TWO EMBEDDING STRATEGIES FOR PAYLOAD DISTRIBUTION IN MULTIPLE IMAGES STEGANOGRAPHY

Xin Liao, Jiaojiao Yin

College of Computer Science and Electronic Engineering, Hunan University, China.

ABSTRACT

With the coming of the era of big data, digital images are growing explosively on the Internet. Traditional steganography which embeds payload into one cover image is facing new challenges. In fact, a steganographer could utilize multiple images to embed payload simultaneously. How to fully exploit image features to allocate payload for performance enhancement is still an open issue. In this paper, we first establish a framework to formulate data embedding in multiple images. Two new embedding strategies based on image texture complexity and distortion distribution are designed for payload distribution, which can be implemented together with these state-of-art single image steganographic algorithms. Experimental results demonstrate that two proposed embedding strategies in multiple images steganography could obtain better statistical undetectability.

Index Terms— Image steganography, multiple images, embedding payload distribution, pooled steganalysis

1. MOTIVATIONS

Steganography is a technique which makes use of the redundancy of digital medias to conceal secret information, so as to achieve covert communication [1]. In recent years, many effective image steganographic methods are proposed, including HUGO [2], WOW [3], S-UNIWARD [4], HILL [5] and so on. Note that these methods focus on embedding payload in one cover image. However, the explosion of large-scale images has posted new challenges. It is more reasonable in practical application that a steganographer simultaneously embeds payload into multiple images.

How to spread payload among multiple images is a challenging problem today [6]. Some embedding strategies are proposed to realize multiple images steganography. Ker first postulated it and utilized game theory to analyze, in which the embedding payloads are spread based on the opponent's pooling evidence [7, 8]. Later, according to the principle that the statistical detectability of payload is proportional to the square of embedding changes, the embedding payload is likely to extremely concentrate in as few cover images as possible, or the opposite that the payload is spread as thinly as possible [9]. Due to the lack of practical pooled steganalyzer, the above theoretical results could not be validated. The blind universal pooled steganalyzer was proposed [10], and some data embedding strategies and corresponding experiments are designed for massive JPEG images [11]. Cogranne et al. [12] derived an optimal pooling function as a likelihood ratio in the form of a matched filter by adopting a statistical model for the output of the single-image detector, and then tested several productive embedding strategies.

In this paper, on the assumption that the receiver is informed of the embedding strategy, we attempt to present a framework for multiple images steganography. We design two new embedding strategies based on image texture complexity and distortion distribution respectively. The former one embeds payload into fewer number of cover images, and the sub-payload for each cover image is equal to its estimated capacity. A new estimation method of cover image capacity is presented by using image entropy. In the latter, we allocate embedding payload according to the distribution of embedding distortion values. Two proposed strategies could be incorporated with these state-of-the-art signal image steganographic algorithms. Experimental results show that two proposed embedding strategies could achieve better performances against the modern universal pooled steganalysis.

The rest of the paper is organized as follows. We formulate the problem in section 2. In section 3, we propose two embedding strategies and describe an intuitive embedding strategy. The detailed experiments and comparative results are given in section 4. Finally, the conclusions are made.

2. PROBLEM FORMULATION

A steganographer could spread payload among multiple images by the embedding strategy, and it is more suitable to the practical application scenario. Given a cover image set $X = \{x_1, x_2, \cdots, x_n\}$ with capacities $(c_1, c_2, \cdots, c_n)$, where n is the number of cover images and the capacity c_i is the maximum length of payload which can be embedded into cover image x_i. The total capacity of all cover images can be expressed as $\sum_{i=1}^{n} c_i$. M is a given secret information set, and

This work is supported by National Natural Science Foundation of China (Nos. 61402162, 61772191, 61472131), Hunan Provincial Natural Science Foundation of China (No. 2017JJ3040).

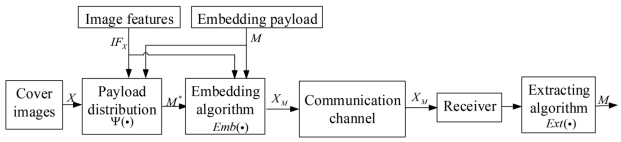


Fig. 1. The framework of multiple images steganography.

$|M|$ denotes the length of secret information. Generally, we suppose $\sum_{i=1}^{n} c_i \gg |M|$, i.e., the total capacity of cover images is more than the length of embedding payload.

Let $\Psi(\bullet)$ represent a strategy for distributing payload. The payload distribution associates with the image features IF_X of cover set X, and the payload distribution is shown as below.

$$\begin{cases} M^* = \Psi(M, X, IF_X) = \{m_1, m_2, \cdots, m_n\} \\ |M| = \sum_{i=1}^{n} |m_i| \end{cases} \tag{1}$$

where M^* is the distributed sub-payload set, and m_i is the corresponding sub-payload of cover image x_i.

The steganographer could embed sub-payloads into the corresponding cover images by different embedding algorithms, because the embedding operators are independent for cover images. The stego image set X_M can be obtained by

$$\begin{cases} X_M = (x_{1,m_1}, x_{2,m_2}, \cdots, x_{n,m_n}) \\ x_{i,m_i} = Emb(x_i, m_i) \end{cases} \tag{2}$$

where x_{i,m_i} represents the stego image by embedding the sub-payload m_i into the cover image x_i, and $Emb(\bullet)$ represents the embedding algorithm.

The stego image set X_M is transmitted via communication channel. If $|m_i| = 0$, it means the cover image x_i that are not embedded, i.e., $x_i = x_{i,m_i}$. The embedding strategy is shared between the steganographer and receiver. After acquiring the stego image set, the receiver could use the sharing information to get the payload distribution, and then extract each sub-payload by $m_i = Ext(x_{i,m_i})$. The payload is obtained by combining all sub-payloads.

Therefore, as shown in Fig. 1, the multiple images steganography can be formulated by cover image set X, payload M, payload distribution strategy $\Psi(\bullet)$, embedding algorithm $Emb(\bullet)$ and extracting algorithm $Ext(\bullet)$. It is required to meet the following challenges:

Concealment: The images which are transmitted via the internet may include cover and stego images. It is difficult for attackers to differentiate stego images from innocent images.

Diversity: The embedding and extracting operations of images are independent. The embedding and extracting algorithms could be different for each image.

Multisource: Cover images could be in various formats, and they can be acquired by different ways.

3. TWO PROPOSED EMBEDDING STRATEGIES FOR MULTIPLE IMAGES STEGANOGRAPHY

In this section, we propose two embedding strategies based on image texture complexity (ES-ITC) and distortion distribution (ES-DD) to realize embedding payload distribution. We also introduce an intuitive embedding strategy based on uniform payload distribution (ES-UPD) which will be compared with the proposed strategies in the experiments. These embedding strategies can be combined with these existing embedding algorithms which focus on embedding in one cover image, so as to achieve multiple images steganography.

3.1. The Proposed Embedding Strategy Based on Image Texture Complexity

In the embedding strategy based on image texture complexity (ES-ITC), we attempt to embed payload into fewer number of cover images. We iteratively select the cover image with the highest capacity to embed and allocate the sub-payload which is equal to the maximum capacity for each image.

The maximum capacity depends on image content [11]. For images with the same size, the more complex the image content is, the higher capacity the image has. In addition, when images possess the same content, the larger image has the higher capacity. Therefore, we estimate the capacity c_i of cover image x_i by its size and image entropy which could represent image texture complexity well. Furthermore, we firstly carry out a high-pass filter F to cover image x_i in the image set X to sharpen image texture, so that the image texture of the filtered image can be captured more precisely.

Assuming that the size of image x_i is $r_i \times s_i$, the gray co-occurrence matrix is

$$\begin{aligned} &P(u, v, d, \theta) = \\ &\quad \xi\{(a_1, b_1), (a_2, b_2) | x_i(a_1, b_1) = u, x_i(a_2, b_2) = v, \\ &\quad |(a_1, b_1) - (a_2, b_2)| = d, < (a_1, b_1), (a_2, b_2) > = \theta \} \end{aligned} \tag{3}$$

where $1 \le a_1, a_2 \le r_i$, $1 \le b_1, b_2 \le s_i$, $\xi\{W\}$ represents the number of elements in set W, $x_i(a_1, b_1)$, $x_i(a_2, b_2)$ are two pixels in the positions (a_1, b_1), (a_2, b_2) of cover image x_i, and u, v are the corresponding pixel values. d is the distance between (a_1, b_1) and (a_2, b_2), and θ is the angle between the two points and abscissa axis. The co-occurrence matrix $P(u, v, d, \theta)$ is applied to count the number of times that the pixel values u and v appear simultaneously.

The entropy h_i of image x_i is computed on the basis of the above gray co-occurrence matrix $P(u, v, d, \theta)$

$$h_i = -\sum_{u} \sum_{v} P(u, v, d, \theta) \log_2 P(u, v, d, \theta) \tag{4}$$

We set $d = 1$, $\theta = 0°, 45°, 90°, 135°$ to get four image entropies h_i and compute the average $\bar{h_i}$ for image x_i.

Therefore, the image entropy of the cover image set X is $H = \{\bar{h_1}, \bar{h_2}, \cdots, \bar{h_n}\}$. Finally we calculate the capacity c_i

of image x_i by using the below equation.

$$c_i = \frac{r_i s_i(\bar{h}_i - \bar{h}_{min})}{\bar{h}_{max} - \bar{h}_{min}} \tag{5}$$

where $\bar{h}_{min}$ and $\bar{h}_{max}$ denote the minimum and maximum value in H, respectively.

Suppose all cover images are sorted by their capacities $c_1 \geq c_2 \geq \cdots \geq c_n$. We embed the payload into the images in front of the order, and the total capacity of these images should be not less than the length of embedding payload. The sub-payload of each image is equal to its estimated capacity. Therefore, the payload distribution is shown as below.

$$|m_i| = \begin{cases} c_i & i = 1, 2, \cdots, p-1 \\ |M| - \sum_{i=1}^{p-1} |m_i| & i = p \\ 0 & i = p+1, p+2, \cdots, n \end{cases} \tag{6}$$

where p represents the fewest number of cover images satisfying the payload requirement $\sum_{i=1}^{p} c_i \geq |M|$.

We could use these state-of-art single image steganographic algorithms to embed the sub-payload into each selected image, so as to complete multiple images steganography.

3.2. The Proposed Embedding Strategy Based on Distortion Distribution

The embedding strategy ES-DD mainly distributes the payload depending on the distribution of embedding distortion values. We calculate the distortion values ρ_i of cover image x_i by applying the cost function from the existing steganographic schemes. For example, the distortion values ρ_i can be computed by adopting the cost function in HILL [5].

All pixels in the cover image set X are sorted in an ascending order based on their distortion values. We focus on the first $|M|$ pixels in the ascending order, where $|M|$ is the length of embedding payload. The payload distribution is determined by the distribution of distortion values in the first $|M|$ pixels. We count the number n_i of pixels for the image x_i, and the length of sub-payload m_i will be equal to n_i.

3.3. The Intuitive Embedding Strategy Based on uniform payload distribution

In the intuitive embedding strategy based on uniform payload distribution (ES-UPD), the embedding payload is distributed uniformly into all cover images. Thus, the length of sub-payload for each image can be computed by $|m_i| = |M|/n$.

The only requirement is that the sub-payload m_i cannot exceed the capacity c_i of its corresponding image, i.e., $|m_i| \leq c_i$. Otherwise, we set $|m_i| = c_i$ and recalculate the average amount of sub-payload for the remaining images.

4. EXPERIMENTAL RESULTS

In this section, some comparative experiments are presented to prove the effectiveness of two proposed embedding strategies ES-ITC and ES-DD. Section 4.1 gives the detailed experimental procedures including the parameter setting, the embedding processes and pooled steganalysis. The experimental results and analyses are shown in section 4.2.

4.1. Experimental Procedures

In our experiments, the embedding algorithms WOW [3] and HILL [5] are combined with the proposed embedding strategies ES-ITC and ES-DD. The testing images are 10000 grayscale images with the size of 512×512 from the BOSSBase set [13]. We adopt the blind universal pooled steganalysis [11] for evaluating the security and undetectability of these steganographic methods. Suppose that there are some actors and each of them transmits multiple images. All images are detected by the steganalyst, and he knows the images that each actor sent. The aim of the pooled steganalysis is to identify a guilty actor or actors, who have executed steganographic operations on the corresponding images. The LOF method [14] is used to measure the possibility that an actor is guilty. The evaluation criterion is the guilty actor ranking. The better the guilty actor ranking, the higher possibility that the guilty actor is to be identified, i.e., the lower security performance of the steganographic methods.

We vary the number of actors $n_a \in \{10, 20, 30, 40, 50\}$. For each n_a, divide the 10000 images into n_a groups, each of which is assigned to one of the actors randomly. In the experiments, the number of guilty actors is set as 1, because the performance of the universal pooled steganalyzer is best in this case [10]. We carry out the experiments by adopting all pairs of the embedding strategies ES-ITC, ES-DD, ES-UPD and the embedding algorithms WOW, HILL for different numbers of actors. The payloads are 0.1, 0.2, 0.3, 0.4, 0.5 bpp (bits per pixel). The detailed procedures are as below.

1) Select the number n_a of actors, and randomly divide the 10000 images into n_a groups. The number of cover images per actor is $10000/n_a$.

2) Randomly assign and record a guilty actor from n_a actors. The guilty actor embeds payload into cover images by using a pair of the embedding strategy and algorithm.

3) Since SRM steganalytic method [15] could detect the tested embedding algorithms precisely, we use it to extract 34671-dimensional features for all images.

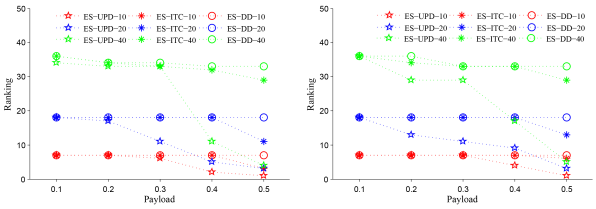
4) Group the extracted features by actor, and calculate the distances between all pairs of two actors based on their features using the maximum mean discrepancy [16].

5) We compute the guiltiness of each actor by using LOF method. According to the record in step 2, the guilty actor's ranking is obtained.

Repeat the above experiment ten times to average the LOF

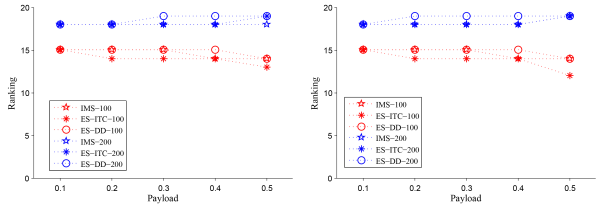
Table 1. Experimental results by combining ES-ITC with WOW against the universal pooled steganalysis. The underline results are the average LOF values of the guilty actor.

Ranking	0.1 bpp	0.2 bpp	0.3 bpp	0.4 bpp	0.5 bpp
1	1.2399	1.2398	1.2380	1.2586	1.2340
2	1.1261	1.1339	1.2128	1.2324	1.2312
3	1.1183	1.1183	1.1904	1.2299	1.2056
4	1.1183	1.1183	1.1166	1.1116	1.0874
5	1.0783	1.1170	1.1166	1.1116	1.0874
6	1.0526	1.0527	1.0512	1.0464	1.0563
7	1.0222	1.0161	0.9939	1.0080	1.0484
8	0.9781	0.9780	0.9623	0.9444	0.9307
9	0.9501	0.9501	0.9487	0.9340	0.9137
10	0.8610	0.8609	0.8597	0.8558	0.8372



(a) (b)

Fig. 2. Comparisons of ES-ITC, ES-DD, ES-UPD with WOW (a), HILL(b) when the numbers of actors are 10 (red color), 20 (blue color) and 40 (green color).



(a) (b)

Fig. 3. Comparisons of ES-ITC, ES-DD, IMS with WOW (a), HILL (b) when the number of actors is 20. The number of cover images per actor is 100 (red color), 200 (blue color).

values of all actors. We obtain the average ranking of the guilty actor over 10 random assignations of images to actors.

4.2. Comparison Results

This section mainly shows the comparison experimental results to testify the security performances of ES-ITC, ES-DD.

The security performances are compared based on the guilty actor rankings. Take Table 1 as an example. The number n_a of actors is 10, and the LOF values of 10 actors are shown under the five payloads by combining the embedding strategy ES-ITC and the embedding algorithms WOW. The LOF values of the actors with the same payload are sorted in a descending order. The underline results are the LOF values of the guilty actor (the steganographer). The guilty actor rankings are 7, 7, 7, 7, 3 in this case.

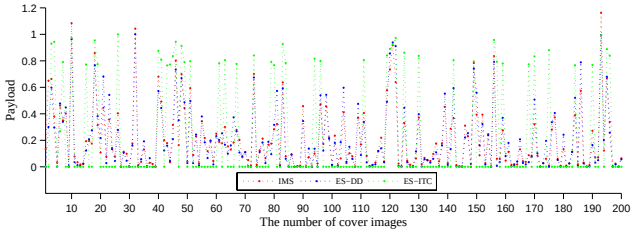


Fig. 4. The numerical distribution of payload among 200 images for these embedding strategies.

More scenarios with different numbers of actors are taken into account, $n_a = 10, 20, 30, 40, 50$. Due to space limitations, we only include the most interesting results regarding the proposed strategies. Fig. 2(a) and Fig. 2(b) show the comparison results when we combine ES-ITC, ES-DD, ES-UPD with WOW, HILL respectively. From the figures, it can be found that for the same number of actors and payload, the guilty actor rankings obtained by ES-ITC, ES-DD are worse than that of ES-UPD. The guilty actor is more likely to be identified by using ES-UPD. Thus, two proposed embedding strategies ES-ITC, ES-DD perform better than the intuitive strategy ES-UPD against the universal pooled steganalysis.

Furthermore, we compare ES-ITC, ES-DD with the existing embedding strategy IMS [12]. Fig. 3 indicates the security performance of ES-DD is similar to that of IMS, and the performance of ES-ITC is somewhat worse than that of IMS. Fig. 4 shows the numerical distribution of payload among 200 cover images for these embedding strategies when the payload is 0.2 bpp. ES-ITC tends to embed payload into fewer textured images, and some other images are not concealed. ES-DD is similar to IMS, and both of them are different from the uniform intuitive payload distribution. Similar results have been observed for other cases.

5. CONCLUSIONS

In this paper, we focus on investigating the embedding payload distribution in multiple images steganography. We briefly present a framework for data embedding in multiple images. Two new embedding strategies based on image texture complexity and distortion distribution are proposed for payload distribution. Experimental results show that the proposed embedding strategies achieve better performances on resisting the modern universal pooled steganalysis.

We believe that multiple images steganography is of significance to both theoretical approaches and practical implementations. A lot of further works need to be done in this direction. Some effective embedding strategies DeLS, DiLS [12] should be investigated with these modern embedding algorithms, such as MVGG [17], MiPOD [18]. The new pooled steganalysis based on the sequential [19] should also be used to evaluate the security and undetectability.

6. REFERENCES

[1] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," *IEEE Journal of Selected Areas in Communication*, vol. 16, pp. 474-481, 1998.

[2] T. Pevný, P. Bas and T. Filler, "Using high-dimensional image models to perform highly undetectable steganography," *Proceeding of International Workshop on Information Hiding*, pp. 161-177, 2010.

[3] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," *Proceeding of IEEE International Workshop on Information Forensic and Security*, pp. 234-239, 2012.

[4] V. Holub, J. Fridrich and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," *EURASIP Journal on Information Security*, vol. 1, pp. 1-13, 2014.

[5] B. Li, M. Wang and J. Huang et al., "A new cost function for spatial image steganography," *Proceeding of IEEE International Conference on Image Processing*, pp. 4026-4210, 2014.

[6] A. D. Ker, P. Bas and R. Böhme 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*, pp. 45-48, 2013.

[7] A. D. Ker, "Batch steganography and pooled steganalysis," in *Proceeding of International Workshop on Information Hiding*, pp. 265-281, 2006.

[8] A. D. Ker, "Batch steganography and the threshold game," *Proceeding of International Conference on Security, Steganography and Watermarking of Multimedia Contents*, pp. 401-413, 2007.

[9] A. D. Ker, "Steganographic strategies for a square distortion function," *Proceeding of International Conference on Security, Forensics, Steganography and Watermarking of Multimedia Contents*, pp. 401-413, 2008.

[10] A. D. Ker and T. Pevný, "Identifying a steganographer in realistic and heterogeneous data sets," *Proceeding of International Conference on Media Watermarking, Security, and Forensics*, pp. 1-13, 2012.

[11] A. D. Ker and T. Pevný, "Batch steganography in the real world," *Proceeding of ACM Workshop on Multimedia Security*, pp. 1-10, 2012.

[12] R. Cogranne, V. Sedighi and J. Fridrich, "Practical strategies for content-adaptive batch steganography and pooled steganalysis," *Proceeding of IEEE International Conference on Acoustics, Speech and Signal Processing*, 2017.

[13] P. Bas, T. Filler and T. Pevný, "Break our steganographic system – the ins and outs of organizing boss," *Proceeding of International conference on Information hiding*, pp. 59-70, 2011.

[14] M. M. Breunig, H. P. Kriegel and R. T. Ng et al., "LOF: identifying density-based local outliers," *Proceeding of ACM SIGMOD International Conference on Management of Data*, pp. 93-104, 2000.

[15] J. Fridrich and J. Kodovský, "Rich models for steganalysis of digital images," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 868-882, 2011.

[16] 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.

[17] V. Sedighi, J. Fridrich and R. Cogranne, "Content-adaptive pentary steganography using the multivariate generalized Gaussian cover model," *Proceedings of SPIE, Media Watermarking, Security, and Forensics*, pp. 0H01-0H13, 2015.

[18] 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.

[19] R. Cogranne, "A sequential method for online steganalysis," *IEEE International Workshop on Information Forensics and Security*, 2016.