A reversible information hiding algorithm in AMBTC domain based on human vision system

Tao Zhang*, Jiantao Dinga, Zhewen Tianb
School of Electronic and Control Engineering Chang’an University China

*Corresponding author e-mail: zt@chd.edu.cn, a2019132008@chd.edu.cn, b2020132004@chd.edu.cn

Abstract. Compression is a common processing method of digital image, and the compression of carrier image usually affects the performance of hidden information. Therefore, it is necessary to research on the preprocessing method to improve some performance of hidden information in the compressed domain. Aiming at the problem of tampering attack on compressed domain image and the security of secret information preprocessing in the previous information hiding algorithms, we propose a reversible information hiding algorithm in AMBTC domain based on human vision system. Firstly, RGB color image is converted to YCbCr image, AMBTC coding is used to generate high and low average value sequence in brightness component. Secondly, the secret information is compressed by run length coding and scrambled. Thirdly, the histogram shift technique is used to embed the information into the mean sequence and generate the reserved information at the same time. Fourth, the color component is divided into normal block and absolute smooth fast, the specific position of the bit plane of the normal block is deleted, and the reserved information is embedded. The experimental results show that, compared with other algorithms, the proposed algorithm has better invisibility and robustness, and after a certain attack, the extracted secret information still has high recognizability.

Keywords: Information hiding; Chaotic scrambling; YCbCr; Histogram shift technique; Absolute moment block truncation coding.

1. Introduction
The development of Internet and rapid data processing provide a convenient channel for information processing. At the same time, confidential information may encounter unknown attacks in the transmission channel. To ensure that confidential information is free from all kinds of attacks in the transmission channel is the main problem in the field of information security transmission. As an important research field of information transmission, information hiding technology achieves the purpose of secure transmission by hiding secret information in ordinary media [1].

The technologies used in information hiding include communication, cryptography, image processing and pattern recognition. According to the different purposes of application, they can be divided into digital fingerprint [2], "steganography [3]." hidden channel [4] and digital watermark [5]. From the perspective of protection object and research status, the two most widely used branches are
steganography and digital watermarking. As an important means of concealment channel, steganography is based on the principle of hiding important information in the mass of digital information, providing secure and secret communication methods for both sides of communication. Therefore, it has important research value and application value in national defense security.

Although information hiding technology has made great progress, it still faces many problems and challenges. The previous research on information hiding is mainly embedded in space domain and transform domain. However, the digital images used on the Internet are basically compressed. In the past, many algorithms based on space domain and transform domain for uncompressed images are no longer suitable for the compressed format of the map, the lack of image information hiding based on compressed domain hinders the practical application of information hiding technology to some extent. Therefore, it is necessary to strengthen the research of information hiding based on compressed domain.

2. Related Work

According to the different embedded domain, information hiding technology can be divided into three categories: spatial domain, transform domain and compressed domain. Simple implementation and high embedding capacity are the advantages of spatial domain algorithm, but geometric attacks will have a great impact on this kind of algorithm. Although the transform domain method can resist a variety of attacks, the embedding capacity is not high [7]. The storage capacity and transmission bandwidth of the original image are high, which brings great difficulties to the transmission, so the image can be effectively compressed to solve this problem. Therefore, information hiding method in compressed domain becomes an important aspect of research.

Absolute moment block truncation coding (AMBTC) [9] is an efficient compression coding method with high compression ratio and good image quality. This method is suitable for gray-scale images. In color images, each color component should be separated and AMBTC should be applied respectively. Kumar et al. [10] proposes a new image compression method based on enhanced AMBTC, which converts RGB image into YCbCr color space and compresses each component with AMBTC. In addition to the compression methods, the embedding capacity and the security and robustness can also rely on histogram shift for embedding space construction.

Analytical research on hidden carrier differential histograms, such as histogram shifting methods can construct new embedding spaces. Ni et al. [12] proposed a histogram shift method, which can generate a histogram of the image, then detect the peak and zero points, and move the pixels with gray values between zero and the peak to the zero point. In the figure, create an empty bin, and use the empty bin to embed the secret message. The hiding capacity of this method depends on the number of pixels at the peak point in the histogram. In order to improve the embedding ability, Fallahpour and Sedaghi [13] introduced an algorithm in 2007 that divides the image into a series of blocks and embeds the secret message by finding the zero point and peak point of each block. Chen et al. [14] proposed an adaptive two-way histogram shift method in 2016, which reduces the distortion of visual images and uses pixel value sorting technology to increase the embedding capacity; Amita et al. [15] proposed a multi-level histogram shift technology in the compressed domain in 2018, and added an adaptive block scheme to increase the embedding capacity and reduce bandwidth utilization. Wang et al. [16] proposed the second-order difference to obtain a steeper difference histogram in 2020. The algorithm outperforms the previous state-of-the-art RDH methods in terms of the computational complexity, image distortion and the embedding performance. Sukumar et al. [17] proposed a robust image steganography model based on the Laplacian Pyramid, Redundant Integer Wavelet Transform and Histogram Shifting has been delineated in 2020. Xie et al. [18] proposed a prediction error histogram shifting (PEHS)-based reversible data hiding scheme in 2020. The algorithm transforms the secret binary stream into a signed digital stream, and embeds the converted signed digital stream into the prediction error to obtain the adaptive embedding capacity. The proposed scheme has better embedding capacity than the existing schemes while maintaining good image quality.
3. Related Theories

3.1. Run Length Encoding
The preprocessing methods of information hiding are generally divided into several categories, such as scrambling encryption, information expansion, information verification processing, data compression, etc. Data compression can reduce the amount of data to be processed and reduce the amount of embedding. In this paper, we will use data compression as a carrier preprocessing method.

Run length encoding (RLE) algorithm is a method of data compression using spatial redundancy. Its basic idea is to replace a continuous string with its string length and a representative value with the same value. The continuous string is called the run length. In this algorithm, the repeated characters are expressed in a simple way, which saves the storage space and does not change the original data, so it achieves the purpose of lossless compression.

3.2. Scrambling Algorithm
Chebyshev map is a chaotic map with order as parameter proposed by Chebyshev. Let the vector space composed of all real valued continuous functions on \( C \{ -1,1 \} \) be a set of bases on \( C \{ -1,1 \} \). \( T_n(x) = \cos(n \arccos x) \), then \( T_n(x) \) is called the nth order Chebyshev polynomials.

When the number of iterations is \( k \), the Chebyshev map is as in (1).

\[
x_{n+1} = \cos(k \arccos x_n)
\]

Among this, \( x_n \in (-1,1) \), when \( k \geq 2 \), the mapping enters the chaotic region. Scrambling algorithm based on Chebyshev map is divided into the following steps.

**Step 1:** The chaotic random sequence \( X = \{x_1, x_2, \ldots \} \) is obtained. After iteration \( 8m \times n \) times of formula (1), \( m \) and \( n \) are the width and height of the image.

**Step 2:** Select 8 numbers from random sequence \( Y = \{y_1, y_2, \ldots \} \) to get a sequence \( X \).

**Step 3:** The sequence \( Y \) is scrambled once to get \( Y' = \{y'_1, y'_2, \ldots \} \).

**Step 4:** Get an index sequence \( D \), \( D = \{d_1, d_2, \ldots \} \), where \( d_i \) represents the position of the \( i \)-th number in the \( D \) sequence.

3.3. AMBTC Algorithm
The core of AMBTC algorithm is to ensure that the first-order absolute central moment of the image block remains unchanged before and after recoding. The calculation methods of the average value of the sample and the first-order absolute center distance of the sample are shown in equations 2 and 3 respectively.

\[
\bar{x} = \frac{1}{m} \sum_{i=1}^{m} x_i \\
\bar{a} = \frac{1}{m} \sum_{i=1}^{m} |x_i - \bar{x}|
\]

Then the bit plane (bit plane or bit map) corresponding to the image block is generated according to the mean value. The size of the bit plane is the same as that of the image block, and the elements in the bit plane may only be 0 or 1. If \( x_i \geq \bar{x} \), the element corresponding to the position in the bit plane is 1, otherwise it is 0. The image block is then reconstructed by a secondary quantizer using sample mean and sample variance. The secondary quantizer is shown in equations 4 and 5, where \( g \) is the number of pixels greater than or equal to \( \bar{x} \) in the image block.

\[
a = \bar{x} - \bar{a} \sqrt{\frac{g}{m - q}}, \text{for } x_i < \bar{x}
\]

\[
b = \bar{x} + \bar{a} \sqrt{\frac{g}{m - q}}, \text{for } x_i \geq \bar{x}
\]
3.4. Histogram Shift Algorithm

The algorithm proposed in this paper is based on the histogram shift. Because the histogram shift method itself is not robust, it is used on the high and low average value in AMBTC compressed domain in order to improve the robustness of the algorithm.

The horizontal axis X is the pixel value, and the vertical axis H is the frequency of the pixel value.

Step 1: Find the maximum frequency pixel value and the minimum frequency pixel value in the histogram of the image, which are $x_{H_{\text{max}}}$ and $x_{H_{\text{min}}}$ respectively. If $H(x_{H_{\text{min}}})$ is not 0, traverse all the pixels in the image, record the position of the pixel whose pixel value is $H(x_{H_{\text{min}}})$ in the image, and then set these pixel values as null, and then $H(x_{H_{\text{min}}}) = 0$.

Step 2: Shift all histogram bins between $x_{H_{\text{max}}}$ and $x_{H_{\text{min}}}$ to $x_{H_{\text{min}}}$ direction, and the shift distance is 1. As shown in Fig. 3, if $x_{H_{\text{max}}} < x_{H_{\text{min}}}$, the pixel value of these histogram bins will be increased by 1, otherwise, 1 will be reduced.

Step 3: If $x_{H_{\text{max}}} < x_{H_{\text{min}}}$, traverse the pixels in the graph in order. When $x_{H_{\text{max}}} = x_{H_{\text{min}}}$, if the embedded information is 0, then the pixel value remains unchanged. If the embedded information is 1, then the pixel value is added by 1, that is, $x = x_{H_{\text{max}}} + 1$, and continue to traverse until all the pixels are traversed or the information is embedded. If $x_{H_{\text{max}}} > x_{H_{\text{min}}}$, when the embedded information is 1, the pixel value is reduced by 1, and the remaining synchronization “Step 2”, as shown in Fig. 4. Therefore, the number of bits of embedded information capacity of this method is equal to $H(x_{H_{\text{max}}})$.

4. The Proposed Method

In this paper, a binary fingerprint image is used as the secret information. Figure 1 shows the process of information embedding.

4.1. Data Embedding

Step 1: Input a RGB based color image $X$ with $L \times L$ pixels. The RGB image $X$ is converted to YCbCr image, and the luminance component Y and color components CB, Cr are obtained.

Step 2: The AMBTC technique is used to compress each component to get two mean sequences (i.e. $L_i$ and $H_i$) and a bit plane $B_i$.

Step 3: The original information $M$ is compressed by RLE and scrambled by Chebyshev to obtain the secret information $\hat{w}$.

Step 4: The secret information $\hat{w}$ is embedded into the high and low average value sequence by histogram shift to obtain the coded mean sequence (i.e. $L'_i$ and $H'_i$). And the reserved information generated by histogram shift method is converted into binary information in the form of [information length, information content], which is recorded as R.

Step 5: Calculate the absolute difference between the mean sequences of color components, and divide the blocks into two categories: absolute smooth and normal.
Step 6: If the set threshold is greater than the absolute difference, the block is an absolute smooth block and use only $\eta$ for representing the block. Append "0" at the beginning of the block as a discriminator.

Step 7: Otherwise, the block is a normal block, and then the bits at positions 2, 4, 5, 7, 10, 12, 13, 15th from the bit-plane $B$ are deleted from the bit plane. "1" is appended at the beginning of the block as a discriminator.

Step 8: A new embedded information is obtained by concatenating the reserved information r and key K, in the form of $[R, \text{information length of key K, information content of key K}]$, and embedding the information into the deleted position.

Step 9: Carry out AMBTC inverse transformation on the mean sequence and the bit plane to obtain the luminance component, and carry out YCbCr inverse transformation on luminance and color component to obtain the carrier containing secret information $X^\ast$.

### 4.2. Data Extraction and Image Restoration

Step 1: Enter the carrier containing secret information $X^\ast$. Convert the RGB based the carrier $X^\ast$ into YCbCr image.

Step 2: In case of luminance component, using AMBTC to get two mean sequence (i.e. $L^\ast$ and $H^\ast$) and a bit plane $B^\ast$.

Step 3: If the classifier bit of color components (i.e., Cb and Cr) is "0", then the block is absolutely smooth. Then $\eta$ is filled in all the pixel positions to reconstruct the block.

Step 4: Otherwise, the block is a normal block, if there is data in the bits of position 2, 4, 5, 7, 10, 12, 13, 15th, the data (i.e. $R$ and $K$) will be extracted.

Step 5: Histogram shift is used to extract the embedded information $\hat{w}$ from the mean sequence (i.e. $L^\ast$ and $H^\ast$).

Step 6: The extracted information $\hat{w}$ is restored to the original information by key K.

Step 7: By replacing "0" and "1" of the transposition plane with $L^\ast$ and $H^\ast$ respectively, the deleted position of the block is reconstructed. Use Eq (6) to calculate the reconstruction value.

$$p_r = \frac{(p_1 + p_2 + p_3)}{3}$$

$$p_r = \frac{(p_1 + p_2)}{2}$$

$$p_r = \frac{(p_1 + p_2 + p_3)}{3}$$

$$p_r = \frac{(p_1 + p_2 + p_3)}{3}$$

$$p_{io} = \frac{(p_4 + p_5 + p_6)}{3}$$

$$p_s = \frac{(p_4 + p_5 + p_6)}{3}$$

$$p_s = \frac{(p_4 + p_5 + p_6)}{3}$$

$$p_{ii} = \frac{(p_7 + p_8 + p_9)}{2}$$

Step 8: The original image is restored by AMBTC and YCbCr technology.

### 4.3. Experiment

Experiment and simulate the algorithm in this paper and compare it with other algorithms from [32-35]. The experimental environment is Matlab2019a and Python 2019.3.3. The material of the carrier image set comes from USC-SIPI (http://sipi.usc.edu/database/) and Corel-5K (https://github.com/watersink/Corel5K).

This paper selects 6 images from three image data sets of USC-SIPI and Corel-5K respectively to store the secret image, and gives the experimental results. The results of invisibility experiment are shown in Figure 3. Where $S$ is the fingerprint image, $A_1-A_5$ are the carrier image and $B_1'-B_5'$ are the embedded image. There is almost no visual difference, which shows that the algorithm has better invisibility.
In PSNR experiment, we compare the algorithm proposed in this paper with the algorithms in literature [15-18]. The experimental data is shown in Figure 2. It can be seen from Figure 2 that the PSNR of this algorithm is superior to other comparison algorithms when \( k > 4 \). Meanwhile, when \( k > 11 \), the PSNR gradually leveled off. When \( k = 19 \), compared with the comparison algorithm, the average PSNR of the proposed algorithm is increased by 8.83%, 11.96%, 20.74% and 26.13% respectively, which indicates that the proposed algorithm has better invisibility.

Figure 2. Invisibility comparison experiment results

Figure 3. Invisibility experiment
The anti-attack of the information hiding algorithm is actually to check the robustness of the image, such as spatial filtering, lossy compression, geometric deformation, etc. In order to check the recovery degree of the extracted fingerprint image, the normalized correlation coefficient between the extracted image and the original image is used as the standard to evaluate the robustness of the algorithm.

The normalized correlation coefficient can be expressed as equation (7). The higher the NC value, the better the robustness of the algorithm.

\[
NC = \frac{N \sum w_i \hat{w}_i}{\sqrt{N \sum w_i^2 \sum \hat{w}_i^2}}
\]

\[\begin{align*}
\geq T, & \text{There is secret information } w \\
\leq T, & \text{There is no secret information } w
\end{align*}\]

In the formula, \( w_i \) is the pixel value of the original image coordinate point, \( \hat{w}_i \) is the pixel value of the extracted image coordinate point, and \( T \) is the preset threshold. After experiments, the value of \( T \) is set to 0.6.

The experimental results of extracting secret information after spatial filtering attack are shown in Figure 4. It can be seen that the NC value of the pre-processed secret information is still greater than 0.6 after being attacked by the spatial filtering. Therefore, it can be considered that the proposed information hiding algorithm can resist spatial filtering attack and Gaussian noise attack.

5. Conclusions

With the popularization and deepening of the Internet, the network environment is becoming more and more complex, and the research work in the field of information hiding has been paid more and more attention. The lack of information hiding algorithm in compressed domain hinders the practical application of information hiding technology to some extent. Therefore, it is necessary to strengthen the research of information hiding based on compressed domain. This paper proposes a color image information hiding algorithm based on AMBTC and histogram shift. After transforming RGB based image into YCbCr image, histogram shift technique is used to embed the information into the mean sequence generated by AMBTC. The simulation results show that, compared with the algorithms in references [15-18], the algorithm in this paper has better invisibility and robustness, the embedding capacity has been significantly improved, it can resist common image processing and attacks. But it is impossible to judge whether the information is attacked before the secret information is extracted. Therefore, in the next research work, we will use artificial neural networks and other algorithms to analyze the carrier to improve the efficiency of extracting secret information, and use support vector machines to classify the attacked carrier image in order to identify the type of attack.
References

[1] Weng S, Tan W, Ou B, et al. Reversible data hiding method for multi-histogram point selection based on improved crisscross optimization algorithm [J]. Information Sciences, 2021, 549:13-33.

[2] Senear H T, Memon N. Digital Image Forensics: There is More to a Picture han Meets the Eye [M]. Springer Publishing Company, Incorporated, 2012.

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

[4] Dong P, Qian H, Lu Z, Lan S. A Network Covert Channel Based on Packet Classification*. International Journal of Network Security, 2012, 14(2):109-116.

[5] Roy S D, Li X, Shoshan Y, Fish A, Yadid-Pecht O. Hardware Implementation of a Digital Watermarking System for Video Authentication [J]. IEEE Transactions on Circuits & Systems for Video Technology, 2013, 23(2): 300-312.

[6] Cheddad A, Condell J, Curran K, Mc Kevitt P (2010) Digital image steganography: survey and analysis of current methods. Signal Process 90: 727–752. https://doi.org/10.1016/j.sigpro.2009.08.010

[7] Subhedar MS, Mankar VH (2014) Current status and key issues in image steganography: a survey. Comput Sci Rev 13–14:95–113. https://doi.org/10.1016/j.cosrev.2014.09.001

[8] Yin Z, Ji Y, Luo B. Reversible Data Hiding in JPEG Images with Multi-objective Optimization [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2020, PP(99):1-1.

[9] LEMA M, MITCffiiLL O. Absolute moment block truncation coding and its application to color images [J]. IEEE Transactions on communications, 1984, 32(10):1148-1157.

[10] Rajeev Kumar, Samayveer Singh, Ki-Hyun Jung,(2019). Human Visual System based Enhanced AMBTC for Color Image Compression using Interpolation, 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN):903-907.

[11] Jayamol Mathews, Madhu S. Nair, and Liza Jo, “A Novel Color Image Coding Technique Using Improved BTC with k-means Quad Clustering”, Advances in Signal Processing and Intelligent Recognition Systems pp 347-357, 2014

[12] Ni, Z., Shi, Y.-Q., Ansari, N., & Wei, S. (2006). Reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology, 16(3), 354–362.

[13] Fallahpour, M., & Sedaghi, M.H. (2007). High capacity lossless data hiding based on histogram modification. IEICE Electronics Express, 4(7), 205–210

[14] Chen H, Ni J, Hong W, et al. Reversible data hiding with contrast enhancement using adaptive histogram shifting and pixel value ordering [J]. Signal Processing Image Communication, 2016, 46: 1-16.

[15] Amita, Amandeep Kaur, Marut Kumar. Reversible data hiding in absolute moment block truncation coding compressed images using adaptive multilevel histogram shifting technique [J]. Information and Computer Security, 2018, 10(2/3):261-275

[16] Wang, W., & Wang, W. (2020). New High Capacity Reversible Data Hiding Using the Second-Order Difference Shifting. IEEE Access, 8, 85367-85379. doi:10.1109/access.2020.2993604

[17] Sukumar, A., Subramaniyaswamy, V., Ravi, L., Vijayakumar, V., & Indragandhi, V. (2020). Robust image steganography approach based on RIWT-Laplacian pyramid and histogram shifting using deep learning. Multimedia Systems. doi:10.1007/s00530-020-00665-6

[18] Xie, X.-Z., Chang, C.-C., & Hu, Y.-C. (2020). An adaptive reversible data hiding scheme based on prediction error histogram shifting by exploiting signed-digit representation. Multimedia Tools and Applications, 79(33-34), 24329-24346. doi:10.1007/s11042-019-08402-6