Journal of Computers Vol. 32 No. 4, 2021, pp. 13-24
doi:10.53106/199115992021083204002

Image Steganography Based on the Absolute Value of Adjacent Pixels

Xiao-Ge Pan[1], Tian Yang[1], Ning Jia[2], Pan-Pan Zhao[2], Ming-Wei Tang[1*]

[1] Department of Computer Science and Software Engineering, Xihua University, Chengdu 610039, China
{Pan085211@126,yangtian184@163,tang4415}@126.com

[2] Department of Electronic and Communication Engineering, Chengdu University of Information Technology, Chengdu 610039, China
{jianing5541@163,zhaopp96}@126.com

Received 2 November 2020; Revised 7 February 2021; Accepted 15 March 2021

Abstract. The development of the Internet has provided great convenience to people's lives, but there are also many problems. Among them, the information security problem is particularly serious. As an important online and offline information communication medium in the Internet, Quick Response (QR) Code has also begun to stand out in the Internet field. This paper uses the combination of two-dimensional code and information hiding technology as the core of secure communication. This method makes use of the large amount of information encoded by the QR code and the high anti-fouling characteristic. Firstly, the secret message is encoded to improve the hidden capacity and the secret message is anti-offensive. Then, according to the image steganography technology of adjacent pixel to an absolute value (AVAP), the steganography of secret message is carried out by comparing with corresponding data bits to ensure the image quality. The experimental results show that compared with the existing LSB steganography methods, the steganographic images not only have better quality, but also have a higher payload. In addition, this method solves the security problem in the field of information hiding by implementing double encryption from the perspective of secret message and carrier.

Keywords: AVAP, image steganography, information security, LSB

1 Introduction

With the development of the Internet and high-resolution display technology [1-4], the transmission of information security has attracted much attention through shared channels. Currently two feasible solutions are: cryptography and image information hiding. Cryptography improves the security of secret information through scrambling based on symmetric or asymmetric keys. However, the main disadvantage of cryptography is that it gives suspicious attention to unauthorized intruders. Image information hiding utilizes the statistical redundancy of image data and human perception redundancy to hide meaningful secret information into the image,and unauthorized persons cannot confirm whether the information is hidden in the carrier to achieve the purpose of covert communication [5]. At present, most of the research on information hiding technology focuses on information hiding of digital images. Information hiding using natural images as the public carrier is mainly due to the large internal correlation of natural images and the existence of redundant information, which is suitable for information hiding. This redundant information in natural images allows us to hide information in it without attracting the attention of third parties.

In recent years, image steganography [6] has received extensive attention in the research, development and application of digital communication. Image information hiding technology presents diversified development, including least significant bits (LSB), discrete Fourier transform (DFT), discrete cosine

[*] Corresponding Author

transform (DCT) [7], the discrete wavelet transform and transform domain method [8], and the height of the improved security cannot detect steganographic algorithm [9], general wavelet relative distortion method in airspace [10], wavelet weighting method content such as adaptive steganography [11], etc. Although these traditional steganographic methods have been gradually improved in transparency and security, there is still room for improvement in steganographic capacity and robustness. The level of image quality, anti-distortion capability and security of secret images have been the major concerns in the past decade [12-17].

With the rise of two-dimensional code, the research of combining information hiding technology with QR code has gradually increased. The research of two-dimensional code concealment is mainly divided into two kinds, such as two-dimensional code as a carrier and two-dimensional code as a secret message. For the former, L. Xue converts the watermark information into binary values and embeds the digital watermark by shifting the PDF147 barcode [18]; S. Vongpradhip proposes a reversible information hiding algorithm in the frequency domain of QR codes [19]; The fact that mobile phones are currently being used extensively has proposed an offline QR code authentication method [20]. Compared with the former, the research on two-dimensional code as a secret message is relatively backward, but with deepening of the research, certain research results have been achieved. For example: D. Shehzad and T. Dag embed the secret message QR bar code into the carrier image [21]; The authentication information of the video was used to generate digital watermark through QR barcode, and then it was embedded into the video information with SVD (singular value decomposition) and DWT technology [22]. PDF147 encoding is applied to secret messages before embedding [23], and human vision system (HVS) features are combined in the embedding algorithm [17]. A security copy system based on two-digit barcode QR code is proposed [24].

In this paper, an efficient image steganography algorithm is proposed based on QR-coded and pixel-to-absolute values. First, the large amount of information and anti-attack of the QR code encoding are used to encode secret information to form cover information to improve security. Then, according to the image steganography technology of the absolute value of adjacent pixels (AVAP), the steganography of the ciphertext is performed by comparing with the corresponding data bits to ensure the image quality. Steganography is usually evaluated by image performance indicators, such as peak signal-to-noise ratio (PSNR) and mean square error (MSE). In image steganography based on QR-coded pixel-to-absolute values, in order to evaluate the prominence of the proposed technology, we considered different attributes proposed in [25-27]. The experimental results show that, compared with the existing LSB steganography methods, AVAP steganography images not only have better quality, but also can withstand certain noise attacks. In addition, the advantage of this method is to realize double encryption from the perspective of secret message and carrier, and solve the security problem in the field of information hiding.

2 Background

2.1 LSB Substitution Method

The least significant bit LSB [28] algorithm embeds the secret message into the least significant bit of the pixel value of carrier image, which is one of the typical algorithms in the spatial domain. The core of the algorithm is to use the secret message to replace the lowest binary bit of the carrier image. The secret information can be extracted from the lowest binary bit of carrier image. The LSB algorithm changes the lowest bit of the image because the lowest bit plane of the image has noise-like characteristics and the human visual system is not sensitive to this. This algorithm has the characteristics of simplicity, large amount of embedded data, and small changes to the information of the image. It is widely used in image steganography. For general RGB images, each color component corresponds to a byte in the computer. The carrier image can be abstracted into a byte stream, and the secret message can be converted into 0,1 binary bit stream.

Assume that the byte stream of the carrier image is:

$$C = B_1 B_2, \ldots, B_n, B_i = b_{i1} b_{i2}, \ldots, b_{i8} = 1, 2, ..., n. \tag{1}$$

The secret information bit is:

$$M = m_1 m_2, \ldots, m_l. \tag{2}$$

The LSB algorithm selects the embedding bit from each byte of the byte stream of the carrier picture, replaces b_{i8} at the agreed position with m_k, and the secret message image is expressed as:

$$C' = B_1' B_2', \ldots, B_n'. \tag{3}$$

If the secret information is embedded in the BMP bitmap of the RGB channel, the length of the bitmap is m pixels and the width is n pixels. A binary number can be written in each color channel, that is, the BMP bitmap in the RGB channel can be written. The capacity of the embedded secret information is m×n×3/8 bytes. Similarly, for grayscale images, the capacity of embeddable secret information is m×n/8.

When using LSB for embedding, for the BMP bitmap of RGB channel, R, G and B channels can be operated respectively. Each pixel of each channel is independent, and each pixel can be converted into an 8-bit binary group. For example, the pixel value is 139, and the conversion result is 10001011. Assuming that the secret message to be written is 0, according to the LSB algorithm, the pixel value is modified to 10001010, and the corresponding pixel value is 138. By replacing the original value of the corresponding position of the carrier image with this pixel value, the embedding of one bit of secret information is completed. In this way, the changes to the pixel values of the picture are small, the least significant, and the embedded secret message is invisible.

2.2 Quick Response (QR) Code Technology

QR code [19] is a graphic that uses features to represent information through different permutations and combinations on a plane, and uses black and white color features of geometry to represent data information. The secret information is extracted by analyzing the arrangement of the black and white blocks. The meaning is different under different code systems. Adjusting the arrangement can get different degrees of error correction. According to the coding principle of two-dimensional codes, they can be roughly divided into two categories: linear stacked barcodes [17] and matrix-type two-dimensional codes [19].

The QR code in the matrix two-dimensional code is a code system with a high degree of social application at present. Compared with other coding systems, QR code has the advantages of high information density, wide coding range, strong fault tolerance, and high decoding reliability. Therefore, the QR code used in this article. The QR code supports a variety of information types, including text, pictures, URL links, audio, video, etc. QR code is a square matrix composed of several black and white square modules arranged into an encoding area and a functional graphics area. The dark module represents the binary '1' and the light module represents the binary '0'. To adapt to adjustment, the supported data types include numeric data, alphanumeric data, 8-bit byte data, and Chinese Kanji character data.

The QR code uses four standardized coding modes to convert the data content into two-dimensional code graphics, and the decoding process of scanning and reading to complete the output of the data content is the inverse process of coding (see Fig. 1).

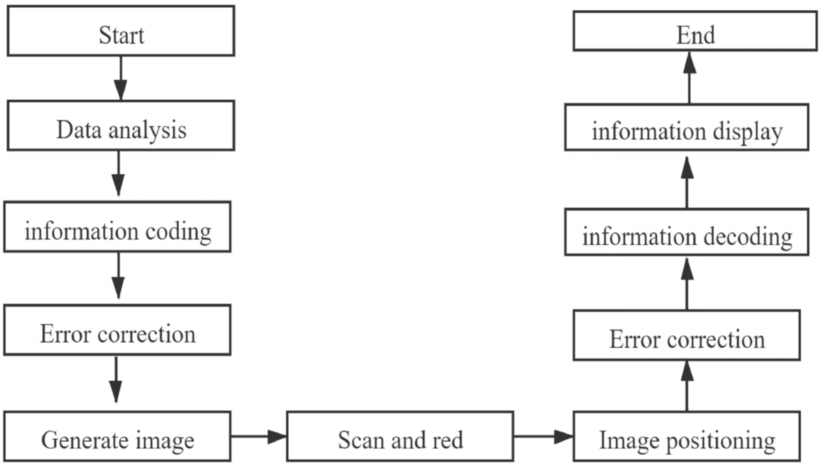


Fig. 1. QR code encoding and decoding process

3 Related Work

The concept of pixel value difference was proposed by Wu [6] et al. The method showed an improvement in terms of embedding capacity as compared with the LSB and LSBMR methods. [29] and Swain [30-31] used the same block structure as the method of Wu et al. [6], but the embedding method was different. The above methods all have overflow problems. The method discussed by Khodaei and Faez [32] uses a block structure with three horizontal pixels. Compared with the method of Wu et al., this method improves the embedding ability. Because it forms two pixel pairs and three horizontal pixels. It has no overflow and underflow problems. The main disadvantage of the above methods is that they cannot use edge values in all directions.

With the rise of edge detection technology, many edge detection methods have emerged, such as: Roberts, Prewitt, Sobel, Kirsch, Log, Canny, Laplacian, etc. In order to extract more edge pixels, in recent years, many researchers have combined several traditional edge detection operators and used hybrid edge detectors to identify the edge of the image. A hybrid edge detection method is also used in reference [10], which forms edge images by using Prewitt and Canny edge detectors. A hybrid edge detection method is also used in reference [15], which forms an edge image by using two edge detection methods, Canny and Sobel. Although the image quality is guaranteed, the embedding capability is limited.

In addition, none of the methods discussed consider the individual contribution of the color plane in the color formation process in the human visual system, and our method considers the influence of the selected color plane when determining the number of bits in the pixel pair to be embedded. And considering the security, we encrypt the secret message once and redesign the cover mode.

4 Proposed Technique

In this section, the paper proposes an image steganographic scheme using QR coding and the absolute value of adjacent pixels. For QR coding, its design purpose is to solve a large amount of information and a series of error correction problems. The cover image is decomposed into pixel pairs using a sliding window, and then the secret bits are embedded into each pair of pixels (p_i, p_{i+1}) based on parity classification.

Compared with existing steganography schemes, the proposed scheme can effectively avoid the burden caused by embedding additional information, and at the same time guarantee the security of secret messages. The proposed technology includes four stages. The first stage is to encrypt the secret message using QR coding, the second stage is to embed the encrypted secret message, the third stage is to realize the extraction of secret information, and the final stage is to decrypt the extracted message.

4.1 QR Code for Secret Information

In this stage, the QR code is applied to process the preprocessing from the secret image I_s. Ensure that extra information can be stored more securely when embedding secret bits in the original image I_c. Therefore, the payload is significantly increased without affecting the hidden image quality.

Firstly, we analyze the data type of secret information. Secondly, the coding mode with the highest coding efficiency is selected according to the analysis results. Finally, the original information is converted into the corresponding binary bit stream to complete the information encoding. The codewords are divided into blocks according to the amount of data, and the corresponding error correction information codes are generated according to the blocks using error correction coding techniques, and then they are combined into the final error correction codes in the order of block division. The data content and the error correction information codes are combined into a final data code, and then a QR code image Q_s is generated by mask processing.

4.2 Embedding

The process of generating QR codes from secret messages has been discussed in Section 4.1. In this section, the process of embedding secret information in the cover image will be discussed in detail. First, the cover image is decomposed into pixel pairs (p_i, p_{i+1}) using a sliding window. The decimal value of 3LSBs for each pixel pair can be calculated, and the difference from the above value can also be calculated. Since one bit secret message can be inserted into one pixel pair, a w-bit secret message will be inserted into the w pixel pairs of the cover image. There are the following four correspondences between the difference between the pixel pairs and the bits of the secret message:

1. The absolute value of the w^{th} group is even and the w^{th} bit of the secret data is 0.
2. The absolute value of the w^{th} group is odd and the w^{th} bit of the secret data is 1.
3. The absolute value of the w^{th} group is odd and the w^{th} bit of the secret data is 0.
4. The absolute value of the w^{th} group is even and the w^{th} bit of the secret data is 1.

If the difference between the pixel pairs and the message bit to be inserted are both odd or even, there is no need to modify any pixels in the block. Therefore, for the first two cases above, the value of the pixel pair does not need to change. When case 3 occurs, by changing the value in the pixel value pair, the difference becomes odd. In the same way, the situation is the same in case 4. In the same way, the situation is the same in case 4.

The process of encoding is also illustrated as a flowchart in Fig. 2.

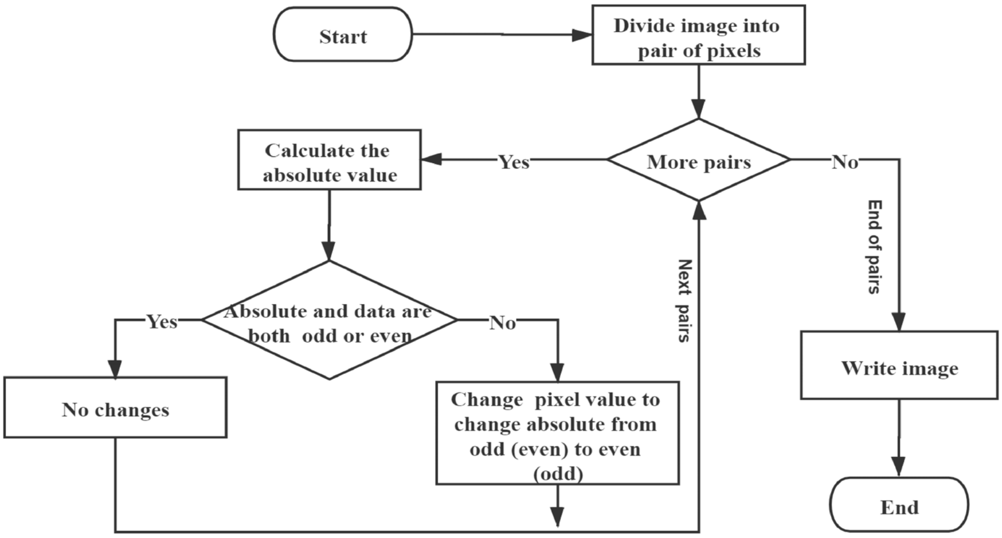

Start
Divide image into pair of pixels
More pairs
Yes
No
Calculate the absolute value
End of pairs
Next pairs
Absolute and data are both odd or even
Yes
No
No changes
Change pixel value to change absolute from odd (even) to even (odd)
Write image
End

Fig. 2. The flowchart for the encoding process of AVAP

The method of changing the pixel value of a group and converting an absolute value from odd to even or from even to odd is as follows:

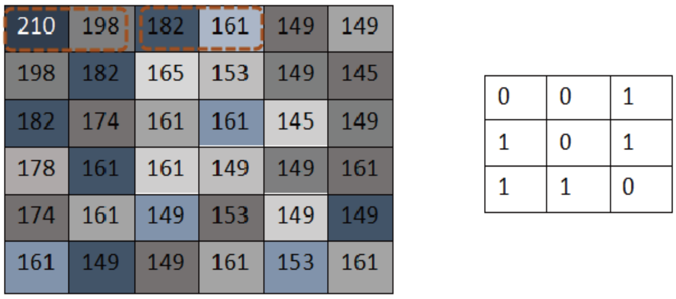
$$A=| p_1 - p_2 |. \quad \textbf{(4)}$$

A is a pixel pair of the cover image, which contains the element values (p_i, p_{i+1}) calculated from the 3LSBs of the corresponding pixel. The difference of block A can be calculated as follow:

$$\begin{gathered}\text{1. if A=|o-o|, then A=E; 2. if A=|e-e|, then A=e} \\ \text{3. if A=|o-e|, then A=o; 4. if A=|e-o|, then A=o.}\end{gathered} \quad \textbf{(5)}$$

Therefore, if the difference between pixel pairs needs to be converted from even to odd or from odd to even, the combination of Equation 2 can be used. There are four different combinations that can change the parity of the difference between pixel pairs. Among the 4 combinations, 2 combinations produce an odd difference and 2 combinations produce an even difference.

The following example illustrates the encoding method. Assume a monochrome cover image with 6x6 pixel values as shown in Fig. 3(a) The secret message to be embedded is shown in Fig. 3(b). The cover image is divided into blocks with a size of 1x2 pixels, as shown in Fig. 3(a)



210	198	182	161	149	149
198	182	165	153	149	145
182	174	161	161	145	149
178	161	161	149	149	161
174	161	149	153	149	149
161	149	149	161	153	161

(a)

0	0	1
1	0	1
1	1	0

(b)

Fig. 3. Data encoding example

The pixel values for first block are 210 and 198. When represented in binary these values are 11010010 and 11000110. Therefore, the block matrix of the first block obtained by mining 3LSBs from each block is shown in Eq.6.

$$A = |2 - 6| = 4. \qquad \textbf{(6)}$$

Since the determinant of the block is even and the first secret data bit to be inserted is 0, no changes will occur in the block. Thus, the bits of data entering the first block are hidden in the cover image without changing the individual pixel values of the block.

The pixel values for the second block are 182 and 161. When represented these values are 10110110,10010101. the block matrix of the first block obtained by mining 3LSBs from each block is shown in Eq.7.

$$A = |6 - 5| = 1. \qquad \textbf{(7)}$$

For the second block, the secret bits to be inserted are 0, but the absolute value is odd. The form of the block matches case 4 of formula 5. In order for the absolute values to be even, this can be converted to Case 1 of Eq. 5 by changing one bit in the block. Convert the LSB of the last pixel, and the second block will take the form shown in Eq.8 below:

$$A = |7 - 5| = 2. \qquad \textbf{(8)}$$

In the Stego image, the pixel values of the third block are 183 and 161.

4.3 Extracting

This section focuses on extracting secret information from I_c. A flowchart of the extraction phase in detail (see in Fig. 4). In the same embedding process, I_s is decomposed into pixel value pairs (p_i, p_{i+1}) using a sliding window. Calculate the difference between the 3LSBs of pixels in each pixel pair. Then extract the secret message through the following three steps:

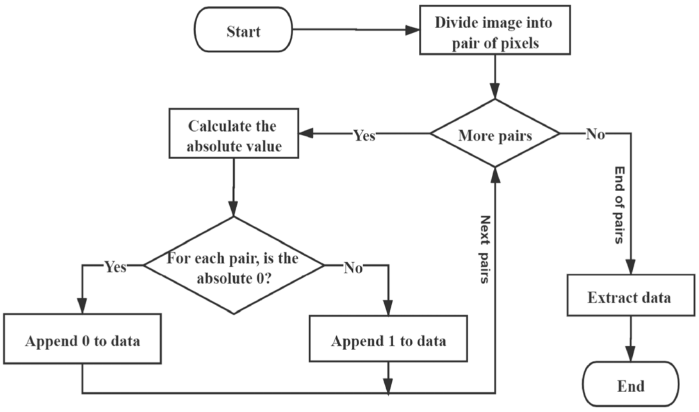


Fig. 4. The flowchart for the decoding process of AVAP

1. If the absolute value of the w^{th} group is even, then the confidential data of w^{th} is 0.
2. If the absolute value of the w^{th} group is odd, then the confidential data of w^{th} is 1.
3. All the extracted data bits are concatenated to form secret data.

The extraction process is shown in the Fig. 4.

4.4 QR Decoding of Secret Information

The direction and position of the QR code are determined by the image finding and positioning figures, the image is corrected, and the sampling network is determined. Identify deep and light modules, read format information and version information, eliminate masks, recover data content and error correction information codes, and use error correction codes for error checking. The data information is decoded after error correction. Output data content.

In summary, when the data bit is consistent with the absolute value, there is no need to change the data bit. When the data bit is not consistent with the absolute value; the pixel pair is changed logically and calculated to ensure that the pixel is encoded during the data encoding. The changes are minimal, resulting in minimal effects and better stego image quality.

5 Experimental Setup and Results

The performance of the proposed scheme is compared with edge detection (ED), LOG edge detection (LOG) and adjacent pixel value (PV). The image quality and stego image distortion tolerance were evaluated after using different methods. In the implementation, four standard images of size 512×512 (Fig. 5(a) to Fig. 5(d)) hide secret images of size 128×128. In order to evaluate the results obtained by our proposed method and other methods, we used the peak signal to noise ratio (PSNR) as the performance index to compare the hidden results. It is a mathematical image quality recognition method based on the pixel difference between the original image and the walk test image. The value of PSNR is calculated as follows:

$$PSNR = 10 * \log \frac{(255)^2}{MSE}. \tag{9}$$

(a)Lean

(b)Jet

(c)Sailboat

(d)pepper

Fig. 5. Standard images used as host images (512×512) (a)-(d)

MSE is used as a commonly used distortion measurement method to perform quality detection on images. The MSE calculation method for stego images is to square the average intensity of the input image and the stego image, as defined below:

$$MSE = \sqrt{\frac{\sum_{i=1}^{M}\sum_{j=1}^{H}(x_{(i,j)} - x'_{(i,j)})^2}{M * H}}. \tag{10}$$

Where $x_{(i,j)}$ and $x'_{(i,j)}$ are the corresponding pixel intensities of the host image and stego image with size M×H, respectively.

To illustrate the effectiveness of AVAP, a secret data of 6 KB is embedded in four different color images Lena, Jet, Sailboat and Pepper of size 512×512 pixels for comparison. For the evaluation of AVAP encoding mechanism, when PSNR are compared; AVAP has the highest PSNR as shown in Table 1. For the classic stego image generated by application of AVAP encoding method PSNR of 63.75 dB is calculated. The visual comparison between images shows that data embedment in these colored images do not have any noticeable affect the pixel values of original cover images confirming the quality of AVAP method.

Table 1. PSNR results of each host image

Host Image	ED [10]	LOG [15]	PV [6]	AVAP
Lena	48.19	58.42	53.70	63.75
Jet	47.49	58.81	50.85	63.75
SailBoat	47.49	57.52	49.77	63.75
Pepper	47.50	59.02	47.88	63.75

Table 2 shows the MSE comparison results of host image and stego image in all methods. The larger MSE, the better the result of image restoration. As can be seen from the table, the MSE results of this method are lower than other methods. Thus, proposed method MDS is more secure, have minimal effect on cover images and reliable than other image steganography techniques.

Table 2. MSE results of each host image

Host Image	ED [10]	LOG [15]	PV [6]	AVAP
Lena	0.987	0.093	0.278	0.027
Jet	1.159	0.085	0.535	0.027
SailBoat	1.158	0.115	0.686	0.027
Pepper	1.156	0.081	1.597	0.027

One of the most common image sizes used to test image processing algorithms is 512×512. We have tested our algorithm for different 384×512 test images. The results obtained have been compared with several traditional prior art and are shown in Table 1. In order to better illustrate the generality of the method, 300 random graphs of arbitrary size were selected from the library for further comparison. It can be seen from Fig. 6 that for different types of images, the PSNR of AVAP is higher than that of other images. Compared with the method of LOG edge detection, AVAP method does not depend on the type of image. No matter what kind of image, the PSNR is stable between 60 and 70 and will not fluctuate greatly.

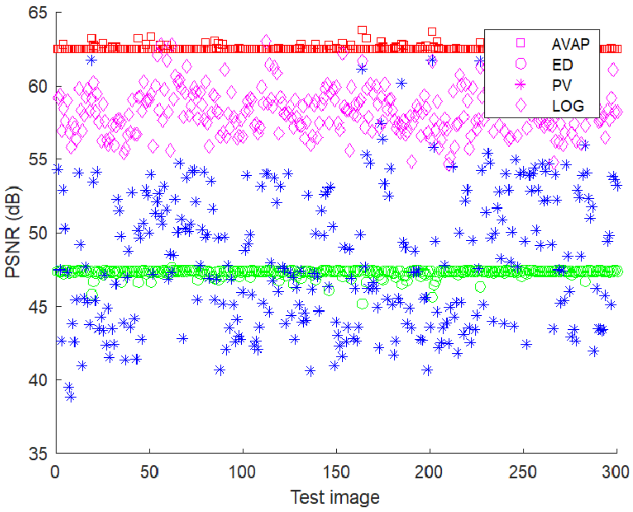


Fig. 6. The flowchart for the decoding process of AVAP

In addition to comparing the PSNR of the images, Fig. 7 also compares the image recovery capabilities. It can be seen from the figure that the MSE is also at its lowest. In summary, the method proposed in this paper obtained the best quantitative evaluation results.

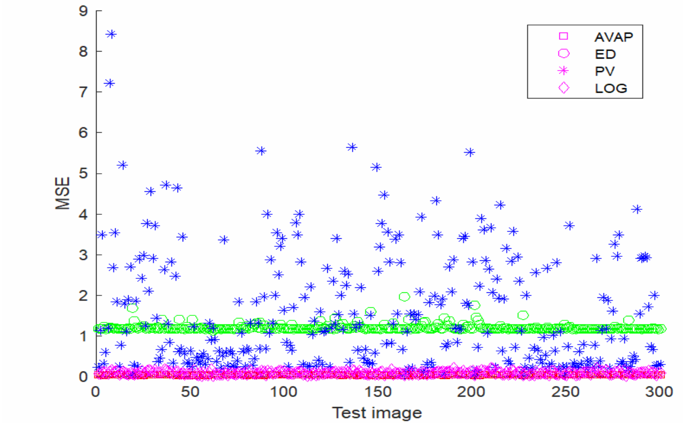


Fig. 7. The flowchart for the decoding process of MSE

In terms of capacity, the method of LOG and ED based on edge detection has a larger capacity to hide the image with obvious line spacing, otherwise, the capacity is smaller. The AVAP proposed in this paper is steganography based on pixel pairs, so there will be no large deviation due to the type of picture. This method is qualitatively analyzed. Histogram analysis is one of the important types of stealth analysis, where pixel-by-pixel comparisons describe the quality of steganography. Fig. 8 is a planar histogram of the cover images Lena, Jet, Sailboat and pepper, and their steganographic images. It can be seen from Fig. 7 that, for the original image and the hidden image, the pixel values are almost the same, and the distortion is not obvious, indicating that this feature makes the steganographic image obtained by this method resistant to statistical attacks.

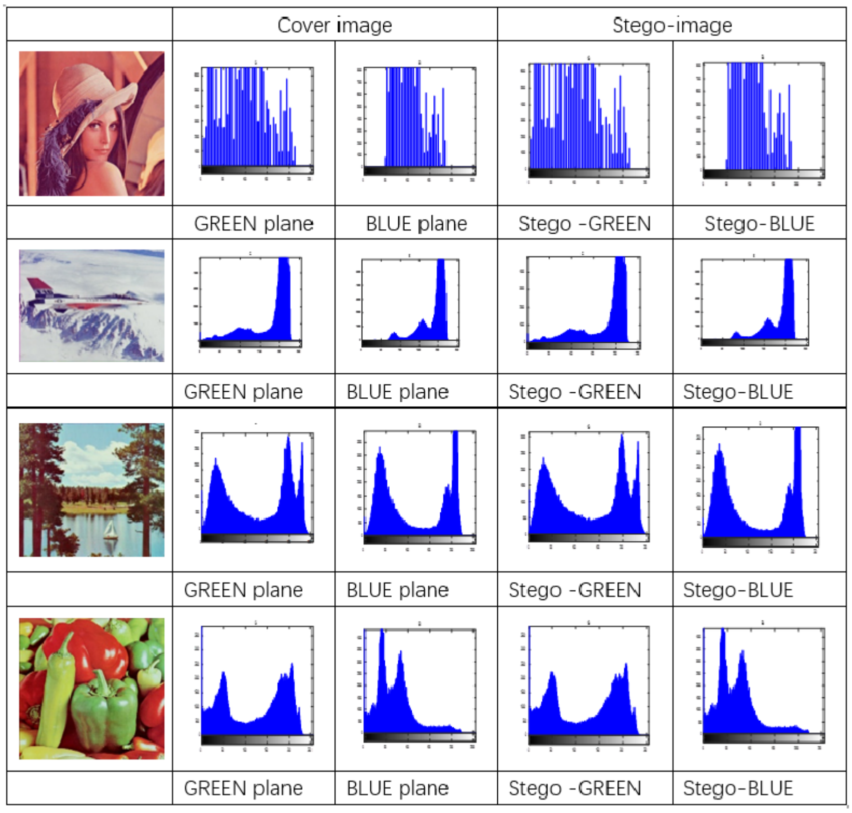


Fig. 8. Histogram of constituent planes of various cover image

In this paper, the secret image extracted from the stego image with 1%~3% impulse noise is shown in Fig. 9. By examining the difference between the extracted secret image and the embedded image, it can be seen from Fig. 8 that as the noise increases, AVAP can still extract the secret image completely.

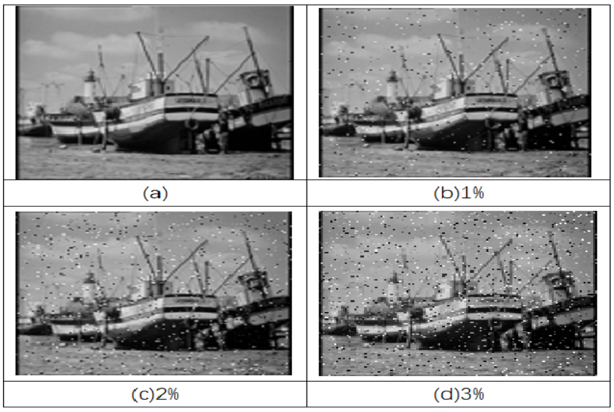


Fig. 9. Comparative secret images extracted from stego image with 1%~3% impulse noise

In addition to the above tests, the proposed scheme was tested against ten randomly selected color images from a 384×512 size UCID repository. Fig. 10 shows the test images and corresponding hidden images obtained using the AVAP embedding technique. It is obvious from the subjective quality of the obtained stealth images that the proposed scheme can provide high-quality stealth images.

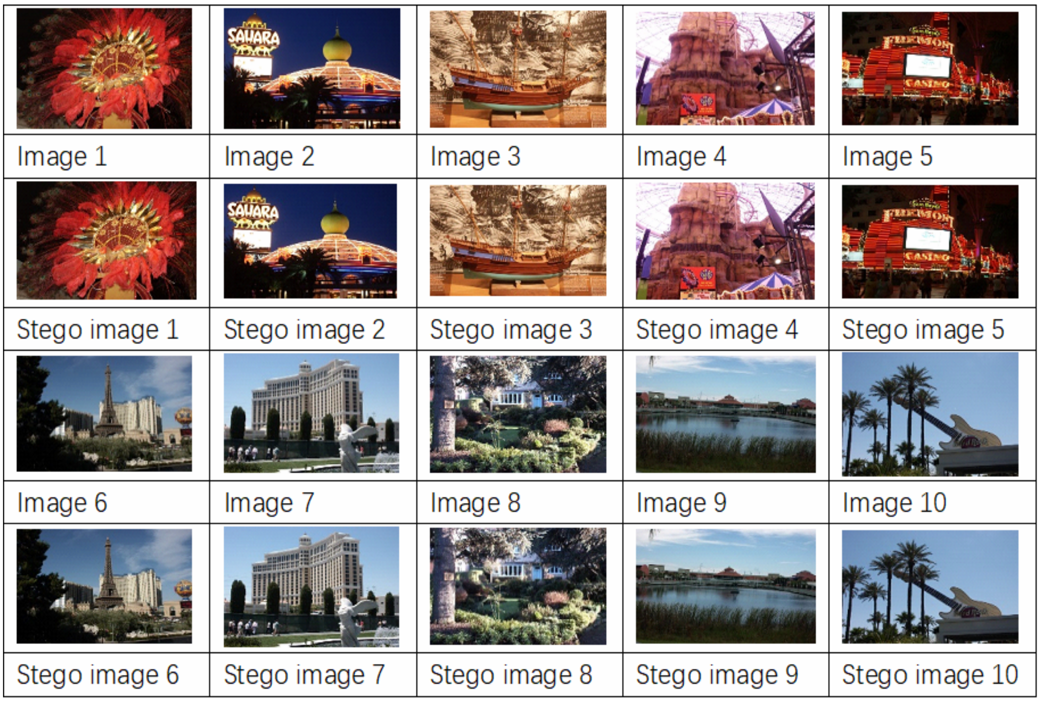


Fig. 10. Comparative secret images extracted from stego image with 1%~3% impulse noise

6 Conclusion

The method is proposed using QR code and the absolute value of adjacent pixel in this paper. The preprocessing stage no longer directly converts the secret message into a data stream. Instead, it uses the anti-attack property of the QR code to convert secret messages to form protection. In the embedding process, in order to ensure the complete transmission of information without affecting the quality of the image, the parity between the pixel pairs of the carrier picture and each secret message is compared. In other words, the same without any processing, one pixel value needs to be changed in case of inconsistency. The experimental results show that this method has good performance in generating high quality steganographic images and recovering secret images after the steganographic images are attacked by noise. In addition, in terms of security, the secret message is QR coded when steganographic. Therefore, it is impossible to recover a secret image from a stego image without knowing the encoding rules. Therefore, from the aspects of image quality and security performance, the QR-based LSB method with multiple absolute values of pixels is efficient, and this method can be used as a useful alternative method in the image steganography field. However, there is still room for improvement in the adaptability of this method. In the future, the ability of steganography can be increased by analyzing the structure of the image.

Acknowledgements

This work is supported by the Scientific Research Funds project of Science and Technology Department of Sichuan Province (No. 2016JY0244,2017JQ0059, 2019GFW131, 2020JY, 2020GFW), Funds Project of Chengdu Science and Technology Bureau (No. 2017-RK00-00026-ZF), the National Natural Science Foundation of China (No. 61902324),the Fund of Sichuan Educational Committee (17ZA0360) and the Foundation of Cyberspace Security Key Laboratory of Sichuan Higher Education Institutions (No. sjzz2016-73).

References

[1] X. Xin, C. Livermore, A pivot-hinged, multilayer SU-8 micro motion amplifier assembled by a self-aligned approach, in: IEEE International Conference on Micro Electro Mechanical Systems, 2016.

[2] X. Xin, C. Livermore, Passively self-aligned assembly of compact barrel hinges for high-performance, out-of-plane mems actuators, in: IEEE International Conference on Micro Electro Mechanical Systems, 2017.

[3] X. Xie, Y. Zaitsev, Compact, Scalable, High-Resolution, Mems-Enablerd Tactile Displays, in: Research, Innovation, Scholarship Expo (RISE 2016), 2016.

[4] X. Xie, Y. Zaitsev, L.F. Velásquez-García, S.J. Teller, C. Livermore, Scalable, MEMS-enabled, vibrational tactile actuators for high resolution tactile displays, Journal of Micromechanics & Microengineering 24(12)(2014) 125014.

[5] C.X. Shen, H.G. Zhang, D.G. Feng, Z.F. Cao, J.W. Huang, Survey of information security, Science in China Series F: Information Sciences 50(3)(2007) 273-298.

[6] H.C. Wu, N.-I. Wu, C.-S. Tsai, M.-S. Hwang, Image steganographic scheme based on pixel-value differencing and LSB replacement methods, IEE Proceedings - Vision Image and Signal Processing, 152(5)(2005) 611-615.

[7] Y.L. Bei, D.Q. Yan, N. Li, Color digital watermarking based on amplitude modulation and visual masking, Computer Engineering & Applications 43(27)(2007) 44-46.

[8] T. Pevny, T. Filler, P. Bas, Using High-Dimensional Image Models to Perform Highly Undetectable Steganography, Lecture Notes in Computer Science 6387(2010) 161-177.

[9] V. Holub, J. Fridrich, T. Denemark, Universal distortion function for steganography in an arbitrary domain, Eurasip Journal on Information Security 2014(1)(2014) 1.

[10] S.A. Parah, J.A. Sheikh, J.A. Akhoon, N.A. Loan, G.M. Bhat, Information hiding in edges: A high capacity information hiding technique using hybrid edge detection, Multimedia Tools & Applications 77(1)(2018) 185-207.

[11] K. Bailey, K. Curran, An evaluation of image based steganography methods using visual inspection and automated detection techniques, Multimedia Tools & Applications 31(3)(2006) 327-327.

[12] Y.J. Chanu, T. Tuithung, K.M. Singh, A short survey on image steganography and steganalysis techniques, in: 2012 3rd

National Conference on Emerging Trends and Applications in Computer Science, 2012.

[13] A. Cheddad, J. Condell, K. Curran, P.M. Kevitt, Digital image steganography: Survey and analysis of current methods, Signal Processing 90(3)(2010) 727-752.

[14] B. Li, J. He, J. Huang, Y.Q. Shi, A survey on image steganography and steganalysis, Journal of Information Hiding & Multimedia Signal Processing 2(2)(2011) 142-172.

[15] S.K. Ghosal, J.K. Mandal, R. Sarkar, High payload image steganography based on Laplacian of Gaussian (LoG) edge detector, Multimedia Tools & Applications 77(23)(2018) 30403-30418.

[16] M.S. Subhedar, V.H. Mankar, Current status and key issues in image steganography: A survey, Computer Science Review 13-14 (nov.)(2014) 95–113.

[17] L. Xue, Y. Chao, L. Liu, X. Zhang, Information Hiding Algorithm for PDF417 Barcode, in: 2009 Fifth International Conference on Natural Computation IEEE, 2009.

[18] S. Vongpradhip, S. Rungraungsilp, QR code using invisible watermarking in frequency domain, in: 2011 Ninth International Conference on ICT and Knowledge Engineering, 2012.

[19] J. Lu, Z. Yang, L. Li, W. Yuan, L. Li, C.-C. Chang, Multiple Schemes for Mobile Payment Authentication Using QR Code and Visual Cryptography, Mobile Information Systems 2017(2)(2017) 1-12.

[20] D. Shehzad, T. Dag, LSB Image Steganography Based on Blocks Matrix Determinant Method, KSII Transactions on Internet and Information Systems 13(7)(2019) 3778.

[21] S. Kaur, Pooja, Varsh, A Robust & Quality Improvement of Video Watermarking Using SVD & DWT, in: Computing for Sustainable Global Development IEEE, 2016.

[22] T. Zhao, Y. Zi, W. Zhang, W. Huang, F. Yu, Field depth extension of 2D barcode scanner based on wavefront coding and projection algorithm, Information Optics and Photonics Technologies 6837(2007) 683711.

[23] T. Ma, H. Zhang, J. Qian, X. Hu, Y. Tian, The Design and Implementation of an Innovative Mobile Payment System Based on QR Bar Code, in: International Conference on Network & Information Systems for Computers, 2015.

[24] J.M. Guo, T.N. Le, Secret Communication Using JPEG Double Compression, IEEE Signal Processing Letters 10(2010) 1-1.

[25] W. Bender, D. Gruhl, N. Morimoto, A. Lu, Techniques for Data Hiding, Ibm Systems Journal 35(3.4)(1996) 313-336.

[26] J. Tian, Reversible data embedding using a difference expansion, IEEE Transactions on Circuits & Systems for Video Technology 13(8)(2003) 890-896.

[27] C. Chan, L.M. Chen, Hiding data in images by simple LSB substitution, Pattern Recognition 37(3)(2004) 469-474.

[28] F. Liu, X.J. Leng, The application status of two-dimensional barcode technology and feasibility analysis of its application to traceability system for food additives, Journal of Food Safety & Quality 4(5)(2013) 1590-1595.

[29] C. Yang, C. Weng, S. Wang, H. Sun, Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems, IEEE Transactions on Information Forensics and Security 3(3)(2008) 488-497.

[30] G. Swain, Adaptive and Non-adaptive PVD Steganography Using Overlapped Pixel Blocks, Arabian Journal for Science and Engineering 43(12)(2018) 7549-7562.

[31] G. Swain, Very High Capacity Image Steganography Technique Using Quotient Value Differencing and LSB Substitution, Arabian Journal for Science and Engineering 44(4)(2019) 2995-3004.

[32] M. Khodaei, K. Faez, New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing, IET Image Processing, 2012.