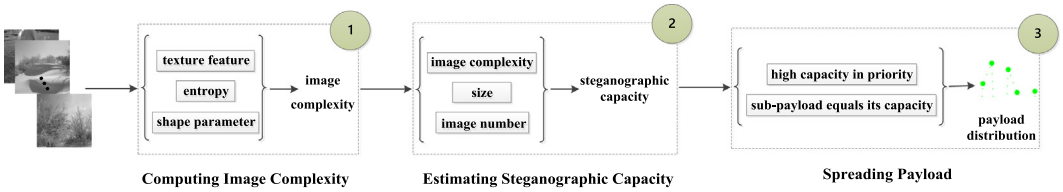

Fig. 1. Overview of the embedding strategy FMF.

to the image texture complexity T, we set the weights of contrast, energy and correlation as 1/3, −1/3, −1/3, respectively. This means that

$$T = \frac{1}{3}G - \frac{1}{3}J - \frac{1}{3}Cov \tag{6}$$

The image entropy: It describes the appearance of each grayscale. Grayscale is the maximum number of different gray levels in an image. The larger the grayscale is, the broader the brightness range of an image is. We can obtain the image entropy using the following equation.

$$H = -\sum_{i=1}^{k} p_i \log_2 p_i \tag{7}$$

where k and p_i are the number of grayscale and appearance probability of grayscale i, respectively, which can be obtained from the gray histogram.

The shape parameter: In [21], the difference of neighboring pixels is regarded as a random variable which follows the generalized gaussian distribution (GGD) whose mean is 0. Because the difference of neighboring pixels contain both horizontal and vertical directions, denoted by x_h and x_v, respectively, x_h and x_v follow the GGD whose mean is 0. Substituting them into the formula of GGD whose mean is 0. Thus

$$\begin{aligned} P_{\alpha_h,\beta_h}(x_h) &= \frac{\beta_h}{2\alpha_h\Gamma(1/\beta_h)} \exp\left(-\left(\frac{|x_h|}{\alpha_h}\right)^{\beta_h}\right) \\ P_{\alpha_v,\beta_v}(x_v) &= \frac{\beta_v}{2\alpha_v\Gamma(1/\beta_v)} \exp\left(-\left(\frac{|x_v|}{\alpha_v}\right)^{\beta_v}\right) \\ \alpha_{h/v} &= \sigma_{h/v}\sqrt{\frac{\Gamma(1/\beta_{h/v})}{\Gamma(3/\beta_{h/v})}}, \quad \sigma_{h/v} > 0 \end{aligned} \tag{8}$$

where $\sigma^2_{h/v}, \alpha_{h/v}$ and $\beta_{h/v}$ denote the variance, scale parameter and shape parameter, respectively, all of them can be obtained by using the fast moment estimation method proposed in [22] (our experiments are also programmed according to this method). And $\Gamma(\bullet)$ is the Gamma function.

Generally, an image with high complexity has a big shape parameter. The image shape parameter is defined as the mean of shape parameter in horizontal and vertical directions, i.e.,

$$\beta = 0.5 \times (\beta_h + \beta_v) \tag{9}$$

where β_h and β_v are the shape parameters in horizontal and vertical directions, respectively, we can obtain them using the fast moment estimation method [22].

In this subsection, we introduce three kinds of image features. All of them are in direct proportion to the image complexity. Thus

$$\Omega = T + H + \beta \tag{10}$$

Normalize the image complexity Ω.

$$\bar{\Omega} = \frac{\Omega - \Omega_{min}}{\Omega_{max} - \Omega_{min}} \tag{11}$$

where Ω_{min} and Ω_{max} denote the minimum and maximum value in Ω, respectively.

We further analyze the size of parameters. Grayscale is the maximum number of different gray levels in an image. For images with gray values ranging from 0 to 255, the value range of H is [0, 8]. Three typical characteristic parameters, G,J and Cov, are obtained by the graycoprops function in Matlab. Their value range is [0, 6], [0, 1] and [-1, 1], respectively. And the value of β is in the range of 0 to 2. Therefore, the value range of the image complexity is $[-\frac{2}{3}, 12]$.

2.2. The estimation of steganographic capacity

In 2007, based on some assumptions and Cachin security theory, Ker defined the security theory of multiple images steganography, and demonstrated the proportional relationship between steganographic capacity and the square root of the number of covers [23]. Here, we consider the number N of images in steganographic system and the number $K \subseteq N$ of images assigned to steganographer. Therefore, we can conclude that $C_k \propto \sqrt{N}$ and $C_k \propto \sqrt{K}$. Later, it was proposed that steganographic capacity should be proportional to the square root of the size of image [24]. Assuming that the size of image is $m_k n_k$, $C_k \propto \sqrt{m_k n_k}$. And steganographers usually embed payload into regions with higher complexity to reduce the overall embedding distortion. So $C_k \propto \bar{\Omega}_k$. Thus we estimate steganographic capacity using the following equation.

$$C_k = \sqrt{N} \times \sqrt{K} \times \sqrt{m_k n_k} \times \bar{\Omega}_k \times \lambda \tag{12}$$

N: It is the number of images in data set used in experiments. When performing experiments, N is set accordingly as the number of images in the data set.

K: It means the number of images assigned to steganographer. In principle, the images in the data set are all available to steganographer. However, we tend to assign subset to each actor according to the needs of experiments, and the subset assigned to steganographer is really available to steganographer. Actually, we don't limit the value of K in this paper. Here, the value of K can be any integer in [2, N] ($K > 1$, because it is in multiple images steganography system).

$m_k n_k$: It denotes the size of image k, i.e., the number of pixels in image k.

$\bar{\Omega}_k : \Omega_k$ represents the image complexity of image k, which is computed by using Eq. (10). And $\bar{\Omega}_k$, the value range is [0, 1], is obtainedafter minimum–maximum normalization of Ω_k (namely Eq. (11)).

λ: On the premise that all secret information can be embedded, λ we estimate is based on our experiences from specific experimental work. We call it the control parameter.

2.3. Spreading payload among multiple images

First, we compute all steganographic capacity $C = \{C_1, C_2, \cdots, C_K\}$ of image subset $I = \{I_1, I_2, \cdots, I_K\}$ assigned to steganographer. As Ref. [10] pointed out steganographer embedded payload into the fewest possible number of covers, we sort images in order of descending capacity. Therefore, we can obtain a sequence of descending capacity $C\prime = \{C_{ind(1)}, C_{ind(2)}, \cdots, C_{ind(K)}\}$. $ind(k)$ is the index of sorted image. Finally, we embed payload into corresponding images according to the order $I_{ind(1)}, I_{ind(2)}, \cdots, I_{ind(K)}$, and the sub-payload for each selected image is equal to its estimated capacity, so as to minimize the number of embedded covers. This means that

$$|m_{ind(k)}| = \begin{cases} C_{ind(k)}, & k \in \{1, 2, \cdots, q^* - 1\} \\ |M| - \sum_{k=1}^{q^*-1} C_{ind(k)}, & k = q^* \\ 0, & k \in \{q^* + 1, q^* + 2, \cdots, K\} \end{cases} \tag{13}$$

where M is a secret information set, and $|M|$ denotes the length of secret information. As we know, the steganographic capacity refers that the maximum number of bits can be embedded in cover under the premise that imperceptibility is satisfied. When embedding payload, we select images with high capacity in priority, and the sub-payload for each selected image is equal to its estimated capac-

ity. Therefore, q^* denotes the fewest number of images, when payload can be embedded thoroughly.

After distributing the payload, we combine with some state-of-the-art embedding algorithms used in single image to complete multiple images steganography.

2.4. Computational complexity analysis

Here, we investigate the computational complexity of the proposed embedding strategy. Suppose we possess K cover images, all of them with the same size of $m \times n$. In this strategy, we first traverse K images to calculate the steganographic capacity of each image based on their image complexity. The computational complexity of the above operations is $O(Kmn)$. Then we sort K images in order of descending capacity. Finally, we allot sub-payload into corresponding images according to this order. And sorting and allotting operations' cost is $O(KlogK)$. So far, if $Kmn > KlogK$, the computational complexity of FMF is $O(Kmn)$. Otherwise, the computational complexity is $O(KlogK)$. Therefore, the multiple images steganographic schemes incorporated with the proposed strategy FMF could be solved in polynomial time.

3. Experimental parts

In this section, we give detailed experimental settings, including embedding strategies, embedding algorithms, pooled steganalysis, etc. Furthermore, detailed experimental steps are also described. And experimental results are shown to demonstrate the effectiveness of proposed embedding strategy FMF.

3.1. Experimental settings

In this subsection, specific experimental settings are presented. To achieve multiple images steganography, we combine the proposed embedding strategy FMF with some state-of-the-art embedding algorithms which are used in single cover image.

Our experiments are tested on 10000 gray level images with the size of 512×512, obtained from BOSSBase v1.01 set [25]. We employ the blind universal pooled steganalysis [13] to estimate the detectability of these steganographic methods. The application scenario of this steganalysis method is that multiple users and each of them transmits multiple images. It aims to identify a guilty actor or actors, who have embedded payload into the selected images. Because it is the most effective when only one user is steganographer, we set a guilty actor in experiments. The embedding strategies involved in experiments include the proposed embedding strategy FMF and the embedding strategy UPD [14]. And the embedding algorithms include the state-of-the-art steganographic algorithms WOW [5], S-UNIWARD [6], HILL [7] and MiPOD [8]. We perform experiments by adopting all pairs of the above embedding strategies and algorithms. Moreover, we must confirm the length of secret information, so as to draw like-for-like comparisons among different pairs of embedding strategies and algorithms. Hence, we will define the total payload as the number of bits per pixel of images for the guilt actor. Here, the mean payload rate is set to 0.1, 0.2, 0.3, 0.4, 0.5 bpp (bits per pixel).

3.2. Experimental steps

In this subsection, we will give specific experimental steps.

Step 1: The number of users is set as 20, and the number of images per user are 100 and 200, respectively. Randomly select a guilty actor, and mark the selected actor. Then the guilty actor embeds payload into the corresponding images, using different pairs of embedding strategies and algorithms.

Step 2: Because the spatial rich model (SRM) [26] is a classical steganalysis method for spatial domain, and can detect the embedding algorithm well, we use it to extract 34671-dimensional features for all images.

Step 3: According to actor, group these extracted features. And use the maximum mean discrepancy (MMD) [27] method to compute the distances between all pairs of users.

Step 4: Use the local outlier factor (LOF) [28] method to calculate the guiltiness of each user. Sort LOF values in descending order. Then we can obtain the LOF value ranking of the guilty actor according to the mark in Step 1.

Repeat the above experimental steps to obtain the average ranking of each user. The higher the average ranking of the guilty actor is, the lower the possibility that the guilty actor is to be detected is, i.e., the more undetectable embedding strategy is.

3.3. Comparison results

In this subsection, comparative experiments are shown to demonstrate the effectiveness of the proposed embedding strategy FMF. Table 1 shows the experimental results under five payloads, combining two embedding strategies FMF, UPD with the embedding algorithm WOW, when the number of actors is 20 and the number of images each actor is 100. To further illustrate the security performance of the proposed strategy FMF clearly, we show the results using figures.

Fig. 2 displays the comparative results. The array of charts varies the embedding algorithm (WOW, S-UNIWARD, HILL and MiPOD). Within each chart, the x-axis denotes the payload in bpp, and the y-axis denotes the average ranking of the guilty actor. Different embedding strategies are denoted by different point types. Observing the results, it can be found that the average ranking of the guilty actor obtained from FMF is higher than that from UPD, under the same number of images and payload. Moreover, with the increase of payload, the performance difference between FMF and UPD is more obvious.

Last, but not least, Fig. 3 provides a useful insight about the proposed strategy FMF. This figure shows the numerical results of payload distribution among 100 guilty actor's images under the proposed embedding strategy at the mean payload rate 0.1 and 0.4 bpp. It is obvious that the numerical results of payload distribution among 100 guilty actor's images is uneven. The proposed strategy FMF spreads payload into as the fewest number of cover images as possible. It also can be observed that the assigned sub-payload for some cover images are zero, and these innocent images can further confuse the detector. Note that the intuitive strategy UPD equally spreads payload for each image, thus we ignore it in this figure.

Table 1
The average ranking of the guilty actor by combining FMF, UPD and WOW, resisting the blind universal pooled steganalysis.

Embedding Strategy	Payload				
	0.1 bpp	0.2 bpp	0.3 bpp	0.4 bpp	0.5 bpp
FMF	12.8	12.9	12.8	12.2	12.2
UPD	12.9	12.9	12.7	11.7	9.5

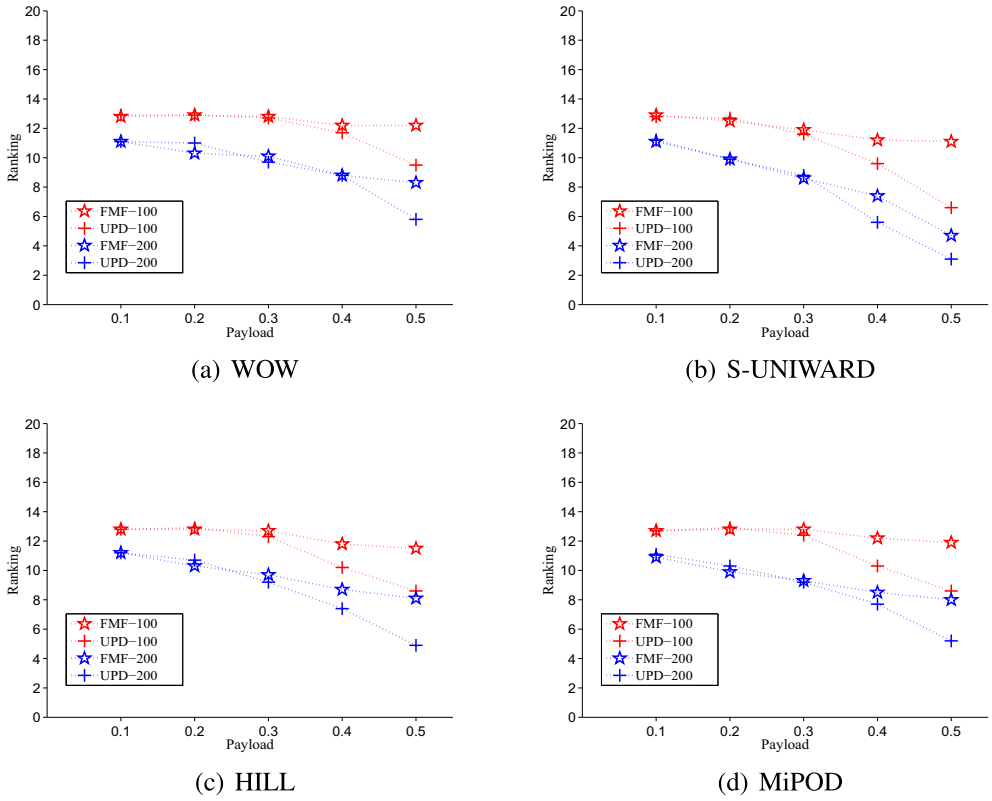

Fig. 2. The comparative results with UPD by combining orderly with WOW (a), S-UNIWARD (b), HILL (c) and MiPOD (d), when the number of actors is 20, and the number of images each actor are 100 (red color) and 200 (blue color), respectively. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

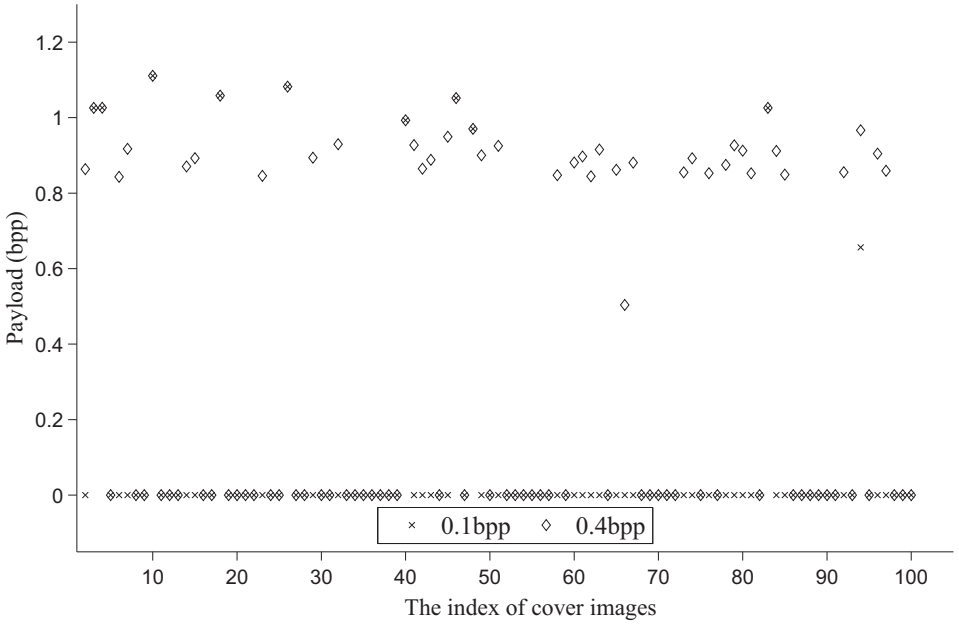

Fig. 3. The numerical results of payload distribution among 100 guilty actor's images under the proposed embedding strategy at the mean payload rate 0.1, 0.4 bpp.

4. Conclusions

An embedding strategy on fusing multiple features is presented in this paper. In the proposed strategy, we utilize multiple features to quantitatively describe image complexity. And then we combine with the new estimation method to estimate steganographic capacity. At last, the performance of the proposed strategy is verified by experiments.

According to the experimental settings, our experiments are tested on gray level images. In fact, color images are more

prevalent on the Internet. Unlike gray level images, color images contain red, green and blue channels. As Ref. [29] pointed out, steganographer exploited inter-channel correlations to allocate payload for performance enhancement. In further work, we will attempt to extend the proposed strategy to color images incorporating with inter-channel correlations.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This work is supported by National Natural Science Foundation of China (Nos. 61972142, 61772191), National Hunan Provincial Natural Science Foundation of China (No. 2020JJ4212), CERNET Innovation Project (No. NGII20180412), Open Project Program of National Laboratory of Pattern Recognition (No. 201900017).

References

[1] R.J. Anderson, F.A.P. Petitcolas, On the limits of steganography, IEEE J. Sel. Areas Commun. 16 (1998) 474–481.
[2] R. Atta, M. Ghanbari, A high payload steganography mechanism based on wavelet packet transformation and neutrosophic set, J. Vis. Commun. Image Represent. 53 (2018) 42–54.
[3] J.H. Zhang, W. Lu, et al., Binary image steganography based on joint distortion measurement, J. Vis. Commun. Image Represent. 58 (2019) 600–605.
[4] X. Liao, Z. Qin, L.P. Ding, Data embedding in digital images using critical functions, Signal Process.: Image Commun. 58 (2017) 146–156.
[5] V. Holub, J. Fridrich, Designing steganographic distortion using directional filters, in: Proceeding of IEEE International Workshop on Information Forensic and Security, 2012, pp. 234–239.
[6] V. Holub, J. Fridrich, T. Denemark, Universal distortion function for steganography in an arbitrary domain, EURASIP J. Informat. Sec. 1 (2014) 1–13.
[7] B. Li, M. Wang, J. Huang, et al., A new cost function for spatial image steganography, in: Proceeding of IEEE International Conference on Image Processing, 2014, pp. 4026–4210.
[8] V. Sedighi, R. Cogranne, J. Fridrich, Contentadaptive steganography by minimizing statistical detectability, IEEE Trans. Inf. Forensics Secur. 11 (2) (2016) 221–234.
[9] T. Filler, J. Judas, J. Fridrich, Minimizing additive distortion in steganography using syndrome-trellis codes, IEEE Trans. Inf. Forensics Secur. 6 (3) (2011) 920–935.
[10] A.D. Ker, "Batch steganography and pooled steganalysis," in Proceeding of International Workshop on Information Hiding, pp. 265–281, 2006.
[11] A.D. Ker, P. Bas, R. Bohme et al., Moving steganography and steganalysis from the laboratory into the real world, in: Proceedings of The First ACM Workshop on Information Hiding and Multimedia Security, 2013, pp. 45–48.
[12] A.D. Ker, Steganographic strategies for a square distortion function, in: Proceeding of International Conference on Security, Forensics, Steganography and Watermarking of Multimedia Contents, 2008, pp. 401–413.
[13] A.D. Ker, T. Pevný, Identifying a steganographer in realistic and heterogeneous data sets, in: Proceeding of International Conference on Media Watermarking, Security, and Forensics, 2012, pp. 1–13.
[14] A.D. Ker, T. Pevný, Batch steganography in the real world, in: Proceeding of ACM Workshop on Multimedia Security, 2012, pp. 1–10.
[15] Z. Zhao, Q. Guan, X. Zhao et al., Universal embedding strategy for batch adaptive steganography in both spatial and JPEG domain, in: Proceeding of IWDW 2016: Digital Forensics and Watermarking, vol. 10082, 2017, pp. 494–505.
[16] R. Cogranne, V. Sedighi, J. Fridrich, Practical strategies for content-adaptive batch steganography and pooled steganalysis, in: Proceeding of IEEE International Conference on Acoustics, Speech and Signal Processing, 2017.
[17] W. Wang, X.J. Wang, et al., The segmentation algorithm based on image complexity, J. Detect. Control 37 (3) (2015) 5–9.
[18] C. Chen, H. Li, Y. Wei, et al., A local contrast method for small infrared target detection, IEEE Trans. Geosci. Remote Sens. 52 (1) (2013) 574–581.
[19] S.G. Chang, B. Yu, M. Vetterli, Adaptive wavelet thresholding for image denoising and compression, IEEE Trans. Image Process. 9 (9) (2000) 1532–1546.
[20] N. Mccormick, J. Lord, Digital image correlation, Mater. Today 13 (12) (2010) 52–54.
[21] Q. Liu, A.H. Sung, B. Ribeiro, et al., Image complexity and feature mining for steganalysis of least significant bit matching steganography, Inf. Sci. 178 (1) (2008) 21–36.
[22] T.Y. Wang, Z.M. Li, A fast moment estimation method of generalized gaussian distribution, J. Eng. Geophys. 3 (2006) 172–176.
[23] A.D. Ker, A capacity result for batch steganography, IEEE Signal Process. Lett. 14 (3) (2007) 525–528.
[24] A.D. Ker, T. Pevný, J. Kovodský, The square root law of steganographic capacity, in: Proceeding of the 10th ACM Workshop on Multimedia and Security, 2008, pp. 107–116.
[25] P. Bas, T. Filler, T. Pevný, Break our steganographic system: the ins and outs of organizing boss, in: Proceeding of International Conference on Information Hiding, 2011, pp. 59–70.
[26] J. Fridrich, J. Kodovský, Rich models for steganalysis of digital images, IEEE Trans. Inf. Forensics Secur. 7 (3) (2011) 868–882.
[27] A. Gretton, K.M. Borgwardt and M.J. Rasch et al., "A kernel method for the two-sample problem," Advances in Neural Information Processing Systems, pp. 513–520, 2007.
[28] M.M. Breunig, H.P. Kriegel, R.T. Ng et al., LOF: identifying density-based local outliers, in: Proceeding of ACM SIGMOD International Conference on Management of Data, 2000, pp. 93–104.
[29] X. Liao, Y. Yu, B. Li, et al., A new payload partition strategy in color image steganography, IEEE Trans. Circuits Syst. Video Technol. 30 (3) (2020) 685–696.