Journal of Computers Vol. 32 No. 2, 2021, pp. 1-7
doi:10.3966/199115992021043202001

Dual Stego-images Based Lossless Steganographic Scheme with Interval Scale Table

Tzu-Chuen Lu*, Ning Yang, Thanh Nhan Vo

[1] Department of Information Management, Chaoyang University of Technology
168, Jifeng East Road, Wufeng District, Taichung, 41349, Taiwan, ROC
tclu@cyut.edu.tw; en96321@gmail.com

Received 1 June 2019; Revised 1 November 2019; Accepted 6 January 2020

Abstract. Lu et al. proposed a dual-image based hiding method uses the center folding strategy and the interval scale in 2018. Their method uses the variable k value to improve the hiding amount and image quality by setting the interval scale, where k is the total number of binary bits that a pixel can be hidden. However, the interval scale in the scheme is manually set, and different types of images need to be manually determined an appropriate interval scale. However, how to find a suitable interval scale is a difficult task. This paper automatically finds the most suitable interval scale table through the preprocessing process, and finds the optimal rules for different images. The experimental results show that the proposed method can effectively increase the amount of hiding payload while maintaining a good image quality.

Keywords: information hiding, reversible, dual image, center folding strategy, interval scale, adaptive

1 Introduction

With the rapid development of information technology and the rapid dissemination of information on the Internet, message s can be easily transmitted. The illegal third party also can easily steal, destroy and tamper with the message [1]. In order to prevent information from being stolen, information hiding technology uses the cover media to disguise the message to generate the stego-media and achieve the purpose of not being perceived and protected by third parties. The key point of information hiding technology is to hide as much secret message as possible and reduce the difference between the stego-medias and the original medias. Therefore, the third parties cannot find the secret message.

Reversible Data Hiding (RDH) is an important technology in information hiding technology. It is one of the mainstream developments of information hiding [2]. The sender conceals the secret message into a cover image to generate the stego-image. When the receiver extracts the secret data from the stego-image, the scheme can restore the original image from the stego-image without distortion. The original image can be reused, and it is mostly used for high value image media such as medical imaging and military.

There are many kinds of RDH technologies proposed so far, one of which is Dual Images Techniques [3-8]. The dual image technology copies the original image into two pieces, and then modifies the pixels according to different hiding rules. Since the hidden information is split into two stego-images, the hiding capacity can be effectively enhanced. In the hiding process, the scheme only needs to modify the image value by simple addition and subtraction to achieve the purpose of low distortion camouflage image.

Lu et al. [9] proposed a dual-image based hiding method in 2018, which divides the original image into several blocks with size 1×2, and then computes the difference of the pixels in the blocks. The difference is used to determine the total number of the secret message k which can be concealed into the block. Then, the scheme converts the secret message of the k-bit into a decimal value m. Lu et al. perform a half-reduction through the center folding strategy to reduce the distortion. Finally, m is divided into two secret symbols. This method uses the dual image and interval meter to improve the image quality of the

* Corresponding Author

stego-image and the elasticity of the hiding payload. However, the k value of this method is manually setting. Not every original image can apply the same interval scale. In order to solve this problem, this paper uses the pre-processing process to generate the most appropriate interval scale table. Compared with Lu et al.'s method, the proposed method can automatically generate an interval scale and generate a corresponding scale according to different types of images.

2 Related Works

Lu et al. proposed a dual-image reversible technique based on interval and center folding strategies in 2018. In their scheme, image is divided into several 1×2 non-overlapping blocks and computes the difference between the pixels in the block. The difference d is computed by Equation (1), where $p_{(i,j)}$ and $p_{(i,j+1)}$ are two adjacent pixel values within the block,

$$d = | p_{(i,j)} - p_{(i,j+1)} | . \quad \textbf{(1)}$$

Then use the difference value d to refer to the defined interval scale, as shown in Fig. 1, to determine the total number of the secret data that can be concealed into each block, and k indicates the number of bits that can be hidden.

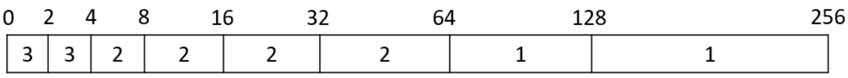

Fig. 1. Example interval scale table

Then convert the secret message of k bits into a decimal number and narrow down the value by the center folding method. Assume that the original secret message value field is R, then $R = \{0, 1, 2, \ldots, 2^k - 1\}$. The value range after the conversion of the folding method will become $\tilde{R} = \{-2^{k-1}, -2^{k-1}+1, \ldots, -1, 0, 1, \ldots, 2^{k-1} - 2, 2^{k-1} - 1\}$. The folding equation is

$$\tilde{m} = m - 2^{k-1}, \quad \textbf{(2)}$$

$\tilde{m}$ is the secret message after the center folding, and 2^{k-1} is the intermediate value. Then copy the image into two parts, $p'_{(i,j)}$ and $p''_{(i,j)}$, and assign the new secret message $\tilde{m}$ to $p'_{(i,j)}$ and $p''_{(i,j)}$ by Equation (3).

$$\{p'_{(i,j)} = p_{(i,j)} + \lfloor \frac{\tilde{m}}{2} \rfloor, p''_{(i,j)} = p_{(i,j)} - \lceil \frac{\tilde{m}}{2} \rceil . \quad \textbf{(3)}$$

$p_{(i,j+1)}$ represents the new pixel value of the first stego-image, and $p''_{(i,j)}$ is the new pixel value of the second stego-image. The $p_{(i,j+1)}$ pixel is also hidden using the same method to generate $p'_{(i,j+1)}$ and $p''_{(i,j+1)}$.

When restoring an image and extracting the secret message, the two images are respectively divided into 1×2 non-overlapping blocks. The second image pixel is subtracted from the first image pixel, respectively. The folded message is computed by Equation (4).

$$\tilde{m} = p'' - p' \quad \textbf{(4)}$$

Then, the original pixel of the block is restored by the Equation (5), and then the interval value is added into $\tilde{m}$ to restore m.

$$p = \left\lceil \frac{p' + p''}{2} \right\rceil, \quad \textbf{(5)}$$

$$m = \tilde{m} + 2^{k-1}. \quad \textbf{(6)}$$

After that, a lot of papers have been proposed to improve their scheme [11-15].

3 Proposed Methods

In order to analyze the most suitable interval scale table, this paper calculates the most suitable k value for each interval range by preprocessing, counting each interval difference, and then turning the binary confidential information into a decimal value to bring in the middle fold. In the strategy, the image distortion is reduced, and finally the confidential information is evenly distributed into two images to complete the hiding.

3.1 Pre-Processing Procedure

First, the image is divided into several non-overlapping blocks size 1×2. Then, the scheme computes the absolute difference of each block and placed in the interval quantity. The difference range is {2^^{0}~2^^{1}, 2^^{1}~2^^{2}, …, 2^^{7}~2^^{8}}, then set the k value of the interval with the maximum number to be 2, the interval with the second maximum number to be 3, and the rest interval are set to be 2. The interval block is shown in Fig. 2.

0 2 4 8 16 32 64 128 256

2	3	2	2	2	2	2	2

Fig. 2. Preprocessing interval scale table

The k value setting here can be adjusted. In this paper, we also try to use 3 as the first interval and 2 as the second interval. However, the result shows that the first interval set to be 2 can get better results.

Taking Fig. 3 as an example. Most differences of each block in Fig. 3 are falls in the range 2^0~2^1. Hence, the k values of the range 2^0~2^1 is set to be 2, the value of the second range 2^1~2^2 is set to be 3, and the other intervals are set to be 2.

200	201	201	202
200	202	208	222
221	225	224	223
112	113	123	124

Fig. 3. Example image

3.2 Hiding Processing

The embedding procedure is the same with the embedding procedure of Lu et al.'s method. The host image is first divided into several non-overlapping blocks size 1×2. The difference d of the inner two adjacent pixels ($p_{(i,j)}$, $p_{(i,j+1)}$) is computed by Equation (1). The difference d is brought into the interval scale table to get the region and obtain the number of bits k. Note here, if the host pixels are fall in the range [2, 254], then the block is embeddable. Because the maximum possible number of hidden bits k is 3, and the embeddable range is computed by [2^{k-2}, 256-2^{k-2}]. If the pixel is outside of this range, it is very likely to cause an overflow or underflow problem. Then, the scheme converts the secret data to a decimal number and use Equation (2) to fold it in a half to reduce the distortion. The secret message after the center fold is called $\tilde{m}$. Next, the original image is copied into two copies, p' and p'', and the new secret message is split evenly by Equation (3) to p' and p''. The complete hiding process is shown below:

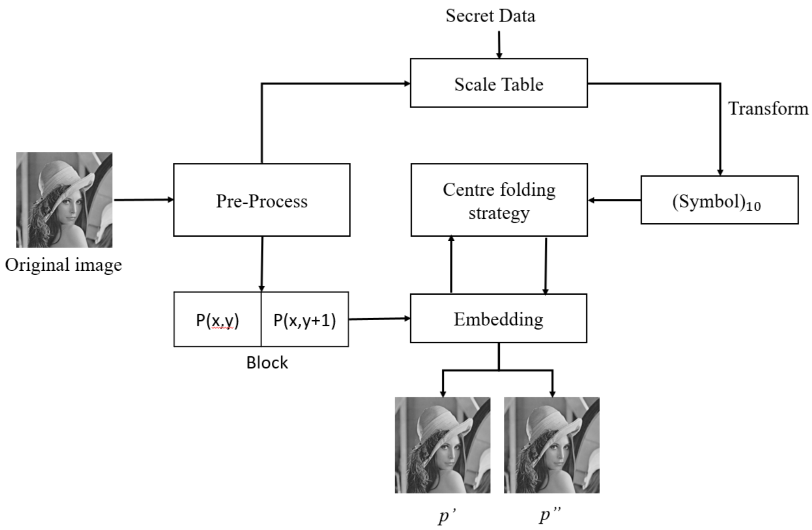

Fig. 4. The diagram of the hiding procedure

Taking the pixel pair (80, 81) as an example. The difference between the two pixels is $d = |80\text{-}81| = 1$, and then the interval scale table generated in the preprocessing is used to judge the hidden value. The value d is 1, hence the total number of the secret bits is 2 according to the interval scale table.

Taking the secret string $m = (0111)_2$ as an example, the pixel 80 can be used to hide $(01)_2$, and the pixel 81 can be used to hide $(11)_2$. Then the secret message is converted to a decimal symbol, and the center fold conversion is performed by Equation (2). Therefore, the new secret message $\tilde{m}$ will be changed to -1 and 1, respectively. The scheme copies the image into two copies, and $\tilde{m}$ will be converted to Equation (3). The calculation is evenly distributed into two images, and the new stego-pixels are (80, 80) and (79, 81).

3.3 Extraction and Recovery

In the extraction and recovery procedures, the two stego-images are first divided into 1×2 non-overlapping blocks. Because the maximum and the minimum value of the embeddable pixel is [2, 254], the scheme checks whether the stego-pixels are fall in the range [2, 254] or not. If two stego-pixels are out of range, then the pixels are non-embeddable. There are no secret data concealed in the pixels. Otherwise, if one of the stego-pixel is fall in the range, then the block is embeddable. The scheme computes the difference between the pixels in the block to get the folded message. In order to restore the secret message after the center folding, we need to know the value of k of the block first. The scheme restores the original pixels ($p_{(i,j)}$, $p_{(i,j+1)}$) through Equation (5). Then use Equation (1) and refer to the interval scale table to get the k value. The secret message can be extracted by using Equation (6). Taking (80, 80) and (79, 81) as an example. The difference of the first pixel of (80, 80) and (79, 81) is 79 - 80 = -1 and the difference of the second pixel of (80, 80) and (79, 81) is 81 - 80 = 1, respectively. Hence, the folded secret message $\tilde{m}$ are -1 and 1, respectively. The original pixels are $p_{(i,j)} = \lceil (80+79)/2 \rceil = 80$ and $p_{(i,j+1)} = \lceil (80+81)/2 \rceil = 81$.

After restoring the original pixel, the difference can be obtained by Equation (1). The interval scale table is used to obtain the k value of block, where k is 2. The final secret message is restored through Equation (6) $m = -1 + 2^{(2-1)} = (1)_{10} = (01)_2$, $m = 1 + 2^{(2-1)} = (3)_{10} = (11)_2$.

4 Experimental Results

This study is compared with the dual image interval scale method proposed by Lu et al. Six grayscale images with size 512×512 were used to test the performance of the proposed scheme. The images are shown in Fig. 5, where $h \times w$ is the original image size.

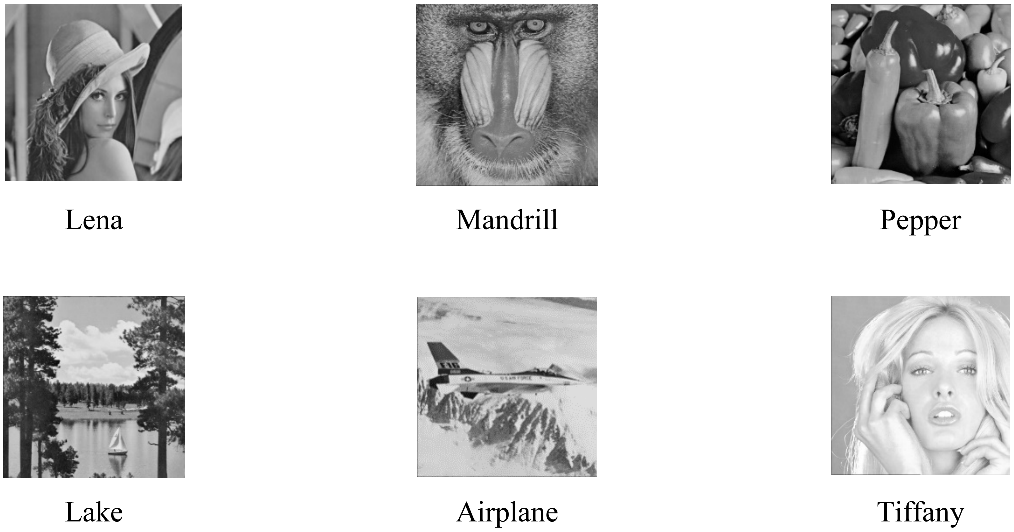

Fig. 5. Test images

Peak Signal to Noise Ratio (PSNR), MatlabR2017a's SSIM and QIndex [10] are used to measure the image quality. The formula for PSNR is as follows:

$$PSNR = 10 \times \log_{10}\left[\frac{255^2}{\frac{1}{h \times w} \times \sum_{i=1}^{h}\sum_{j=1}^{w}(p'_{ij} - p''_{ij})^2}\right] \tag{7}$$

The image quality of the first stego-image is PSNR(1) and the second stego-imaeg is PSNR(2). The average value of PSNR(1) and PSNR(2) is PSNR(Avg). The interval scale table used by Lu et al. is shown in Fig. 6.

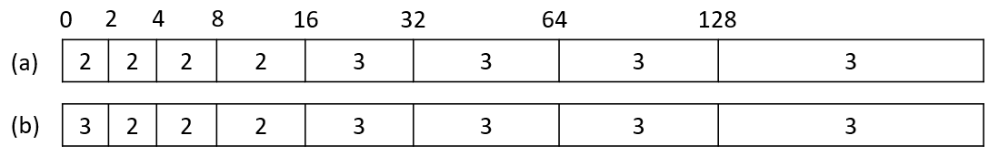

Fig. 6. The interval scale table of Lu et al.'s scheme

Table 1 shows the experimental results. From the table we can see that the hiding capacity of the proposed scheme is higher than that of Lu et.al (A). Although the hiding capacity of Lu et.al (B) is higher than that of the proposed scheme, the image quality of Lu et al.'s scheme is worse than that of the proposed scheme.

Table 1. Comparisons results of the proposed scheme and Lu et al.'s method

Method	Measurement	Lena	Mandrill	Pepper	Lake	Airplane	Tiffany
Proposed scheme	PSNR (1)	50.26	50.36	50.25	50.30	50.48	50.32
	PSNR (2)	50.25	50.36	50.26	50.29	50.48	50.31
	PSNR (Avg)	50.25	50.36	50.26	50.30	50.48	50.32
	SSIM (1)	0.9968	0.9992	0.9969	0.9981	0.9972	0.9968
	SSIM (2)	0.9949	0.9986	0.9952	0.9967	0.9950	0.9946
	SSIM (Avg)	0.9958	0.9989	0.9961	0.9974	0.9961	0.9957
	QIndex (1)	0.9997	0.9997	0.9999	0.9999	0.9998	0.9995
	QIndex (2)	0.9997	0.9997	0.9999	0.9999	0.9998	0.9995
	Qindex(Avg)	0.9997	0.9997	0.9999	0.9999	0.9998	0.9995
	Capacity	550,458	546,392	549,648	548,628	541,792	548,770

Table 1. Comparisons results of the proposed scheme and Lu et al.'s method (continue)

Method	Measurement	Lena	Mandrill	Pepper	Lake	Airplane	Tiffany
Lu et.al (k=2,2,2,2,3,3,3,3) (A)	PSNR (1)	50.78	49.91	50.86	50.52	50.86	50.90
	PSNR (2)	50.78	49.93	50.88	50.53	50.86	50.92
	PSNR (Avg)	50.78	49.92	50.87	50.52	50.86	50.91
	SSIM (1)	0.9979	0.9992	0.9978	0.9985	0.9978	0.9977
	SSIM (2)	0.9960	0.9986	0.9962	0.9971	0.9956	0.9955
	SSIM (Avg)	0.9970	0.9989	0.9970	0.9978	0.9967	0.9966
	QIndex (1)	0.9997	0.9997	0.9999	0.9999	0.9998	0.9995
	QIndex (2)	0.9997	0.9997	0.9999	0.9999	0.9998	0.9995
	Qindex(Avg)	0.9997	0.9997	0.9999	0.9999	0.9998	0.9995
	Capacity	531,426	563,164	528,882	539,768	529,128	528,546
Lu et.al (k=3,2,2,2,3,3,3,3) (B)	PSNR (1)	47.42	47.33	47.54	47.52	47.25	47.43
	PSNR (2)	47.42	47.34	47.54	47.51	47.26	47.44
	PSNR (Avg)	47.42	47.34	47.54	47.52	47.25	47.43
	SSIM (1)	0.9926	0.9977	0.9931	0.9950	0.9912	0.9917
	SSIM (2)	0.9906	0.9971	0.9915	0.9936	0.9890	0.9896
	SSIM (Avg)	0.9916	0.9974	0.9923	0.9943	0.9901	0.9907
	QIndex (1)	0.9996	0.9995	0.9998	0.9999	0.9998	0.9992
	QIndex (2)	0.9996	0.9995	0.9998	0.9999	0.9998	0.9992
	Qindex(Avg)	0.9996	0.9995	0.9998	0.9999	0.9998	0.9992
	Capacity	697,174	703,472	689,926	691,752	710,720	699,390

5 Conclusions

This paper improves the method of Lu et al.'s scheme. The scheme pre-calculates the error of all the blocks before locating and counts the statistics, and obtains the most suitable interval scale table to achieve the optimization effect.

The contributions of this paper includes

(1) Develop a pre-processing procedure to generate a suitable interval scale table for each image.

(2) Use the interval scale table to control the distortion and the hiding capacity.

(3) Find the optimal rules for different images according to the image characteristics.

The experimental results show that the PSNR, SSIM and Qindex values of the proposed scheme is better than that of Lu et al.'s scheme.

References

[1] K.-C. Choi, C.-M. Pun, Adaptive image encryption for high capacity reversible data hiding, in: Proc.2017 IEEE Conference on Dependable and Secure Computing, 1996.

[2] W.C. Kuo, C.C. Wang, H.C. Hou, Signed digit data hiding scheme, Information Processing Letters 116(2)(2016) 183-191.

[3] H. Yao, C. Qin, Z. Tang, Y. Tian, Improved dual-image reversible data hiding method using the selection strategy of shiftable pixels' coordinates with minimum distortion, Signal Processing 135(2017) 26-35.

[4] B. Jana, Dual image based reversible data hiding scheme using weighted matrix, International Journal of Electronics and Information Engineering 5(1)(2016) 6-19.

[5] B. Jana, D. Giri, S.K. Mondal, Dual-image based reversible data hiding scheme using pixel value difference expansion, IJ Network Security 18(4)(2016) 633-643.

[6] C.-C. Chang, Y.-C. Chou, T.-D. Kieu, Information hiding in dual images with reversibility, in: 2009 Third International Conference on Multimedia and Ubiquitous Engineering, 2009.

[7] T.C. Lu, C.Y. Tseng, J.H. Wu, Dual imaging-based reversible hiding technique using LSB matching, Signal Processing

108(2015) 77-89.

[8] T.C. Lu, J.H. Wu, C.C. Huang, Dual-image-based reversible data hiding method using center folding strategy, Signal Processing 115(2015) 195-213.

[9] T.C. Lu, N. Yang, T.C. Chang, Reversible hiding method based on double image using center folding strategy and interval scale, Communications of the CCISA 24(2)(2018) 1-17.

[10] Wang, Zhou, A.C. Bovik, A universal image quality index, IEEE signal processing letters 9(3)(2002) 81-84.

[11] L. P. Chi, C. H. Wu, H. P Chang, Reversible data hiding in dual stegano-image using an improved center folding strategy, Multimedia Tools and Applications 77(7)(2018) 8785-8803.

[12] H. Y. Chuan, Q. Z. J. Tang, Y. Tian, Improved dual-image reversible data hiding method using the selection strategy of shiftable pixels' coordinates with minimum distortion, Signal Processing 135(2017) 26-35.

[13] K. H. Jung, Authenticable reversible data hiding scheme with less distortion in dual stego-images, Multimedia Tools and Applications 77(5)(2018) 6225-6241.

[14] S. Shastri, V. Thanikaiselvan, Dual image reversible data hiding using trinary assignment and center folding strategy with low distortion, Journal of Visual Communication and Image Representation 61(2019) 130-140.

[15] H. Yao, C. Qin, Z. Tang, X. Zhang, A general framework for shiftable position-based dual-image reversible data hiding, in: Proc. Eurasip Journal on Image and Video, 2018.