symmetry

MDPI

Article

An Effective Dual-Image Reversible Hiding for UAV's Image Communication

Yung-I Lin [1], Ying-Hsuan Huang [1,*] and Chih-Cheng Chen [2]

[1] Aeronautical Systems Research Division, National Chung-Shan Institute of Science and Technology, Taichung 40722, Taiwan; robin.bravo@msa.hinet.net

[2] Department of Computer Science and Engineering, National Chung Hsing University, Taichung 40227, Taiwan; salu.chen@gmail.com

* Correspondence: ying.hsuan0909@gmail.com; Tel.: +886-921-002469

Received: 5 June 2018; Accepted: 3 July 2018; Published: 10 July 2018

Abstract: Compared with traditional hiding methods, dual-image reversible data hiding methods have a higher embedding rate and a better quality stego image. Also, this is a special case of secret sharing, because secret data cannot be extracted from any stego image. In the literature, the frequencies of occurrence of secret data were used as reference information for data encoding, in which most digits were transformed into smaller ones. The encoding strategy can effectively decrease the modification level of the pixel. However, only limited literature has analyzed the relationship between the adjacent secret data. In this paper, we proposed an exclusive-or (XOR)-based encoding method to convert the neighboring values, thereby reducing the distortion. Since there are significant similarities between the two stego images and the original image, the first stego image is stored on an unmanned aerial vehicle (UAV) to avoid a hacker's interception attack. The second stego image on the UAV is sent to the command station. After completion of the UAV mission, the proposed method extracts the secret data from the two stego images to identify whether the second stego image has been tampered with.

Keywords: dual-image reversible data hiding; selection strategy; frequency-based encoding; XOR-based encoding

1. Introduction

Data hiding means that secret data can be embedded into different multimedia, e.g., digital images, videos, and audio files. After data hiding, the image is very similar to the original one that has been extensively used in various applications, e.g., secret communications, message authentication, and data annotation [1]. Unlike irreversible hiding, reversible data hiding can recover the original image after the data have been extracted, as shown in Figure 1. This property implies that reversible data hiding is very suitable for some special environments that do not allow the distortion of images, i.e., medical and military applications. For example, the private data of a patient were embedded into the medical image, which causes the distortion problem and erroneous judgments by doctors. Figure 2 shows that reversible data hiding methods can be classified mainly into two types, i.e., the frequency domain [2,3] and the spatial domain [4–19]. The frequency domain is used to transform the cover pixels in the image into coefficients and embed data into the coefficients. Consequently, it needs more computational costs.

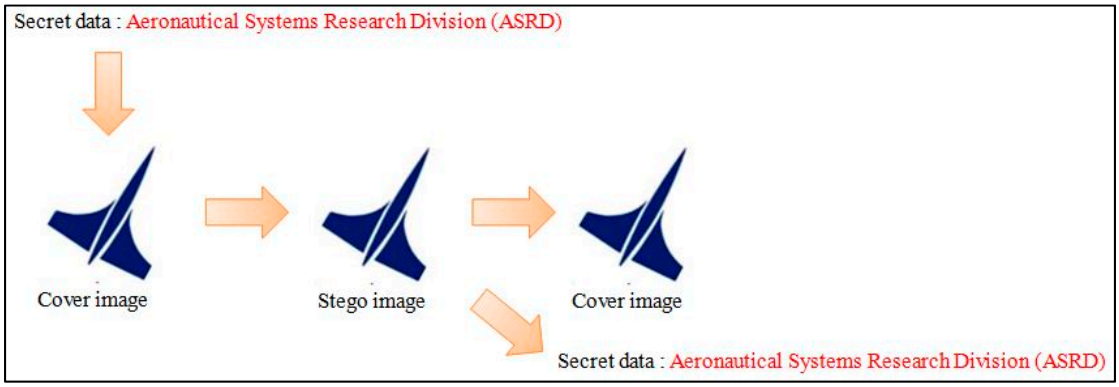


Figure 1. Reversible data hiding.

The current methods in the spatial domain can be classified mainly into five types, i.e., the compression method [4], difference expansion [5], prediction [6–11], histogram [12–14], and dual-image [15–23]. In 2002, Celik et al. [4] proposed a compression-based hiding method that quantified the pixels in the image and recorded the values of remainders, which were used as recovery information. By arithmetic coding, both the recorded values and the secret data were compressed, and the compressed results were embedded into the cover image. However, arithmetic coding requires massive computational costs. Tian [5] proposed a difference expansion method that was different from the compression-based method. In Tian's method, the difference of a pair of pixels is doubled to embed one secret bit. However, expanding the larger difference in the complexity region of the image causes serious distortion of the stego image. In order to solve this problem, Thodi and Rodriguez [6] proposed a prediction-based hiding method that used the inherent edge-detection method to derive the prediction value of the cover ones. Since the inherent edge-detection analyzes the relationship among three neighboring pixels of the cover pixels, the prediction error is smaller than the difference between two adjacent pixels. Consequently, the expansion level of Thodi and Rodriguez's method is smaller than that of Tian's method. In 2008, Fallahpour [8] proposed a gradient-adjusted prediction (GAP) that expanded the number of relationships of neighboring pixels from 3 to 8. However, the inherent edge-detection and GAP cannot generate the prediction value in the boundary of an image. In order to solve this problem, Lee et al. [9] and Qin et al. [10] calculated the mean of several adjacent pixels as the prediction value of the cover pixel. (The above methods can effectively reduce the expanded level, thereby decreasing the modification level of the pixels). However, these methods still had overflow and underflow problems; to avoid them, Ni et al. [12] proposed a histogram shifting method that only modifies the pixels between the peak point and the zero point to reduce the probability of occurrence of the overflow and underflow problems. However, the method still has overflow and underflow problems when there is no zero point that exists in the histogram. In this case, the coordinates of the pixels with the lowest frequency of occurrence were recorded, which decreased hiding capacity. In order to solve this problem, Chen et al. [13] proposed an asymmetric-histogram shifting of prediction errors to increase the number of embeddable pixels. In 2017, Lu et al. [14] used multiple predictors to generate several asymmetric-histograms to reduce the number of shifted pixels.

Lee et al. [16] proposed a method that was different from the above methods. Their method was a dual-image reversible data hiding approach in which four directions were used to embed secret data into two stego images. However, the secret data could not be embedded in some special cases, which decreased the embedding capacity. In order to overcome this problem, Lee et al. [17] expanded the number of directions from 4 to 5. Unlike the direction-based hiding methods, Horng et al. [18] proposed a (k, n)-images hiding method that can embed k secret images into n stego images. Also, the method can embed $(n - k)$ meaningfulness images to cheat the hackers or charge them more for the analytical process. In 2015, Lu et al. [19] used the LSB matching rules to embed secret data, in which the maximum modification level of the pixels is controlled within 1; however, the embedding

rate was 1 bpp, at most. To enhance the hiding capacity, Lu et al. [20] proposed a center folding strategy that can embed a set of K secret bits into a pair of pixels. In addition, the strategy can effectively reduce the absolute value of the secret digits and decrease the modification level of the pixels. In 2017, Lu et al. [21] improved the center folding strategy further by the appearance frequency of the secret data. However, the strategy does not analyze the relationships between adjacent secret messages. Therefore, Chi et al. [22] proposed a dynamic encoding method that used the similarity of the neighboring data to encode secret data. These methods can effectively reduce the modification level of pixels. In 2017, Yao et al. [23] proposed a selection strategy of shiftable pixels' coordinates to improve the hiding capacity of the center folding strategy. In addition, the method does not invoke more distortion after embedding extra secret data. However, their method does not analyze the frequency of the occurrence of secret data or their relationships. As most of the secret digits become large, the distortion of the image increases in the data embedding phase.

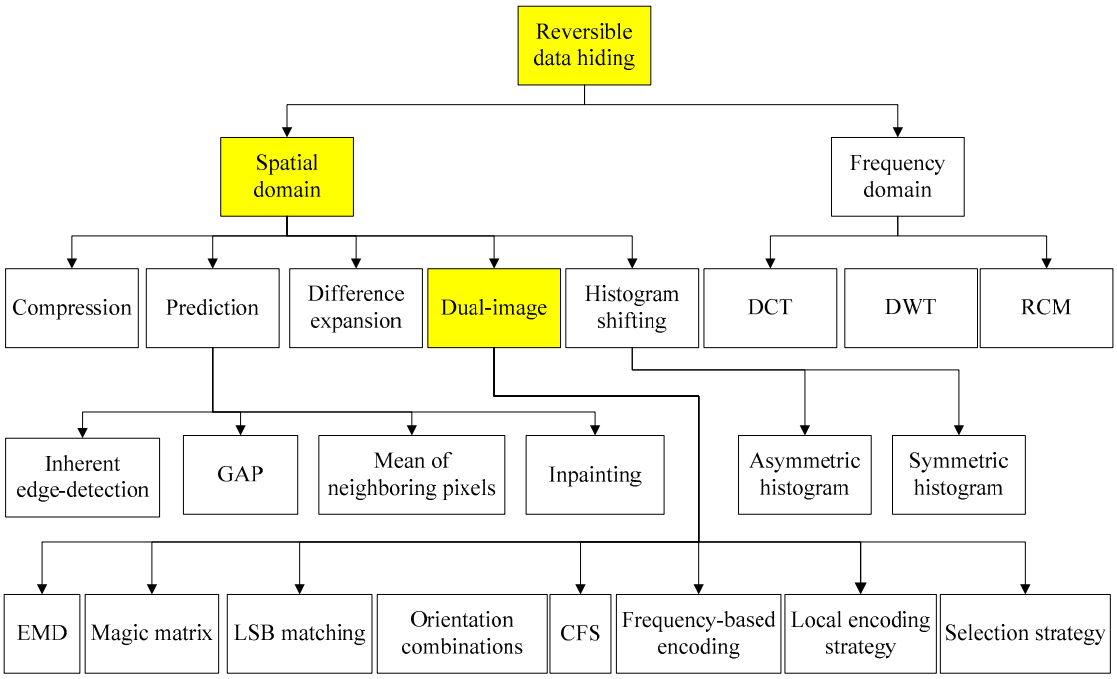


Figure 2. Classification of reversible data hiding methods.

In this paper, we proposed a XOR-based encoding strategy to transform secret digits into smaller ones, owing to which the adjacent secret data have are highly similar. In addition, the proposed method is combined with the frequency-based encoding strategy to further encode the transformed digits, in which the digit with the highest frequency of occurrence is encoded as the absolute minimum value "0", and the digit with the lowest frequency of occurrence is encoded as the maximum value. Consequently, the proposed method can effectively decrease the frequency of the modification of pixels and the modification level, and those are the reasons the quality of the stego image of the proposed method is better than that of previous methods.

The rest of the paper is organized as follows. Sections 2 and 3 describe the selection strategy of shiftable pixels' coordinates and our method, respectively. Section 4 compares our method and the eight dual-image hiding methods. Conclusions are given in Section 5.

2. Related Method

In 2017, Yao et al. [23] proposed a selection strategy that can embed at least K bits into two pixels. First, a set of K secret bits $\{S_1, S_2, \ldots, S_K\}$ was transformed into the decimal value d, i.e.,

$d = \sum_{i=1}^{K} 2^{i-1} \times s_i$ and $d \in [0,\ 2^K - 1]$. If decimal value d is equal to the maximum value "$2^K - 1$", then it is increased by one extra secret bit e, i.e.,

$$d' = \begin{cases} d + S_{i+1}, & \text{if } d = 2^K - 1, \\ d, & \text{otherwise.} \end{cases} \tag{1}$$

Finally, the decimal value was embedded into two stego images, i.e.,

$$P'_{x,y} = \begin{cases} P_{x,y} + \lfloor d'/4 \rfloor, & \text{if } d' \bmod 2 = 0, \\ P_{x,y} - \lceil d'/4 \rceil, & \text{otherwise.} \end{cases} \tag{2}$$

$$P''_{x,y} = \begin{cases} P'_{x,y} - d'/2, & \text{if } d \bmod 2 = 0, \\ P'_{x,y} + \lceil d'/2 \rceil, & \text{otherwise.} \end{cases} \tag{3}$$

in which $P'_{x,y}$ and $P''_{x,y}$ are the pixels in the first stego image and the second stego image, respectively.

An example is used to illustrate the selection strategy. Let K = 2 and assume that $P_{1,1}$ = 100 and $\{S_1, S_2, S_3\} = \{1, 1, 1\}$. First, the pair of secret bits {1, 1} was transformed into the decimal value, i.e., $d = \sum_{i=1}^{2} 2^{i-1} \times s_i = 2^0 \times 1 + 2^1 \times 1 = 3$. Since the decimal value satisfies the first condition of Equation (1), it can be increased by another secret bit S_3, i.e., $d' = d + S_3 = 3 + 1 = 4$. According to Equations (2) and (3), the value "4" is embedded by $P'_{1,1} = P_{1,1} + \lfloor d'/4 \rfloor = 100 + \lfloor 4/4 \rfloor = 101$ and $P''_{1,1} = P'_{1,1} - \frac{4}{2} = 101 - 4/2 = 99$.

3. Proposed Method

An effective application and the proposed method are presented in this section. The latter includes the embedding algorithm and the extraction and recovery algorithm.

3.1. Effect Application

To date, digital images on UAVs can be transmitted to the command station wirelessly. However, hackers may interrupt the transmitted images and send fake images to the military. Note that it is difficult for hackers to attack or control UAV. In order to avoid this problem, a dual-image reversible data hiding system must be implemented, as shown in Figure 3. First, the secret data consist of the mission parameters on UAVs, e.g., date of flight, altitude, latitude, and longitude. Second, the secret data were embedded into two stego images, each of which was very similar to the original image.

The first stego image was stored in the storage of UAV. Even if hackers interrupted the transmitted image, the military still obtains the first stego image after aircraft landing. The second stego image was transmitted to the command station; thus, the military can analyze the image immediately. After aircraft landing, the military extracts the first stego image from the storage of UAV and reveals secret data by the two stego images. If the revealed secret data are not equal to the mission parameters on UAV, then the military only records the UAV's mission parameter and the first stego image in the database. This is because the second stego image is a fake image, which should not be recorded in database. Otherwise, the military can recover the original image losslessly by calculating the mean of the two images. Afterwards, the original image and the mission parameters are inserted into the database.

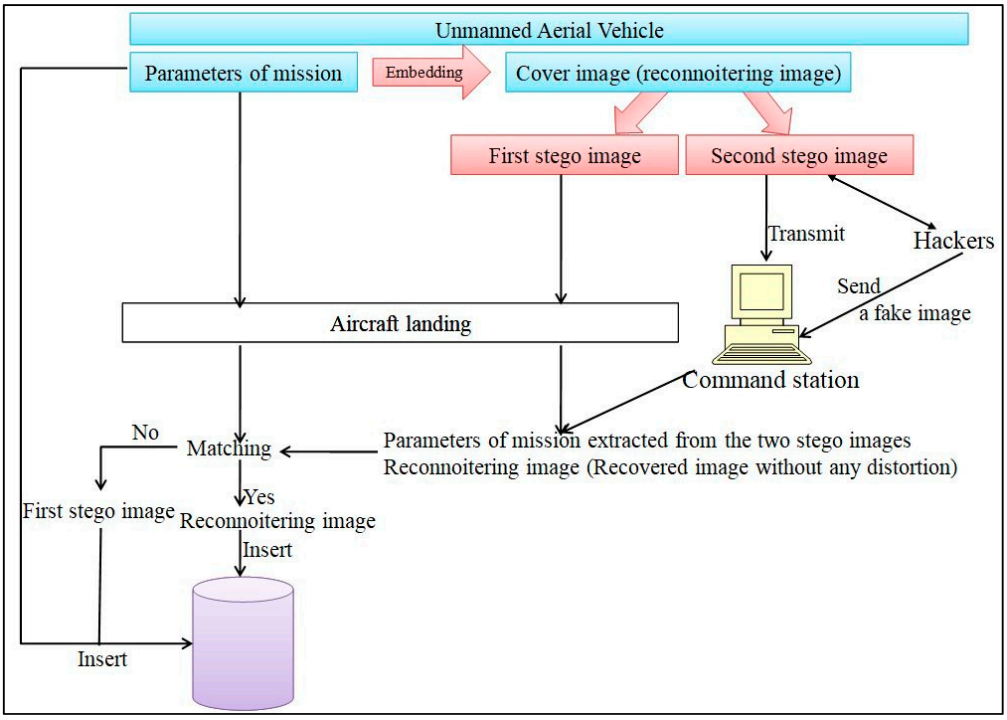


Figure 3. Reversible data hiding for UAV's image communication.

3.2. Data Embedding Algorithm

Figure 4 shows the data embedding flowchart. Since there is a high correlation coefficient between the mission's digits, their bytes can be encoded as smaller values by XOR operator, i.e., $B_i = T(S_i) \oplus T(S_{i-1}) = \{b_{i,1}, b_{i,2}, \ldots, b_{i,8}\} \oplus \{b_{i-1,1}, b_{i-1,2}, \ldots, b_{i-1,8}\} = \{b'_1, b'_2, \ldots, b'_8\}$, in which $T(\cdot)$ denotes the byte of parameters. Note that the byte of the first secret digit remains unchanged, because it does not have the previous secret message, i.e., $B_1 = T(S_1)$. The XOR operator makes it possible for the different bytes to be transformed effectively into similar bytes.

The above bits are transformed into the decimal digits, i.e.,

$$d'_j = \begin{cases} d_j + b'_{j+1}, & \text{if } \sum_{j=1}^{K} 2^{j-1} \times b'_j = 2^k - 1, \\ d_j, & \text{otherwise.} \end{cases} \tag{4}$$

in which k is a pre-established threshold that determines the control of the hiding capacity and the quality of the stego images. The embedding equation is the same as that of the selection strategy [23], so our maximum hiding capability is equal to that of the selection strategy. However, in the proposed method, the frequencies of the occurrences of decimal digits are counted and sorted in descending order, in which the sorted indices are $I(d'_j)$ and $I(d'_j) \in [1, 2^K + 1]$. In other words, the minimum sorted index represents the decimal value with the highest frequency of occurrence.

The sorted indices can be encoded further by

$$I'(d'_j) = \begin{cases} \lfloor I(d'_j)/2 \rfloor, & \text{if } I(d'_j) \text{ is an even number,} \\ -\lfloor I(d'_j)/2 \rfloor, & \text{otherwise.} \end{cases} \tag{5}$$

The absolute value of $I'(d'_j)$ is smaller than the original index, so embedding these reduced values $I'(d'_j)$ into the image does not invoke serious distortion. The encoded value $I'(d'_j)$ is embedded into the pixels by

$$P'_{x,y} = \begin{cases} P_{x,y} - \lfloor I'(d'_j)/2 \rfloor, & \text{if } P_{x,y} - \lfloor I'(d'_j)/2 \rfloor > 0 \text{ and } P_{x,y} + \lceil I'(d'_j)/2 \rceil < 255, \\ P_{x,y}, & \text{otherwise.} \end{cases} \quad (6)$$

$$P''_{x,y} = \begin{cases} P_{x,y} + \lceil I'(d'_j)/2 \rceil, & \text{if } P_{x,y} - \lfloor I'(d'_j)/2 \rfloor > 0 \text{ and } P_{x,y} + \lceil I'(d'_j)/2 \rceil < 255, \\ P_{x,y} + \lceil \max(d'_j)/2 \rceil + 1, & \text{if } P_{x,y} - \lfloor I'(d'_j)/2 \rfloor < 0, \\ P_{x,y} - \lceil \max(d'_j)/2 \rceil - 1, & \text{if } P_{x,y} + \lceil I'(d'_j)/2 \rceil > 255, \end{cases} \quad (7)$$

in which $P_{x,y}$ represents the cover pixel, and $P'_{x,y}$ and $P''_{x,y}$ represent the pixels in the first and second stego images. The above equation can avoid the overflow and underflow problems, because the proposed method does not embed any secret data when the overflow or underflow problem occurs. To discriminate the non-embeddable pixel-pair or the embeddable pixel-pair, the difference between pixels in the non-embeddable pixel-pair is expanded by $\lceil \max(d'_j)/2 \rceil + 1$, in which the expansion level is higher than that of the embeddable pixel-pair.

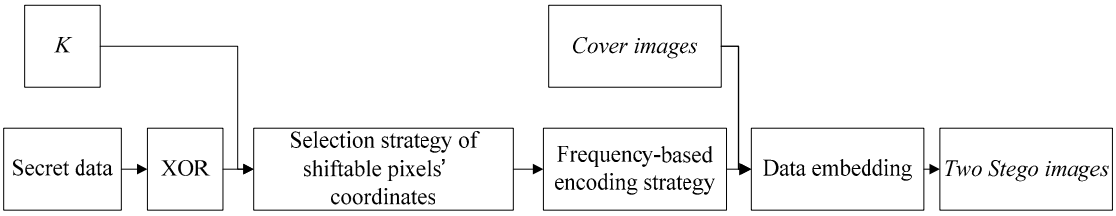


Figure 4. Flowchart of the proposed method for embedding data.

Figure 5 shows an example of embedding data. Let $K = 2$ and assume that two altitudes on UAV are 150 and 157, and their bytes are $(10010110)_2$ and $(10011101)_2$, respectively. The first value remains unchanged, because it does not have a previous value. The byte of the second altitude value can be encoded by the XOR operator, i.e., $11 = (00001011)_2 = (10010110)_2 \oplus (10011101)_2$. After the above procedure, the 16 secret bits $(1001011000001011)_2$ can be embedded by the following procedures.

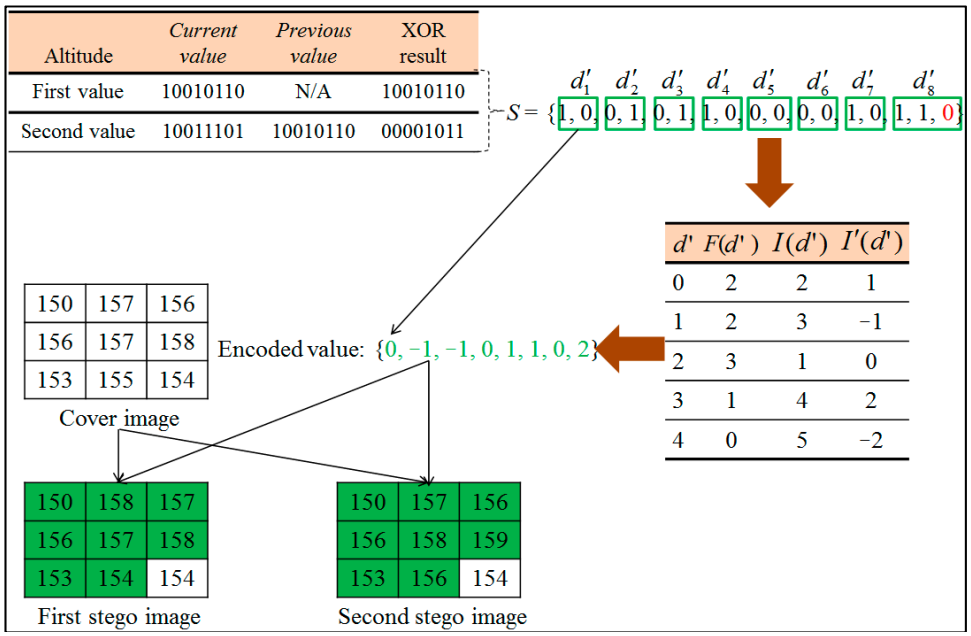


Figure 5. Example of our data embedding.

According to Equation (4), the first and second bits $(10)_2$ are converted into the first decimal value "2". The remaining bits are transformed by the same procedure. Note that the last set of secret bits $(11)_2$ cannot satisfy Equation (4), because there is no remaining bit in the secret sequence. To solve this problem, the set is padded with one bit $(0)_2$ to successfully convert the secret set as the decimal value "3". After decimal conversation, the decimal values are {2, 1, 1, 2, 0, 0, 2, 3}.

The occurrence frequencies of decimal values are counted, i.e., {2, 2, 3, 1, 0}. To encode the decimal value as the smaller value effectively, the occurrence frequencies are sorted in descending order, in which the sorted indices are {2, 3, 1, 4, 5}. According to Equation (5), these indices are reduced by {1, −1, 0, 2, −2}. After accomplishing the secret mapping rules, the first decimal value "2" is encoded as "0". The remaining values are processed by the same procedure to obtain the encoded values {0, −1, −1, 0, 1, 1, 0, 2}.

These encoded values are embedded by the following procedure. Assuming that the nine pixels in the cover image are {150, 157, 156, 156, 157, 158, 153, 155, 154}, the first encoded value "0" is then embedded into the first cover pixel to yield two stego pixels, i.e., $P'_{1,1} = P_{1,1} - \lfloor 0/2 \rfloor = 150 - 0 = 150$ and $P''_{1,1} = P_{1,1} + \lceil 0/2 \rceil = 150 + 0 = 150$. The other encoded values are embedded in the same way.

3.3. Data Extraction and Image Recovery Algorithm

Figure 6 shows the flowchart of the data extraction and image recovery. After obtaining two stego images, the difference between the pixels in the two stego images is calculated to identify whether there is an encoded value in the pixel-pair or not, i.e., $I'(d'_j) = P''_{x,y} - P'_{x,y}$. If $I'(d'_j) = \lceil \max(d'_j)/2 \rceil + 1$, then there are no secret data. Otherwise, the secret data can be revealed by the following procedures. First, they are expanded by

$$I(d'_j) = \begin{cases} 2I'(d'_j), & \text{if } I'(d'_j) > 0, \\ 2 \times \left| I'(d'_j) \right| + 1, & \text{otherwise.} \end{cases} \tag{8}$$

Afterwards, according to Equation (4) and the sorted index of the frequency of occurrence, the secret mapping table can be established, as shown in Table 1. The index is mapping by the secret mapping table to obtain the secret bits. Each set of eight secret bits $\{b'_1, b'_2, \ldots, b'_8\}$ is re-encoded by XOR operator to recover the mission's parameters, i.e., $T(S_i) = B_i \oplus T(S_{i-1}) = \{b'_{i,1}, b'_{i,2}, \ldots, b'_{i,8}\} \oplus \{b_{i-1,1}, b_{i-1,2}, \ldots, b_{i-1,8}\} = \{b_{i,1}, b_{i,2}, \ldots, b_{i,8}\}$, in which $T(S_i)$ denotes the byte of the i^{th} mission's parameter. Note that the first byte keeps unchanged, because it not has the reference digit. Moreover, the image is recovered by

$$P_{x,y} = \begin{cases} P'_{x,y}, & \text{if } I'(d'_j) = \lceil \max(d'_j)/2 \rceil + 1, \\ \lfloor (P'_{x,y} + P''_{x,y})/2 \rfloor, & \text{otherwise.} \end{cases} \tag{9}$$

in which the recovered image is the same as the original image.

The example in Section 3.2 is used repeatedly to illustrate how to extract secret data and recover the original image, as shown in Figure 7. First, the difference between the first pixels in the two stego images is calculated, i.e., $I'(d'_1) = P''_{1,1} - P'_{1,1} = 150 - 150 = 0$. Since $I'(d'_1) < \lceil 4/2 \rceil + 1$, there is one encoded value. According to Equation (8), the encoded value "0" is increased by "1" to obtain the sorted index "1". The sorted index "1" is mapped by Table 1 to obtain the two secret bits {1, 0}. The difference between the second pixels in the two stego images is calculated, i.e., $I'(d'_2) = P''_{1,2} - P'_{1,2} = 157 - 158 = -1$. According to Equation (8), the encoded value -1 is doubled and increased by 1 to obtain the sorted index ", i.e., $I(d'_2) = 2 \times |-1| - 1 = 3$. The sorted index "3" is mapped by Table 1 to obtain the two secret bits {0, 1}. The other secret bits are revealed in the same way. The secret bits are $(10010110000010110)_2$, in which the first set of the eight bits are just the byte of the first altitude value, i.e., $S_1 = (10010110)_2 = 150$, and the ninth through sixteenth bits are re-encoded by $S_2 = B_2 \oplus S_1 = (00001011)_2 \oplus (10010110)_2 = (10011101)_2 = 157$.

Afterwards, the original image is recovered losslessly by calculating the mean of the pixels in the same position of the two stego images. For example, the mean of the first pixels in the two stego images is just the first pixel in the original image, i.e., $P_{1,1} = \lfloor (150 + 150)/2 \rfloor = 150$. Then, the mean of the second pixels in the two stego image is just the second pixel of the original image, i.e., $P_{1,2} = \lfloor (158 + 157)/2 \rfloor = 157$.

Table 1. Secret mapping table.

Sorted Indices	Decimal Values	Secret Patterns
2	0	{0, 0}
3	1	{0, 1}
1	2	{1, 0}
4	3	{1, 1, 0}
5	4	{1, 1, 1}

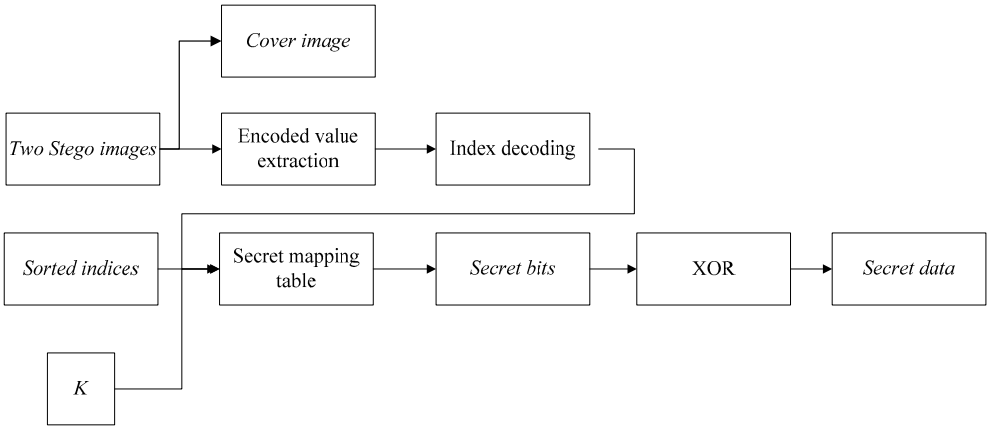


Figure 6. Flowchart of our data extraction and image recovery process.

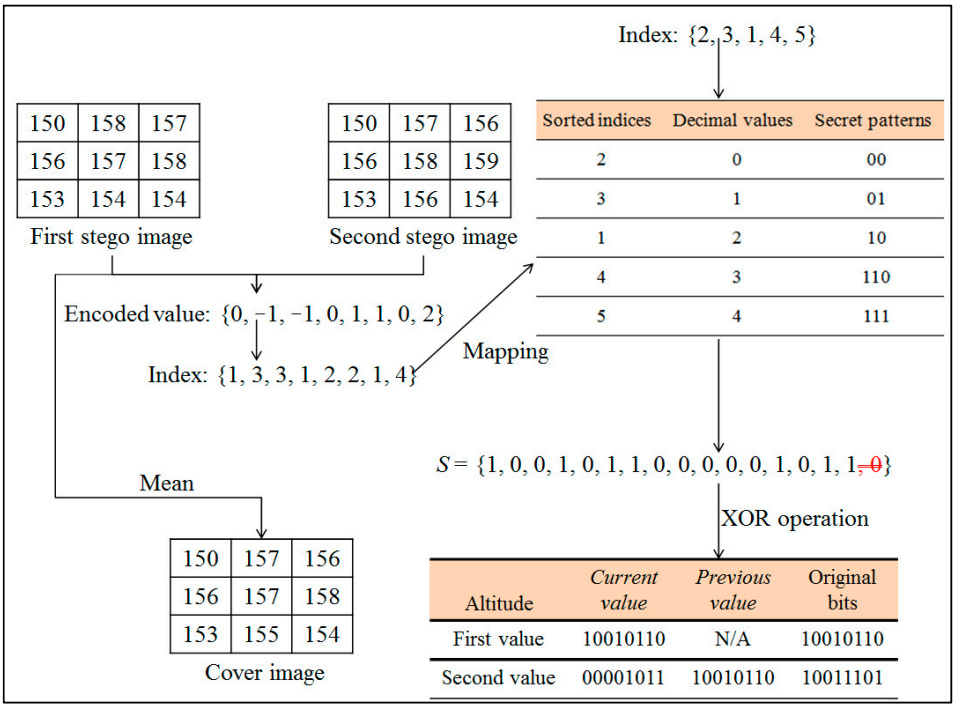


Figure 7. Example of our data extraction and image recovery.

4. Experimental Results

The experimental environment consists of a PC with 3.3 GHz intel® Core (TM) i5-4590 and 4 GB RAM with Window 7 Professional. In addition, the proposed method was developed by MATLAB R2017a. Figures 8 and 9 show six secret images and the first six images of 1338 UCID images, respectively. Each UCID image is used as the cover image. The measurement indexes of the experiments include the embedding rates R and the PSNR values, and are expressed as

$$R = \frac{\|S\|}{2 \times L \times W}(\text{bpp}), \tag{10}$$

$$\text{PSNR} = 10 \times \log_{10}\left(\frac{255^2}{\text{MSE}}\right)(\text{dB}), \text{ where MSE} = \frac{1}{L \times W}\sum_{x=1}^{L}\sum_{y=1}^{W}(P'_{x,y} - P_{x,y})^2, \tag{11}$$

in which ||S|| is the number of secret bits; L and W are the length and width of the cover image, respectively; MSE is the mean square error between the stego image $P'_{x,y}$, and the cover image $P_{x,y}$. Consequently, a higher value of R implies that the hiding method can embed more secret data. In addition, a higher value of PSNR indicates that there is a high similarity between the stego image and the cover image.

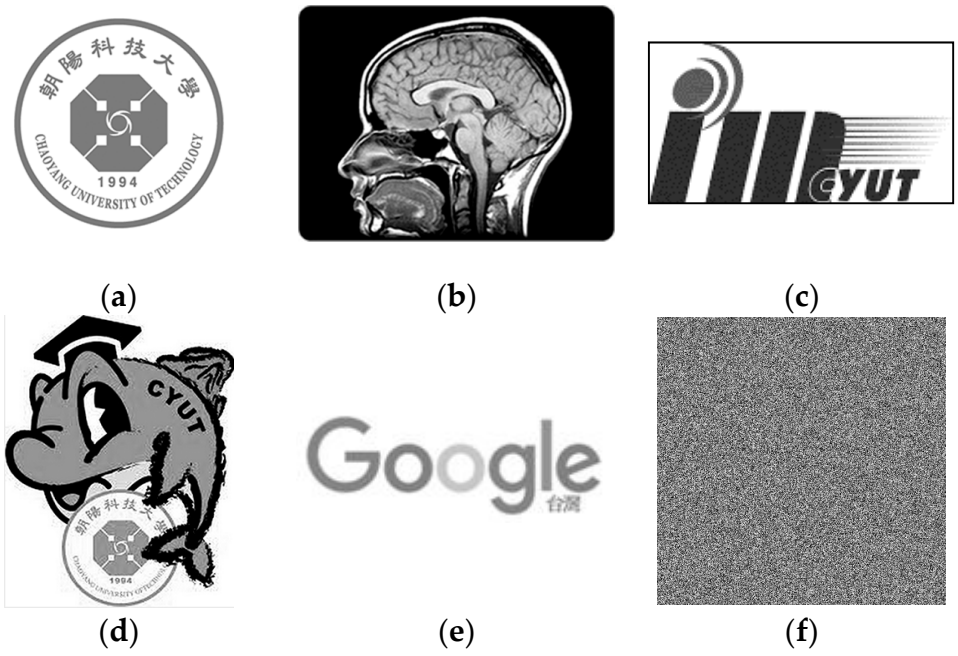


Figure 8. Six secret images: (**a**) logo, (**b**) brain, (**c**) IM, (**d**) dolphin, (**e**) Google, and (**f**) random image.

The other measurement index is the SSIM index, i.e.,

$$\text{SSIM} = (P,\ P') = (2\mu_P\mu_{P'} + C_1)(2\sigma_{PP'} + C_2)/(\mu_P^2 + \mu_{P'}^2 + C_1)(\sigma_P^2 + \sigma_{P'}^2 + C_2) \tag{12}$$

in which P and P' are the cover image and the stego image, respectively; μ_P and $\mu_{P'}$ are the means of the pixels in P and P', respectively; C_1 and C_2 are two constants that assure that the denominator is greater than 0, in which $C_1 = C_2 = 1$; and σ_P and $\sigma_{P'}$ are the standard deviations of the pixels in the two images that compare the contrast between the two images. As the value of SSIM increases, the visual quality of the stego image gets better.

In theory, the performance of the proposed method is analyzed as follows. Assume that each pixel in the cover image does not have an overflow or underflow problem. The minimum embedding

rate is $K/2$ bpp, because a pair of pixels can be used to embed at least two secret bits. In addition, the maximum embedding rate is $(K+1)/2$ bpp due to the $(K+1)$ secret bits that may be embedded into a pair of pixels. In general, the expected embedding rate is derived according to the possibility of occurrence of patterns of K secret bits, i.e., $\{1/2^K, 1/2^K, \ldots, 1/2^K, 1/2^{K+1}, 1/2^{K+1}\}$. The equation of the expected embedding rate is as follows:

$$\overline{R} = \frac{1}{2} \times \left[\frac{(2^K - 1) \times K}{2^K} + \frac{2 \times (K+1)}{2^{K+1}} \right]. \tag{13}$$

Assume that $K = 2$. The secret patterns of $K = 2$ are {00, 01, 10, 110, 111}, and the possibilities of occurrence are {0.25, 0.25, 0.25, 0.125, 0.125}. According to Equation (13), the expected embedding rate can be obtained, i.e., $\overline{R} = \frac{1}{2} \times \left[\frac{(4-1)\times 2}{4} + \frac{2\times(2+1)}{8} \right] = 1.125$.

The PSNR value in theory is analyzed as follows. Assume that all of the secret digits are 0. These digits will be encoded as "0" by the proposed method. Embedding the decimal digits "0" into the image does not invoke any distortion; thus, the stego image is lossless. In the second case, all of the secret digits are 255. By the XOR operator, the first secret digit is unchanged, and the other digits are transformed into "0". Then, the eight bits of the first secret digit are embedded dispersedly into $8/K$ pairs of pixels, and the bits of the other digits are embedded without any distortion of the modification of the pixels. The frequency and level of modification of pixels of the proposed method are significantly smaller than that of Yao et al.'s method [23], because they did not use the frequency of the occurrence of secret data or the relationship between the adjacent digits for encoding the secret data. In the third case, the possibilities of occurrence of $(2^K + 1)$ patterns of K secret bits are the same, which causes the ineffectiveness of the frequency-based encoding strategy. Their possibilities are expressed as $\{1/(2^K + 1), 1/(2^K + 1), \ldots, 1/(2^K + 1)\}$, and the modification levels are $\{|-2^{K-1}|, |-2^{K-1}| + 1, \ldots, |2^{K-1}|\}$; thus, the expected modification levels can be calculated by

$$\overline{M} = \frac{1}{2} \times \sum_{i=0}^{2^K} \frac{1}{2^K + 1} \times \left(\left| -2^{k-1} + i \right| \right) \tag{14}$$

In the worst case, overflow or underflow problems occur on each of the cover pixels. All of the cover pixels are modified by $\lceil \max(d'_j)/2 \rceil + 1$; thus, the modification level is $\lceil \max(d'_j)/2 \rceil + 1$. However, the possibility of the occurrence of the worst case is very low.

Assume that $K = 2$. According to Equation (14), the modification level of a pixel on average is $\overline{M} = \frac{1}{2} \times (0.2 \times |-2| + 0.2 \times |-1| + 0.2 \times 0 + 0.2 \times |1| + 0.2 \times |2| = 0.6$, and it is substituted into the PSNR formula, Equation (11), to obtain the expected PSNR value of the proposed method, i.e.,

$$\text{PSNR} = 10 \times \log_{10} \left(\frac{255^2}{0.6} \right) = 50.35 \text{ (dB)}$$

Afterwards, assume that $K = 2$ and that all of the cover pixels have overflow or underflow problems. The modification level of the pixels in the second stego image is 3, and it is substituted into the PSNR formula, i.e.,

$$\text{PSNR} = 10 \times \log_{10} \left(\frac{255^2}{3} \right) = 43.35 \text{ (dB)}$$

The first experiment mainly set an appropriate K. Figure 10 shows the experimental results. When $K = 4$, a few PSNR values were smaller than 40 dB, and the SSIM values were also smaller than 0.9. This is because the number of pixels with overflow or underflow problems grew as the K value increased. Table 2 listed that the number of images with overflow or underflow problems of $K = 4$ is 59 more than that of $K = 2$. When $K = 4$, the total number of the pixels with overflow or underflow problems is 91,501. In addition, the modification level of the non-embeddable pixels is $\lceil \max(d'_j)/2 \rceil + 1 = \lceil 16/2 \rceil + 1 = 9$, which is greater than that of $K = 3$,

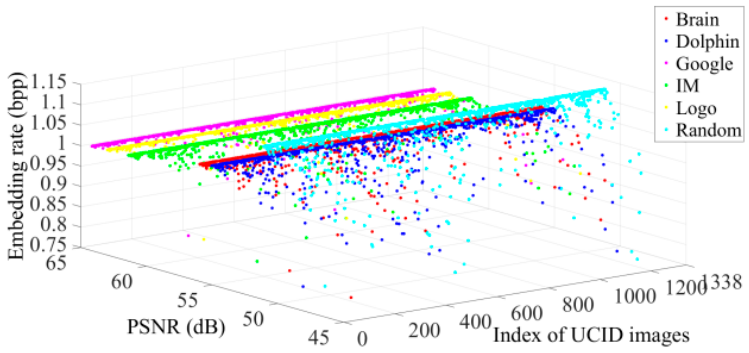
$\lceil \max(d'_j)/2 + 1 \rceil = \lceil 8/2 \rceil + 1 = 5$. These reasons cause the PSNR value to be smaller than 40 dB and the SSIM value to be smaller than 0.9. Consequently, the maximum value of K must be limited to 4 or less. For the same embedding rate, the PSNR value became larger as the K value decreased. This explains that the proposed method can effectively embed secret data into the entire image with the smaller K value. Additionally, for larger K values, only a part of the image is used to embed the secret data. In other words, a part of pixels suffered from the larger modification. As a result, the appropriate K is set to 2.

Figure 12 compares the eight related methods and the proposed method. The seven related methods [15–20,23] did not use the frequency of the occurrence of secret data or the relationship of the adjacent secret data to encode secret data, thus embedding secret data invokes serious distortion of the image. The reason confirms that the proposed method has better image quality than the seven related methods [15–20,23]. To be more precise, the PSNR values of the proposed method are at least 1.6 dB more than that of the selection strategy [23]. For the secret image Google, the PSNR value of the proposed method is at least 11.98 dB more than that of the selection strategy, because Google consists of more values of 255. The proposed method can transform these digits from 255 to 0, thereby reducing the modification level of pixels. Although the dynamic encoding strategy used codebook to encode adjacent secret data after decimal transformation, the transformation decreases the relationship between the adjacent secret data. Our encoding strategy is different from the dynamic encoding strategy due to the fact it is executed before transforming the K secret bits; thus, the proposed method keeps the significant relationship between the adjacent secret data to encode secret data. The advantage explains why the PSNR value of the proposed method is at least 0.98 dB more than that of the dynamic encoding method for all images.

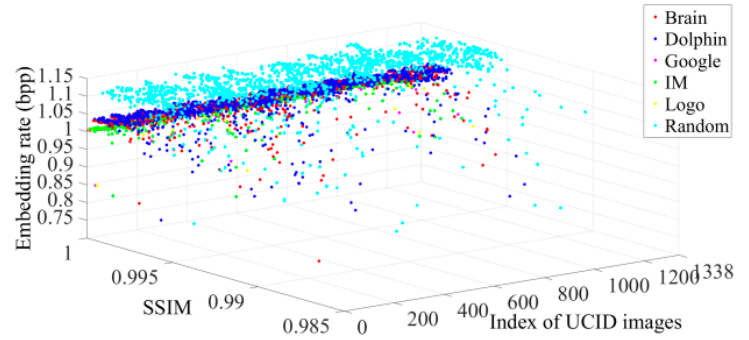
Table 2. Number of overflow and underflow problems using different K.

K	Number of Images Having the Overflow or Underflow Problems	Number of Pixels Having the Overflow or Underflow Problems
2	1185	83,313
3	1215	90,376
4	1244	91,501

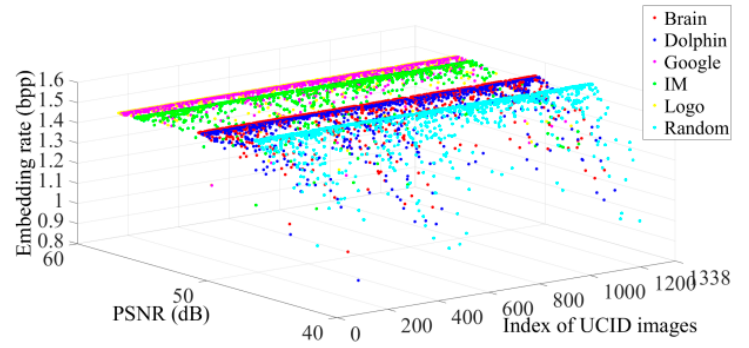
Figure 9. First six cover images in 1338 images that were obtained from the uncompressed color image database (UCID). (**a**) house; (**b**) statue; (**c**) chair; (**d**) trail; (**e**) people; (**f**) pavilion.



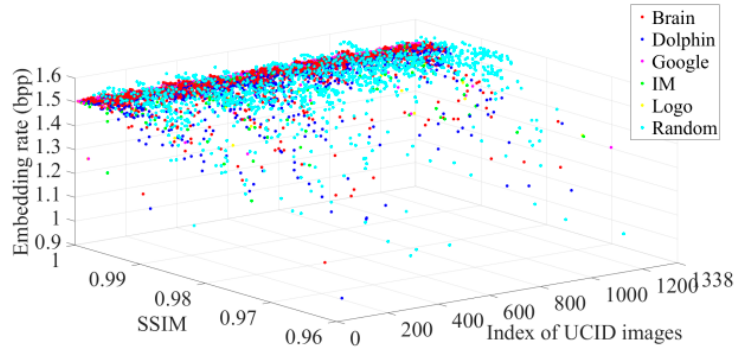
(**a**) Embedding rates and the corresponding PSNR value of 1338 UCID images for $K = 2$.



(**b**) Embedding rates and the corresponding SSIM value of 1338 UCID images for $K = 2$.

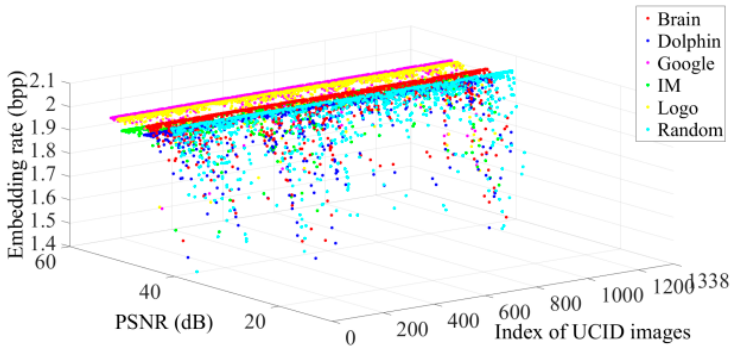


(**c**) Embedding rates and the corresponding PSNR value of 1338 UCID images for $K = 3$.

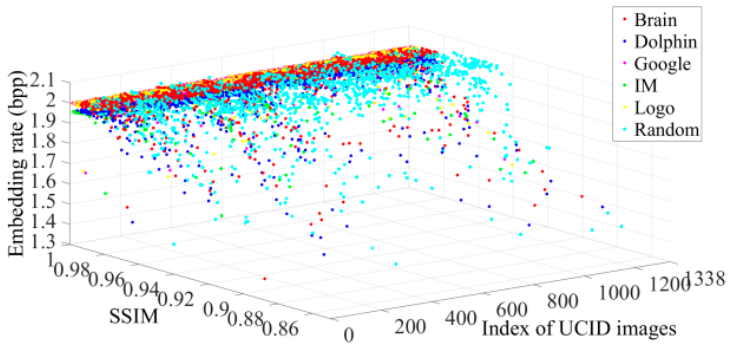


(**d**) Embedding rates and the corresponding SSIM value of 1338 UCID images for $K = 3$.

Figure 10. *Cont.*

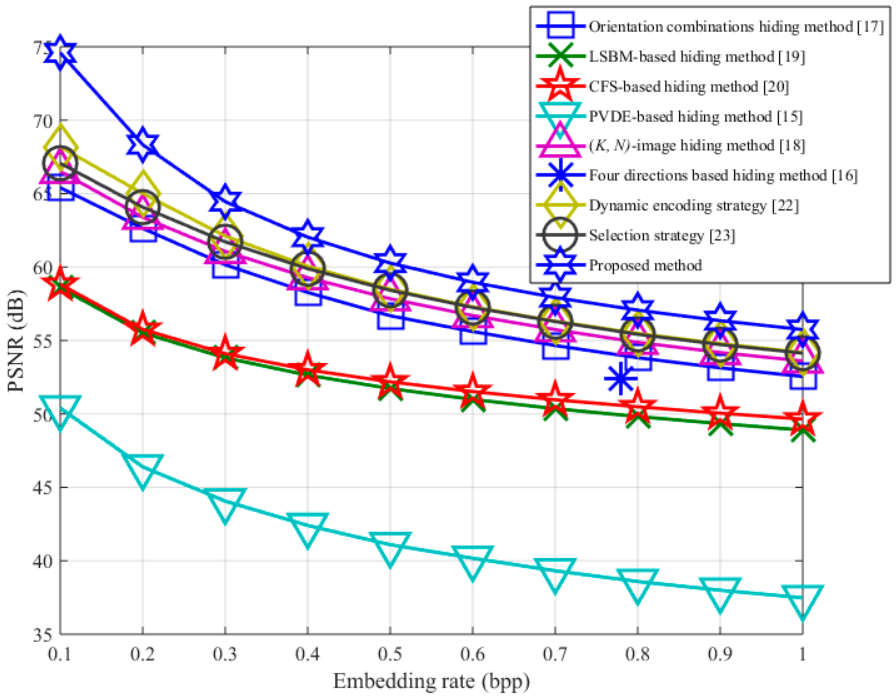


(**e**) Embedding rates and the corresponding PSNR value of 1338 UCID images for $K = 4$.



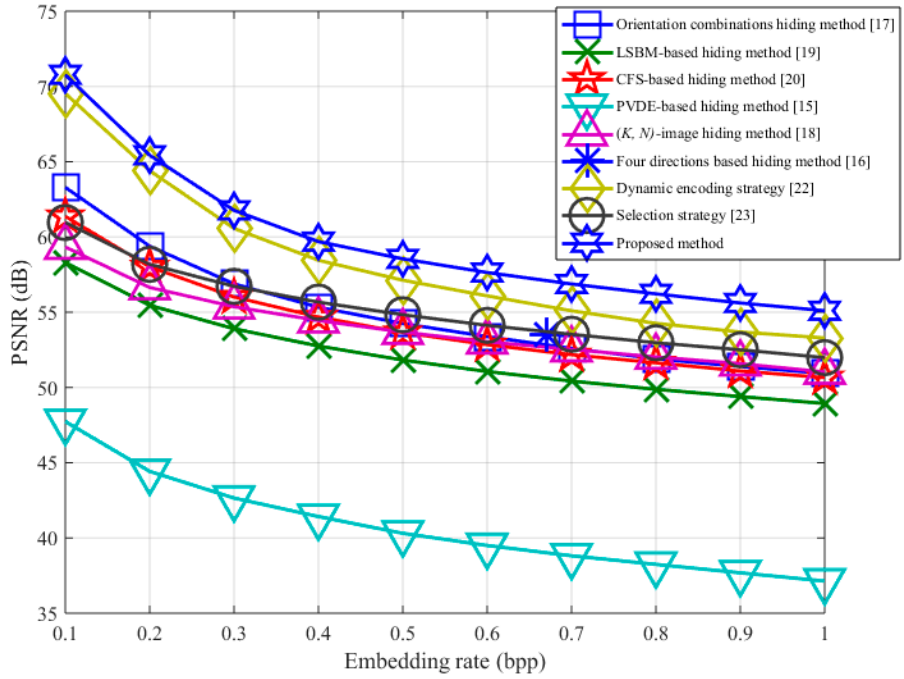
(**f**) Embedding rates and the corresponding SSIM value of 1338 UCID images for $K = 4$.

Figure 10. PSNR values and SSIM values of 1338 images obtained by various K values with the maximum embedding rate: (**a**) and (**b**) $K = 2$; (**c**) and (**d**) $K = 3$; (**e**) and (**f**) $K = 4$.

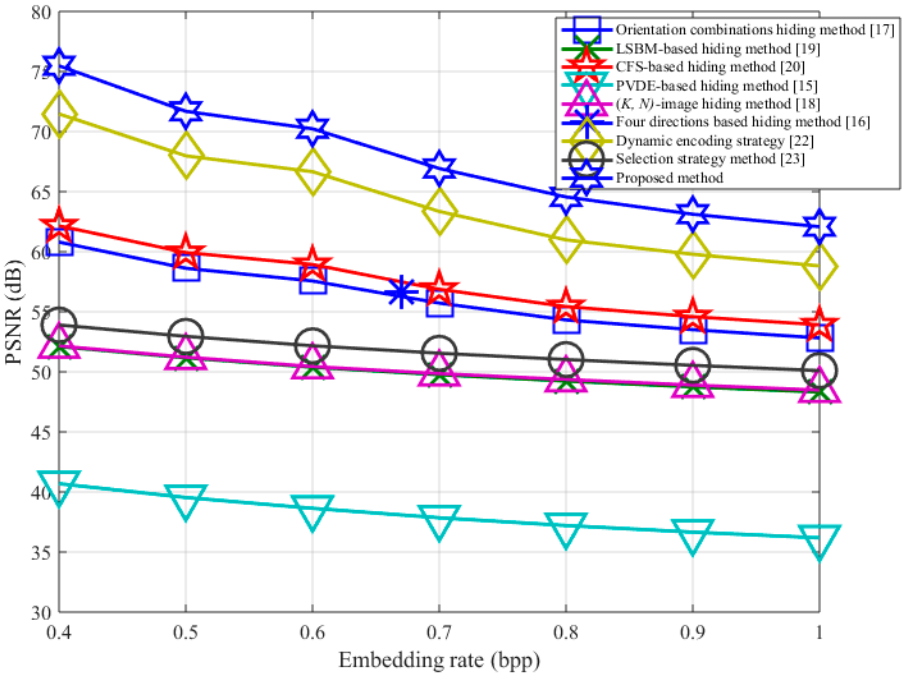


(**a**) Brain

Figure 11. *Cont.*

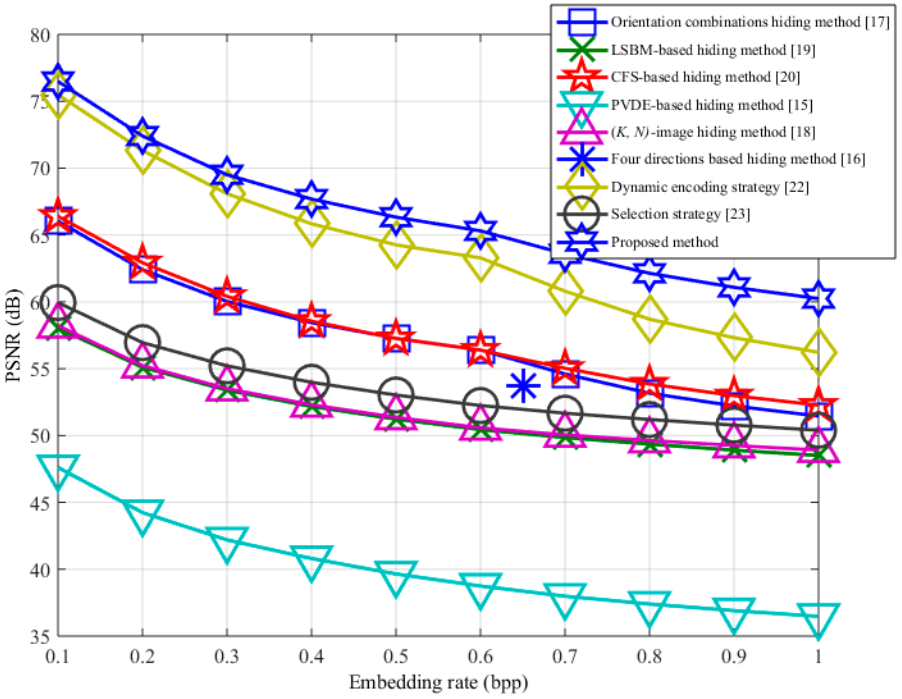


(**b**) Dolphin

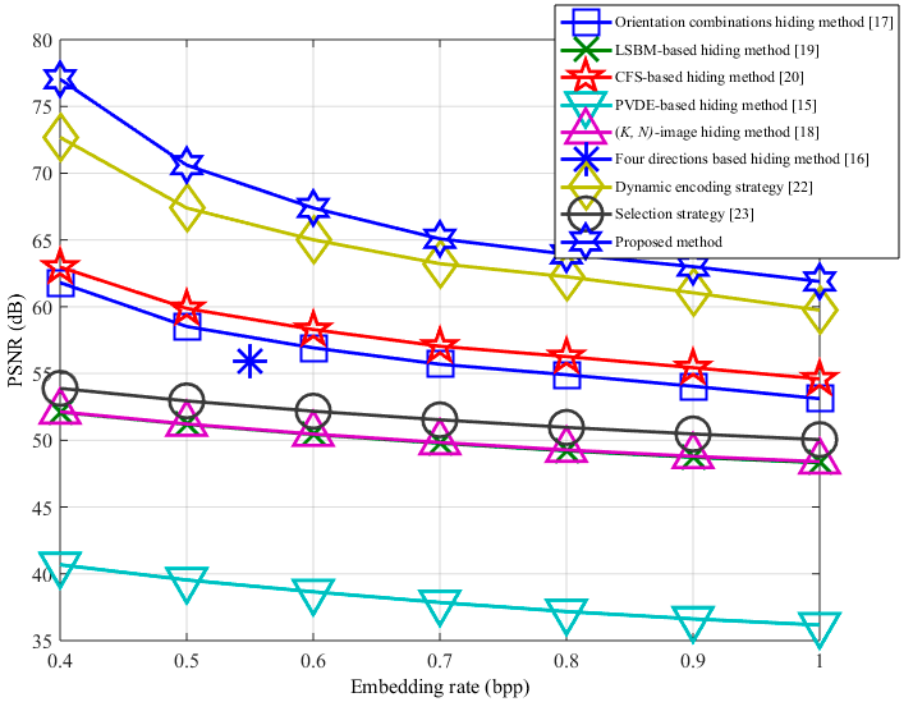


(**c**) Google

Figure 12. *Cont*.



(**d**) IM



(**e**) Logo

Figure 12. Comparison of the proposed method with eight related methods [15–20,22,23], in which the cover image is used to embed difference secret images: (**a**) Brain; (**b**) Dolphin; (**c**) Google; (**d**) IM; (**e**) Logo.

5. Conclusions

In this paper, we propose a dual-image reversible data hiding structure that achieves three advantages. The first stego image is stored on the storage of UAV, and the second stego image is sent

to the command station. For the first advantage, even if hackers interrupt the second stego image, the military obtains the first stego image that is highly similar after aircraft landing. For the second advantage, the command station can immediately analyze the content of the second stego image. For the third advantage, the proposed method can effectively detect tampered images.

In addition, we propose an XOR-based encoding strategy that uses the significant relationship between adjacent secret data to transform the secret data from large digits to smaller digits. Our encoding strategy is different from previous methods, because it is executed before transforming the K secret bits. The transformation decreases the relationship between the adjacent secret data. Consequently, the proposed method is superior to the previous methods. In the future, we will try to embed the mission's parameters into videos on UAV.

Author Contributions: Y.I. Lin proposed the application and the algorithms. Y.H. Huang wrote this manuscript. C.C. Chen conducted experiments. All authors read and approved the final manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Petitcolas, F.A.P.; Anderson, R.J.; Kuhn, M.G. Information hiding—A Survey. *Proc. IEEE* **1999**, *87*, 1062–1078. [CrossRef]
2. Chan, Y.K.; Chen, W.T.; Yu, S.S.; Ho, Y.A.; Tsai, C.S.; Chu, Y.P. A HDWT-based reversible data hiding method. *J. Syst. Softw.* **2009**, *82*, 411–421. [CrossRef]
3. Yang, W.C.; Chen, L.H. Reversible DCT-based data hiding in stereo images. *Mult. Tools Appl.* **2015**, *74*, 7181–7193. [CrossRef]
4. Celik, M.U.; Sharma, G.; Tekalp, A.M.; Saber, E. Reversible data hiding. *IEEE Trans. Image Proc.* **2005**, *14*, 253–266. [CrossRef]
5. Tian, J. Reversible data embedding using a difference expansion. *IEEE Trans. Circuits Syst. Video Tech.* **2003**, *13*, 890–896. [CrossRef]
6. Thodi, D.M.; Rodriguez, J.J. Prediction-error based reversible watermarking. *IEEE Image Proc.* **2004**, *3*, 1549–1552.
7. Thodi, D.M.; Rodriguez, J.J. Expansion embedding techniques for reversible watermarking. *IEEE Trans. Image Proc.* **2007**, *16*, 721–730. [CrossRef]
8. Fallahpour, M. Reversible image data hiding based on gradient adjusted prediction. *IEICE Electron Expr.* **2008**, *5*, 870–876. [CrossRef]
9. Lee, C.F.; Chen, H.L.; Tso, H.K. Embedding capacity raising in reversible data hiding based on prediction of difference expansion. *J. Syst. Softw.* **2010**, *83*, 1864–1872. [CrossRef]
10. Qin, C.; Chang, C.C.; Liao, L.T. An adaptive prediction-error expansion oriented reversible information hiding scheme. *Pattern Recogn. Lett.* **2012**, *33*, 2166–2172. [CrossRef]
11. Qin, C.; Chang, C.C.; Huang, Y.H.; Liao, L.T. An inpainting-assisted reversible steganographic scheme using histogram shifting mechanism. *IEEE Trans. Circuits Syst. Video Tech.* **2013**, *23*, 1109–1118. [CrossRef]
12. Ni, Z.; Shi, Y.Q.; Ansari, N.; Su, W. Reversible data hiding. *IEEE Trans. Circuits Syst. Video Tech.* **2006**, *16*, 354–362.
13. Chen, X.; Sun, X.; Sun, H.; Zhou, Z.; Zhang, J. Reversible watermarking method based on asymmetric-histogram shifting of prediction errors. *J. Syst. Softw.* **2013**, *86*, 2620–2626. [CrossRef]
14. Lu, T.C.; Chen, C.M.; Lin, M.C.; Huang, Y.H. Multiple predictors hiding scheme using asymmetric histograms. *Multimed Tools Appl.* **2017**, *76*, 3361–3382. [CrossRef]
15. Jana, B.; Giri, D.; Mondal, S.K. Dual-image based reversible data hiding scheme using pixel value difference expansion. *Inter. J. Netw. Sec.* **2016**, *18*, 633–642.
16. Lee, C.F.; Wang, K.H.; Chang, C.C.; Huang, Y.L. A reversible data hiding scheme based on dual steganographic images. In Proceedings of the Third International Conference on Ubiquitous Information Management and Communication, Suwon, Korea, 15–16 January 2009; pp. 228–237.
17. Lee, C.F.; Huang, Y.L. Reversible data hiding scheme based on dual stegano-images using orientation combinations. *Telecommun. Syst.* **2013**, *52*, 2237–2247. [CrossRef]

18. Horng, G.; Huang, Y.H.; Chang, C.C.; Liu, Y. (*k*, *n*)-image reversible data hiding. *J. Inf. Hiding Multimed. Signal Proc.* **2014**, *5*, 152–164.
19. Lu, T.C.; Tseng, C.Y.; Wu, J.H. Dual imaging-based reversible hiding technique using LSB matching. *Signal Proc.* **2015**, *108*, 77–89. [CrossRef]
20. Lu, T.C.; Wu, J.H.; Huang, C.C. Dual-image-based reversible data hiding method using center folding strategy. *Signal Proc.* **2015**, *15*, 195–213. [CrossRef]
21. Lu, T.C.; Chi, L.P.; Wu, C.H.; Chang, H.P. Reversible data hiding in dual stego-images using frequency-based encoding strategy. *Multimed. Tools Appl.* **2017**, *76*, 23903–23929. [CrossRef]
22. Chi, L.P.; Wu, C.H.; Chang, H.P. Reversible data hiding in dual stegano-image using an improved center folding strategy. *Multimed. Tools Appl.* **2017**, *77*, 1–19. [CrossRef]
23. Yao, H.; Qin, C.; Tang, Z.; Tian, Y. Improved dual-image reversible data hiding method using the selection strategy of shiftable pixels' coordinates with minimum distortion. *Signal Proc.* **2017**, *135*, 26–32. [CrossRef]