Reversible data hiding method based on double-side histogram shifting of Image sub-blocks

Conference Paper · December 2022

1 author:

Mehmet Zeki Konyar
Kocaeli University

REVERSIBLE DATA HIDING METHOD BASED ON DOUBLE-SIDE HISTOGRAM SHIFTING OF IMAGE SUB-BLOCKS

Mehmet Zeki Konyar
Kocaeli University, Engineering Faculty, Software Engineering Department
mzeki.konyar@kocaeli.edu.tr, ORCID: 0000-0001-8914-5553

Abstract
Data hiding studies that using the images as carriers are still remain popular. One of the important reasons for this case is that it is easier to manipulate images than other carriers. In addition, images are highly preferred because they offer higher capacity than other carriers. Reversible data-hiding (RDH) approaches are also an important research area. RDH aims to restore the stego object to its original state after the extraction of secret data The most important disadvantage of reversible data hiding methods is that the data hiding capacity is lower than classical methods. In this study, in order to increase the capacity of the most known RDH method, namely the histogram shifting-based method is proposed to use double-sided shifting of the histograms of the adaptive sub-blocks in the image. In the proposed study, the peak value in the histogram of each block in the image divided into square sub-blocks is preserved, while the pixel values on both sides of the peak value are shifted and emptied. For data hiding, secret messages are added to both gap regions. After the data extraction is done successfully, the carrier image is returned to its original state. Experimental studies for Lena image is showed that while the square sub-block size was 128x128, 48.34 dB PSNR and 0.998 SSIM values were obtained for 12563 hidden bits. While the sub-block size was 8x8, 49.03 dB PSNR and 0.995 SSIM values were obtained for 33917 hidden bits. Although the hiding capacity increased as the block size decreased, there were minor changes in the visual quality metrics.

Keywords: reversible data hiding, histogram shifting, secret communication.

1. INTRODUCTION

Data hiding is a secure communication method used to hide a message inside a carrier object. In addition to military and intelligence units, illegal organizations also communicate with data hiding methods. For this purpose, a technical activity report has been published by NATO Science and Technology Organization for the use of Data Hiding methods for Information Warfare Operations [1]. It is used for secret communication and content protection in data hiding. Data hiding differs from encryption in that the object containing the message does not raise any suspicion at first glance. The sender must use a data hiding algorithm to transmit the secret message to the receiver. With this algorithm, a stego object is obtained by hiding the secret message inside the cover object. The receiver uses stego object and data extraction algorithm to extract the secret message. The use of a key for the security of communication is also a preferred method.

The most used cover files for data hiding are images. Because they offer high capacity, and they can be processed more easily. In addition, videos [2], medical images [3], sounds [4] are also used for data hiding. Data is hidden in images with spatial domain or transform domain approaches. Spatial domain methods are more susceptible to attacks or disruptive effects. The capacities of data hiding in the transform domain may be less than the spatial domain methods. However, spatial methods are easier to implement than transform domain methods. Methods such as the least significant bit (LSB) [5], exploiting modification direction, EMD [6], pixel value differencing, PVD [7], histogram shifting come to the fore for data hiding in the spatial domain [8]. These methods can be applied not only to the brightness channel of the image, but also to all color channels. Wavelet transform [9], DCT [10] and DFT [11] based methods are generally used in data hiding studies on the transform domain.

After removing the hidden message from the hidden stego object, reversible methods have emerged to obtain the original cover object. The most basic reversible data hiding method is shifting the histogram distribution. In the histogram distribution method, which was first proposed in the [8] study, the values between the histogram peak value and the max pixel value are shifted one right and the side of the peak is emptied. Pixel values are scanned for each bit of the secret message. As for the peak value, if the secret message is 0, the peak value is not changed, if the secret message is 1, the peak value is increased by one. After the hiding process is completed, the stego object is obtained after the value of the peak point is hidden in the image. The receiver looks for the peak in the stego image histogram and the value of its right to extract data. If the corresponding pixel value is equal to the peak, the hidden message bit is 0, if the peak point is equal to the value 1, the hidden message is output. After the secret message extraction is finished, the pixel values are shifted to their previous places. Thus, both the secret message and the original cover object are obtained.

The most important disadvantages of histogram methods are that their hiding capacity is limited to the peak value, and they have to send the peak value information to the receiver. To solve this problem, the [12] method used pairs of pixels on the right or left of the vertex, depending on whether it is odd or even. While the [13] study used the value to the right of it instead of the peak, the [14] study used as a multi-level histogram. In the [15] study, histogram shift-based data are hidden in JPEG image coefficients. [16] suggested the use of adaptive block sizes to increase data hiding capacity based on histogram shifting. Near maximum histogram and LSB methods were utilized in the [17] study, which is a continuation of the [12] study.

2. MATERIALS AND METHODS

In this paper, it is proposed to use double side of the histogram peak to increase data embedding capacity. Also, instead of overall histogram that used by most of the previous methods, in this paper histogram of the adaptive sub-blocks used for embedding. The proposed method is providing a lossless and reversible data hiding by using the histogram shifting. Proposed method uses two side, namely the right and left values of the histogram peak value of the sub-blocks are shifted. Secret data is embedded with second right and second left nearest value of the histogram peak. If the secret message bit is 0 then keep these pixels same. If the secret bit is 1, then increase or decrease the values of second left or second right pixel of peak value respectively. The detail of the proposed method is given step by step as follows:

1. Get the grayscale cover images with size of 512x512 pixels
2. Divide the cover image into equal sub-blocks. The square sub-block size is start from 512x512 and shrinks to the 4x4. For each size the following operations are done separately
3. Obtain the histogram of the sub-block of the cover image.
4. Get the peak (P) value of the histogram
5. Shift left the histogram value of left side between P-1 and 1.
6. Shift right the histogram value of the right side between P+1 and 254.
7. Now the bins of P-1 and P+1 are free. There is no intensity/pixel value has P-1 or P+1 in the sub-block.
8. Get secret message bits (0 or 1)
9. Scan the sub-block pixels and find the pixel value that has P-2 or P+2
10. Embed the secret bits to the image as follows:
    a. If the secret message bit is 0 do nothing
    b. If the secret message bit is 1 and pixel value is P-2 then increase this pixel value to P-1
    c. If the secret message bit is 1 and pixel value is P+2 then decrease this pixel value to P+1
11. Repeat the step 3-8 for all sub-blocks for the same size.
12. Obtain the stego image
13. Change the sub-block size and repeat the previous operation.

The embedding procedure is continued until all sub-blocks utilized for data hiding. After the embedding is finished the stego image was sent to the receiver. In the data extraction phase, the receiver gets the secret message as embedding levels. The receiver starts to scan sub-blocks. If the pixel value is P-1 or P+1 then save the secret message value as 1 and recover the pixel to the P-2 or P+2. If the scanned pixel value is P-2 or P+2, then save the secret message value as 0 and keep the pixel value same. If all blocks scanned, then the sub-blocks histogram of left side between 0 and P-2 shift to the right. The histogram of right side between P+2 and 255 shifts to the left. As a result of these processes, both the hidden message is completely extracted and the stego image is recovered to its original cover image.

3. EXPERIMENTAL RESULTS

In the experimental results four common test images Lena, Baboon, Airplane and Fruits used with size of 512x512 in grayscale. The test images are given in Fig.1. An English text is converted into a binary bitstream to use as secret message. The performance of the proposed method is evaluated with image quality metrics [3] Peak Signal-Noise Ratio (PSNR), Multi-structure similarity index (SSIM) and embedding capacity.

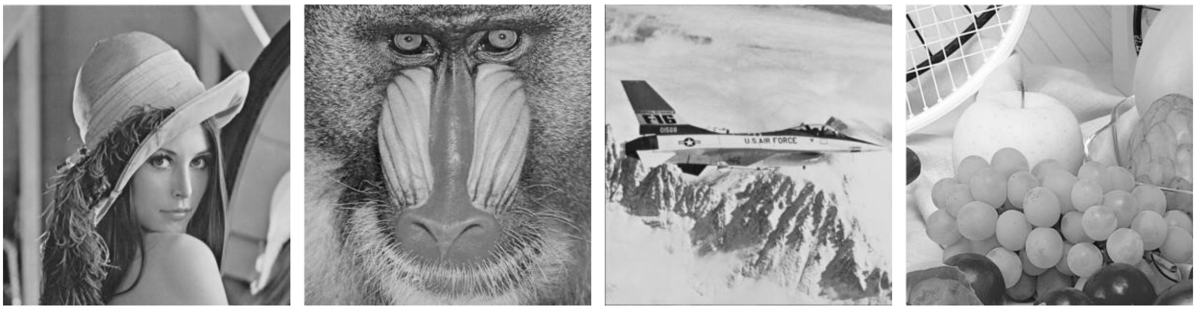
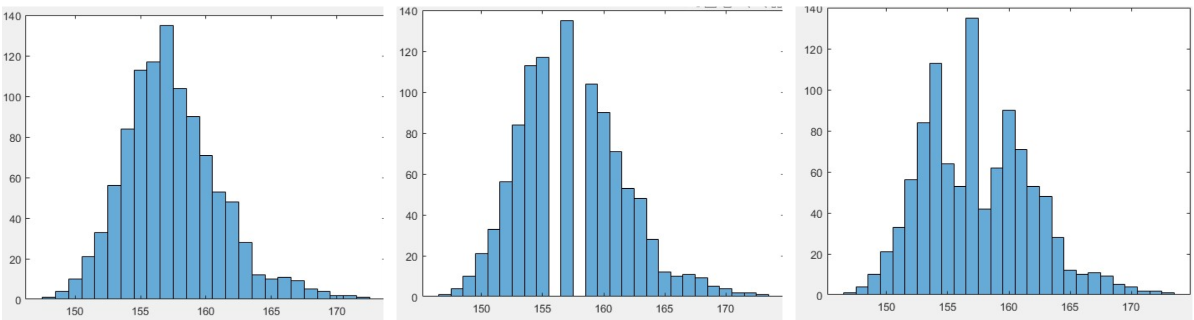


Figure 1. The test images: Lena, Baboon, Airplane and Fruits

The histogram of a sub-block, shifting operations and embedding operation of the proposed method is given in the Fig.2. First, the peak value of sub-block is detected. Then, the two sides of the peak value is emptied. According to the secret bits the pixel values of the nearest right or left sides of the peak value are modified. The embedding process is continued until there is any pixel has P-2 or P+2 value. When all the blocks used for data hiding, the stego image is obtained and sent to the receiver. The receiver can easily detect the peak value of each block. Because there is not any modification for the peak values of all blocks. So, the secret data extracted easily.

The test results of the proposed method are given in Table 1 for PSNR (dB), SSIM and Capacity (bits). PSNR and SSIM shows the visual quality. According to the Table 1, PSNR is over the 48dB at least. The SSIM varied between 0 and 1, where the highest value is better. The SSIM values are closed to 0.99 for all block sizes. Based on the PSNR and SSIM result, it can see that the visual quality of the stego images is good enough. But the visual quality is not only enough to evaluate data hiding. Another important parameter for evaluation is embedding capacity.



(a) (b) (c)

Figure 2. The histogram shifting and embedding operations of the proposed method (a) original histogram of sub-block, (b) right and left shifted histogram, (c) histogram of the stego sub-block

In the proposed method embedding capacity is increased when the image divided into sub-blocks, where the visual qualities are nearly same. Because of the double side embedding, the embedding capacity of the proposed method for the undivided image is better than many literatures. The embedding capacity of the 4x4 block is a little lower than 8x8 blocks because in the 4x4 blocks contains too low pixel values. Thanks to the sub-block's histogram method, proposed method increases the embedding capacity remarkable.

Table 1. Experimental results of proposed method for stego images

	Airplane			Baboon			Fruits			Lena		
Block size	PSNR	SSIM	Cap.	PSNR	SSIM	Cap.	PSNR	SSIM	Cap.	PSNR	SSIM	Cap.
512	48,39	0,998	15347	48,22	0,999	5269	48,25	0,999	6976	48,22	0,999	5285
256	48,53	0,998	23254	48,22	0,999	5615	48,30	0,999	8290	48,28	0,998	8963
128	48,61	0,998	26783	48,25	0,999	7124	48,42	0,998	14133	48,34	0,998	12563
64	48,75	0,997	32348	48,29	0,998	8754	48,55	0,998	19040	48,45	0,997	18127
32	48,91	0,996	38660	48,34	0,998	10595	48,74	0,997	26405	48,59	0,996	24049
16	49,12	0,996	44001	48,41	0,998	11387	49,03	0,995	35389	48,77	0,995	29510
8	49,40	0,995	47714	48,54	0,998	11789	49,38	0,995	41394	49,03	0,995	33917
4	49,87	0,995	46386	48,86	0,998	10961	49,90	0,995	41888	49,47	0,995	33275

4. CONCLUSION

In this study, a reversible data hiding method is proposed. In the proposed method, the image is divided into sub-blocks and the histogram of these blocks used for embedding procedures. The peak value of the histogram distribution is obtained, and double side of the peak is emptied. The secret bits embedded to the emptied bins and their first neighbors. Proposed method increases the embedding capacity of the histogram-based data hiding method with two contributions. Firstly, using the double side nearest value of peak value provides higher capacity than single side methods of the literature. The second contribution of the proposed method for high capacity is dividing the image into sub-blocks. Instead of the one peak value of biggest image, this paper proposes to use a lot of different peak values for every sub-block histogram. Proposed method increases the secret message capacity remarkable while the visual quality of the stego image is almost same.

ACKNOWLEDGEMENTS

The author would like to acknowledge the support of Kocaeli University Software Technologies Research (STAR) Laboratory for this study.

REFERENCES

[1] NATO Science and Technology Organization (STO), 2022, Data Hiding in Information Warfare Operations, Available at: https://www.sto.nato.int/publications/Pages/Technical_Reports_List.aspx [Access Date: 28.11.2022]

[2] Kaçar, S., Konyar, M. Z., & Çavuşoğlu, Ü. (2022). 4D chaotic system-based secure data hiding method to improve robustness and embedding capacity of videos. Journal of Information Security and Applications, 71, 103369.

[3] Konyar, M. Z., & Öztürk, S. (2020). Reed Solomon coding-based medical image data hiding method against salt and pepper noise. Symmetry, 12(6), 899.

[4] Altinbaş, A. E., & Yalman, Y. (2021, September). Bit Reduction Based Audio Steganography Algorithm. In 2021 6th International Conference on Computer Science and Engineering (UBMK) (pp. 703-706). IEEE.

[5] Sahu, A. K., & Swain, G. (2019). High fidelity based reversible data hiding using modified LSB matching and pixel difference. Journal of King Saud University-Computer and Information Sciences.

[6] Solak, S. (2020). High embedding capacity data hiding technique based on EMSD and LSB substitution algorithms. IEEE Access, 8, 166513-166524.

[7] Singh, S. (2020). Adaptive PVD and LSB based high capacity data hiding scheme. Multimedia Tools and Applications, 79(25), 18815-18837.

[8] Ni, Z., Shi, Y. Q., Ansari, N., & Su, W. (2006). Reversible data hiding. IEEE Transactions on circuits and systems for video technology, 16(3), 354-362.

[9] Zhang, H., Sun, S., Hu, L., & Meng, F. (2022). A novel data hiding scheme based on improved diamond encoding in IWT domain. Multimedia Tools and Applications, 1-19.

[10] Sabeti, V., & Aghabagheri, A. (2022). Developing an adaptive DCT-based steganography method using a genetic algorithm. Multimedia Tools and Applications, 1-24.

[11] Melman, A., & Evsutin, O. (2022). Comparative study of metaheuristic optimization algorithms for image steganography based on discrete Fourier transform domain. Applied Soft Computing, 109847.

[12] Kurnaz, H., Konyar, M. Z., & Sondaş, A. (2020). Yakın Histogramlar Temelli Yeni Bir Hibrit Veri Gizleme Yöntemi. Avrupa Bilim ve Teknoloji Dergisi, (18), 683-694.

[13] Islamy, C. C., & Ahmad, T. (2019). Histogram-based multilayer reversible data hiding method for securing secret data. Bulletin of Electrical Engineering and Informatics, 8(3), 1128-1134.
[14] Jabbari, F., & Sedaaghi, M. H. (2019). Adaptive multilevel technique based on histogram shifting for reversible data hiding. Multidimensional Systems and Signal Processing, 30(3), 1563-1581.
[15] Li, Y., Yao, S., Yang, K., Tan, Y. A., & Zhang, Q. (2019). A high-imperceptibility and histogram- shifting data hiding scheme for JPEG images. IEEE Access, 7, 73573-73582.
[16] Lee, C. W., & Tsai, W. H. (2010). A lossless data hiding method by histogram shifting based on an adaptive block division scheme. Pattern Recognition and Machine Vision, 1-14.
[17] Sondas, A., & Kurnaz, H. (2022). HNMH: A New Hybrid Approach Based on Near Maximum Histogram and LSB Technique for Image Steganography. Wireless Personal Communications, 126(3), 2579-2595.