IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 4, 2019, accepted May 25, 2019, date of publication May 31, 2019, date of current version June 18, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2920178

A High-Imperceptibility and Histogram-Shifting Data Hiding Scheme for JPEG Images

YUANZHANG LI, SHANGJUN YAO, KAI YANG, YU-AN TAN, AND QUANXIN ZHANG
School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China

Corresponding author: Quanxin Zhang (zhangqx@bit.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant U1636213 and Grant 61876019.

ABSTRACT Data hiding technology plays an important role in many areas related to people's life, such as military and medical images. However, it is difficult to obtain high embedding capacity in compressed images, and it may cause obvious image distortion. Also, the target image's file size should be controlled, as a significant increase in file size may cause the interceptor's attention. In the field of data hiding, many people have proposed feasible solutions. However, considering the visual quality and embedding rate of images, more improvements are needed. In this paper, the histogram shift is used to realize data hiding of JPEG images. The secret message bits are embedded in the high-frequency coefficients to ensure a higher embedding rate, and the high-frequency coefficients are obtained by histogram distribution. The optimal threshold is used to select a discrete cosine transform (DCT) coefficient sub-block that is suitable to embed the secret message and further improve the visual quality of the target image. The experiments show that our solution is significantly better than the most advanced technology in terms of embedding rate and visual quality.

INDEX TERMS Data hiding, JPEG images, DCT coefficient, histogram shift.

I. INTRODUCTION

Joint Photographic Experts Group (JPEG) is a kind of the images in a compressed format, which not only achieves high compression ratios but also high visual quality. At present, this format is the most commonly used picture format for mobile devices such as mobile phones and cameras. It is widely stored and transmitted on the network, becoming a hot spot in the multimedia industry. With the widespread use of JPEG format pictures in life, data hiding technology in JPEG pictures is becoming more and more crucial. It is widely used in medical [1], [2], military and other fields to achieve image archive management, image authentication, image privacy, and other functions.

Privacy protection [4], [5] is increasingly essential in life, and data hiding is one of the effective means of privacy protection. Data hiding is to hide secret information in its information carrier and uses the insensitivity of human senses to information and the redundancy of the carrier itself to achieve the invisible information embedding. According to the purposes of application, typical data hiding schemes can be divided into reversible data hiding [6], [7], digital watermarking [9], and steganography [12]. The reversible data hiding scheme can recover the carrier and hidden data excellently, and the steganography pays attention to the intangibility of the hidden data. Digital watermarking focuses on the ability to extract secret data from target images, therefore the need for robustness is far greater than the recoverability of the carrier.

Histogram shift is one of the most successful methods in reversible data hiding. It was first proposed by Chen *et al.* [6] in 2006. The basic idea is to shift the pixel between the peak point and the zero point of the image histogram. This process generates a histogram gap and then embeds information in the histogram gap. Since the information embedding process has little changes to the carrier image, the information hiding scheme based on the histogram modification can maintain high carrier image quality after embedding the information.

Lee *et al.* [15] made use of the features of differential image histogram to improve the image, fine-tuned the image pixel value and improved the embedding capacity. Yan *et al.* [16] modified the histogram of the difference image based on the first and second highest histogram peaks of the image. Not only can tamper with positioning but

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaojiang Du.

also increase the embedding capacity and operating efficiency relative to [15]. Many studies combine histograms and prediction error techniques to generate more evenly distributed prediction histograms using advanced prediction techniques. Secret messages are embedded by extending and moving the predicted extended histogram. Luo *et al.* [17] used the differences between the interpolation and the corresponding pixel value to extend the residual value by adding the embedded bit, which has the characteristics of small distortion and large capacity. However, this method has the problem of significant information overhead. Hu *et al.* [18] proposed a scheme to optimize the histogram, embedding the message into the generated PE sequence Gaussian mixture, which is superior to the similar existing methods in prediction accuracy and final embedding performance. Yin *et al.* [20] used the block histogram shift (BHS) method of self-hiding peak pixels to implement data hiding operation of multi-level encrypted pictures based on stream cipher and Joseph traversal. Compared with the algorithm for predicting error [19], the algorithm has higher embedding load, better decryption image quality, and error-free recovery.

Huang *et al.* [3] proposed a JPEG image reversible data hiding scheme based on histogram shifting, and block selection strategy is used to achieve the effect of adaptive selection of DCT coefficients for data hiding. Compared with the previous method, this method improves the embedding capacity and visual quality of the target image. However, when embedding data into texture images, the visual quality is not ideal. Xie *et al.* [21] improved [3] by extending the internal coefficients for some blocks and reducing the movement of external coefficients, which improved not only the embedding rate but also the image quality.

Through the threshold judgment, the coefficient block that has less influence on the image is adequately selected for the embedding operation. The length of the auxiliary information is effectively controlled, therefore even if a small amount of information is embedded, the auxiliary information has little effects on the visual quality. Based on the above observations, we propose a data hiding scheme based on histogram shift. The innovations between the scheme in this paper and other schemes are as follows: 1) the appropriate AC coefficient is selected according to the histogram as an internal coefficient to expand, and the invalid shift of the external coefficient is effectively avoided. 2) the scheme guarantees a higher embedding capacity of the picture while ensuring visual quality, and also has an advantage in terms of file size.

The remainder of this paper is organized as follows: In section II, we present the preliminaries including JPEG and DCT coefficients. In section III, we propose a reversible data hiding method and explain in detail the principle of data embedding and extraction. Then, in section IV, we give the experimental results and discuss them in comparison with existing algorithms. In section V, we review related work on existing data hiding. Finally, we conclude in section VI.

II. PRELIMINARIES

A. JPEG COMPRESSION OVERVIEW

JPEG is a common standard compression method for digital images. Figure 1 shows the main steps from the original image to the compressed image. First, the input image is divided into several sub-blocks. Then, each sub-block is encoded by an encoder with discrete cosine transform, quantization processing and entropy. Discrete cosine transform is another form of Fourier transform.

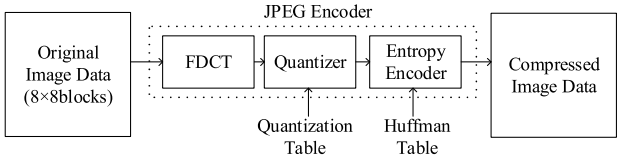


FIGURE 1. JPEG encoder block diagram.

B. CHOOSING THE COEFFICIENT FOR DATA HIDING

For JPEG files, the data hiding coefficient can be determined according to the following three steps when the histogram shift-based method is adopted: First, the coefficient histogram should be obtained, and the quantized DCT coefficient histogram is very easy to get for JPEG images. Second, the internal and external coefficients need to be distinguished. The regions associated with the peak are named as the internal regions, and the corresponding elements are called as the internal coefficients. The rest are named as the external regions, and the corresponding elements are called as the external coefficients. The last step is to ensure that after embedding the message bit, the external coefficient and the internal coefficient can still be distinguished, to achieve the extraction of the message bits.

Reference [22] shows that even slight changes in the quantized DC coefficient will lead to visual distortion of the smooth area, and the embedding capacity is very limited, therefore the data hiding algorithm we proposed is only for the quantized AC coefficient histogram. Through observation, we found that in JPEG images with different quality factors, the AC coefficients with the value of "0" are concentrated in the high-frequency part of the image.

If the "0" coefficient is selected for modification, on the one hand, excessive expansion coefficient will lead to severe image distortion, and on the other hand, the stroke in the run length coding of the AC coefficient is increased, thus leading to the size of the target image not being proportional to the number of embedded bits. Based on considerations of visual quality and size of the image, we chose an AC coefficient with a non-zero value for data hiding. Considering the embedding rate of the image, if the low-frequency non-zero AC coefficient is selected for hiding, the binary bit stream carried by the image will be less. Therefore, we chose the non-zero coefficient within the range of 2 as the internal coefficient, which can better balance the relationship between the embedding rate and image quality.

C. CRITERIA FOR EVALUATING THE DATA HIDING SCHEMES

Among applications such as archive management and image verification, some special data needs to be hidden in JPEG format files for transmission. Data hiding algorithms try to provide users with a reliable way to carry. And through some mechanisms, users can get a target image with high visual quality, and can extract these special data completely and accurately. Therefore, an efficient data hiding algorithm should have the following characteristics:

1) HIGH EMBEDDING CAPACITY

The increase of embedding capacity often causes image distortion. The algorithm should embed more data as much as possible while ensuring image quality.

2) HIGH IMPERCEPTIBILITY

The difference between the original image and the target image obtained by data hiding should be as small as possible, and it is usually measured by peak signal-to-noise ratio (PSNR). The higher PSNR value means the better imperceptibility.

3) ACCEPTABLE SIZE INCREASE

The increased file size between the mark image and the original image should be controlled within an acceptable range. Otherwise, a small number of message bits are embedded, and the file size may be significantly increased.

III. PROPOSED SCHEME

Based on the method from Huang, the data hiding algorithm of the JPEG image is improved to ensure that the marked image still has higher visual quality and smaller file size after embedding the secret message bits with a larger capacity.

A. DATA HIDING BY MODIFYING THE COEFFICIENTS

$C = \{C_1, C_2, \ldots C_N\}$, C represents the set of all quantized AC coefficients in the original image, and N is the number of elements in the set. The proposed algorithm takes into account the non-zero ac coefficients with amplitude less than 2, and other coefficients remain unchanged in the process of data hiding. The specific data hiding algorithm can be described as follows:

$$\text{Sign}(C) = \begin{cases} 1 & C > 0 \\ 0 & C = 0 \\ -1 & C < 0 \end{cases} \tag{1}$$

$$\widetilde{C}_i = \begin{cases} C_i + \text{sign}(C_i) * b & if \ \ |C_i| = 1 \\ C_i + \text{sign}(C_i) * (b-1) & if \ \ |C_i| = 2 \\ C_i & \text{otherwise} \end{cases} \tag{2}$$

In (2), C_i and $\widetilde{C}_i$ represent AC coefficients before and after embedding message bits, respectively. And b $\in$ {0,1} indicates the embedded message bit we are about to embed. In the proposed algorithm, the internal coefficient is the AC coefficient with the absolute value of 1 and 2. According to the above formula, the expanded internal coefficient is still the value with the absolute value of 1 and 2, so there is no need to shift the external coefficient, and the coefficient histogram can distinguish them. Figure 2 intuitively describes the process of changing the coefficients of the DCT coefficients during embedding. In this process, no coefficients are modified except for the internal coefficients, so most of the coefficients remain unchanged. The modified internal coefficient is extended by at most one bit, so it is possible to ensure a high visual quality of the target image.

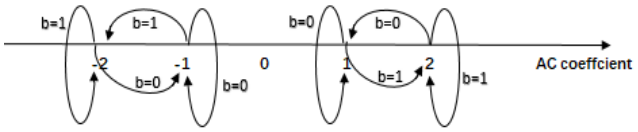


FIGURE 2. Example of data embedding.

However, there is a large correlation between the pixels of the JPEG image and the quantized DCT coefficients. Improper modification of the coefficients is likely to cause distortion of the target image, hence the selection of the region in which the secret information is embedded is very important. For the frequency sensitivity in the human visual characteristics, the resolution for the higher frequency portion is lower, that is, the sensitivity to the modification is lower. After the JPEG compression, the high-frequency region contains the most zero AC coefficient. Huang et al. found that blocks with more 0 AC coefficients may contain more internal coefficients and fewer external coefficients. Therefore, a packet sorting method based on zero AC coefficients is proposed. The 8×8 DCT coefficient block with more zero AC coefficients is preferentially selected for data embedding, which reduces the invalid shift of the external coefficients. Our strategy effectively guarantees image quality and avoids the marked file size increasing significantly. In this scheme, a similar block sorting strategy is used. The more the number of blocks with zero AC coefficient, the higher the embedding priority. The method for judging whether the embedding standard is satisfied is as follows:

$$T_z = \arg\max_{T} \{S \geq (L + l_1 + l_2)\} \tag{3}$$

According to the magnitude relationship between the zero coefficient and the threshold T_z ($0 \leqslant T \leqslant 63$), all coefficient blocks are divided into embeddable blocks and non-embedded blocks, and S is the number of coefficients with the value of (1, −1, 2, −2) in all embeddable blocks. L is the message bit to be embedded, l_1 is the number of bits required to represent the L value, and l_2 is the number of bits required to represent T_z. In order to ensure that the proposed method can extract the hidden data completely, it is necessary to embed the effective embedded capacity length L and the embedded priority judgment condition range T_z as auxiliary messages. We use the size of 512 × 512 gray image

-26	-3	-6	2	2	-2	0	0
0	-2	-4	1	2	0	0	0
-3	1	5	-1	0	0	0	0
-4	2	-2	-2	0	0	0	0
1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

FIGURE 3. Marked DCT coefficient block.

experiment, so can be embedded in the maximum capacity of not more than 2^{18}, so desirable $l_1 = 18$, $l_2 = 5$, the auxiliary information is 23 bits.

The method of data extraction is the inverse process of hiding secret information. Firstly, the embedded sub-block and the non-embedded sub-block in the image are distinguished according to the auxiliary message, and then the embedded binary stream is obtained from the embedded sub-block according to the extraction algorithm. The extraction algorithm can be described as:

$$b' = \begin{cases} 0 & if \ \left|\widetilde{C}_i\right| = 1 \\ 1 & if \ \left|\widetilde{C}_i\right| = 2 \end{cases} \tag{4}$$

In (4), b' denotes the message bit to be extracted. When the hidden image has a DCT coefficient value of 1 or -1, the secret information bit 0 can be extracted; when the hidden image has a DCT coefficient value of 2 or -2, the secret information bit 1 can be extracted. A block of DCT coefficient embedded in the message is given in Fig.3, the yellow portion is the extended position. According to the proposed extraction method, a binary stream of values (1,1,0,0,1,0,1,1,1,0,1,1) can be extracted in zig-zag order.

B. DATA EMBEDDING

Combined with the data embedding formula, the data is hidden unconsciously in the JPEG image.

The process of embedding information has the following steps:

Step 1: The original image is divided into several 8×8 sub-blocks. All sub-blocks are entropy decoded to obtain quantized DCT coefficients, counting the number of internal coefficients, if the number of message bits L is less than the internal coefficients, perform the second step. Otherwise, the image embedding capacity will be limited and cannot be fully embedded.

Step 2: Count the number of AC coefficients with a value of 0 in each sub-block (denoted as N_0), calculate T_z according to Eq. (3), and then embed the auxiliary message (i.e., message length L and threshold T_z) into the DCT coefficient block according to the zig-zag scanning manner. Since there are fewer auxiliary messages, it can be embedded in a well-defined location, such as the first DCT coefficient block.

Step 3: DCT coefficient blocks of 8×8 are divided into two groups according to the threshold: embeddable blocks (i.e. $N_0 \geqslant T_z$) and non-embeddable blocks (i.e. $N_0 < T_z$).

Step 4: For the embeddable block, according to Eq. (1), the secret binary streams consisting of 0 and 1 are sequentially embedded in the DCT coefficient block in a zig-zag manner; for non-embedded blocks, no changes are made during the data hiding process.

Step 5: Entropy encodes a modified coefficient due to data hiding, thus generating a target image carrying data.

Algorithm 1 Data Embedding Algorithm

```
Input: original image p, message bits
Output: marked image m
Divided p into D blocks
L ← count the length of message bits
I ← count the number of (1,−1,2,−2)
if I > L then
 T_z ← GetThreshold (p, L)
 for D_j in D:
  if(auxiliary messages are not fully embedded) then
    embed auxiliary message
  else
    N_0 ← count the number of zero coefficients
    if N_0 > T_z then
     embed message bits
    end if
  end for
end if
m← Entropy coded modified DCT coefficients
return m
```

C. DATA EXTRACTING

In the data hiding technology, it should be ensured that the embedded load can be effectively extracted. First, the DCT coefficients are retrieved from the target JPEG image, the threshold and the length of the message bits are extracted. Then, after determining the position of the embedded sub-block, the extraction is performed according to the extraction formula.

The specific process is as follows:

Step 1: The target image is divided into several 8×8 sub-blocks. All sub-blocks are entropy decoded to obtain quantized DCT coefficients, and count the number of zero AC coefficients in each sub-block (denoted as N_1).

Step 2: According to (4), auxiliary messages (i.e., message length L and threshold T_z) are obtained from the marked image. Comparing the threshold and the number of N_1 in each 8×8 DCT coefficient sub-block in the target image distinguishes embeddable blocks and non-embeddable blocks.

Algorithm 2 Data Extraction Algorithm

Input: marked image M
Output: message bits
Divided M into D blocks
for D_i **in** D:
 if(auxiliary messages are not fully extracted) **then**
  $(T_z, L) \leftarrow$ extraction the auxiliary messages
 else
  $N_1 \leftarrow$ count the number of zero coefficients
  if $N_1 > T_z$ **then**
   S{} $\leftarrow$ extraction message bits
  end if
 end for
 return S{}

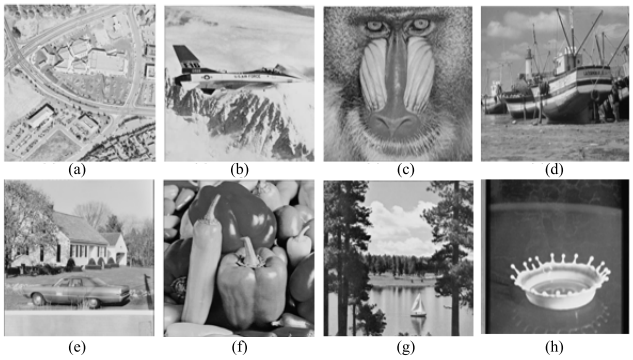


FIGURE 4. Test images. (a) Aerial. (b) Airplane. (c) Baboon. (d) Boat. (e) House. (f) Peppers. (g) Sailboat. (h) Splash.

Step 3: Also extract messages from the embedded block using the method of (4). The non-embedded block does nothing and continues to access the next sub-block of the marked image in order.

Step 4: After extracting all the secret message bits, the coefficients are entropy encoded again to generate a JPEG image.

IV. EVALUATION

In this experiment, some gray images of 512 ×512 in usc-sipi database [29] were selected and compressed according to quality factors QF = 60, 70, 80, and 90 using the optimized Huffman table of JPEG library Libjpeg. Figure 4 (a-h) shows the test pictures when the quality factor is 70. To increase the reliability of the experiment, we selected random binary strings as secret message bits. The scheme of Huang *et al.* [3] was selected as the comparison test, and the performance of our method was verified by embedded capacity, visual quality, and increased file size.

A. EMBEDDING CAPACITY

We compared the maximum image size and embedding rate for different schemes with a quality factor of 70. As can be seen from Fig.5, the embedding rate has no fixed range. As the picture changes, it will fluctuate up and down. For this scheme, the embedding rate of the image "Baboon" can reach 22.164%, and the embedding rate of the image "splash" is only 9.344%. However, for all test images,

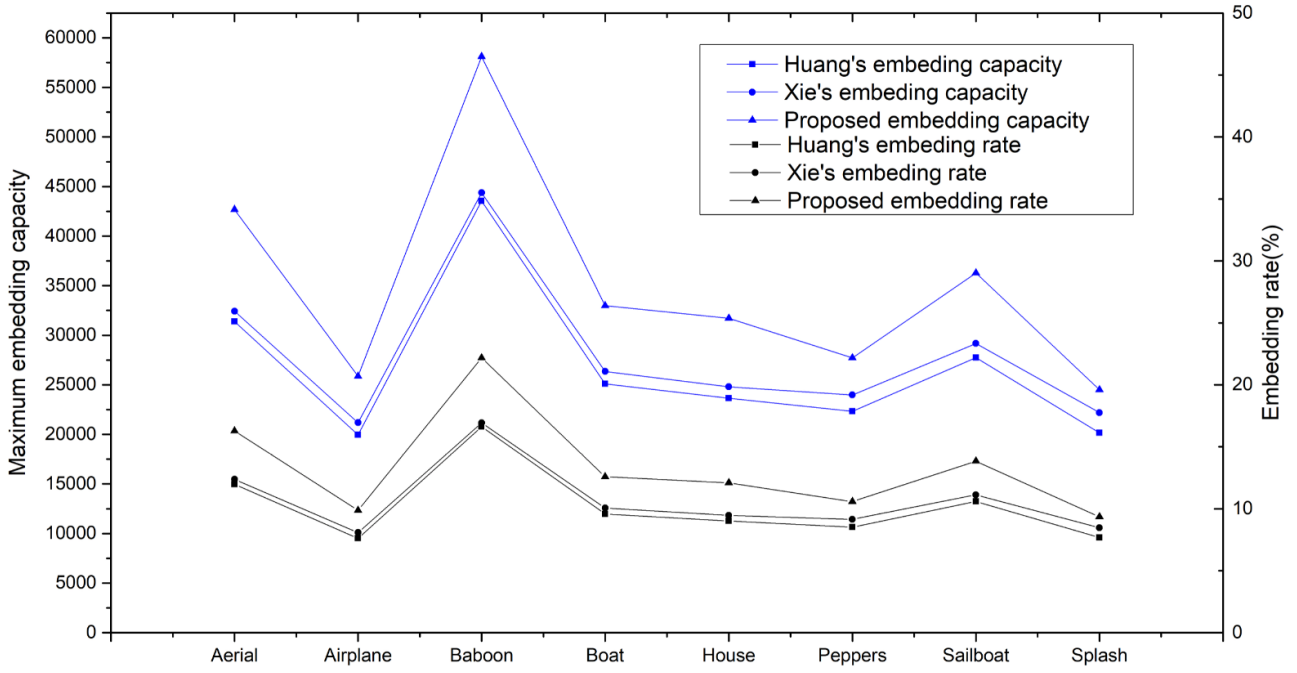


FIGURE 5. Maximum embedding capacity and embedding rate when QF = 70.

TABLE 1. Comparison with the maximum embedding capacity of other methods.

QF	Aerial			Airplane			Baboon			Boat		
	Proposed	Huang et al's	Xie et al's	Proposed	Huang et al's	Xie et al's	Proposed	Huang et al's	Xie et al's	Proposed	Huang et al's	Xie et al's
60	38833	28622	29810	22150	17092	18295	51790	38932	39995	28563	21760	23095
70	42677	31385	32426	25869	19941	21185	58101	43555	44377	32973	25085	26347
80	49093	36137	36892	31760	24410	25843	68651	51440	51984	40501	31086	32267
90	62302	46240	46757	44446	33769	35110	86032	63396	63561	58722	45338	46484

QF	House			Peppers			Sailboat			Splash		
	Proposed	Huang et al's	Xie et al's	Proposed	Huang et al's	Xie et al's	Proposed	Huang et al's	Xie et al's	Proposed	Huang et al's	Xie et al's
60	28255	21190	22405	22241	17982	19371	31166	23994	25371	18993	15987	17566
70	31709	23644	24807	27715	22321	23974	36278	27745	29173	24495	20142	22195
80	37129	27702	28712	36206	28824	30838	45049	34731	35996	32081	25562	27832
90	48273	36045	36775	57967	45421	46831	69049	54130	55050	46311	35039	36439

the embedding rate of this scheme is higher than other schemes.

Table 1 specifically tests the picture embedding rate for all quality factors. From this table, we also analyzed the reasons why the embedded capacity fluctuates with different images. In contrast, the embedding capacity has different degrees of change for images of different textures and different quality factors. In contrast, for complex texture images such as Baboon, can embed more bits than images with simpler texture such as Peppers. And as the picture quality factor increases, the distribution of non-zero AC coefficient histograms is sharper. Hence images with larger quality factors have more internal coefficients than images with smaller quality factors.

In Huang's method, data was embedded into DCT coefficients with values in (1, −1). Xie analyzed the statistical characteristics of JPEG image quantization DCT coefficient blocks, it was concluded that many blocks have no value in (3, −3, 4, −4), then the internal coefficient values in these special blocks extend from (1, −1) to (1, −1, 2, −2). The proposed method extends the embeddable values to AC coefficients of all blocks with values in (−1, +1, −2, +2).

The increased embedding capacity compared with [3] is shown in Table 2. The increased capacity is also affected by the quality factor and picture texture. The larger the quality factor, the higher the embedding capacity; the more complex the picture texture, the higher the embedding capacity. Compared with the Xie's method, since the specific block decreases with the increase of the quality factor, when QF = 90, the increase of embedding coefficient in many images is not obvious. The method we proposed, is superior to the previous method for all test images with varying QFs.

B. VISUAL QUALITY

The peak signal noise ratio (PSNR) of an image is a general indicator for evaluating image quality. In order to measure whether the results of image processing are satisfactory, this value is usually calculated. In this section, we also used PSNR to measure the visual quality of the target image obtained by various methods. The PSNR is calculated as:

$$PSNR = 10 \times \lg \frac{255^2}{MSE}(\text{dB}) \tag{5}$$

TABLE 2. Comparison with the maximum embedding capacity of other methods.

QF		60	70	80	90
Aerial	Proposed	10211	11292	12956	16062
	Xie et al's	1188	1041	755	517
Airplane	Proposed	5058	5928	7350	10677
	Xie et al's	1203	1244	1433	1341
Baboon	Proposed	12858	14546	17211	22636
	Xie et al's	1063	822	544	165
Boat	Proposed	6803	7888	9415	13384
	Xie et al's	1335	1262	1181	1146
House	Proposed	7065	8065	9427	12228
	Xie et al's	1215	1163	1010	730
Peppers	Proposed	4259	5394	7382	12546
	Xie et al's	1389	1653	2014	1410
Sailboat	Proposed	7172	8533	10318	14909
	Xie et al's	1377	1428	1265	920
Splash	Proposed	3006	4353	6489	11272
	Xie et al's	1579	2053	2210	1400

Mean Squared Error (MSE) is the Mean Squared Error of hidden image and original carrier image. Typically, the more significant distortion of the mark image, corresponding to the lower MSE value, and the higher PSNR value.

Figure. 6 - Figure. 9 show the average PSNR values of the eight images under different quality factors and the same embedding capacity. The horizontal axis represents the embedded payload, and the vertical axis represents the average PSNR. The method proposed by Xie et al. requires secondary embedding of auxiliary messages in the first layer of labeled DCT coefficients, including the location map, the message length, and the threshold values. Since it is necessary to record metrics for distinguishing between moving blocks and non-moving blocks, it still causes a certain degree of visual loss to the original image even when fewer message bits are embedded.

The proposed scheme avoids the invalid displacement of the external coefficient, and the influence of auxiliary message on image visual quality is not obvious. Compared with two other schemes, the average PSNRs of the proposed scheme is higher no matter how many message bits are

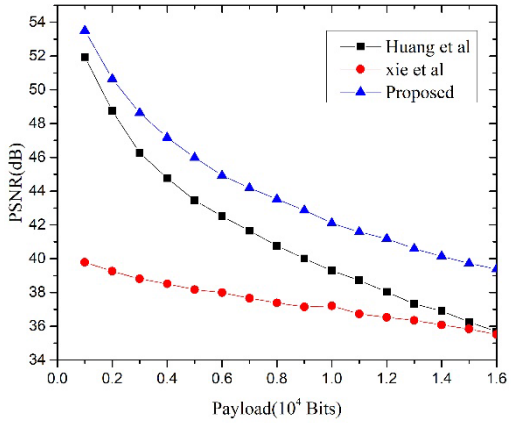


FIGURE 6. Average PSNR values corresponding to different payloads (QF = 60).

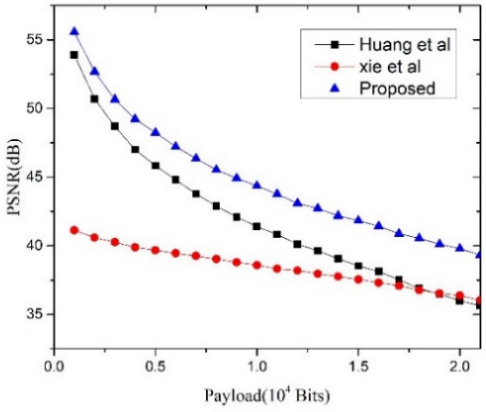


FIGURE 7. Average PSNR values corresponding to different payloads (QF = 70).

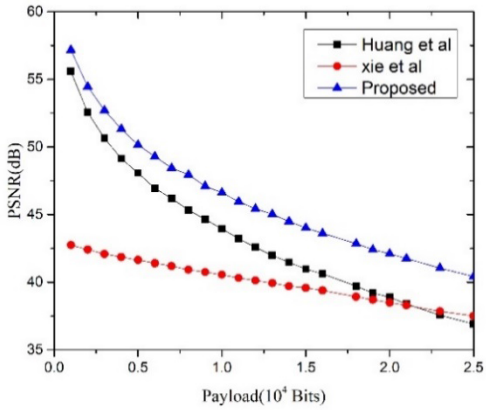


FIGURE 8. Average PSNR values corresponding to different payloads (QF = 80).

embedded. When QF = 70, embedding 2.1k bits of message bits, the average value of PSNR is increased by 3.29db compared with Xie's method.

The scheme proposed in this paper has not only the high embedding rate but also high visual quality when embedding

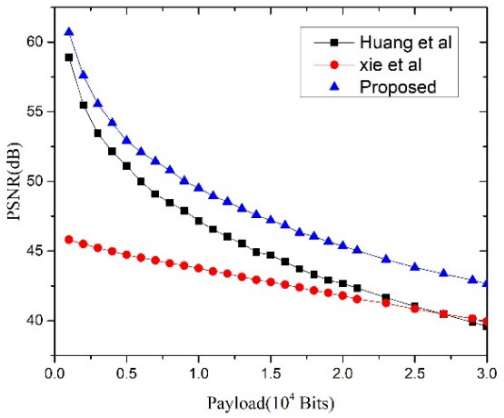


FIGURE 9. Average PSNR values corresponding to different payloads (QF = 90).

the maximum capacity binary bits. When QF = 70, the visual quality when embedding the maximum capacity message bit is shown in Fig.10. Compared with the other two schemes, the PSNR value of the target image obtained by this method is always the largest. The larger the PSNR, the better the invisibility, therefore this method has better imperceptibility.

C. FILE SIZE INCREASE

In general, the size of a file is important for data hiding in JPEG images. From Fig.11, it is shown that when QF = 70, after embedding the message bits of the same number of bits, the file size obtained by the different methods has a significant difference in file size. Through experimental comparisons, the results obtained by the Xie's methods and Huang's method are not much different when embedding a 16000-bit binary stream. Both of these methods require invalid shifting of a large number of external coefficients, which greatly increases the imbalance between file size and embedded bits. This method avoids this problem, so the target image has a much smaller file size than the other two methods. Moreover, the increased file size is even smaller than the number of bits carried. The target image has little differences from the file size of the original image, which also implies that the visual differences between the two images are relatively small.

V. RELATED WORKS

With the development of information security technology [11], [36], there are a variety of carriers carrying confidential information, including audio, video, picture, etc. Secret messages can also be hidden in the entities of network communication through hidden channels [9], [10]. We mainly analyzed the algorithms of JPEG image carrier.

According to the ability to recover the original image, the data hiding schemes including digital watermarking and steganography can be divided into irreversible data hiding [28] and reversible data hiding technology [8]. The minimum effective bit (LSB) [12], [34], [35], substitution and pixel value difference (PVD) techniques can usually

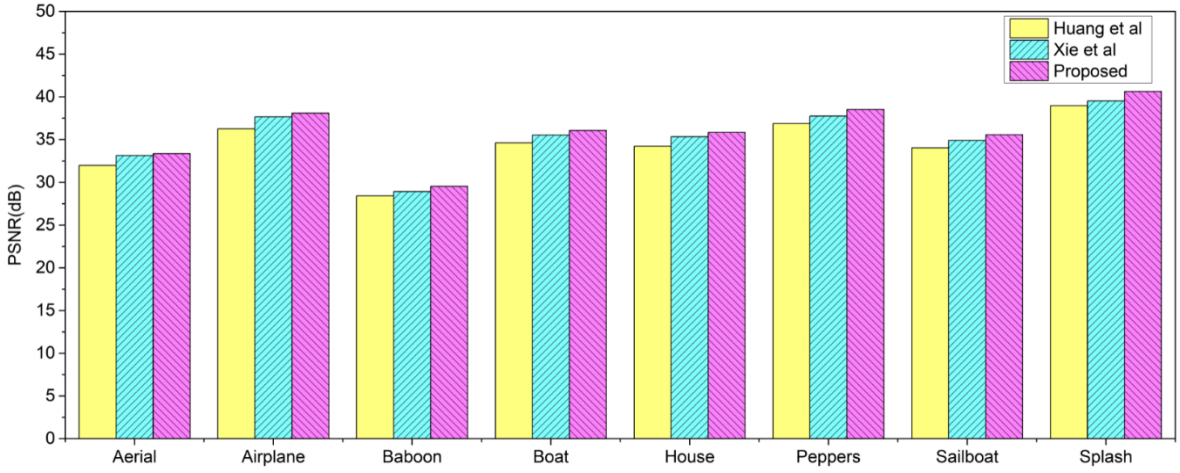


FIGURE 10. PSNR when the respective maximum embedding capacity is achieved (QF = 70).

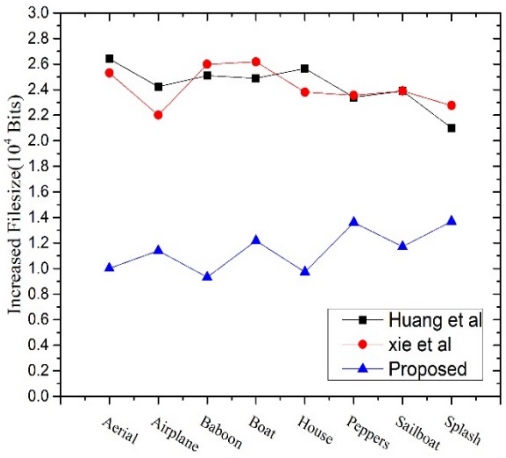


FIGURE 11. The file size increases when the embedded capacity is 16 000 bits (QF = 70).

achieve irreversible data hiding schemes. Common methods to achieve reversible data hiding schemes include difference expansion (DE) [14], histogram shift (HS) [27] and prediction error expansion (PEE) [6], [13].

The least significant bit (LSB) technique replaces the least significant bit of the pixel with the secret bit-stream, which hides large capacity but is extremely poorly robust. Tian [14] first proposed a differential expansion scheme, first calculating the difference between adjacent vertex coordinate values, then doubling the difference and adding the embedded bit information to form a new difference. Finally, the original pixel values are modified according to the new difference, thereby implementing information embedding. This method allows more message bits to be embedded and avoids severe image distortion. The difference expansion technique has excellent plasticity and transformed into algorithms suitable for different purposes [22]–[25].

Jung and Yoo [22] proposed a data hiding scheme based on neighborhood mean interpolation, embedding secret data according to the specific relationship between adjacent pixels. On this basis, Yang *et al.* [23] used the least efficient (LSB) replacement and optimal pixel adjustment process (OPAP), which improves the image quality compared to the [22] scheme. Jung [24] proposed a scheme of bit field segmentation using the least effective bit technology and pixel difference technology on the same bit plane, which maintained strong embedding ability and improved visual quality. Dragoi and Coltuc [25] split the image into blocks and calculated the least squares predicted value on a square centered on each pixel. This local prediction scheme was significantly better than the [32], [33] global prediction scheme. Later in [26], the author calculated the prediction factor of the pixel group, which improved the computational efficiency compared with the previous work [25].

The combination of data hiding and encryption has also received attention in recent years. In many scenarios, to securely store and share media files, it is necessary to encrypt the transmitted media data and wish to attach some additional messages to the carrier, which means that the encryption domain signal processing research is involved. Qian *et al.* [30] proposed a method of concealing reversible data in an encrypted JPEG bit streams, which is controlled by an encryption key and an embedded key, respectively. Complete data extraction and image recovery by analyzing blocking artifacts to restore the original bitstream. Kittawi and Al-Haj [31] proposed a new algorithm to detach the data into the encrypted image in a detachable way, using the replacement method and the histogram modification method to hide the two watermarks in the original encrypted image. The algorithm guarantees the authenticity and integrity of the data while maintaining the security and confidentiality of the original content.

VI. CONCLUSION

By analyzing the process of JPEG format file compression and the distribution of quantized DCT coefficients,

we propose an improved algorithm based on histogram shift. In this paper, the data hiding algorithm is analyzed from three aspects: image quality, embedding capacity and file size. The experimental results show that the scheme is suitable for JPEG images with different quality factors, which not only provide large embedding capacity but also has better imperceptibility than previous methods. It can be applied to the field of secret information transmission requiring large embedding capacity.

The improvement of this scheme is mainly from the following three aspects. Firstly, it guarantees that all the external coefficients are not shifted except for the internal coefficients that need to carry the messages so that the marked image has a high visual quality. Secondly, due to the expansion of the embedding coefficient, a large embedding capacity can be obtained. Besides, this scheme can reduce the storage size of the JPEG files very well.

As the core of privacy protection, data hiding faces the challenge of being attacked during transmission, thus the data hiding algorithm should have better anti-attack capability. Our approach needs to be improved in terms of robustness and further research is needed to find the right solution.

REFERENCES

[1] G. Coatrieux, C. Le Guillou, J.-M. Cauvin, and C. Roux, "Reversible watermarking for knowledge digest embedding and reliability control in medical images," *IEEE Trans. Inf. Technol. Biomed.*, vol. 13, no. 2, pp. 158–165, Mar. 2009.

[2] F. Bao, R. H. Deng, B. C. Ooi, and Y. Yang, "Tailored reversible watermarking schemes for authentication of electronic clinical atlas," *IEEE Trans. Inf. Technol. Biomed.*, vol. 9, no. 4, pp. 554–563, Dec. 2005.

[3] F. Huang, X. Qu, H. J. Kim, and J. Huang, "Reversible data hiding in JPEG images," in *IEEE Trans. Circuits Syst. Video Technol.*, vol. 26, no. 9, pp. 1610–1621, Sep. 2016.

[4] Z. Guan, Y. Zhang, L. Wu, J. Wu, J. Li, Y. Ma, and J. Hu, "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT," *J. Netw. Comput. Appl.*, vol. 125, pp. 82–92, Jan. 2019.

[5] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82–88, Jul. 2018.

[6] H. Chen, J. Ni, W. Hong, and T.-S. Chen, "High-fidelity reversible data hiding using directionally enclosed prediction," *IEEE Signal Process. Lett.*, vol. 24, no. 5, pp. 574–578, May 2017.

[7] X. Cao, L. Du, X. Wei, D. Meng, and X. Guo, "High capacity reversible data hiding in encrypted images by patch-level sparse representation," *IEEE Trans. Cybern.*, vol. 46, no. 5, pp. 1132–1143, May 2016.

[8] D. Hu, D. Zhao, and S. Zheng, "A new robust approach for reversible database watermarking with distortion control," *IEEE Trans. Knowl. Data Eng.*, vol. 31, no. 6, pp. 1024–1037, Jun. 2018. doi: 10.1109/TKDE.2018.2851517.

[9] X. Zhang, C. Liang, Q. Zhang, Y. Li, J. Zheng, and Y.-A. Tan, "Building covert timing channels by packet rearrangement over mobile networks," *Inf. Sci.*, vols. 445–446, pp. 66–78, Jun. 2018.

[10] Y. Tan, X. Zhang, K. Sharif, C. Liang, Q. Zhang, and Y. Li, "Covert timing channels for IoT over mobile networks," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 38–44, Dec. 2018.

[11] Q. Zhang, Y. Li, Q. Zhang, J. Yuan, R. Wang, Y. Gan, and Y. Tan, "A self-certified cross-cluster asymmetric group key agreement for wireless sensor networks," *Chin. J. Electron.*, vol. 28, no. 2, pp. 280–287, 2019.

[12] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 201–214, Jun. 2010.

[13] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, Mar. 2007.

[14] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

[15] S.-K. Lee, Y.-H. Suh, and Y.-S. Ho, "Reversiblee image authentication based on watermarking," in *Proc. IEEE Int. Conf. Multimedia Expo*, Toronto, ON, Canada, Jul. 2006, pp. 1321–1324.

[16] Y. Yan, W. Cao, and S. Li, "High capacity reversible image authentication based on difference image watermarking," in *Proc. IEEE Int. Workshop Imag. Syst. Techn.*, Shenzhen, China, May 2009, pp. 179–182.

[17] L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 187–193, Mar. 2010.

[18] X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum rate prediction and optimized histograms modification for reversible data hiding," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 653–664, Mar. 2015.

[19] X. Wu and W. Sun, "High-capacity reversible data hiding in encrypted images by prediction error," *Signal Process.*, vol. 104, pp. 387–400, Nov. 2014.

[20] Z. Yin, A. Abel, X. Zhang, and B. Luo, "Reversible data hiding in encrypted image based on block histogram shifting," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Shanghai, China, Mar. 2016, pp. 2129–2133.

[21] X. Xie, C. Lin, and C. Chang, "A reversible data hiding scheme for JPEG images by doubling small quantized AC coefficients," in *Multimedia Tools and Applications*. New York, NY, USA: Springer, 2018, pp. 1–10.

[22] K.-H. Jung and K.-Y. Yoo, "Data hiding method using image interpolation," *Comput. Standards Interfaces*, vol. 31, no. 2, pp. 465–470, Feb. 2009.

[23] C.-N. Yanga, S.-C. Hsua, and C. Kim, "Improving stego image quality in image interpolation based data hiding," *Comput. Standards Interfaces*, vol. 50, pp. 209–215, Feb. 2017.

[24] K.-H. Jung, "Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane," *J. Real-Time Image Process.*, vol. 14, no. 1, pp. 127–136, Jan. 2018.

[25] I.-C. Dragoi and D. Coltuc, "Local-prediction-based difference expansion reversible watermarking," *IEEE Trans. Image Process.*, vol. 23, no. 4, pp. 1779–1790, Apr. 2014.

[26] I. C. Dragoi and D. Coltuc, "On local prediction based reversible watermarking," *IEEE Trans. Image Process.*, vol. 24, no. 4, pp. 1244–1246, Apr. 2015.

[27] Y.-Q. Shi, X. Li, X. Zhang, H.-T. Wu, and B. Ma, "Reversible data hiding: Advances in the past two decades," *IEEE Access*, vol. 4, pp. 3210–3237, 2016.

[28] W. Hong and T.-S. Chen, "A novel data embedding method using adaptive pixel pair matching," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 176–184, Feb. 2012.

[29] C.-F. Lee, J.-J. Shen, and K.-T. Lin, "The study of steganographic algorithms based on pixel value difference," in *Advances in Intelligent Information Hiding and Multimedia Signal Processing*. Berlin, Germany: Springer, 2017, pp. 99–106.

[30] Z. Qian, X. Zhang, and S. Wang, "Reversible data hiding in encrypted JPEG bitstream," *IEEE Trans. Multimedia*, vol. 16, no. 5, pp. 1486–1491, Aug. 2014.

[31] N. Kittawi and A. Al-Haj, "Reversible data hiding in encrypted images," in *Proc. 8th Int. Conf. Inf. Technol. (ICIT)*, Amman, Jordan, May 2017, pp. 808–813.

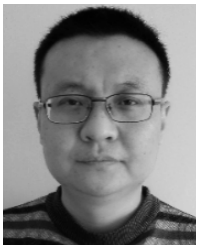
[32] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, Jul. 2009.

[33] B. Ou, X. Li, Y. Zhao, and R. Ni, "Reversible data hiding based on PDE predictor," *J. Syst. Softw.*, vol. 86, no. 10, pp. 2700–2709, Oct. 2013.

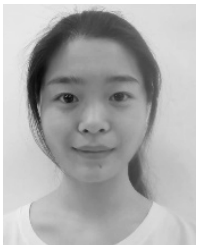
[34] S. Khan, T. Khan, T. Mahmood, and N. Ahmad, "Analysis of data hiding in R, G and B channels of color image using various number of LSBs," in *Proc. 6th Int. Conf. Innov. Comput. Technol. (INTECH)*, Dublin, Ireland, Aug. 2016, pp. 270–274.

[35] S. Shen, L. Huang, and Q. Tian, "A novel data hiding for color images based on pixel value difference and modulus function," in *Multimedia Tools Appl.*, vol. 74, no. 3, pp. 707–728, Feb. 2015.

[36] Y.-A. Tan, Y. Xue, C. Liang, J. Zheng, Q. Zhang, J. Zheng, and Y. Li, "A root privilege management scheme with revocable authorization for Android devices," *J. Netw. Comput. Appl.*, vol. 107, pp. 69–82, Apr. 2018.



YUANZHANG LI is currently a Lecturer with the Beijing Institute of Technology. He is involved in high-performance and massive storage systems.



SHANGJUN YAO is currently pursuing the M.A. degree with the Beijing Institute of Technology. Her main research interests include information security and coding theory.

KAI YANG received the B.E. degree in network engineering from the Information Engineering University, in 2012. He is currently pursuing the M.A. degree with the Beijing Institute of Technology. His main research interests include information security and coding theory.

YU-AN TAN is currently a Professor and a Ph.D. Supervisor with the Beijing Institute of Technology. His main research interests include network storage, storage security, and embedded systems. He is also a Senior Member of the China Computer Federation.

QUANXIN ZHANG is currently a Lecturer with the Beijing Institute of Technology. His main research interest includes mobile computing.