symmetry

MDPI

Article

Multisource Data Hiding in Digital Images

Zichi Wang [1,2]

[1] School of Communication and Information Engineering, Shanghai University, Shanghai 200444, China; wangzichi@shu.edu.cn
[2] Guangxi Key Lab of Multi-Source Information Mining & Security, Guangxi Normal University, Guilin 541004, China

Abstract: In this paper, we propose a new data-hiding framework: multisource data hiding, in which multiple senders (multiple sources) are able to transmit different secret data to a receiver via the same cover image symmetrically. We propose two multisource data-hiding schemes, i.e., separable and anonymous, according to different applications. In the separable scheme, the receiver can extract the secret data transmitted by all senders using the symmetrical data-hiding key. A sender is unable to know the content of the secret data that is not transmitted by them (non-source sender). In the anonymous scheme, it is unnecessary to extract all secret data on the receiver side. The content extracted by the receiver is a co-determined result of the secret data transmitted by all senders. Details of the secret data are unknown to the receiver and the non-source senders. In addition, the two proposed schemes achieve multisource data hiding without decreasing the undetectability of data hiding.

Keywords: data hiding; multisource; digital image

Citation: Wang, Z. Multisource Data Hiding in Digital Images. *Symmetry* **2022**, *14*, 890. https://doi.org/10.3390/sym14050890

Academic Editors: Paolo Emilio Ricci and Jeng-Shyang Pan

Received: 11 March 2022
Accepted: 25 April 2022
Published: 27 April 2022

1. Introduction

The technology of data hiding has been well developed in recent years [1], in which secret data can be embedded into a given cover media without causing serious distortion. In the past decades, digital images have been widely transmitted over social networks, e.g., Twitter, Facebook(Meta), and WeChat, and have become the most popular media used for data hiding. Currently, data-hiding methods are designed with a single source: secret data are transmitted by one sender. In this paper, we aim to achieve data hiding with multiple sources: multiple senders transmit different secret data to a receiver using the same image.

Modern data hiding aims to minimize the distortion on a given cover image, which is caused by the modification operation of embedding. To achieve minimal distortion, a user-defined distortion function [2] is designed to assign an embedding cost for each cover element. The obtained embedding costs are able to quantify the distortion caused by modification. After that, secret data are embedded into a given cover image with minimal theoretical distortion using a near-optimal steganographic coding, e.g., STC (syndrome trellis coding) [3] and SPC (steganographic polar codes) [4]. A mass of distortion functions have been developed for digital images in the literature, e.g., HILL (high-pass, low-pass, and low-pass) [5], MiPOD (minimizing the power of optimal detector) [6], and UT-GAN (ternary embedding U-Net with generative adversarial networks) [7].

In the existing data-hiding framework, as shown in Figure 1a, a sender (single source) embeds secret data into a given cover media. The obtained stego media are then transmitted through public channels without drawing suspicion. In some situations, e.g., military intelligence collection, multiple spies (the senders) intend to transmit different intelligence (secret data) to their commander (the receiver). In addition, the media contain multiple secret data that should be sent only once to guarantee satisfactory security and efficiency. In this situation, the intelligence should be embedded into the same given media and then sent to the commander; therefore, multisource data-hiding is desirable, as shown in Figure 1b.

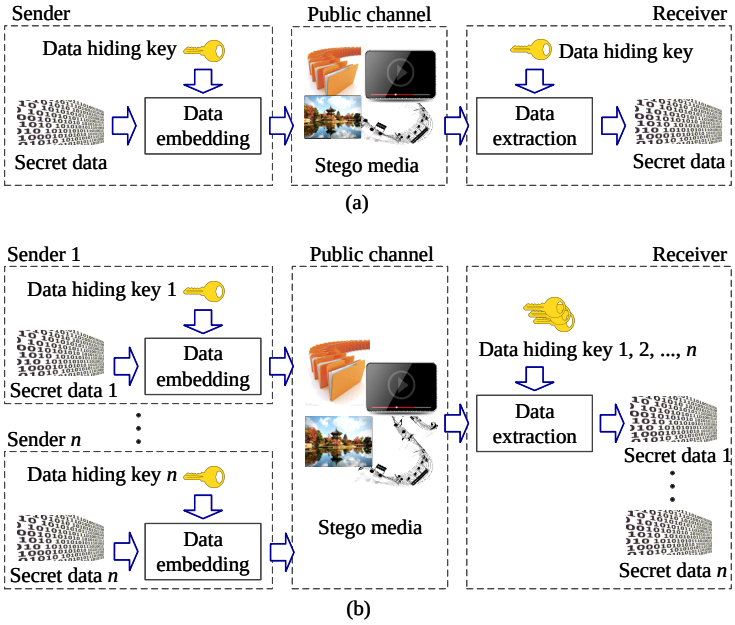

Figure 1. Ideas of (**a**) single source and (**b**) multisource data hiding.

In this paper, we propose two schemes to achieve multisource data hiding in separable and anonymous manners, respectively. In the separable scheme, the receiver can extract the secret data transmitted by all senders using the symmetrical data-hiding key. On the other hand, a sender is unable to discover the content of the secret data that is not transmitted by them (non-source sender). In the anonymous scheme, the content extracted by the receiver is a co-determined result of all secret data instead of the details. Details of the secret data are unknown to the receiver and the non-source senders. To achieve the separable scheme, non-overlapping locations for embedding are determined for different senders. For the anonymous scheme, data embedding is executed in sequence, and data extraction is executed after the last embedding operation. More details are presented in Section 3. The novelty and contributions of this paper are summarized as follows:

(1) We propose a new concept called multisource data hiding, which is a new form in the field of data hiding. It is an extension of existing data hiding instead of an application;
(2) We propose two schemes to achieve multisource data hiding to fit different scenarios by improving the data-hiding coding, which are enriched versions of the existing data-hiding framework.
(3) The proposed two schemes achieve new functions (multisource data hiding) with the same rate-distortion performance. It is verified by experiments that our schemes have not decreased the undetectability of existing data hiding.

2. Related Work

In this section, we introduce some related work, including modern data hiding and steganalytic methods for digital images.

2.1. Modern Data Hiding

Modern data hiding aims to minimize the distortion on a given cover image, which is caused by the modification during the embedding process. The embedding distortion can be measured by a user-defined distortion function, e.g., HUGO (highly undetectable stego) [8], WOW (wavelet-obtained weights) [9], SUNIWARD (spatial universal wavelet relative distortion) [10], HILL [5], MiPOD [6], and UT-GAN [7]. The distortion function is used to assign an embedding cost for each cover element. With assigned embedding costs $\boldsymbol{\rho} = [\rho(1), \rho(2), \ldots, \rho(k)]^{\mathrm{T}}$, secret data can be embedded into a given cover sequence

$\mathbf{c} = [c(1), c(2), \ldots, c(k)]^{\mathrm{T}} \in \{0,1\}^k$. Then, the minimal embedding distortion theoretically with capacity L (bits) is

$$D = \sum_{i=1}^{k} p(i)\rho(i) \tag{1}$$

where

$$p(i) = \frac{e^{-\lambda\rho(i)}}{1 + e^{-\lambda\rho(i)}} \tag{2}$$

is the probability for modifying $c(i)$, and $\lambda > 0$ is used to make information entropy of the modification probabilities equal to L (the capacity), $L < k$, as shown in Equation (3).

$$-\sum_{i=1}^{k}\{p(i)log_2 p(i) + [1 - p(i)]log_2[1 - p(i)]\} = L \tag{3}$$

With the distortion minimization framework, the improvements can be achieved by the embedding costs $\boldsymbol{\rho}$. At present, the embedding costs can be obtained by designing the distortion function, e.g., HILL, MiPOD, as introduced above, or improving the designed distortion function, e.g., direction aggregation strategy [11], block artifact compensation [12], reference construction [13], and adversarial embedding [14]. With the given embedding costs, minimal distortion can be approximated by practical embedding with STC coding, in which secret bits $\mathbf{m} = [m(1), m(2), \ldots, m(L)]^{\mathrm{T}} \in \{0,1\}^L$ can be embedded into $\mathbf{c}$ by modifying cover elements to fit Equation (4).

$$\mathbf{Hs} = \mathbf{m} \tag{4}$$

where $\mathbf{s}$ is the corresponding stego sequence after embedding, $\mathbf{H} \in \{0,1\}^{L\times k}$ is a low-density parity-check matrix depending on the embedding efficiency and payload. It is clear that $\mathbf{m}$ can be directly extracted by the matrix computation in Equation (4). Meanwhile, distortion D caused by modification can be minimized with the distortion function.

In Section 3, we use the STC-based framework to achieve two multisource data-hiding schemes, which is a symmetry work of previous work: multichannel data hiding [15]. In this work, there are multiple senders and one receiver (multiple senders transmit different secret data to a receiver via the same cover image). While in [15], there is one sender and multiple receivers (a sender transmits different secret data to multiple receivers via the same cover image). The two frameworks are achieved using different strategies and used for different scenarios.

2.2. Steganalysis for Digital Images

As the adversarial technique of data hiding, modern steganalysis for digital images can be classified into two categories: handcrafted feature-based steganalysis and deep-learning-based steganalysis.

In handcrafted feature-based steganalysis [16], a large number of methods have been proposed to extract features of digital images [17–20]. With the steganalytic feature sets, the ensemble classifier [21] is popularly used to evaluate the feature property. The ensemble classifier consists of many FLD (Fisher linear discriminant)-based sub-learners with low complexity. The aggregation of decisions made by all FLD learners is used as the final decision of the ensemble classifier.

In deep-learning-based steganalysis, the phases of feature extraction and image classification are joined using a CNN (convolutional neural network) [22–24]. In [22], the basic high-pass filters defined in SRM are employed to initialize the weights in the first layer of the CNN. Moreover, a linear unit with a truncated threshold is improved as the activation function of the steganalytic network. In [23], the popular residual network is firstly used for steganalysis, which minimizes the utilization of external elements enforced by heuristics. The method in [24] fully employed the embedding probability of data hiding. In

Section 4, some of the above steganalytic tools are employed to examine the undetectability of data hiding.

3. Proposed Data-Hiding Schemes

In this paper, we focus on multisource data hiding for the applications of multiple senders. Based on the STC framework, two schemes are designed to achieve multisource data hiding in separable and anonymous manners, respectively, without decreasing the undetectability of data hiding.

3.1. Separable Multisource Data Hiding

In the situations such as military intelligence collection, multiple spies (the senders) intend to transmit different intelligence (secret data) to their commander (the receiver). The image containing multiple secret data should be sent only once to guarantee satisfactory security and efficiency. To this end, the multiple pieces of intelligence should be embedded into the same cover image and then sent to the commander; therefore, separable multisource data hiding is desirable.

The procedure of the proposed separable multisource data-hiding scheme is shown in Figure 2. For n senders, the i-th sender can transmit the i-th secret data $\mathbf{m}_i$ to the receiver using the i-th data-hiding key K_i, but is unable to know the content of other parts of secret data without the symmetrical (correct) data-hiding key, $i \in \{1, 2, \ldots, n\}$.

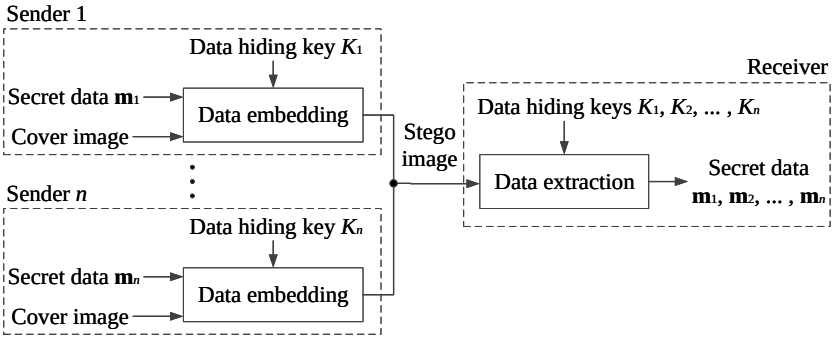

Figure 2. Architecture of separable multisource data hiding.

In a modern data-hiding framework (one sender), secret bits $\mathbf{m} = [m(1), m(2), \ldots, m(L)]^{\mathrm{T}} \in \{0,1\}^L$ are embedded into a given cover sequence $\mathbf{c} = [c(1), c(2), \ldots, c(k)]^{\mathrm{T}} \in \{0,1\}^k$ by modifying its elements to meet Equation (4). In digital images, LSB (least significant bits) of the pixels are used as the cover elements. To achieve separable multisource data hiding, non-overlapping locations used for embedding should be determined for different senders. The cover sequence $\mathbf{c}$ with k elements $\{c(1), c(2), \ldots, c(k)\}$ are divided into n subsequences $\{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n\}$, where $\mathbf{c}_i = [c_i(1), c_i(2), \ldots, c_i(\omega)]$, $\omega = \lfloor k/n \rfloor$. To guarantee that the locations of the elements in the n subsequences are non-overlapping, $c_i(j) = c(\omega \times (i-1) + j)$, $j \in \{1, 2, \ldots, \omega\}$. Then, the n subsequences $\{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n\}$ are correspondingly assigned to the n senders for data embedding. Before embedding, α elements ($1 \leq \alpha < \omega$) in each subsequence $\mathbf{c}_i$ are removed to obtain $\hat{\mathbf{c}}_i$ using the corresponding data-hiding key K_i. That means the i-th sender embeds the i-th secret bits $\mathbf{m}_i$ into $\hat{\mathbf{c}}_i$, where $\mathbf{m}_i = [m_i(1), m_i(2), \ldots, m_i(L_i)]^{\mathrm{T}} \in \{0,1\}^{L_i}$, $L_1 + L_2 + \ldots + L_n = L$. Thus, there are C_ω^α possibilities to obtain $\hat{\mathbf{c}}_i$; "C" is the combination operation in mathematics. Satisfactory security on secret data can be achieved since the number of the possibilities is huge. For example, there are 2.74×10^{33} possible $\hat{\mathbf{c}}_i$ when $\alpha = 10$ and $\omega = 10000$, and the number of pixels in an image is much larger than 10,000 (there are 262,144 pixels in an image sized 512×512). As a result, the embedded secret bits cannot be extracted without the corresponding data-hiding key, since the subsequence $\hat{\mathbf{c}}_i$ after removing is unknown.

During embedding, the i-th sender modifies $\hat{\mathbf{c}}_i$ to obtain $\hat{\mathbf{s}}_i$, which meets

$$\hat{\mathbf{H}}\hat{\mathbf{s}}_i = \mathbf{m}_i \tag{5}$$

where $\hat{\mathbf{H}} \in \{0,1\}^{L_i \times (\omega-\alpha)}$. In this way, the i-th secret bits $\mathbf{m}_i$ can be embedded into $\hat{\mathbf{c}}_i$. On the side of receiver, all the secret bits $\{\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n\}$ can be extracted using Equation (5) with the corresponding data-hiding key.

3.2. Anonymous Multisource Data Hiding

In some tasks such as anonymous voting, only the final result is necessary instead of the ballot content of each voter. In this case, the content of each secret data transmitted by multiple senders is unnecessary to the receiver. To this end, we propose an anonymous multisource data-hiding scheme, in which the data extracted by the receiver are a co-determined result of all secret data instead of the details. The procedure of the proposed scheme is shown in Figure 3, in which data embedding is executed in sequence, and data extraction is executed after the last embedding operation. The n senders sequentially embeds secret bits $\{\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n\}$ into a given cover image using the same data-hiding key K. On the receiver side, a co-determined result $f(\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n)$ of $\{\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n\}$ is extracted, while the details of each $\mathbf{m}_i$ kept unknown. This is achieved by the data-hiding key K_0, which is only held by receiver and the first sender symmetrically. Details are as follows.

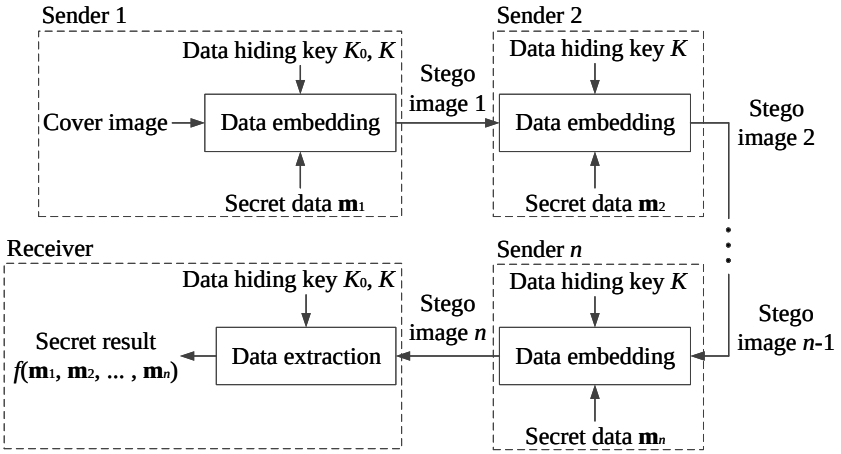

Figure 3. Architecture of anonymous multisource data hiding.

In anonymous multisource data hiding, the LSB (least significant bits) of the pixels in the cover image are also employed as the cover sequence $\mathbf{c} = [c(1), c(2), \ldots, c(k)]^{\mathrm{T}} \in \{0,1\}^k$. To achieve anonymous multisource data hiding, data embeddings of the n senders are executed in sequence, and data extraction of the receiver is executed after the last embedding operation. In contrast to separable multisource data hiding, which divides $\mathbf{c}$ into non-overlapping parts, in the anonymous scheme, all n senders employ the whole $\mathbf{c}$ for the embedding. In other words, the i-th sender embeds the i-th secret bits $\mathbf{m}_i$ into $\mathbf{c}_i$, where $\mathbf{m}_i = [m_i(1), m_i(2), \ldots, m_i(L)]^{\mathrm{T}} \in \{0,1\}^L$.

For the task of anonymous voting, the final result (extracted data by the receiver) is the summation value of all ballots (embedded data by the senders). That means

$$f(\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n) = \sum_{i=1}^{n} \varphi(\mathbf{m}_i) \tag{6}$$

where $\varphi(\mathbf{m}_i) \in \{0,1\}$ means the i-th sender gave an affirmative vote ($\varphi(\mathbf{m}_i) = 1$) or dissenting one ($\varphi(\mathbf{m}_i) = 0$). On the receiver side, the value of $f(\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n)$ should be obtained, while the value of each $\varphi(\mathbf{m}_i)$ should not be revealed. To this end, L binary bits $\mathbf{m}_0 = [m_0(1), m_0(2), \ldots, m_0(L)]^{\mathrm{T}} \in \{0,1\}^L$ are pseudo-randomly generated using the

data-hiding key K_0, and then the last L_0 bits $\{m_0(L-L_0+1), \ldots, m_0(L-1), m_0(L)\}$ are set as zero ($log_2(n) < L_0 < L$). Thus, the values of bits in $\mathbf{m}_i$ can be calculated as

$$m_i(u) = mod(\lfloor \gamma(i)/2^{u-1} \rfloor, 2), u \in \{1, 2, \ldots, L\} \tag{7}$$

where "$mod(\cdot)$" stands for the modulo operator, "$\lfloor \cdot \rfloor$" means the operation of rounding down, and

$$\gamma(i) = \varphi(\mathbf{m}_i) + \sum_{u=1}^{L} 2^{u-1} \cdot m_{i-1}(u) \tag{8}$$

Since the extracted data on the receiver side is $\mathbf{m}_n$, that is $\{m_n(1), m_n(2), \ldots, m_n(L)\}$, the value of $\gamma(n)$ can be obtained by

$$\gamma(n) = \sum_{u=1}^{L} 2^{u-1} \cdot m_n(u) \tag{9}$$

In addition, it can be deduced from Equations (7) and (8) that

$$\gamma(n) = \sum_{i=1}^{n} \varphi(\mathbf{m}_i) + \sum_{u=1}^{L} 2^{u-1} \cdot m_0(u) \tag{10}$$

That is

$$\gamma(n) = f(\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n) + \sum_{u=1}^{L} 2^{u-1} \cdot m_0(u) \tag{11}$$

The values of $\{m_0(1), m_0(2), \ldots, m_0(L)\}$ are determined by the data-hiding key K_0, which is held by the receiver; therefore, the final result $f(\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n)$ can be obtained by the receiver using

$$f(\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n) = \sum_{u=1}^{L} 2^{u-1} \cdot [m_n(u) - m_0(u)] \tag{12}$$

Thus, the co-determined result (the summation value of all $\varphi(\mathbf{m}_i)$ can be obtained on the receiver side. Meanwhile, the value of each $\varphi(\mathbf{m}_i)$ will not be revealed. Since the number of secret bits for all senders are the same, we employ the repeatable data-hiding strategy [25] for embedding, which is also based on the STC framework. Using the repeatable strategy, the distortion caused by data hiding is invariable no matter how many times the embedding operation is executed. In this way, the undetectability of data hiding can be maintained during the n times of embedding.

4. Experimental Results

To verify the feasibility and effectiveness of our schemes, we conducted a number of experiments in this section. We first describe the experimental conditions and environments. After that, we provide the results and discussions about undetectability checked by some modern steganalytic tools. Finally, we discuss the computational complexity of our scheme.

4.1. Experiment Setup

In our experiments, the popular image dataset UCID [26] was employed, which contains 1338 color images sized 512 × 384. All the images in UCID were used as cover images. The popular data-hiding methods HILL [5] and MiPOD [6] were employed for data embedding.

To examine the undetectability of steganographic schemes, the steganalytic methods maxSRMd2 (selection-channel-aware rich model) [18] and SCRMQ1 (spatial color rich model) [20] were employed. One-half of the image features were employed for training, while the remaining half were employed for testing. The criterion to measure the unde-

tectability of the data hiding was the minimal total error P_E obtained from the testing sets [21], as shown in Equation (13),

$$P_E = \min_{P_{FA}}\left(\frac{P_{FA} + P_{MD}}{2}\right) \tag{13}$$

where P_{FA} is the false alarm rate and P_{MD} is the missed detection rate. Higher P_E stands for higher undetectability. All of the results are the average value of P_E over 10 random tests.

4.2. Undetectability

For the cases of a different quantity of senders, the undetectability (values of P_E) of the proposed separable multisource data-hiding scheme is shown in Figure 4, where the horizontal axis represents the embedding payload (bits per pixel), secret data are embedded using the baseline embedding algorithm HILL. The results indicate that values of P_E are approximate to each other with different number of senders. The slight fluctuation is caused by the randomness of testing, which means that the undetectability performance is independent of the number of senders. The reason is that undetectability is determined by the embedding algorithm and payload, which is always L/k bits per pixel for different number of senders; therefore, an increment on the quantity of senders will not change the undetectability of the data hiding.

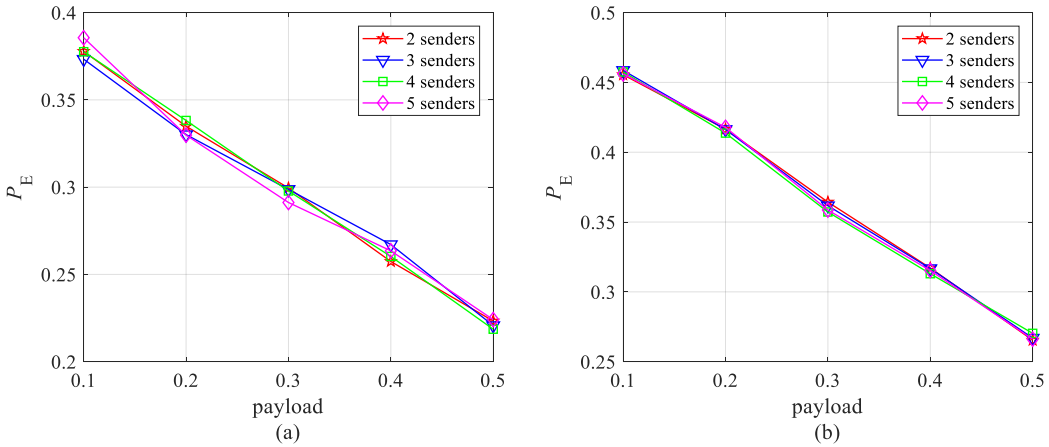

Figure 4. Undetectability for different number of senders against (**a**) maxSRMd2 and (**b**) SCRMQ1.

Since our scheme is based on the baseline embedding algorithms, e.g., HILL, MiPOD, it is necessary to verify that our scheme will not decrease the undetectability of the existing data-hiding methods. The undetectability comparisons between our scheme and the baseline embedding algorithms with 5 senders ($n = 5$) are shown in Figures 5 and 6, where "HILL-Separable" and "MiPOD-Separable" stand for the cases of our scheme with secret data embedded using HILL and MiPOD, respectively. It can be observed that our scheme that achieves multisource data hiding has not decreased the undetectability of the existing data-hiding methods. This is reasonable since the undetectability is determined by the embedding matrices, which are obtained using an existing data-hiding framework and kept unchanged in our schemes. This verifies that our scheme achieves multisource data hiding without decreasing the undetectability of the data hiding.

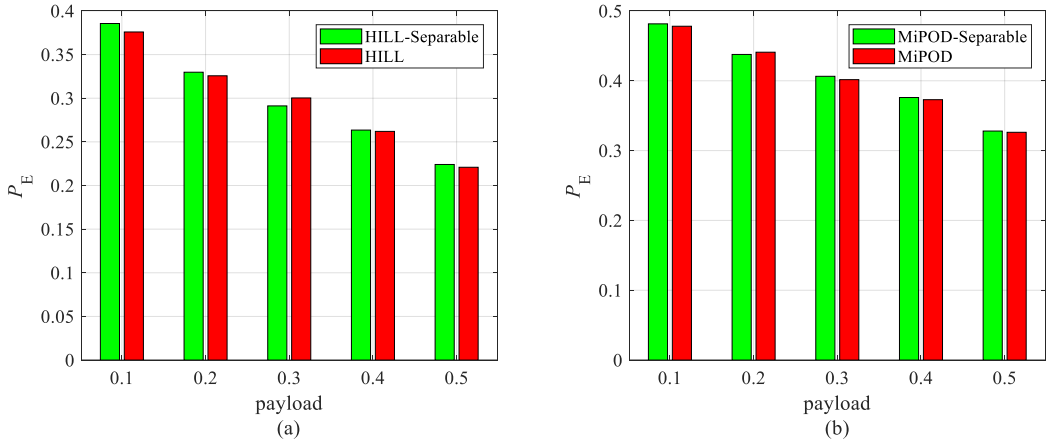

Figure 5. Undetectability comparisons against maxSRMd2 with embedding algorithms (**a**) HILL and (**b**) MiPOD.

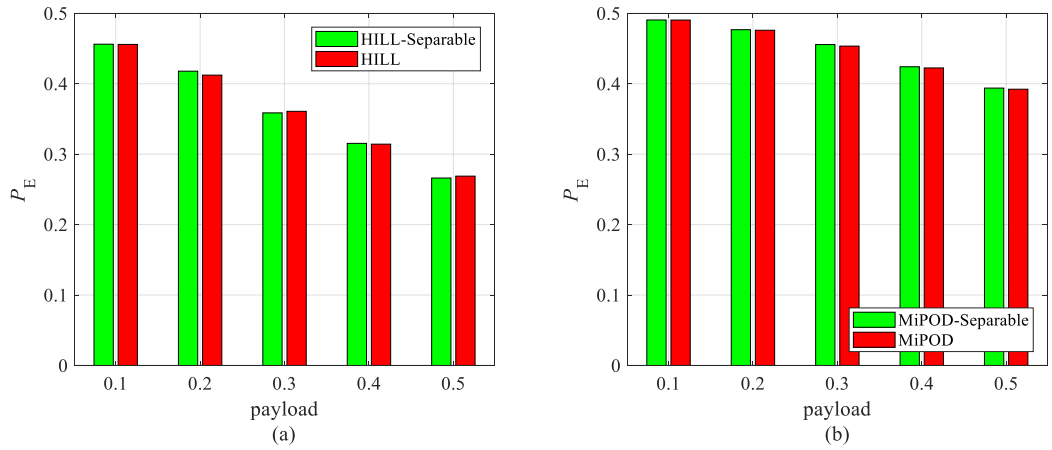

Figure 6. Undetectability comparisons against SCRMQ1 with embedding algorithms (**a**) HILL and (**b**) MiPOD.

To further verify the effectiveness of our scheme, we considered the cases of a big number of senders. With embedding algorithm HILL and payload 0.5 bpp, the undetectability of our scheme for the cases of 100, 200, 300, 400, and 500 senders ($n = 100, 200, \ldots, 500$) are shown in Figure 7. The results indicate that the P_E values for big number of senders are comparable with the case of one sender. That means the increment of number of senders have not cause inferior undetectability. This is reasonable since the undetectability of data hiding is determined by the embedding algorithm and payload. In our scheme, the two issues are unchanged; therefore, our scheme achieved the function of multisource without decreasing the undetectability of the existing data hiding ability.

For the proposed anonymous multisource data-hiding scheme, the repeatable data-hiding strategy was employed for embedding. With the repeatable strategy, the repeatability of undetectability has been theoretically proved in [25]. Thus, we do not demonstrate the undetectability performance of the anonymous scheme.

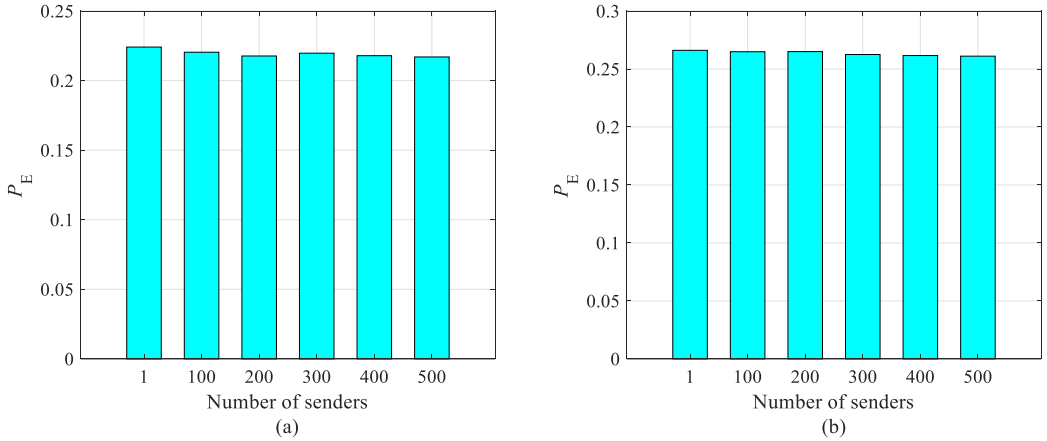

Figure 7. Undetectability comparisons for large number of senders with HILL and 0.5 bpp against (**a**) maxSRMd2 and (**b**) SCRMQ1.

4.3. Computational Complexity

For data hiding, computational complexity is also an important indicator. We also conducted experiments to compare the computational complexity between our scheme and the baseline embedding algorithms. All 1338 images in UCID were employed for data embedding, and then the average embedding time (s) for each image is shown in Figure 8. Similarly, "HILL-Separable" and "MiPOD-Separable" stand for the cases of our scheme with secret data embedded using HILL and MiPOD, respectively. The results were tested on a server with 3.7 GHz CPU, 16 GB memory, and Windows 7. The type of system is 64 bit and the version of MATLAB is R2017b.

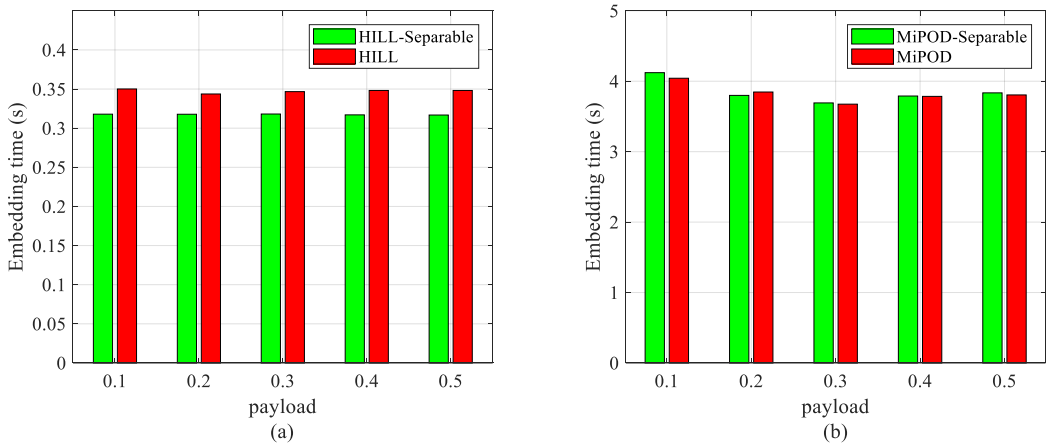

Figure 8. Complexity comparisons between the proposed scheme and baseline algorithms (**a**) HILL and (**b**) MiPOD.

It can be observed from Figure 8 that the computational complexity of our scheme is comparable or less than that of the baseline embedding algorithms. That means our scheme achieves the function of multisource in the modern data-hiding framework without increasing the computational complexity simultaneously. In addition, it can be noticed that the embedding time is not increased with a larger payload. This is because the computational complexity of a modern data-hiding framework is mainly determined by the distortion function. With the obtained embedding costs, secret data can be embedded quickly via the near-optimal steganographic coding.

5. Conclusions

A new field of data hiding called multisource data hiding is explored in this paper. In multisource data hiding, multiple senders are able to transmit different secret data to a receiver via the same cover image. Two schemes are proposed to achieve multisource data hiding in separable and anonymous manners, respectively. In the separable scheme, the receiver can extract the secret data transmitted by all senders using the corresponding data-hiding key. In the anonymous scheme, the receiver aims to extract a co-determined result of the secret data transmitted by all senders, instead of the details of all secret data. The proposed schemes are suitable for many scenarios, e.g., military intelligence collection or anonymous voting. Experimental results show that the two schemes achieve multisource data hiding without decreasing the undetectability of data hiding.

Funding: This work was supported in part by the Natural Science Foundation of China under Grant 62002214, and supported in part by the Research Fund of Guangxi Key Lab of Multi-source Information Mining & Security under Grant MIMS21-M-03.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Wang, Z.; Feng, G.; Qian, Z.; Zhang, X. JPEG Steganography with Content Similarity Evaluation. *IEEE Trans. Cybern.* **2022**. [CrossRef]
2. Fridrich, J.; Filler, T. Practical methods for minimizing embedding impact in steganography. *Secur. Steganography Watermarking Multimed. Contents IX* **2007**, *6505*, 650502.
3. Filler, T.; Judas, J.; Fridrich, J. Minimizing additive distortion in steganography using syndrome-trellis codes. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 920–935. [CrossRef]
4. Li, W.; Zhang, W.; Li, L.; Zhou, H.; Yu, N. Designing near-optimal steganographic codes in practice based on polar codes. *IEEE Trans. Commun.* **2020**, *68*, 3948–3962. [CrossRef]
5. Li, B.; Wang, M.; Huang, J.; Li, X. A new cost function for spatial image steganography. In Proceedings of the 2014 IEEE International Conference on Image Processing (ICIP), Paris, France, 27–30 October 2014; pp. 4206–4210.
6. Sedighi, V.; Cogranne, R.; Fridrich, J. Content-adaptive steganography by minimizing statistical detecta-bility. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 221–234. [CrossRef]
7. Yang, J.; Ruan, D.; Huang, J.; Kang, X.; Shi, Y. An embedding cost learning framework using gan. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 839–851. [CrossRef]
8. Pevny, T.; Filler, T.; Bas, P. Using high-dimensional image models to perform highly undetectable ste-ganography. In Proceedings of the 12th International Conference on Information Hiding, Calgary, AB, Canada, 28–30 June 2010; pp. 161–177.
9. Vojtech, H.; Fridrich, J. Designing steganographic distortion using directional filters. In Proceedings of the IEEE International Workshop on Information Forensics and Security, Costa Adeje, Spain, 2–5 December 2012; pp. 234–239.
10. Vojtech, H.; Fridrich, J.; Tomas, D. Universal distortion function for steganography in an arbitrary domain. *EURASIP J. Inf. Secur.* **2014**, 1–13.
11. Li, B.; Wang, M.; Li, X.; Tan, S.; Huang, J. A strategy of clustering modification directions in spatial image steganography. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1905–1917.
12. Wang, Z.; Yin, Z.; Zhang, X. Asymmetric distortion function for JPEG steganography using block artifact compensation. *Int. J. Digit. Crime Forensics* **2019**, *11*, 90–99. [CrossRef]
13. Wang, Z.; Qian, Z.; Zhang, X.; Yang, M.; Ye, D. On improving distortion functions for JPEG steganography. *IEEE Access* **2018**, *6*, 74917–74930. [CrossRef]
14. Tang, W.; Li, B.; Tan, S.; Barni, M.; Huang, J. CNN-based adversarial embedding for image steganography. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2074–2087. [CrossRef]
15. Wang, Z.; Feng, G.; Ren, Y.; Zhang, X. Multichannel steganography in digital images for multiple receivers. *IEEE Multimed.* **2021**, *28*, 65–73. [CrossRef]
16. Wang, Z.; Qian, Z.; Zhang, X.; Li, S. An improved steganalysis method using feature combinations. In Proceedings of the 5th International Conference on Artificial Intelligence and Security (ICAIS 2019), New York, NY, USA, 26–28 July 2019; pp. 115–127.
17. Fridrich, J.; Kodovsky, J. Rich models for steganalysis of digital images. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 868–882. [CrossRef]
18. Denemark, T.; Sedighi, V.; Holub, V.; Cogranne, R.; Fridrich, J. Selection-channel-aware rich model for steganalysis of digital images. In Proceedings of the 2014 IEEE International Workshop on Information Forensics and Security (WIFS), Atlanta, GA, USA, 3–5 December 2014; pp. 48–53.

19. Li, B.; Li, Z.; Zhou, S.; Tan, S.; Zhang, X. New steganalytic features for spatial image steganography based on derivative filters and threshold LBP operator. *IEEE Trans. Inf. Forensics Secur.* **2017**, *13*, 1242–1257. [CrossRef]
20. Goljan, M.; Fridrich, J.; Cogranne, R. Rich model for steganalysis of color images. In Proceedings of the 2014 IEEE International Workshop on Information Forensics and Security (WIFS), Atlanta, GA, USA, 3–5 December 2014; pp. 185–190.
21. Kodovsky, J.; Fridrich, J.; Holub, V. Ensemble classifiers for steganalysis of digital media. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 432–444. [CrossRef]
22. Ye, J.; Ni, J.; Yi, Y. Deep learning hierarchical representations for image steganalysis. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 2545–2557. [CrossRef]
23. Boroumand, M.; Chen, M.; Fridrich, J. Deep residual network for steganalysis of digital images. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 1181–1193. [CrossRef]
24. Li, Q.; Feng, G.; Ren, Y.; Zhang, X. Embedding Probability Guided Network for Image Steganalysis. *IEEE Signal Process. Lett.* **2021**, *28*, 1095–1099. [CrossRef]
25. Wang, Z.; Feng, G.; Zhang, X. Repeatable Data Hiding: Towards the Reusability of Digital Images. *IEEE Trans. Circuits Syst. Video Technol.* **2022**, *32*, 135–146. [CrossRef]
26. Schaefer, G.; Stich, M. UCID: An uncompressed color image database. *Storage Retr. Methods Appl. Multimed.* **2003**, *5307*, 472–480.