IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 19, 2020, accepted June 29, 2020, date of publication July 2, 2020, date of current version July 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3006560

Multi-Carrier Information Hiding Algorithm Based on Angle Structure Descriptor

SHUAI REN, MENG WANG, KHURRAM SHAHZAD, ZE GAO, AND JIE XU
School of Information Engineering, Chang'an University, Xi'an 710064, China

Corresponding author: Meng Wang (mengwang@chd.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61702050, in part by the Double First Class Guiding Project of the Central University of China under Grant 300104292405, in part by the Fundamental Research Funds for the Central Universities, CHD, under Grant 300102240208, in part by the 2019 Chang'an University Graduate Education and Teaching Reform Construction Special Infrastructure Construction Project under Grant 300103190640, in part by the College Students' Innovation and Entrepreneurship Training Program under Grant 201910710079, Grant 201810710052, Grant 201810710060, Grant 201810710215, and Grant 201810710224, and in part by the Scientific Innovation Practice Project of Postgraduates of Chang'an University under Grant 300103703047.

ABSTRACT Aiming at the problem that the embedded capacity and security of the single-carrier information hiding algorithm can not be further improved because of the number of carriers, the carrier pre-processing and the embedding of secret information are combined with the image angle structure descriptor, and a multi-carrier information hiding algorithm based on the angle structure descriptor (ASD) is proposed. Firstly, the angle structure descriptors of the extracted image are used to classify the carrier set, and the image angle structure descriptor direction field coding is obtained. Secondly, the secret information is segmented according to the carrier classification number and the preprocessing such as scrambling and optimization is performed. Finally, based on the angle structure the coded data of the feature direction field performs information hiding on a plurality of types of carriers according to the information hiding rule. In particular, the ''judgment selection'' option is designed during secret information extraction to further improve the performance of the algorithm. The experimental analysis shows that the algorithm has good concealment, strong anti-analysis ability and robustness, and is suitable for applications such as large-capacity secret information covert communication with high security requirements.

INDEX TERMS Multi-carrier information hiding, secret communication, angle structure descriptor, ASD, HVS color quantization.

I. INTRODUCTION

With the rapid development of the Internet and multimedia technology, the transmission and sharing of multimedia information have become increasingly simple and convenient, which is convenient for people's lives and cause a lot of information security hidden danger. In the field of communication security and copyright protection, information hiding technology has unique advantages comparing with traditional cryptography technology. The transmission of secret information will be achieved by hiding the information to be protected in the public carrier. Digital image is vivid, intuitive nature and has a high popularizing rate and availability on the Internet. Digital image information hiding technology [1]–[4] using human visual redundancy to hide confidential information has become a research hotspot and attracted the attention of scholars.

According to the number of carriers, information hiding algorithms are divided into single-carrier and multi-carrier information hiding. Information hiding algorithm based on a single-carrier has own advantages in the spatial domain [5]–[8] or transform domain [9]–[11], but the shortcomings obviously cannot satisfy the higher application requirements. The information hiding algorithm in the mixed domain considers the strength of both the spatial domain and the transform domain. The reason is that the transform domain processes the carrier to obtain the embedded area that satisfying the requirement, and the secret information is embedded in the spatial domain to complete the information hiding. The algorithms have been favored by researchers. Zhang *et al.* [12] used the Local Binary Patterns (LBP) and texture feature identifying carrier region to embed encrypted information and calculate the difference matrix of adjacent pixels in the barrier area. The embedding space is constructed by shifting the histogram of the corresponding elements of the difference matrix to realize reversible information hiding of encrypted

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

information and the lossless recovery of the carrier image, and the robustness is strong. Yong *et al.* [13] applied color space technology in space domain to convert RGB image to YCbCr color mode, and used DCT for hiding information in YCbCr space, which has good performance in invisibility, embedded information and robustness. Chen *et al.* [14] did legal 5/3 integer wavelet transform for carrier image, and used histogram translation method to achieve secret information hiding in high frequency sub-band. The algorithm reduces the distortion of the image and has a large Embed capacity. Chen *et al.* [15] proposed a reversible information hiding method based on surface difference, encrypting the original image, and then using a random function to obtain the overlay pixels in the encrypted image, according to different inverted bits in the covered pixels. Different hiding methods are used according to different inversion bits in the overlay pixels. Mitekin and Fedoseev [16] proposed two kinds of multimedia information hiding algorithms based on quantization index modulation (QIM): IM-QIM and SIM-QIM, the algorithm can effectively resist statistical analysis, and the algorithm can also complete information hiding on the time and frequency domain of any multimedia data source. Pal *et al.* [17] proposed a weighted matrix based reversible watermarking algorithm. The algorithm decomposed the original image into R, G, B color components and partitions the pixel block, and embedded the secret information in the index file, which improved the embedding capacity of the secret information and the security of the algorithm. Malik *et al.* [18] proposed a new reversible information hiding algorithm for interpolated images based on pixel intensity range. The algorithm divided the pixel intensity range into several groups, and then embedded the secret data bits into the pixels adaptively according to the pixel intensity value. It can not only ensured the visual quality of the image carrier, but also improved the hiding ability of the image carrier. Chowdhuri *et al.* [19] proposed a dual color image information hiding algorithm based on the weighting matrix. The algorithm used shared key to generate different weighting matrices of the same dimension for security and embedding capacity.

Although the above information hiding algorithm based on single-carrier can complete the transmission of secret information, the algorithm cannot further improve the embedding capacity and security due to the limitation of the number of carriers. The explosive growth of image data on the Internet provides a big data application scenarios for steganographic analyst to use multiple carrier images for information hiding. Ker [20] proposed the concept of multi-carrier image steganography for the first time and changed the research goal of information hiding from hiding in a single-carrier to map from secret information to the carrier set [21]. The research represented by Zhang *et al.* [22] summarized the characteristics and necessity of multi-carrier information hiding and proved that multi-carrier information hiding analysis is very difficult. Chen *et al.* [23] constructed a steganography model for image sharing and proposed a multi-carrier image steganography algorithm based on Bernstein polynomial, which expanded the steganography capacity of image sharing and improved the security of secret information. Zhao *et al.* [24] proposed a general embedded strategy for multi-carrier image steganography in spatial domain and JPEG domain based on size-first rule and histogram equalization rule, which improved the security of steganography. Denemark and Fridrich [25] studied the side information of a group of images in the same scene, using multiple JPEG images to achieve information hiding. Zhou *et al.* [26] used BOW model to extract visual words from image sets. Then, each image is divided into several sub-images, visual keywords are calculated for each sub-image and a frequency histogram is counted, and information hiding is realized according to the mapping relationship between the text keyword and the sub-image visual keyword. Singh and Singh [27] proposed a visually meaningful multi-image encryption algorithm, which divided secret information into multiple images and generates new images with visual significance for transmission. The algorithm increased the embedding capacity of secret information, resisted multiple attacks, and had strong robustness. In the face of large-capacity secret information, the multi-carrier image information is concealed by multiple images as a carrier, and the classified information is dispersedly embedded in a plurality of carrier images to achieve more secure secret communication.

However, in the research of [23]–[27], when the information of multi-carrier is hidden, the carrier is reprocessed, and the secret information is embedded separately. So, the characteristics of the carrier image are not considered, and the correlation between the carriers is easily broken, resulting in greater distortion. In this paper, the ASD feature vector of the image is used to classify the carrier set, and the ASD feature vector is transformed into the directional field to represent the secret information. The carrier classification and the secret information are embedded by the image angle structure descriptor, and fully considering the influence of inter-pixel embedding, and a multi-carrier information hiding algorithm based on image angle structural feature is proposed. The ASD is used to preprocess the set of carriers to obtain different types and numbers of carrier images. The number of segments of large-capacity confidential information is determined according to the number of classifications. The same type of carrier embeds the same classified information to improve the robustness of the algorithm. Based on the ASD feature vector combining with the color field structure method, it modifies the carrier image and the invisibility of the algorithm can be enhanced. When the secret information is extracted, because the ASD feature vector includes the magnitude relationship of the image HSV color space quantization value, the consideration of the case where the color quantization difference value is 1 increases the difficulty of information hiding analysis.

The motivation and objective of the proposed algorithm are as follows:

1) *Security.* So far, encrypted image carriers are often attacked by malicious attacks such as signal processing,

lossy compression, random noise and so on in network transmission, which will lead to the loss of hidden information. Therefore, our goal is to propose a more robust and secure information hiding algorithm.

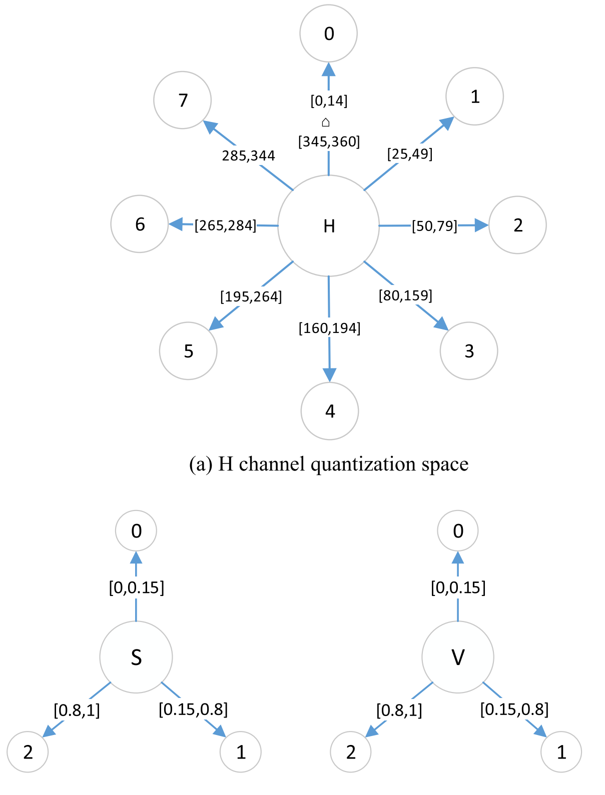
2) *Multi-carrier secret information hiding environment.* The existing information hiding algorithm based on a single carrier is limited by the number of carriers, so it is difficult to further improve the embedding capacity and security. Therefore, our goal is to reduce the embedding density of secret information hiding and propose a multi-carrier large capacity information hiding algorithm.
3) *Invisibility.* The current multi-carrier image information hiding algorithm does not take into account the image characteristics of multi-carrier, often easy to destroy the correlation between the carrier images, resulting in large distortion of the carrier image. Therefore, our goal is to avoid image distortion when embedding secret information and ensure the invisibility of the algorithm.
4) *Perceptual tampering.* Tampering attempts to affect or damage the image of the secret carrier. We hope to effectively detect the tampered situation of the secret carrier in the transmission process, and get complete and correct secret information.
5) *Anti-analysis.* At present, steganalysis detection technology is relatively mature. Our goal is to effectively resist the current steganalysis detection, prevent attackers from judging the existence of hidden information, and successfully extract the hidden information content.

II. ANGLE STRUCTURE DESCRIPTOR (ASD)

ASD was first proposed by Zhao *et al.* [28], which is based on the angle structure of the image. According to different directions, the angle structure is defined in the local block, and the color information in the HSV color space is combined to analyze the internal correlation between adjacent pixels in the structure to form a feature vector. Through the angle structure as a bridge, ASD integrates various information (including color, texture, shape, and spatial layout information) to extract image features, providing appropriate image resolution information for the information hiding algorithm.

A. IMAGE HSV COLOR SPACE QUANTIZATION

In the RGB (Red, Green, Blue) color space, there is a big gap between the chromaticity and perception of the object, while the HSV color space is relatively uniform, and the brightness component and the color difference information are weakly correlated, which is closer to the human visual perception. Using HSV color space to hide information can achieve good invisibility requirements. Based on the above, for an color image of $m \times n$,we transform the RGB color space into the HSV color space and quantize the HSV color space to better describe the color and shape information of the image, which lays the foundation for the subsequent extraction of ASD feature vector for carrier set classification and secret information embedding. The steps are as follows.



(a) H channel quantization space

(b) S channel quantization space (c) V channel quantization space

FIGURE 1. HSV color space quantization.

Step 1: The HSV color space contains three components: hue (H, $H \in [0, 360]$), saturation (S, $S \in [0, 1]$), and brightness (V, $V \in [0, 1]$). The HSV color space is quantized into 72 spaces, of which hue H is quantized into 8 spaces, saturation S and brightness V are quantized into 3 spaces respectively, which can not only integrate image details but also increase image processing space, as in Fig. 1.

Step 2: The three channels are divided based on the limit of human eye perception and the HSV color space characteristic. The H channel is divided into 8 regions (0-7), and the S and V channels are divided into 3 regions (0-2). Define the quantization function as in (1).

$$Q = Q_S Q_V H + Q_V S + V \tag{1}$$

where $Q_S = 3$ is the digitized number of S in the color space and $Q_V = 3$ is the digitized number of V in the color space.

Step 3: The two-dimensional matrix Q_C is obtained by uniformly quantizing the HSV color space of the color image $g(x, y)$ by (1). We define a pixel value (x, y) in the color image $g(x, y)$ as the corresponding quantized pixel value in Q_C, and $C(x, y) = \alpha, \alpha \in (0, 71)$. As in (2).

$$Q_C = \{(x, y)\,|(x, y) \in C, C(x, y) = \alpha, 0 \leq \alpha \leq 71\} \tag{2}$$

B. IMAGE ASD FEATURE VECTOR EXTRACTION

Human visual system is very sensitive to the angle variation, and image angle variation plays an important role in

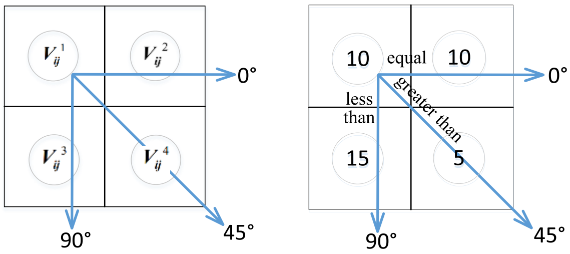


FIGURE 2. Angle and size relationship.

TABLE 1. Representation of size relationship under angle structure.

	Greater than	Equal	Less than
0°	$N_{0^\circ}^G$	$N_{0^\circ}^E$	$N_{0^\circ}^L$
45°	$N_{45^\circ}^G$	$N_{45^\circ}^E$	$N_{45^\circ}^L$
90°	$N_{90^\circ}^G$	$N_{90^\circ}^E$	$N_{90^\circ}^L$

visual perception. Therefore, this paper defines the angle structure in 2×2 image blocks based on three directions and provides an operational space for the information hiding carrier preprocessing while significantly describing the image features. ASD is described by the following steps.

Step 1: For each quantized color value α, $\alpha \in (0, 71)$ of color image $g(x, y)$, starting from the coordinate (0, 0), the "Z" shape from left to right and from top to bottom moves 2×2 local blocks to traverse the quantized color matrix Q_C, with the step d of 2 pixels, so Q_C is divided into a number of partial blocks $V_{ij}(j = \{1, 2 \ldots \frac{n}{2}\} \in N^*, j = \{1, 2 \ldots \frac{n}{2}\} \in N^*)$. For each partial block V_{ij}, if the color value $V_{ij}^1 = \alpha$ of the top left corner of the local block V_{ij}, the local block is retained, otherwise it is removed.

Step 2: For the remaining partial blocks V_{ij}, we obtain V_{ij}^1 of each of V_{ij}, the angle and size relationship of other color values (V_{ij}^2, V_{ij}^3, V_{ij}^4), as in Fig. 2.

Take the 0° angle structure as an example. If $V_{ij}^1 = V_{ij}^2$, it means "equal" relationship. If $V_{ij}^1 < V_{ij}^2$ or $V_{ij}^1 > V_{ij}^2$, it means "less than" or "greater than" relationship.

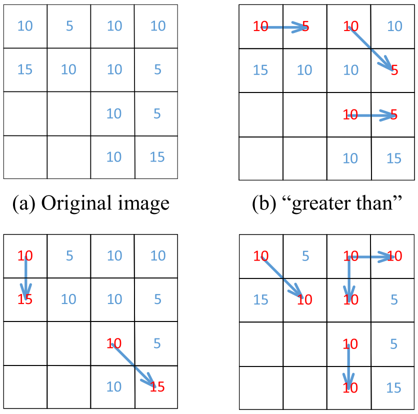
Step 3: Taking all angle structure into account, the size relationship of all local blocks V_{ij} under three angles is calculated. According to Table 1, a 9-dimensional vector describing the angle structure information is obtained.

$$(N_{0^\circ}^E, N_{0^\circ}^L, N_{0^\circ}^G, N_{45^\circ}^E, N_{45^\circ}^L, N_{45^\circ}^G, N_{90^\circ}^E, N_{90^\circ}^L, N_{90^\circ}^G)$$

For example, the image shown in Fig. 3(a) is the original image, and after statistics, the following 9-dimensional vector can be obtained (assuming the current quantized color value $\alpha = 10$).

$$(N_{0^\circ}^E, N_{0^\circ}^L, N_{0^\circ}^G, N_{45^\circ}^E, N_{45^\circ}^L, N_{45^\circ}^G, N_{90^\circ}^E, N_{90^\circ}^L, N_{90^\circ}^G) = (1, 0, 2, 1, 1, 1, 2, 1, 0)$$

Step 4: By combining the three angular directions, three relational graphs can be obtained, which respectively represent the greater than, equal, and less than the relationship in the angle structure. These three diagrams also represent a detailed description and features of the images to a certain extent, as in Fig. 3.



(a) Original image

(b) "greater than"

(c) "less than"

(d) "equal"

FIGURE 3. Original image example and relationship diagram.

Step 5: Multidimensional ASD feature vectors can be obtained by traversing all α values. If constructed directly, each image will get a $72 \times 9 = 648$ dimensional feature vector (a total of 72 quantized colors), and the vector dimension is too high. In order to reduce the vector dimension and the computational complexity, we define a three-dimensional vector $T = (t_1, t_2, t_3)$ to represent the angle structure, let $t_1 = 1$, $t_2 = 0$, $t_3 = 0$, define $T^{\mathrm{G}} = (1, 0, 0)$ means "greater than" relationship, similarly, $T^{\mathrm{E}} = (0, 1, 0)$, $T^{\mathrm{L}} = (0, 0, 1)$ means "equal" and "less than" relationship respectively. And the value is calculated as in (3).

$$T = \sum_{i=1}^{3} t_i 2^{(i-1)} \tag{3}$$

Step 6: Defining $L_{\alpha_{0^\circ}}$, $L_{\alpha_{45^\circ}}$, and $L_{\alpha_{90^\circ}}$ as the values of the three angle structures of the current quantized color value α and taking the 0° angle structure as an example, the value is obtained by (4).

$$L_{\alpha_{0^\circ}} = T^E N_{0^\circ}^E + T^L N_{0^\circ}^L + T^G N_{0^\circ}^G \tag{4}$$

$N_{0^\circ}^E, N_{0^\circ}^L, N_{0^\circ}^G$ can be obtained by *Step2*. Similarly, $L_{\alpha_{45^\circ}}$ and $L_{\alpha_{90^\circ}}$ can also be calculated. For each quantized color value α, we can get a three-dimensional vector $(L_{\alpha_{0^\circ}}, L_{\alpha_{45^\circ}}, L_{\alpha_{90^\circ}})$. ASD feature vector H (216 dimensions) of the image is obtained as in (5).

$$H = \begin{bmatrix} L_{0_{0^\circ}} L_{0_{45^\circ}} \; L_{0_{90^\circ}} \\ \cdots\cdots\cdots\cdots \\ L_{\alpha_{0^\circ}} L_{\alpha_{45^\circ}} \; L_{\alpha_{90^\circ}} \\ \cdots\cdots\cdots\cdots \\ L_{71_{0^\circ}} L_{71_{45^\circ}} \; L_{71_{90^\circ}} \end{bmatrix} \tag{5}$$

III. MULTI-CARRIER INFORMATION HIDING ALGORITHM BASED ON ASD

The core advantage of the multi-carrier information hiding algorithm is that the large-capacity secret information is scattered and hidden on multiple carriers, which reduces the hidden density and brings better invisibility and robustness, and greatly improves the security performance of information hiding. At present, most algorithms research focuses on the classification and fusion of multiple carriers. When a single carrier embeds secret information, it selects the mature information hiding algorithm to hide. However, these secret information hiding algorithms are often unable to effectively form a close relationship with the carrier. It is easy to cause distortion and bring security risks to the secret transmission of information. This paper first classifies the carrier library based on the image ASD features. Secondly, the ASD field structure after taking the mold 2π of ASD features was used to design the secret information hiding rules, so that the embedding of the carrier and the secret information is effectively connected. Finally, we optimize the secret information hiding by the scrambling and optimization algorithm to complete the information hiding.

A. CARRIER PRETREATMENT

Based on the ASD feature vector, the distance measurement formula $D(H, H')$ of two images is defined to calculate the similarity to complete the image classification, as in (6).

$$D(H, H') = \sum_{i=1}^{L} \frac{|Hi - H'i|}{1 + Hi + H_i'} \tag{6}$$

where H and H' are the eigenvectors of the two images respectively, and L is the dimension of the eigenvector.

After classifying the carrier library by using (6), the eigenvectors H of each carrier image, module 2π obtains the respective ASD directional field structure. As in (7), the ASD direction field structure is to express the ASD features in the form of direction field, so as to better implement information hiding by changing direction.

$$M = H \bmod 2\pi = \begin{bmatrix} m_{(0,1)}m_{(0,2)}m_{(0,3)} \\ \cdots\cdots\cdots\cdots \\ m_{(\alpha,1)}m_{(\alpha,2)}m_{(\alpha,3)} \\ \cdots\cdots\cdots\cdots \\ m_{(71,1)}m_{(71,2)}m_{(71,3)} \end{bmatrix} \tag{7}$$

B. INFORMATION HIDING RULES

In this algorithm, the "direction" of ASD direction field structure is used to represent information, and the direction (matrix M) is changed to achieve the purpose of information hiding. The information hiding rules are designed as follows.

Rule 1: the ASD direction field and the information rules represented are shown in Table 1, $\lambda = (0, 1, \ldots, 2^{p-1})$, $p = (0, 1, \ldots, +\infty) \in Z^*$.

Rule 2: when hiding information, the change of direction follows the principle of proximity. According to Table 2, the maximum change is $\pi/2^p$. When $p = 2$, the direction of ASD direction field structure and the schematic diagram of representative information are shown in Fig. 4. For example, all ASD field directions in the black area represent "00".

TABLE 2. Information hiding rule based on ASD direction field.

ASD direction	Represented information
$[\lambda\pi/2p-1,(1+4\lambda)\pi/2p+1)$	"00"
$[(1+4\lambda)\pi/2p+1,(1+2\lambda)\pi/2p)$	"01"
$[(1+2\lambda)\pi/2p,(3+4\lambda)\pi/2p+1)$	"10"
$[(3+4\lambda)\pi/2^{p+1},(1+\lambda)\pi/2^{p-1})$	"11"

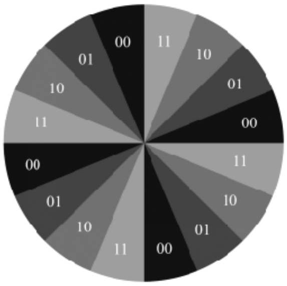


FIGURE 4. Information indicating area of ASD direction.

Rule 3: The carrier library is divided into n categories, make the number of segments l of large-capacity secret information B equal to the number of classifications n, and it is obtained that $B_1, \ldots, B_l, \ldots, B_n (l = 1, 2, \ldots, n)$. Under the maximum length of the embeddable secret information, it is segmented in the order from small to large, that is, $B_1 < \cdots < B_l < \cdots < B_n = B_{\max}$, different carriers embed different information, when extracting information, the segments of information are combined directly in the order of 1 to n. The same secret information B_l is embedded in many carriers of the same kind, at least one can be taken during extraction, which ensures the integrity of secret information transmission.

Rule 4: When modifying, it is preferred to change the "size" relationship to "equal". For example, if there are $V_{12}^1 < V_{12}^2$ and $V_{13}^1 = V_{13}^2$, consider changing the former to $V_{12}^1 = V_{12}^2$. When modifying, follow the principle of "changing small not changing big", define $\left|V_{ij}^1 - V_{ij}^a\right| = d_{ij}^a (a = 2, 3, 4)$. when there are $V_{12}^1 < V_{12}^2$ and $V_{13}^1 < V_{13}^2 (V_{12}^1 = 5, V_{12}^2 = 20, d_{12}^2 = 15, V_{13}^1 = 5, V_{13}^2 = 8, d_{13}^2 = 3)$, consider modifying the latter to $V_{13}^1 = V_{13}^2$. This is because the ASD field structure is obtained by the ASD feature vector which reflects the image features and details. Changing the direction of the ASD field structure is to change the size and quantity of V_{ij}^1 and other color quantization values V_{ij}^a, When the pixels of $d_{ij}^a \to 0$, V_{ij}^1 and V_{ij}^a are close to each other, the color of the original image is changed to the minimum. The human eye vision cannot be effectively identified, which improves the invisibility of the algorithm.

C. INFORMATION HIDING PROCESS AND STEPS

The information hiding of the algorithm in this paper is divided into the following steps, and the overall flow chart is in Fig. 5.

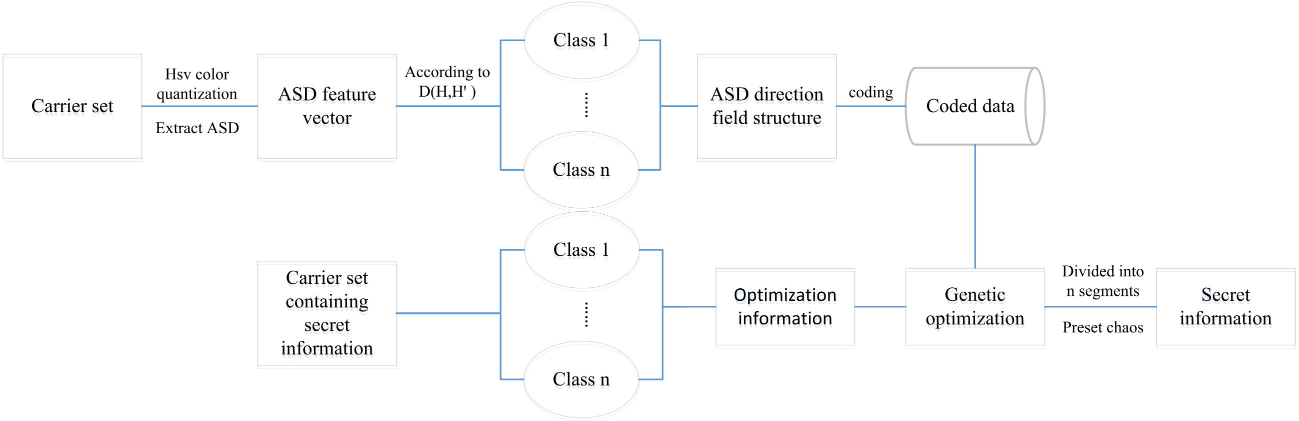


FIGURE 5. Hidden information flow chart.

Step 1: Perform HSV color quantization on the carrier set image, extract the ASD feature vector H of each carrier image in the carrier set, and divide them into n categories according to the distance measurement formula $D(H, H')$ defined in this paper. HSV color space is more uniform than RGB color space, and the correlation between brightness component and color difference information is weak. Quantization of HSV color space is helpful to better describe the color and shape information of image and ensure the invisibility of proposed algorithm.

Step 2: The large-capacity secret information is segmented according to "*Rule 3*" in the information hiding rule, and the number of segments is n. Under the condition that the number of secret information segments is the same as the number of carrier classification, different secret information is embedded in different carriers, and the same secret information is embedded in multiple similar carriers, which improves the robustness of the proposed algorithm. In the process of extracting information, the length of large capacity secret information is combined in order from small to large to avoid the missing of some secret information, ensure the integrity of secret information and realize more secure secret transmission.

Step 3: Calculate the ASD direction field structure M of the carrier picture by using (7). ASD can provide suitable image resolution information by extracting image features from the information of color, texture, shape, and spatial layout. Using ASD directional field structure to design secret information hiding rules to ensure the effectiveness of secret information embedding in the carrier image and enhance the robustness of the algorithm.

Step 4: According to the rules of information hiding in Table 1, the ASD field structure of the carrier picture is encoded by knight parade traversal, which is represented as C. By using knight tour to scramble the color value of the image, the secret information can be evenly distributed in the carrier space, and the recognizable secret information can still be obtained when the image containing the secret is subjected to non-severe attacks such as cutting, which effectively improves the robustness of the proposed algorithm.

$$C = (x_1, x_2, \ldots, x_i) \in \{0, 1\}$$

Step 5: The piecewise secret information uses Logistic mapping for chaotic scrambling. As in (8), the scrambling parameter μ and the initial value g_k are determined, and the piecewise secret information is scrambled according to the parameter g_k, and the scrambled bit sequence is denoted as $B_{IN}^{g}(i)$, $i = 1, 2, \ldots, n$. The complex encryption of secret information increases the complexity of the algorithm, enhances the anti-analysis of the algorithm, and also improves the success rate of secret information extraction.

$$g_{k+1} = \mu g_k(1 - g_k), \quad g_k \in (0, 1) \tag{8}$$

Step 6: Apply genetic algorithm for optimize adjustment. In Logistic mapping, scrambling parameter $\mu \in [3.5699456, 4]$, initial values $g_k \in (0, 1)$. The same number of corresponding bits of $B_{IN}^{g}(i)$ and sequence C are represented by F. Optimize to g_k maximize F as much as possible. The optimization model is shown in (9). First, set the iteration times t of genetic algorithm, make a binary code of the length i of the segmented secret information, and randomly obtain the initial segmented secret information population $B_{IN}^{g_0}(i)$. Then, the fitness of each individual in the secret information population is calculated by (9), so that population $B_{IN}^{g_t}(i)$ can get the next generation population $B_{IN}^{g_t+1}(i)$ after the operation of selection, crossover and variation. Finally, get the optimal parameter g_k when the number of corresponding bits F of sequence $B_{IN}^{g_t}(i)$ and sequence C is the same as large as possible. The optimal embedded bit $B_{IN}^{g_k}(i)$ is obtained by substituting the optimal solution g_k into $B_{IN}^{g}(i)$. The optimization algorithm is used to optimize the desire to hide the information, so that it can achieve maximum consistency with the embedded position of the carrier image. By optimizing parameter g_k, we can make the bit sequence $B_{IN}^{g}(i)$ after scrambling the segmented secret information and the ASD structure field coding sequence of the carrier image correspond to the largest number of bits as much as possible. In this way, while ensuring the maximum consistency, we can improve the matching degree between the information hiding embedding area and the embedding amount, and effectively increase the embedding capacity of the secret information.

$$F(z) = \max F(g_k) = \max \sum (x_n \bar{\oplus} g_n) \tag{9}$$

Step 7: Change the direction of ASD field structure according to the rules shown in Table 1, Hide the $B_{IN}^{g}(i)$ in the knight parade traversal order. According to "*Rule 4*", make corresponding changes to ASD feature vectors and change the size and quantity of corresponding color quantization values in different directions. The algorithm completes the embedding of the secret information by modifying the direction of the ASD direction field structure, that is, the final modification is the color value V_{ij}^{1} of each local block of the color image and the size of the other color quantization value V_{ij}^{a}. The design follows the "changing small not changing big" modification principle to ensure that V_{ij}^{1} and V_{ij}^{a} pixels as close as possible. The minimization of color change of the original diagram not only improves the invisibility of the algorithm, but also reduces the risk of dense images being discovered by third parties in the transmission process, and effectively enhances the security of the algorithm.

Step 8: Repeat the above *Step3-Step7*, and finally get a carrier set containing secret information.

D. EXTRACTION OF INFORMATION

When extracting information, multiple carriers carry multiple copies of the same secret information. When one or more of them are obviously different from most other secret information, it can be determined that they are damaged or tampered with under attack, which improves the perceived tampering of the algorithm. In addition to extracting ASD field structure directly from multiple carriers, multiple copies of the same secret information were extracted according to the rules shown in Table 1. Since the ASD feature quantity changes very little when the information is hidden, especially considering the case where the current color quantization value α is $d_{ij}^{a} = 1$, The size relationship under the angle structure of the two is regarded as equal for secret information extraction, and the secret information extracted in the two cases is compared with other different segment information combinations, and the selection and retention are performed according to the complete meaning of the secret information, further improving the robustness of the algorithm.

Step 1: Perform HSV color quantization on the obtained carrier set image, extract the ASD feature vector H of each carrier image in the carrier set, and classify according to the distance metric formula $D(H, H')$ defined in this paper.

Step 2: For each type of carrier picture, extract multiple pieces of secret information $C_{IN}^{g}(i)$ from the same type of carrier for comparison and judgment. When one or several copies are significantly different from most other secret information, it is determined to be damaged or tampered by attack and discarded.

Step 3: For the 1/2 carrier of the same kind of carriers retained, the ASD directional field structure M of the carrier picture is calculated directly by the ASD feature vector using (7) , and extract secret information $C_{IN}^{g}(i)$ according to the hiding rules shown in Table 1.

Step 4: For the remaining 1/2 carrier, $d_{ij}^{a} = 1$ is regarded as $d_{ij}^{a} = 0$ under the current color quantization value α, that is, the size relationship between them under the angle structure is regarded as equal, and secret information $C_{IN}^{g'}(i)$ is extracted.

Step 5: Repeat *Step2-Step4* above, obtain secret information $C_{IN}^{g}(i)$ and $C_{IN}^{g'}(i)$ of each segment $(i = 1, 2, \ldots, n)$, calculate its length and size, sort and combine them according to "*Rule 3*" in the information hiding rule respectively, obtain complete secret information C_{IN}^{g} and $C_{IN}^{g'}$, selects and retains correct large capacity secret information according to the meaning shown.

IV. PERFORMANCE ANALYSIS AND EXPERIMENTAL COMPARISON

A. PERFORMANCE ANALYSIS OF THE ALGORITHM

1) INVISIBILITY ANALYSIS

The algorithm in this paper performs information hiding by changing the direction of the ASD field structure. Firstly, the ASD field structure is transformed from the ASD feature vector, which fully considers the influence of image's features and details on the invisibility. Secondly, the hidden area can be divided intensively as much as possible with the help of computer (usually, the parameter $k \geq 8$, the maximum change angle is less than 0.7°). Thirdly, when the information is hidden, it follows the principle of "the size relationship is changed to equal" and the principle of difference between the color quantization values is changed to "changing small but not large". The three points above make the algorithm not only consider the human visual rules, but also make the carrier image change less when information hiding. Logistic chaotic map scrambling and genetic optimization algorithm greatly reduce the change of hidden information to the carrier image and ensure the invisibility of the algorithm.

2) ROBUSTNESS ANALYSIS

Information hiding algorithms based on multi carrier have the robustness that the single carrier information hiding algorithm can't compare. When the secret information is transmitted, it is not only one, but also distributed and hidden in multiple types and quantities of carriers, which fully guarantees the robustness of the algorithm. At the same time, the algorithm of this paper is based on ASD design, which covers the characteristics of image energy and color uniformity and enhances the robustness to some extent. After the color values of the image are scrambled by the knight-tour, the secret information is evenly distributed in the carrier space to ensure that the carrier can still get recognizable secret information when it is attacked by non-severe attacks such as cutting, so as to improve the robustness of the algorithm.

3) PERCEIVED TAMPERING ANALYSIS

The algorithm uses the principle of "judging selection" in information extraction, that is, in information extraction, especially considering that the current color quantization value and the adjacent color quantization value are only one difference the extracted secret information is selectively retained, so that the algorithm has a high ability of perceptual tampering.

4) ANTI-ANALYSIS ANALYSIS

The algorithm of this paper is based on ASD. Information hiding is to modify the basic elements (color, structure) of the image. In theory, it can almost completely resist the analysis based on statistical characteristics and random characteristics of bit plane.

B. THE EXPERIMENTAL COMPARISON

In the actual communication process, the transmitted image with secret information may be damaged or seriously attacked by a third party. A series of tests were carried out on the algorithm and compared with other algorithms. The experimental environment is Matlab 8.3.0.532, Python 3.4.6, and the benchmarks standard image databases comes from Corel-5K, Caltech 101, COIL-100. In this paper, the algorithms proposed in [12], [17], [18], and [23] are selected as experimental references.

1) INVISIBILITY EXPERIMENT

According to the rules of information hiding, $p = 10$ and $d_{ij}^{a} = 5$ are selected, and the experimental results are given by taking the scale secret information S of three kinds of six images as an example. The carrier image, hidden information and image with secret information are shown in Fig. 6, where S is the hidden information, A_1-C_2 is the original carrier image, A'_1-C'_2 is the image with secret information.

Compared with the carrier image and the image with secret information, the image with secret information has a good visual effect and imperceptibly. The average PSNR of the image with secret information and the carrier image is 46.4217, which has high invisibility. According to the information hiding rules, p parameter determines the division density of the hidden area. The higher the density is, the smaller the field direction changes, and the higher the invisibility is.

As in Fig. 7 below, when $k > 10$, the PSNR value is higher than other algorithms, and with the increase of embedding capacity, the distortion of the image changes slowly. When $k = 20$, the algorithm in this paper is compared with the proposed algorithm in [12] (LBP), the proposed algorithm in [17] (WMR), the proposed algorithm in [18] (PIR), and the proposed algorithm in [23] (SaS) in the literature, the PSNR increased by 17.93%, 3.09%, 22.21%, and 32.85% respectively. The robustness was superior to that of the other algorithms.

Based on the Corel-5K, Caltech 101, and COIL-100 image databases, we selected 20, 50 and 100 images for embedding secret information, and the data of Fig. 8 show that the PSNR of the algorithm increases with the increase in the number of image carriers. When 100 images of different carrier databases are selected, the high invisibility of the average PSNR of 49.4243 can be achieved.

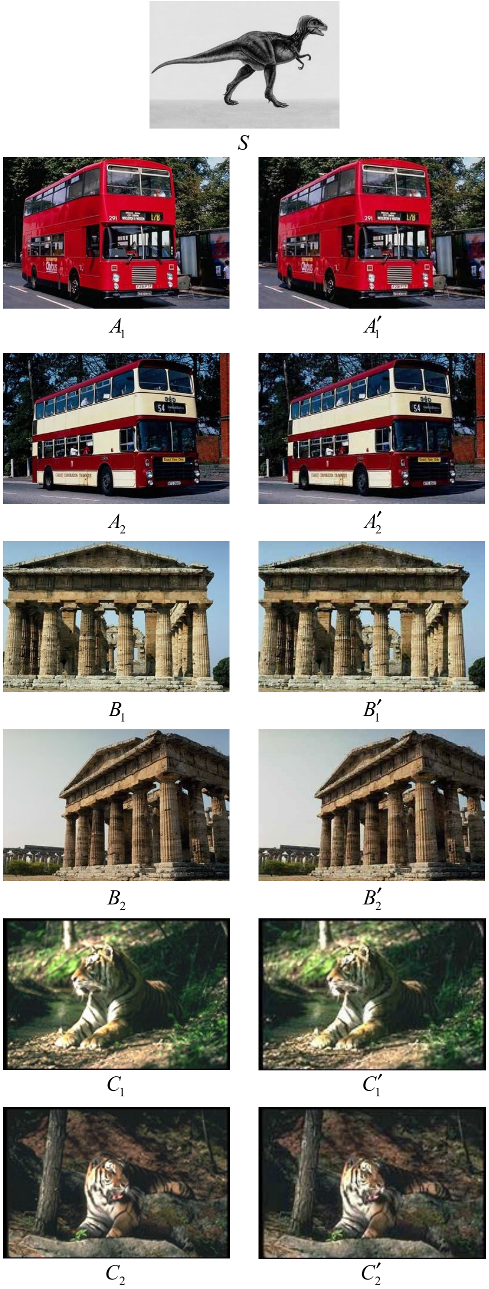


FIGURE 6. **Original carrier and secret carrier.**

2) ROBUSTNESS EXPERIMENT

Robustness is a measure of the degree of modification of secret information after an attack on dense images, and it is also the ability of the algorithm to extract valid information after an attack. In this paper, we measure the robustness of the algorithm, and carry out single attack and compound attack respectively. The single attack includes cutting attack, compression attack, rotation attack and noise attack. Among them, the robustness test value of the multi-carrier information hiding algorithm is represented by the robustness average value of all carrier images.

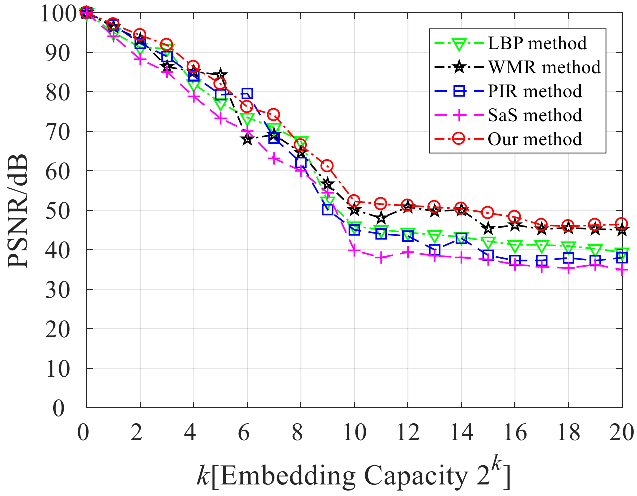


FIGURE 7. Invisibility comparison experiment results.

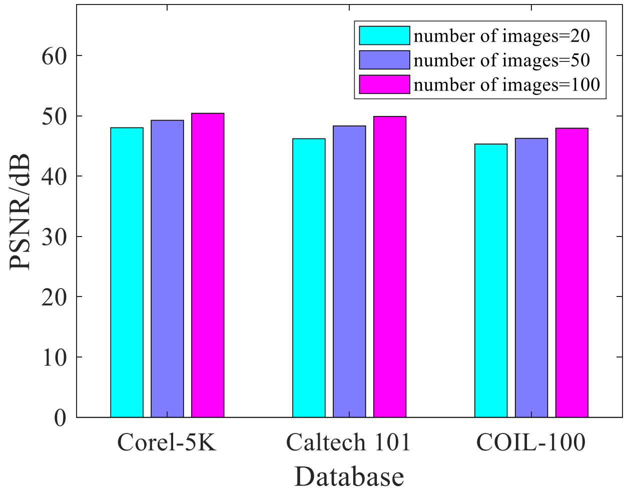


FIGURE 8. Experimental results of PSNR (dB) with images of different databases.

a: SINGLE ATTACK EXPERIMENT

The robustness of multi-carrier information hiding algorithm is based on the robustness of local carrier. Firstly, the robustness of the algorithm on local carrier is tested. In the actual transmission of common channel, image is most vulnerable to compression, cutting, rotation, noise and other related attacks. Taking the dense image A'_1 as an example, Fig. 9, Fig. 10, Fig. 11, and Fig. 12 show the comparison with the experimental results of LBP, WMP, RID, and SaS algorithms under the cutting attack, compression attack, rotation attack and noise attack, where Q represents the robustness test value [29].

As in Fig. 9, in the face of compression attack with 30% compression rate, the robustness Q value of the proposed algorithm is 86.00, while the robustness Q value of LBP, WMR, PIR, and SaS is 75.06, 76.41, 72.42, and 63.80, that is to say, the robustness Q value of the algorithm in this paper is 14.58%, 12.55%, 18.75%, and 34.80% higher than that of LBP, WMR, PIR, and SaS respectively.

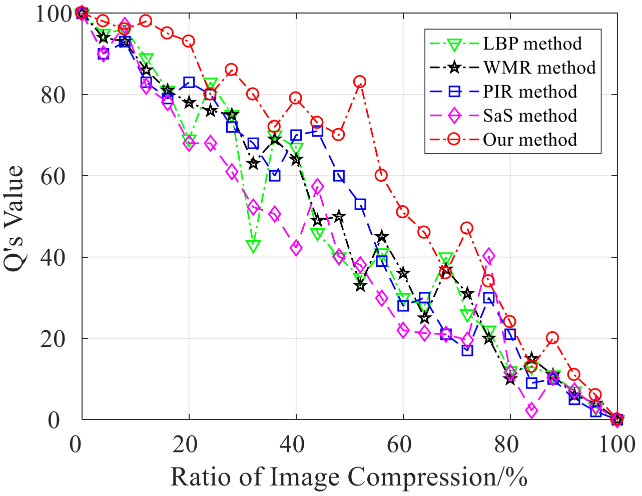


FIGURE 9. Compression attack comparison test result.

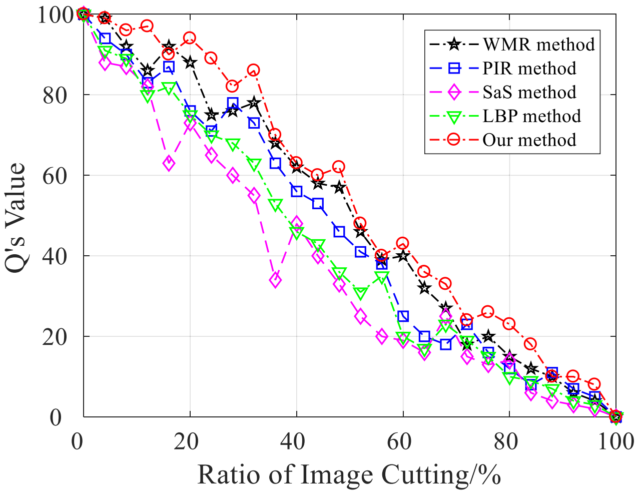


FIGURE 10. Cutting attack comparison test result.

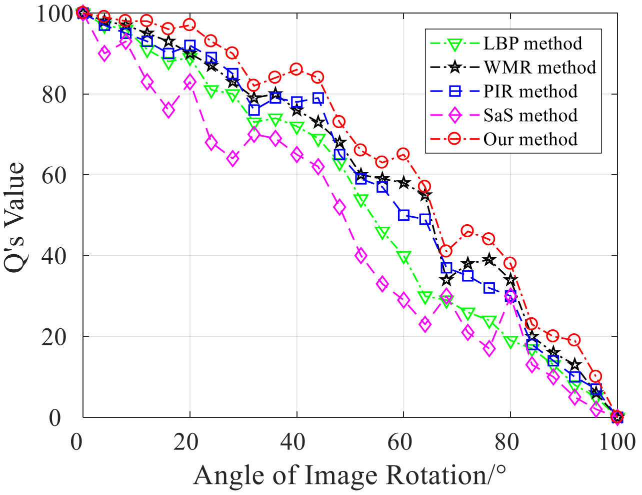


FIGURE 11. Rotation attack comparison test result.

As in Fig. 10, when the cutting rate is 25%, the robustness Q values of our algorithm, LBP, WMR, PIR, and SaS are

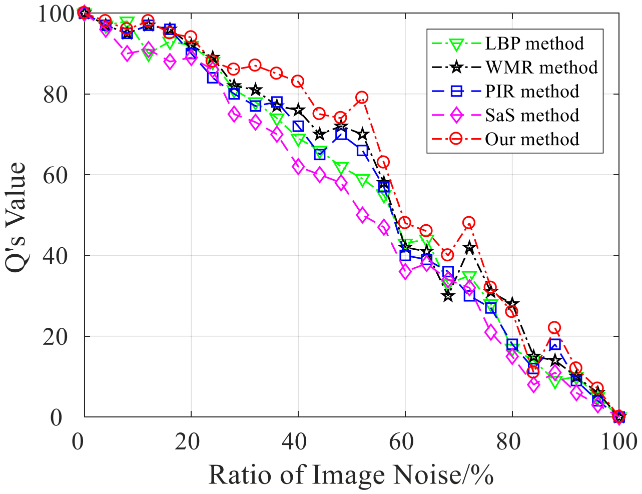


FIGURE 12. Noise attack comparison test result.

89.31, 70.61, 75.25, 71.43, and 64.90 respectively, that is, the robustness Q values of our algorithm are 26.48%, 18.68%, 25.03%, 37.61% and higher than those of LBP, WMR, PIR, and SaS respectively. Fig. 11 shows that the robustness Q values of our algorithm, LBP, WMR, PIR, and SaS are 84.57, 69.22, 73.63, 79.28, and 62.48 respectively when in the face of rotating 45° anticlockwise attack, that is, our algorithm improves the robustness Q values of LBP, WMR, PIR, and SaS by 22.18%, 14.86%, 6.67%, and 35.36%, respectively. Fig. 12 shows that when the noise intensity is 40%, the robustness Q values of our algorithm, LBP, WMR, PIR, and SaS are 83.92, 69.42, 76.02, 72.37, and 62.12 respectively, that is, the robustness Q values of our algorithm are 20.89%, 10.39%, 15.96%, and 35.09% higher than those algorithms of LBP, WMR, PIR, and SaS respectively.

Besides, we randomly selected images from Corel-5k, Caltech 101 and COIL-100 image databases for the same 25% cutting, JPEG2000 compression, 45° counterclockwise rotation, and 40% noise attack experiments. As in Fig. 13, based on the images in the Corel-5K, Caltech 101 and COIL-100 image databases, the algorithm is carried out on the above four single attacks, the average robust value Q of each carrier image databases can reach 84.19, 88.20, 84.76, which shows that the proposed algorithm has good robustness in the face of different image databases.

b: COMPOUND ATTACK EXPERIMENT

In the actual transmission of public channels, images are not only vulnerable to single attacks of compression, cutting, rotation and noise, but also can be compound attacks by these single attacks.

We carried out a series of compound attack experiments on our method. Table 3 and Fig. 14 give the experimental data of 14 compound attacks. As in Table 3, Cut, Com, Rot and Noi represent 25% cutting, JPEG2000 compression, 45° counterclockwise rotation and 40% noise attack, respectively.

As in Table 3 and Fig. 14, the PSNR value of the algorithm is 39.3147 under the attack of 25% cutting,

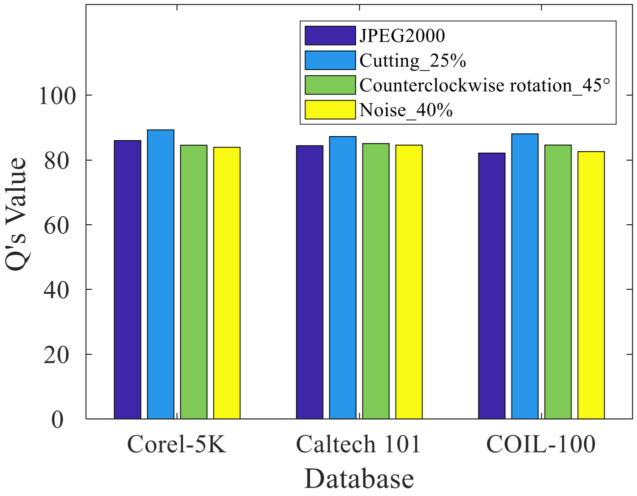


FIGURE 13. Single attack experiment results for different image databases.

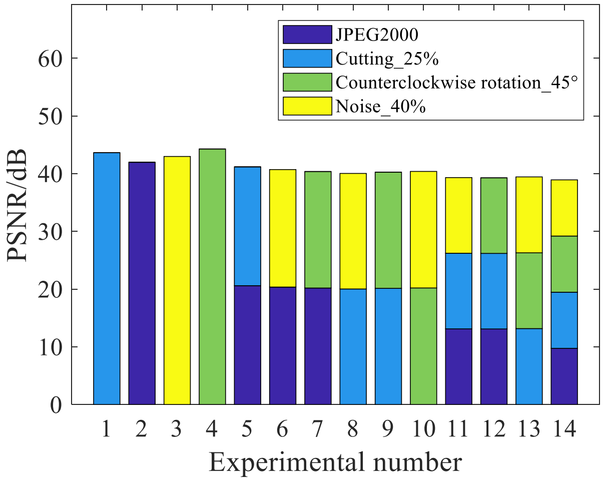


FIGURE 14. Compound attack experiment results of different image databases.

JPEG2000 compression and 40% noise at the same time. The PSNR of the algorithm is 39.4643 under the attack of 40% noise, 45° anticlockwise rotation and 25% cutting at the same time. The PSNR value can still up to 38.9208 under the high-intensity compound attack of 25% cutting, 40% compression, 45° counterclockwise rotation, and 40% noise. In conclusion, the proposed algorithm has good robustness and can resist effectively in the face of high-intensity compound attack.

3) ANTI-ANALYSIS EXPERIMENT

The steganographic analysis of image generally distinguishes whether the carrier information contains secret information according to the change of statistical characteristics of the carrier information before and after hiding. Common analysis methods include χ^2 detection, RS detection, DIH detection, and grayscale analysis detection [30]. The design of steganographic analysis algorithm relies heavily on the design of information hiding algorithm. The joint analysis method for

TABLE 3. Compound attack experimental data (based on PSNR).

Experimental Number		The carrier with secret information						PSNR/dB
		A_1'	A_2'	B_1'	B_2'	C_1'	C_2'	
Experiment 1		Cut	/	/	/	/	/	43.6238
Experiment 2		/	/	Com	/	/	/	41.9642
Experiment 3		/	/	/	/	Noi	/	42.9736
Experiment 4		/	/	/	/	/	Rot	44.2753
Experiment 5		/	Com	Cut	/	/	/	41.1739
Experiment 6		Noi	/	/	Com	/	/	40.7024
Experiment 7	Attacks types	/	/	/	/	Rot	Com	40.3694
Experiment 8		/	/	Cut	/	/	Noi	40.0359
Experiment 9		Cut			Rot	/	/	40.2584
Experiment 10			Rot	Noi	/	/	/	40.5832
Experiment 11		Com	/	/	Noi	Cut	/	39.3147
Experiment 12		/	Cut	/	Com	/	Rot	39.2712
Experiment 13		/	Rot	/	Cut	/	Noi	39.4643
Experiment 14		/	Com	Rot	/	Noi	Cut	38.9208

multi-carrier information hiding proves that the analysis of multi-carrier information hiding is very difficult, but the rapid development of machine learning technology makes it possible to quickly complete the steganalysis of multiple local carriers in the channel by using the mature single-carrier steganalysis method and integrate the analysis results. In this paper, the gray-scale image of carrier A_1 is selected as the experimental sample of anti-detection analysis, and LBP, WMR, PIR, and SaS algorithm are used as the comparison group. The grayscale parameters of the original carrier image and the indexes of each algorithm are shown in Fig. 15(a)-(f).

From the comparison of the genealogical data of each object in Fig. 15, it can be seen that the difference between the genealogical data of the embedded image and the original carrier image is very small in this algorithm, and the anti-analysis is good. The genealogical data of the embedded image and the original carrier image with LBP, WMR, PIR, and SaS algorithm are quite different, with relatively weak anti-analysis. In addition, we use RS detection method and χ^2 detection method to experiment with this algorithm.

a: RS DETECTION METHOD

RS detection method (regular/singular group of pixels, RS), namely double statistics detection analysis method [31], [32], which is an effective analysis method of LSB information hiding by analyzing the relationship and difference between adjacent colors of secret image. RS detection detects whether the information is hidden by comparing the difference between R_m and R_{-m} and between S_m and S_{-m}. The figure below shows the analysis results of RS analysis method for this algorithm.

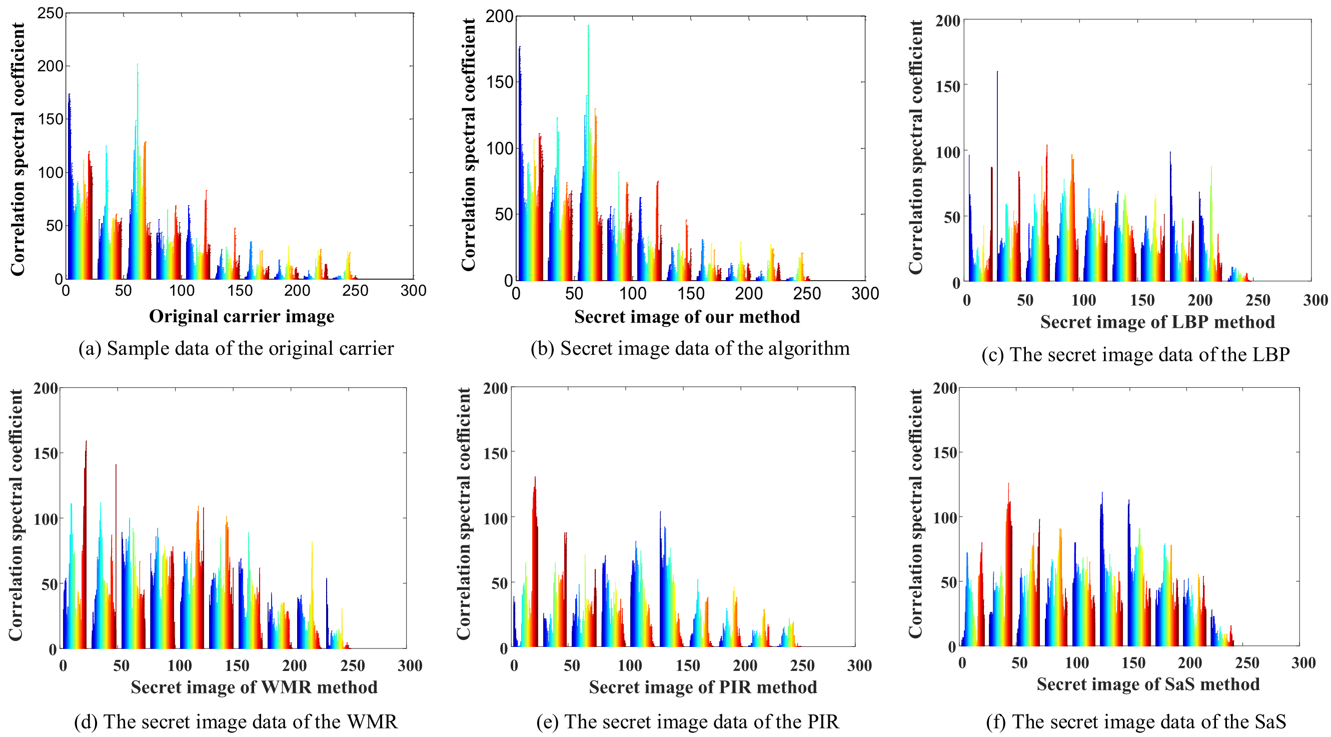
According to the experimental data of Fig. 16, on the basis of the initial deviation (about 165) of RS analysis algorithm, the maximum difference of R is 317, and the maximum difference of S is 149, and the hiding rate has no positive effect on the difference. Randomly select 100, 500, 1000 pictures from Corel-5k, Caltech 101 and COIL-100 image databases for testing, as in Fig. 17, the detection rate is lower than 2.96%, indicating that the algorithm is resistant to RS information hiding analysis.

b: χ^2 DETECTION METHOD

χ^2 analysis method [33] is a detection method for spatial steganography of color image, which detects the existence of secret information according to the statistical characteristics of the proximity of gray value pairs before and after embedding secret information. If the secret information is not embedded in all the pixels, and the embedding position is randomly distributed in the whole image, the method is difficult to work.

Randomly selected 100, 500, 1000 pictures from Corel-5K, Caltech 101, COIL-100 image databases for testing, and as in Fig. 18, the detection rate was less than 1.97%, indicating that the algorithm resists information hiding analysis and proves the effectiveness of the algorithm.

From the experimental data of RS detection method and χ^2 detection method in Fig. 17 and Fig. 18 for different image databases, it can be seen that the detection accuracy of RS



(a) Sample data of the original carrier

(b) Secret image data of the algorithm

(c) The secret image data of the LBP

(d) The secret image data of the WMR

(e) The secret image data of the PIR

(f) The secret image data of the SaS

FIGURE 15. **Anti-analysis comparison experiment results.**

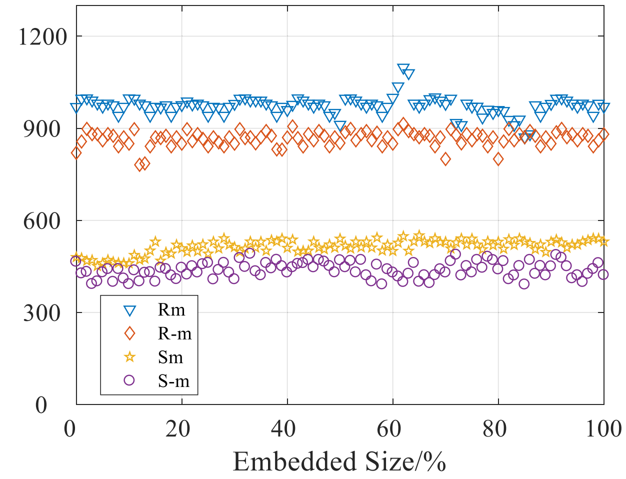


FIGURE 16. **RS detection analysis results.**

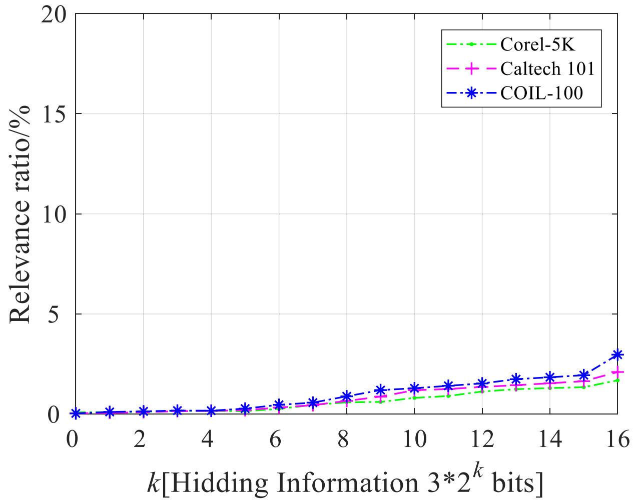


FIGURE 17. **The detection rate of RS detection analysis.**

detection method for COIL-100 image database is significantly higher than that of Corel-5k image database, while the detection accuracy of χ^2 detection method for Caltech 101 image database is lower than that of COIL-100 image database. This is because the performance of current general steganalysis methods depends on images from different sources. When the training image source does not match the detection image source, the performance of steganalysis detection will also be affected. At the same time, although the current general steganalysis technology can detect many hiding methods, it can not reliably detect the low embedding rate. The proposed algorithm is based on the low density hidden space of multi-carrier to realize the embedding of secret information, and the embedding position of secret information is randomly distributed in the whole image, which greatly reduces the embedding density of a single image. Compared with χ^2 detection method, RS detection method is more sensitive to steganalysis in case of low embedding rate. As in the experimental data in Fig. 17 and Fig. 18, the detection rate of RS detection method is slightly higher than that of χ^2 detection method. The experimental data show that the above two detection methods are based on different image data, the detection accuracy is not more than 2.96%, the detection accuracy is low, which shows that the proposed algorithm has good anti-analysis resistance.

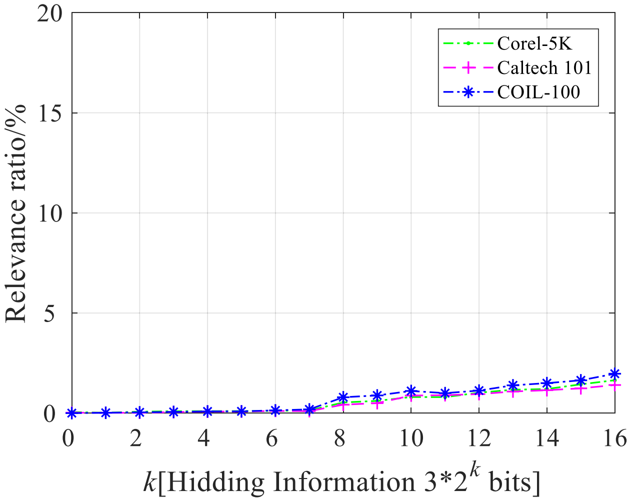


FIGURE 18. The detection rate of χ^2 detection analysis.

V. CONCLUSION

This paper proposes a multi-carrier information hiding algorithm based on angle structure descriptor. Different from the traditional image sharing information hiding algorithm, considering the feature details of carrier image comprehensively, the embedding effect between pixels is considered on the basis of ensuring the connection between the carriers, and the classification of the carrier is closely combined with the embedding strategy of the secret information by using the image angle structure descriptor together, the angle structure characteristic information of the image is transformed into the transformation of the effective information representation of the direction field. The simulation results show that the algorithm is suitable for the application scenarios with large hidden information capacity and high security requirements. The algorithm has excellent concealment and strong anti-analysis ability and can resist most image processing attacks. At the same time, there is still much for improvement in the proposed algorithm. In the next research work, we will explore how to make better use of the correlation between image carriers in order to improve the embedding capacity and robustness of multi-carrier information hiding algorithms. Furthermore, it is one of the key points of future research to find the embedded location of secret information to construct random distribution, and further reduce the embedding rate of secret information, so as to enhance the anti-analysis of the algorithm.

REFERENCES

[1] X. Zhang, Z. Sun, Z. Tang, C. Yu, and X. Wang, "High capacity data hiding based on interpolated image," *Multimedia Tools Appl.*, vol. 76, no. 7, pp. 9195–9218, Apr. 2017.

[2] X. Zhang, Z. Tang, T. Liang, S. Zhang, Y. Zhu, and Y. Sun, "Data hiding method based on local image features," in *Active Media Technology*, vol. 5284. Berlin, Germany: Springer, 2012, pp. 247–256.

[3] C. Qin, P. Ji, X. Zhang, J. Dong, and J. Wang, "Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy," *Signal Process.*, vol. 138, pp. 280–293, Sep. 2017.

[4] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, Mar. 2019.

[5] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho, and K.-H. Jung, "Image steganography in spatial domain: A survey," *Signal Process., Image Commun.*, vol. 65, pp. 46–66, Jul. 2018.

[6] M. C. Trivedi, S. Sharma, and V. K. Yadav, "Analysis of several image steganography techniques in spatial domain: A survey," in *Proc. 2nd Int. Conf. Inf. Commun. Technol. Competitive Strategies (ICTCS)*, Udaipur, India, Mar. 2016, pp. 1–7.

[7] A. H. S. Abdelgader, R. A. Aboughalia, and O. A. S. Alkishriwo, "Combined image encryption and steganography algorithm in the spatial domain," in *Proc. 1st Conf. Eng. Sci. Technol.*, vol. 1, Nov. 2018, pp. 119–138.

[8] N. Mukherjee, G. Paul, and S. K. Saha, "An efficient multi-bit steganography algorithm in spatial domain with two-layer security," *Multimedia Tools Appl.*, vol. 77, no. 14, pp. 18451–18481, Mar. 2018.

[9] M. Y. Valandar, P. Ayubi, and M. J. Barani, "A new transform domain steganography based on modified logistic chaotic map for color images," *J. Inf. Secur. Appl.*, vol. 34, pp. 142–151, Jun. 2017.

[10] A. Miri and K. Faez, "Adaptive image steganography based on transform domain via genetic algorithm," *Optik*, vol. 145, pp. 158–168, Sep. 2017.

[11] X. Hu, J. Ni, and Y.-Q. Shi, "Efficient JPEG steganography using domain transformation of embedding entropy," *IEEE Signal Process. Lett.*, vol. 25, no. 6, pp. 773–777, Jun. 2018.

[12] T. Zhang, Y. Liu, S. Ren, and D. Zhang, "Differential histogram shift lossless information hiding algorithm based on LBP face texture feature," *Appl. Res. Comput.*, vol. 37, no. 6, pp. 1774–1778, May 2019.

[13] Z. Yong, L. L. Cai, L. Q. Shen, and J. Z. Tao, "A blind watermarking algorithm based on block DCT for dual color images," in *Proc. 2nd Int. Symp. Electron. Commerce Secur.*, Nanchang, China, May 2009, pp. 213–217.

[14] L. Chen, H. W. Liu, and X. H. Deng, "Reversible watermarking algorithm for digital image based on integer wavelet transform," *Comput. Appl. Softw.*, vol. 33, no. 4, pp. 286–291, Apr. 2016.

[15] Y. Chen, C. Yu, X. Zhang, Z. Tang, and N. He, "Reversible information hiding method in encrypted image based on surface interpolation," *J. Appl. Sci.*, vol. 36, no. 2, pp. 220–236, Mar. 2018.

[16] V. A. Mitekin and V. A. Fedoseev, "New secure QIM-based information hiding algorithms," *Comput. Opt.*, vol. 42, no. 1, pp. 118–127, Mar. 2018.

[17] P. Pal, P. Chowdhuri, and B. Jana, "Weighted matrix based reversible watermarking scheme using color image," *Multimedia Tools Appl.*, vol. 77, no. 18, pp. 23073–23098, Jan. 2018.

[18] A. Malik, G. Sikka, and H. K. Verma, "A reversible data hiding scheme for interpolated images based on pixel intensity range," *Multimedia Tools Appl.*, pp. 1–7, Jan. 2020.

[19] P. Chowdhuri and B. Jana, "Hiding data in dual color images reversibly via weighted matrix," *J. Inf. Secur. Appl.*, vol. 50, pp. 102420–102434, Feb. 2020.

[20] A. Ker, "Batch steganography and pooled steganalysis," in *Information Hiding*. Alexandria, VA, USA: Springer, Jul. 2006, pp. 265–281.

[21] R. Gonzalez, R. Woods, and S. Eddins, *Digital Image Processing Using MATLAB*. Upper Saddle River, NJ, USA: Prentice-Hall, 2005.

[22] X. Zhang, Z. Qian, and S. Li, "Prospects of information hiding research," *J. Appl. Sci.*, vol. 34, no. 5, pp. 475–489, Mar. 2016.

[23] G. Chen, H. Shen, Y. Wu, and J. Chen, "Research on multi-carrier image separation and steganography algorithm," *Comput. Eng*, vol. 38, no. 4, pp. 116–118, Apr. 2012.

[24] Z. Zhao, Q. Guan, X. Zhao, H. Yu, and C. Liu, "Universal embedding strategy for batch adaptive steganography in both spatial and JPEG domain," *Multimedia Tools Appl.*, vol. 77, no. 11, pp. 14093–14113, Aug. 2017.

[25] T. Denemark and J. Fridrich, "Steganography with multiple JPEG images of the same scene," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 10, pp. 2308–2319, Oct. 2017.

[26] Z.-L. Zhou, Y. Cao, and X.-M. Sun, "Coverless information hiding based on bag-of-words model of image," *J. Appl. Sci. Electron. Inf. Eng.*, vol. 34, no. 5, pp. 527–536, Sep. 2016.

[27] L. D. Singh and K. M. Singh, "Visually meaningful multi-image encryption scheme," *Arabian J. Sci. Eng.*, vol. 43, no. 12, pp. 7397–7407, Feb. 2018.

[28] M. Zhao, H. Zhang, and L. Meng, "An angle structure descriptor for image retrieval," *China Commun.*, vol. 13, no. 8, pp. 222–230, Aug. 2016.

[29] S. Ren, T. Zhang, D. Mu, W. Hu, and D. Zhang, "Research on information hiding algorithm based on GHM multi-wavelet and adaptive color migration," *J. Northwestern Polytech. Univ.*, vol. 28, no. 2, pp. 264–269, Apr. 2010.

[30] T. Pevný and J. Fridrich, "Benchmarking for steganography," in *Information Hiding*, vol. 5284. Berlin, Germany: Springer. 2008, pp. 251–267.
[31] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color, and gray-scale images," *IEEE Multimedia Mag.*, vol. 8, no. 4, pp. 22–28, Dec. 2001.
[32] J. Fridrich and M. Goljan, "Practical steganalysis of digital images: State of the art," *Proc. SPIE*, vol. 4675, pp. 1–13, Apr. 2002.
[33] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *Information Hiding*, vol. 1768. Berlin, Germany: Springer, 2000, pp. 61–76.

SHUAI REN received the Ph.D. degree in computer science from Northwestern Polytechnical University, Xi'an, China, in 2010. He is currently an Associate Professor with the School of Information Engineering, Chang'an University. His research interests include information hiding, image processing, 3D model processing, network communication security technology, digital forensics technology, and information security risk assessment technology.

MENG WANG received the B.S. degree from Weinan Normal University, Weinan, China, in 2018. She is currently pursuing the master's degree with the School of Information Engineering, Chang'an University. Her research interests include information hiding, image processing, and 3D model processing.

KHURRAM SHAHZAD received the B.S. degree from the Islamia University of Bahawalpur, Punjab, Pakistan, in 2013. He is currently pursuing the master's degree with the School of Information Engineering, Chang'an University. His research interests include information hiding, computer networking, and image processing.

ZE GAO received the B.S. degree from the North University of China, Taiyuan, China, in 2018. He is currently pursuing the master's degree with the School of Information Engineering, Chang'an University. His research interests include information hiding algorithm and image compression.

JIE XU received the B.S. degree from Pingdingshan University, Pingdingshan, China, in 2017. He is currently pursuing the master's degree in information engineering with Chang'an University. His research interests include information hiding technology, image processing, and 3D model representation.