IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 18, 2020, accepted November 11, 2020, date of publication November 24, 2020,
date of current version December 10, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3040005

Identifiable Tampering Multi-Carrier Image Information Hiding Algorithm Based on Compressed Sensing

SHUAI REN[1], TAO ZHANG[2], MENG WANG[1], AND KHURRAM SHAHZAD[1]

[1]School of Information Engineering, Chang'an University, Xi'an 710064, China
[2]School of Electronic and Control 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 security problem of secret information preprocessing and the difficulty of improving the capacity and robustness of the single-carrier image information hiding algorithm, an identifiable tampering multi-carrier image information hiding algorithm based on compressed sensing is proposed. Firstly, the angle structure descriptor feature vector was used to preprocess and classify the image carrier set. Secondly, the GHM multiwavelet transform was applied to different types of image carriers to obtain the secret information hiding area which can balance the invisibility and robustness. Thirdly, the secret image was processed by compressed sensing, the resulting observation matrix was decomposed by singular value, and the chaotic scrambling was encoded by logistic mapping. Finally, the secret information was embedded in the image singular value to complete the information hiding of different types of multi-quantity image carriers. Combined with the angle structure descriptor of the image, the algorithm proposed an effective way to organize multiple carriers, which improved the embedding quality and efficiency of secret information. The verification data and segmented secret information classification and embedding strategy made the proposed algorithm have a keen ability to detect tampering and effectively improve the efficiency and integrity of secret information extraction. Experimental results show that compared with image sharing information hiding algorithm and the single-carrier information hiding algorithm based on compressed sensing, the invisibility and robustness of our algorithm are significantly improved. At the same time, the proposed algorithm has strong anti-analysis ability, can effectively resist most image processing attacks, and is suitable for large capacity secret communication and high-security applications.

INDEX TERMS Multi-carrier information hiding, compressed sensing, angle structure descriptor, multiwavelet transform, singular value decomposition.

I. INTRODUCTION

In the network communication environment with no boundary and low-security threshold, security problems related to digital media occur frequently. Using these free spreading digital media to hide information to realize the transmission and communication of secret information can effectively solve the information security problem. In the era of big data, various types of image data have exploded, providing a large number of big data scenarios suitable for practical applications for information hiding technology based on digital images. Among many information hiding algorithms, the pursuit of algorithm performance improvement is the main research purpose, and the selection and processing of carriers have become an important breakthrough for performance improvement.

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

Xiang and Luo [1] proposed a novel reversible data hiding scheme for encrypted images by using homomorphic and probabilistic properties of the Paillier cryptosystem. The algorithm uses reference pixels and host pixels to generate a mirroring ciphertext group (MCG) for data embedding, to avoid oversaturation of pixels in the plaintext domain, and extract hidden data directly from the encrypted domain. This algorithm has low computational complexity, high-security performance, and good embedding performance. Li and Zhang [2] proposed a construction-based data hiding technique that transforms a secret message into a fingerprint image directly. They proposed to map the secret message to a polynomial and encode it into a set of points with different polarities, from which the spiral phase is computed and constructed. The synthesized fingerprint image is decomposed to construct continuous phase. The spiral phase and the continuous phase are combined to form the hologram phase. The algorithm has good data extraction accuracy and robustness, and can effectively resist the existing steganalysis. Wang and Zhang [3] proposed a cover selection method which is secure in both image and individual level by restraining MMD distance and searching the minimal steganographic distortion images, which selected the smallest steganographic distortion image to embed information in the acceptable computational complexity. The algorithm can effectively resist pooled steganalysis and single object steganalysis meanwhile. Yin *et al.* [4] proposed a high-capacity RDHEI algorithm based on multi-MSB (most significant bit) prediction and Huffman coding. In this algorithm, Huffman coding is used to compress auxiliary information better and make more space for embedding information. Multi-MSB replacement is used to adaptively embed multiple bits, which improves the embedding capacity of secret information. Huang *et al.* [5] proposed a reversible data hiding in encrypted image capable of ciphertext-only attack (COA). Under the encryption strategy of XOR and scrambling, this algorithm proposes a way to free space by combining wave function and lossless compression, and realizes information hiding by bit flipping technology. The algorithm is completely reversible, which effectively overcomes the defect that the existing bit flipping algorithm can not extract secret information from the ciphertext image. Based on the number of carriers, information hiding algorithms can be divided into the single-carrier and multi-carrier information hiding. The current information hiding algorithms based on digital images are mainly divided into three categories: spatial domain algorithms, transform domain algorithms, and hybrid domain algorithms (use both spatial domain and transform domain) according to the embedded area, each of which has its unique advantages and disadvantages. Based on the information hiding algorithm of single-carrier, it has a good inability to implement information hiding directly in the space domain, but its robustness is weak. However, when information hiding is implemented on the transform domain alone, the robustness is strong, but the invisibility is poor. The single-carrier information hiding algorithm based on spatial domain and transform domain has its advantages, but it is difficult to meet the higher application requirements. The information hiding algorithm based on hybrid domain processes the carrier and obtains the embedding area which meets the requirements. The secret information is embedded in the spatial domain to complete the information hiding, which takes into account the advantages of both the spatial domain and the transform domain. At present, the information hiding algorithm based on single-carrier is relatively mature and has achieved many research results. Most of the existing information hiding algorithms are based on single-carrier. According to the design, analysis, and experiment of information hiding algorithm based on single carrier, there are some limitations such as relatively small capacity of secret information hiding and low absolute security.

The concept of multi-carrier image information hiding was first proposed by Ker in 2006. Since then, Ker *et al.* have carried out a series of researches on multi-carrier image information hiding, mainly focusing on both implicit capacity and embedded strategy. In terms of steganography capacity, in 2006, Ker [6] defined the security of multi-carrier information hiding based on certain assumptions and proved that the secure steganography capacity of multi-carriers is proportional to the square root of the number of carriers. Subsequently, in 2009, Ker [7] studied the difference of steganography capacity between finite and infinite number of carriers. In 2010, Ker [8] proposed keyless embedding. When using multiple pixels to transmit 1 bit of secret information, as long as the amount of secret information does not exceed the limit of the square root law, even without any key, the steganography security can be nearly perfect. The embedding strategy mainly studies how to distribute secret information among multiple carriers. In 2006, Ker [9] proposed to select as few carriers as possible to embed secret information based on the security analysis of the test. In the subsequent research on multi-carrier adaptive image steganography game theory, Ker [10] proposed two relatively secure strategies in 2007. One is to select as few carriers as possible to embed secret information, and the other is to embed secret information into all carriers as widely as possible. In addition, in order to solve the problem that the embedding strategy mentioned above is limited by a certain detection framework, Ker [11] in 2008 proposed the optimal embedding strategy for multi-carrier steganography with fixed number of carriers and continuous steganography with infinite number of carriers by linking the statistical detectability of embedding strategy and payload with the square of embedding change. At the same time, Ker [12] pointed out that the best embedding strategy for independent and distributed vectors is to distribute secret information evenly across all carriers. Then, in 2012, Ker and Pevny [13] proposed five embedding strategies, max-greedy, max-random, linear, even, and sqroot, respectively. They tested the performance of the five different steganalysis strategies against the universal joint steganalysis method and pointed out the nonlinear relationship between the embedding distortion and the payload.

The research results of the multi-carrier image information hiding algorithm provide strong support for the construction of large capacity secret information embedding space, and also provide a new idea for the research of information hiding algorithm. Liao and Yin [14] proposed two steganography strategies for multi-carrier images. Among them, the embedding strategy based on the texture complexity of the carrier image calculates the maximum steganography capacity of the carrier quantitatively according to the texture complexity of the image, and embeds the secret information into the part with the largest steganography capacity. The embedding strategy can allocate more secret information for the carrier image with complex texture. The embedding strategy based on the statistical distribution of carrier image distortion distributes the secret information to all the carrier images, and embeds the secret information by combining the statistical distribution proportion of all image distortion values. The embedding strategy can allocate more secret information for the carrier image with less distortion. The above two steganography strategies reduce the overall distortion of multi-carrier image steganography and enhance the security of multi-carrier image steganography. Zhao *et al.* [15] proposed a universal embedding strategy for multi-carrier image steganography in both spatial domain and JPEG domain based on size first rule and histogram equalization rule respectively, which improved the security of steganography. Huang and Shao [16] proposed a multi-carrier dense image sharing method based on EMD-c^l, which used the embedding method to store any gray level dense image into multiple carriers. The algorithm has low complexity and high security, and is suitable for security scenarios with high requirements on visual quality of the embedded carrier and different resolution and gray level dense image sharing. Liao *et al.* [17] proposed a multi-image adaptive payload distribution steganography algorithm based on image texture features. The algorithm proposed two payload allocation strategies based on image texture complexity and distortion. These two strategies have high-security performance in multi-image information hiding. Yang and Liao [18] proposed a multi-image information hiding strategy by fusing multiple image features. The algorithm used multiple features to quantitatively describe the complexity of the image. Considering the number of images in the steganalysis system and the number and size of the images allocated to the steganographic system, the algorithm iteratively selected the maximum capacity image embedding payload that has not been used. The algorithm has good security performance for blind pool steganalysis.

In recent years, compressed sensing (CS) technology has attracted much attention in image, audio, and video signal processing. As long as the receiver adopts reasonable reconstruction algorithm, it can solve the problem of information sparseness caused by compressed sensing and recover the original information. It is widely used in image encryption. In 2006, Candes *et al.* [19] proved mathematically that some Fourier transform coefficients can accurately reconstruct the original signal, laying a theoretical foundation for CS. Based on these researches, Donoho [20] formally proposed the concept of compressed sensing theory and related theoretical frameworks. Huang *et al.* [21] studied the weakness of CS-based encryption schemes that cannot resist the chosen-plaintext attack and proposed a parallel image encryption method based on compressed sensing. The algorithm designs a block cipher structure composed of scrambling, mixing, and S-box with chaotic lattice, which can resist selected plaintext attacks. Bao and Zhou [22] used simple image encryption technology (such as changing the position and value of image pixels) to pre-encrypt the original image, and then used the content conversion based on integer wavelet transform to transform the pre-encrypted image into a visually meaningful encrypted image and output it. The algorithm has good security and security. Zhang *et al.* [23] designed the SCS encryption model and designed a secure parallel compressed sensing scheme using random permutation, which realized asymptotically spherical secrecy. The algorithm is robust to additive white Gaussian noise and cutting attacks. Xiao *et al.* [24] proposed an encrypted image watermarking algorithm based on compressed sensing for high-quality image reconstruction and watermarking performance. The algorithm creatively generates the watermark location key according to the image's characteristics, and then uses it to embed the watermark information into the compressed sensing domain, which can not only improve the embedding capacity and robustness of the watermark but also make use of the reconstruction characteristics of the compressed sensing to obtain a higher quality restored image. The algorithm has the potential for efficient privacy-preserving signal processing applications. Chen *et al.* [25] proposed a cryptosystem for simultaneous image encryption and compression. Its compression performance is realized by CS, and the contribution of security comes from CS and permutation diffusion process. The scheme has good compression and encryption performance, and is suitable for the safe transmission and compression of images on the public network. Xu *et al.* [26] proposed an image encryption algorithm based on CS and 2D-SLIM mapping. In this algorithm, row and column permutation is applied to transform coefficients of common images before compression, which improves image compression performance. A diffusion algorithm based on Galois field multiplication is designed to encrypt the compression matrix, and the cipher image with small size and high security is obtained. The algorithm has good compression performance and high security. Wang *et al.* [27] proposed a secure compressive sensing method based on the combination of chaotic discrete wavelet transform (DWT) and chaotic discrete cosine transform (DCT) measurement matrix. The algorithm can not only achieve image encryption and compression simultaneously but also enlarges the keyspace and improves the quality of the reconstructed image. Chai *et al.* [28] proposed a color image compression and encryption scheme based on compressive sensing and double random encryption strategy. The algorithm used compressive sensing makes the volume of cipher image be less, and then the transmission bandwidth and storage space have been saved. The algorithm has large keyspace, high key sensitivity, and may resist some known attacks.

The current information hiding mainly preprocesses the hidden carrier to select a suitable hidden area, and the preprocessing of secret information mostly relies on the scrambling algorithm in cryptography, such as the commonly used Arnold scrambling processing. Due to the inherent periodicity of the Arnold scrambling algorithm, the original secret image after the scrambling process can also be restored through a limited number of anti-scrambling processes. Therefore, the secret information after Arnold scrambling may also be due to poor security. It is easy to be attacked, and when the secret image is destroyed, it is difficult to extract effective and complete secret information, which reduces the security of information transmission. When the compressed sensing technology is used as the preprocessing method of secret information, as long as the receiver adopts reasonable reconstruction algorithm, the problem of sparse secret information caused by compressed sensing can be solved and the original information can be recovered, which can effectively improve the security problem caused by the destruction of the secret carrier and the difficulty of extracting the original secret information effectively.

Based on the security problem of secret information preprocessing in the previous image information hiding algorithms and the difficulty in further improving the capacity and robustness of the single-carrier image information hiding algorithm, this paper proposes an identifiable tampering multi-carrier image information hiding algorithm based on compressed sensing. The algorithm preprocesses the image carrier set through the ASD feature vector of the image to obtain different types and numbers of carrier images. According to the classification number, the segment number of large-capacity secret information is determined. The same secret information is embedded in the same type of carrier to improve the robustness of the algorithm. The carrier image is decomposed by the GHM multiwavelet transform theory. According to the characteristics of energy distribution, the sub-image with lower energy weight is selected as the secret information hiding area, which effectively enhances the invisibility and anti-analysis of the algorithm. In the secret information preprocessing stage, the secret information is directly sparsely observed and then compressed and sensed, which can avoid the problem of weak security caused by the preprocessing of the scrambling algorithm, thereby improving the anti-attack of the secret information and the robustness of the algorithm. Using the stability of singular values to embed secret information, reduce the difference between the carrier image and the dense image, and further enhance the robustness of the algorithm.

The innovative points and main motivations of the algorithm proposed in this paper are as follows.

(1) *Large-capacity and low-density multi-carrier information hiding environment.* While the mass transmission in the era of big data provides the possibility of large-capacity information hiding algorithms, it also puts forward higher requirements on the algorithms. We hope to build a large-capacity and low-density secret information embedding environment to realize information hiding.

(2) *Propose a way to effectively organize multiple carriers.* In the process of multi-carrier image information hiding, the characteristics of the carrier image should be considered, and the correlation between carriers should be maintained as much as possible to reduce embedding distortion. We hope to fully consider the correlation between the pixels of the carrier image, and propose a way to effectively organize multiple carrier images to preprocess the multi-image carrier to improve the embedding quality and efficiency of secret information.

(3) *Invisibility. Invisibility is the basic security requirement that information hiding algorithms need to meet.* Our goal is to combine the correlation between multi-carrier image features to complete information hiding, avoid image distortion, make human senses unable to perceive the existence of secret information, and ensure the invisibility of the algorithm.

(4) *Robustness.* In the process of network transmission, the encrypted image carrier will inevitably suffer from single attacks such as signal processing, lossy compression, random noise, or their combined attacks. Our goal is to make the algorithm robust against common malicious attacks and ensure the safe transmission and successful extraction of secret information.

(5) *Perceive tampering.* The encrypted carrier is not only vulnerable to malicious attacks in the process of open channel transmission but also may encounter the situation that the encrypted carrier is tampered with by a third party. We hope that the algorithm has a keen ability to perceive tampering, to quickly determine the perceptual tampering in the secret extraction stage. While improving the efficiency of secret information extraction, it can ensure the final extraction of complete and correct secret information.

(6) *Anti-analysis resistance.* Compared with invisibility, anti-analysis resistance has higher security requirements. We hope to make the hidden information have good distribution and hiding characteristics to improve the anti-analysis performance of the algorithm and effectively resist the current steganalysis detection.

The rest of the paper is organized as follows. Section II introduces the latest four related theories. Section III describes the proposed method in detail. Section IV shows experimental results and analysis. Section V concludes this paper and explains the future work.

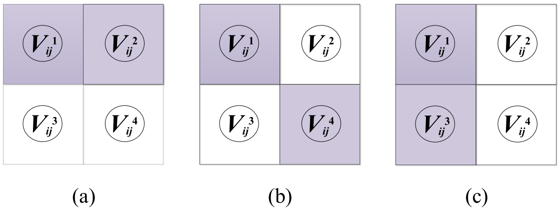

FIGURE 1. Angel structures based on three directions. (a) angle structure of 0°. (b) angle structure of 45°. (c) angle structure of 90°.

II. RELATED THEORIES

A. IMAGE ANGLE STRUCTURE DESCRIPTOR(ASD)

The image is composed of many local blocks, which can be used to describe different image attributes to a certain extent. Zhao *et al.* [29] proposed an image feature representation method based on the angle structure of the image, namely the angle structure descriptor. ASD combines the color information in the HSV (Hue, Saturation, Value) color space to analyze the internal correlation between adjacent pixels in the structure, and defines the angle structure in the 2 × 2 local blocks according to the difference in direction. ASD can effectively describe image features by exploring the internal connections of local blocks. The steps to extract the image ASD are as follows.

Step1. HSV color space quantization. The HSV color space is more uniform and closer to human visual perception. The HSV quantization of the image can not only integrate the image details but also increase the image processing space, which meets the invisibility requirements of the information hiding algorithm. For a pixel value (x, y) in the color image $Q(x, y)$, defined $C(x, y)$ as the corresponding quantized pixel value in the two-dimensional matrix after the color image is uniformly quantized in the HSV color space, and $C(x, y) = \alpha, \alpha \in (0, 71)$.

Step2. Partial image block division. For each quantized color value α, $\alpha \in (0, 71)$ of the color image $g(x, y)$, starting from the coordinate $(0, 0)$, moving from left to right and from top to bottom in a "Z" shape 2 × 2 local block $V_{2\times2}$, traverse the quantized color matrix M_C with 2 pixels as the step size, so that M_C is divided into many local blocks $V_{ij}(i = \{1, 2\cdots\frac{m}{2}\} \in N^*, j = \{1, 2\cdots\frac{n}{2}\} \in N^*)$, and all image blocks V_{ij} are arranged in rows, denoted as Q_i. For each local blockV_{ij}, when the color value V_{ij} of the upper left corner of the local block $V_{ij}^1 = \alpha$, the local block is retained, otherwise it is removed.

Step3. Angle structure calculation. For the retained partial block V_{ij}, obtain the angle and size relationship between V_{ij}^1 and other color values (V_{ij}^2, V_{ij}^3, V_{ij}^4) in each V_{ij}, as shown in Fig. 1. Taking the angle structure of 0° in Fig. 1(a) as an example, if the value V_{ij}^1 is equal to the value of V_{ij}^2, it means equal correlation. If the value V_{ij}^1 is less than or greater than the value of V_{ij}^2, it means that the correlation is small or the correlation is greater. Taking into account the structure of all angles, the size relationship of all the local blocks V_{ij} under the three angles as shown in Table 1, we obtain a 9-dimensional vector $(N_{0^\circ}^E, N_{0^\circ}^L, N_{0^\circ}^G, N_{45^\circ}^E, N_{45^\circ}^L, N_{45^\circ}^G, N_{90^\circ}^E, N_{90^\circ}^L, N_{90^\circ}^G)$.

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°	$N_{90^\circ}^G$	$N_{90^\circ}^E$	$N_{90^\circ}^L$

Step4. ASD feature vector dimensionality reduction. The three-dimensional vector $T = (t_1, t_2, t_3)$ is defined to represent the angle structure to reduce the vector dimension and computational complexity. Let $t_1 = 1$, t_2=0, $t_3 = 0$, define $T^{\mathrm{G}} = (1, 0, 0)$ to represent the relationship of "greater than", and similarly, $T^{\mathrm{E}} = (0, 1, 0)$ and $T^{\mathrm{L}} = (0, 0, 1)$ represent the relationship of "equal to" and "less than" respectively. T value can be calculated by (1).

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

Step5. Define $P_{\alpha_{0^\circ}}$, $P_{\alpha_{45^\circ}}$ and $P_{\alpha_{90^\circ}}$ as the values of the three angle structures whose quantized color value is α. Taking the 45° angle structure as an example, the values can be obtained by (2).

$$P_{\alpha_{0^\circ}} = T^E N_{45^\circ}^E + T^L N_{45^\circ}^L + T^G N_{45^\circ}^G \tag{2}$$

For each quantized color value α, a three-dimensional vector $(P_{\alpha_{0^\circ}}, P_{\alpha_{45^\circ}}, P_{\alpha_{90^\circ}})$ can be obtained. Thus, the ASD feature vector H of the image is obtained as shown in (3).

$$H = \begin{bmatrix} P_{0_{0^\circ}}\ P_{0_{45^\circ}}\ P_{0_{90^\circ}} \\ \cdots\cdots\cdots\cdots \\ P_{\alpha_{0^\circ}}\ P_{\alpha_{45^\circ}}\ P_{\alpha_{90^\circ}} \\ \cdots\cdots\cdots\cdots \\ P_{71_{0^\circ}}\ P_{71_{45^\circ}}\ P_{71_{90^\circ}} \end{bmatrix} \tag{3}$$

B. COMPRESSED SENSING

Compressed sensing theory is mainly for sparse signals or compressible signals. The data is properly compressed while acquiring the signal. Its sampling frequency is much lower than that of Nyquist sampling frequency, which can reduce the sampling data, save storage space, and contain enough information. As long as the appropriate reconstruction algorithm is selected during reconstruction, enough data points can be recovered based on the obtained data for subsequent use.

Suppose the collected signal is $x \in \boldsymbol{R}$, and it is sparsely expressed as $\boldsymbol{X} = \boldsymbol{\Psi}x$ on the orthonormal basis $\boldsymbol{\Psi}$, and then the perception matrix $\boldsymbol{\Phi}$ is used for sensing to obtain the observation matrix $\boldsymbol{Y}$, as shown in (4).

$$\boldsymbol{Y} = \boldsymbol{\Phi X} = \boldsymbol{\Phi\Psi}x = \boldsymbol{\Theta}x \tag{4}$$

Among them, $\boldsymbol{\Theta} = \boldsymbol{\Phi\Psi}$, compressed sensing is to recover all the information of the original signal x by using a measurement matrix much smaller than the amount of data collected by the signal $\boldsymbol{X}$.

C. SIGNAL RECONSTRUCTION

Signal reconstruction is the process of finding the optimal solution of the underdetermined equation $\boldsymbol{Y} = \boldsymbol{\Theta} x$. Commonly used algorithms include greedy pursuit algorithm, convex relaxation algorithm, and combination algorithm [30]. Under the condition that the signal $\boldsymbol{X}$ is sparse or compressible, the problem of solving the underdetermined equation can be transformed into a minimum l_1-norm problem. The approximate accurate value $\boldsymbol{X}$ can be obtained by (5).

$$\min \|x\|_{l_1} \ s.t. \ Y = \boldsymbol{\Theta} x \tag{5}$$

The Regularized Adaptive Matching Pursuit (RAMP) algorithm estimates the sparsity of the signal step by step by setting a variable step size, which effectively solves the problem of accurate reconstruction of the signal in the case of unknown signal sparsity K, and avoids the phenomenon of too many iterations or inaccurate reconstruction signal caused by inaccurate prediction of sparsity. This algorithm combines the advantages of accurate reconstruction of the former reconstruction matching algorithm and the sparsity of the adaptive matching pursuit algorithm, which makes it possible to reconstruct the original signal accurately, stably, and quickly even when the sparsity is unknown [31]. In this paper, we used a regularized adaptive matching pursuit algorithm, and the specific implementation steps are as follows.

Step1. Initialize parameters, residual $r_0 = y$, reconstruction signal $\hat{x} = 0$, index set $\boldsymbol{\Gamma}_0 = \varphi$, step size $s = 0$, stage $j = 1$, number of iterations $n = 1$, atom set $\boldsymbol{\Phi} = \varphi_t$, candidate set $J = \varphi_t^*$.

Step2. If $|r_k| \leq \varepsilon_1$ (ε_1 representing the threshold for termination of iteration), stop iteration and use the obtained atomic set to reconstruct the signal, otherwise go to the next step.

Step3. The correlation coefficient is calculated by (6), and a total of s maximum elements $u_{\max}$ and their corresponding indexes are stored in the candidate set J to complete the primary screening of atoms.

$$u_i = \left\{u_j | u_j | \langle r_j, \varphi_j \rangle |, \quad j = 1, 2, \ldots, N\right\} \tag{6}$$

Step4. Store the result of the atomic correlation coefficient corresponding to the index value in the candidate set $\boldsymbol{J}$ into the set $\boldsymbol{J}_0 \subset \boldsymbol{J}$ through regularization, where u_i must satisfy (7).

$$|u(i)| \leq 2\,|u(j)| \tag{7}$$

Step5. The approximate solution $\hat{x}$ is found by using (8), and the residual r_i is updated by using (9). If $\|r_i - r_{i-1}\| \leq \varepsilon_2$ (ε_2 represents the threshold of stage transition), return to *Step3* and update $j = j + 1$, $s = sj$, otherwise return to *Step2*.

$$\arg\min \left\|y - \Phi_n \hat{x}\right\| \tag{8}$$

$$r_i = \left|y - \Phi_n \hat{x}\right| \tag{9}$$

D. GHM MULTIWAVELET TRANSFORM

GHM (Geronimo Hardin Msaaopust) multiwavelet transform [32] is the earliest constructed and most widely used multiwavelet. It has significant characteristics such as compact support, second-order approximation, integer translation of the scaling function orthogonal to each other, high-order vanishing moments, and symmetry. $L(n)$ and $H(n)$ of GHM multiwavelet are shown in (10) and (11).

$$L(0) = \begin{bmatrix} \frac{3}{5\sqrt{2}} & \frac{4}{5} \\ -\frac{1}{20} & -\frac{3}{10\sqrt{2}} \end{bmatrix} L(1) = \begin{bmatrix} \frac{3}{5\sqrt{2}} & 0 \\ \frac{9}{20} & \frac{1}{\sqrt{2}} \end{bmatrix} \tag{10}$$

$$\begin{gathered} L(2) = \begin{bmatrix} 0 & 0 \\ \frac{9}{20} & -\frac{3}{10\sqrt{2}} \end{bmatrix} L(3) = \begin{bmatrix} 0 & 0 \\ -\frac{1}{20} & 0 \end{bmatrix} \\ H(0) = \begin{bmatrix} -\frac{1}{20} & -\frac{3}{10\sqrt{2}} \\ \frac{1}{10\sqrt{2}} & \frac{3}{10} \end{bmatrix} H(1) = \begin{bmatrix} \frac{9}{20} & -\frac{1}{\sqrt{2}} \\ -\frac{9}{10\sqrt{2}} & 0 \end{bmatrix} \\ H(2) = \begin{bmatrix} \frac{9}{20} & -\frac{3}{10\sqrt{2}} \\ \frac{9}{10\sqrt{2}} & -\frac{3}{10} \end{bmatrix} H(3) = \begin{bmatrix} -\frac{1}{20} & 0 \\ -\frac{1}{10\sqrt{2}} & 0 \end{bmatrix} \end{gathered} \tag{11}$$

GHM multiwavelet pre-filter $P_{re}(n)$ and post-filter $P_{ost}(n)$ are shown in (12) and (13).

$$P_{re}(0) = \begin{bmatrix} \frac{3}{8\sqrt{2}} & \frac{10}{8\sqrt{2}} \\ 0 & 0 \end{bmatrix} P_{re}(-1) = \begin{bmatrix} \frac{3}{8\sqrt{2}} & 0 \\ 1 & 0 \end{bmatrix} \tag{12}$$

$$P_{ost}(1) = \begin{bmatrix} 0 & 1 \\ 0 & -\frac{3}{10} \end{bmatrix} P_{ost}(0) = \begin{bmatrix} 0 & 0 \\ \frac{4\sqrt{2}}{5} & -\frac{3}{10} \end{bmatrix} \tag{13}$$

As shown in Fig. 2, the first-order GHM multiwavelet transform is applied to the carrier image to obtain four sub-image components of the image. As shown in Table 2, after the first-order GHM multiwavelet transform, 97.31% of the energy of the original image is concentrated in the first-order lowest resolution sub-image, and the energy distribution of the four component sub-images is approximately 4.5:2.2:2.2:1.1. Using the characteristics of its energy distribution, information hiding is carried out in the middle energy area (LH_2 and LH_2), and tampering judgment is made in the high energy area (LL_2) and low energy area (HH_2), making the invisibility, robustness, capacity, and analysis resistance of the algorithm reach a more balanced state.

E. SINGULAR VALUE DECOMPOSITION

Singular value decomposition [33] refers to the orthogonal transformation that diagonalizes a matrix. It is an important matrix decomposition in linear algebra. In the image-based singular value decomposition, the singular value represents the energy information of the image. Suppose matrix

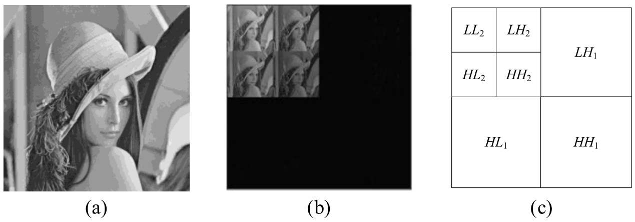

FIGURE 2. GHM multiwavelet transform. (a) Original image of Lena. (b) GHM multiwavelet transform for Lena. (c) Location of component diagram.

TABLE 2. The energy distribution of GHM multiwavelet first-order transform.

LL_1 percentage of energy (%)	LL_1 percentage of energy in each sub-image (%)			
	LL_2	LH_2	HL_2	HH_2
97.31	44.76	21.80	22.24	11.20

$\boldsymbol{A} \in \mathrm{R}^{\mathrm{m}\times\mathrm{n}}$, then its singular value decomposition is shown in (14).

$$\boldsymbol{A} = \boldsymbol{U} \cdot \boldsymbol{S} \cdot \boldsymbol{V}^{\mathrm{T}} \tag{14}$$

Among them, the matrix $\boldsymbol{U} \in \mathrm{R}^{\mathrm{m}\times\mathrm{n}}$, $\boldsymbol{V} \in \mathrm{R}^{\mathrm{m}\times\mathrm{n}}$ is the unitary matrix, and each column vectors of them is a pairwise orthogonal unit vector. Singular value matrix $\boldsymbol{S} = \boldsymbol{U}^{\mathrm{T}} \cdot \boldsymbol{A} \cdot \boldsymbol{V} = diag(\sigma_1, \sigma_2, \ldots, \sigma_p)$, the singular values of A are $\sigma_1, \sigma_2, \ldots, \sigma_p$, where $\sigma_1 > \sigma_2 > \ldots > \sigma_p$, $p = \min\{m, n\}$. When a slight disturbance matrix $\boldsymbol{A}$ is applied to the image matrix $A \in \mathrm{R}^{\mathrm{m}\times\mathrm{n}}$, the singular values of $\boldsymbol{B} = \boldsymbol{A} + \boldsymbol{A}$, $\boldsymbol{A}$ and $\boldsymbol{B}$ are σ_{Ai} and σ_{Bi} respectively, then $|\sigma_{Ai} - \sigma_{Bi}| \leq \|\boldsymbol{A} - \boldsymbol{B}\|_2 = \|\boldsymbol{A}\|_2 = \sigma_{\max}$, $\sigma_{\max}$ is the largest singular value of $\boldsymbol{A}$. Therefore, when a small disturbance is applied to the image, the singular value of the image will not change too much, which shows that the singular value of the image has good stability.

III. PROPOSED ALGORITHM

The multi-carrier information hiding algorithm effectively breaks the limitations of the single-carrier information hiding algorithm, such as small embedding capacity, low security, and weak robustness. By embedding the large capacity secret information into multiple image carriers, the algorithm reduces the embedding density and ensures good invisibility, which improves the capacity and invisibility of the algorithm. The multi-carrier information hiding algorithm is a secure and reliable covert communication strategy with good comprehensive performance. The working principle of the multi-carrier information hiding algorithm mainly includes multi-carrier preprocessing, secret information preprocessing, secret information embedding, and secret information extraction. In this paper, firstly, image ASD features are used to classify and preprocess the carrier library. Secondly, the single-layer multiwavelet transform and compressed sensing technology are used to preprocess the secret image to be embedded. At the same time, the GHM multiwavelet transform is applied to the carrier image, and the information hiding area is selected according to the energy characteristics. Finally, the secret information and carrier image are decomposed and optimized by SVD to complete the information hiding.

A. CARRIER PRETREATMENT

Taking the ASD feature vector as the descriptive factor, this paper defines the distance measurement formula $R(H, H')$ of two images for similarity calculation to realize the classification of multiple image carriers, as shown in (15).

$$R(H, H') = \sum_{i=1}^{l} \frac{|Hi - H'i|}{1 + Hi + H'_i} \tag{15}$$

Among them, H and H' are the feature vectors of the two images, and l is the dimension of the feature vector, l=216.

B. INFORMATION HIDING RULES

In our algorithm, the singular value difference of the sub-image block of the carrier image is used to represent the information. The purpose of information hiding is achieved by changing the singular value of the image slightly. The specific information hiding rules are as follows.

Rule1. After preprocessing, the image carrier set is divided into n categories, then the secret information B is divided into n segment, namely $B_1, B_2, \ldots, B_n$. Record the length of each secret message as L, and segment it according to the sequence of secret information length from small to large, then there is $L_{B_1} < L_{B_2} < \ldots < L_{B_n}$. When the secret information is embedded, the same kind of carrier image is embedded with the same secret information to avoid the situation that it is difficult to extract the secret information after the secret image is transmitted through the public channel. Different segmented secret information is embedded in different carrier images. When extracting information, the complete secret information is obtained by combining the secret information of each segment in $L_{B_1} \sim L_{B_n}$ order.

Rule2. The diagonal matrix $\boldsymbol{S}_i = Diag(\sigma_{i1}, \sigma_{i2}, \ldots, \sigma_{in})$ is obtained by singular value decomposition for each sub-image block Q. Let $D_i = |\sigma_{i1} - \sigma_{i2}|$, and obtain the set $D = \{D_1, D_2, D_3, \ldots, D_n\}$ of singular value difference. Define the difference distance as $\Delta D = D_{\max} - D_{\min}$, where $D_{\max}$ is the maximum value and $D_{\min}$ is the minimum value.

Rule3. According to the distribution characteristics of 0 and 1 in secret information B, the interval $[D_{\min}, D_{\max}]$ is non-linear divided, and the singular value of the image carrier is encoded to generate bit sequence C.

$$\begin{cases} C_i = 0, & D_{\min} \leq D < D_{\min} + \dfrac{b_1}{b}\Delta D \\ C_i = 1, & D_{\min} + \dfrac{b_1}{b}\Delta D \leq D < D_{\max} \end{cases} \tag{16}$$

where b_1 and b_2 respectively represent the number of 0 and 1 in the secret information bit sequence B, $b = b_1 + b_2$.

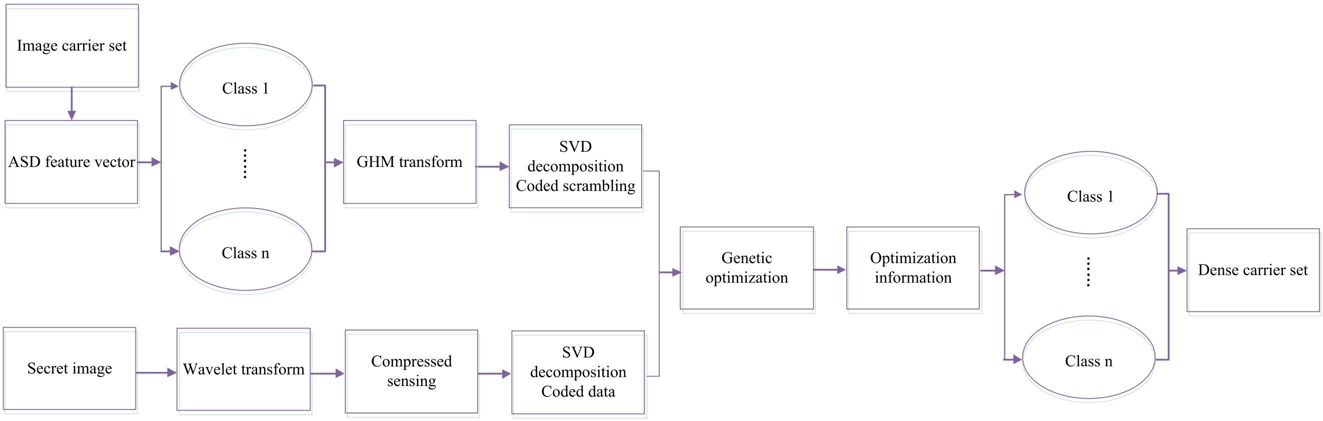

FIGURE 3. **The flowchart of the information hiding process.**

Rule4. According to the principle of whether the secret information B is equal to the carrier information bit sequence to determine whether to modify or not, there are two cases.

(1) If $C_i = B_i$, it indicates that the bit information and secret information of the hidden area are the same according to *Rule2*, then the secret information has been embedded in the carrier image, and no processing is needed for the hidden area.

(2) If $C_i = B_i$, the carrier data should be modified according to the value of secret information.

If $B_i = 0$, $C_i = 1$, the singular values σ_{i1} and σ_{i2} are modified according to (12) so that $D_i \in [D_{\min}, D_{\min}+\frac{b_1}{b}\Delta L)$, and then $C_i = B_i = 0$.

If $B_i = 1$, $C_i = 0$, the singular values σ_{i1} and σ_{i2} are modified according to (12) so that $D_i \in [D_{\min}+\frac{b_1}{b}\Delta L, D_{\max}]$, and then $C_i = B_i = 1$.

C. INFORMATION HIDING PROCESS AND STEPS

The information hiding of this algorithm is divided into the following steps, and the overall process is shown in Fig. 3.

Step1. Preprocess the image of carrier set. According to the image distance measurement formula $R(H, H')$ defined in this paper, the image carrier set is divided into n classes by using ASD feature vector. By classifying the image carrier set, we can get different kinds and a large number of carrier images, which is convenient to construct the multi-carrier embedding environment with large capacity and low density.

Step2. The carrier image $Q(N \times N)$ is transformed by the first-order GHM multiwavelet transform, and four distinct first-order quantum graphs, namely LL_2, LH_2, HL_2 and HH_2 are obtained. According to the characteristics of its energy distribution, the area (LH_2 and HL_2) with the middle energy ratio is selected to embed the secret image, the area (LL_2) with high energy ratio is used as the information recovery and tampering judgment part, and the area (HH_2) with low energy ratio is used as the tamper detection part, which can make the algorithm achieve a relative balance in invisibility, robustness, anti-analysis and embedding capacity.

Step3. The local blocks contained in LL_2, LH_2, HL_2 and HH_2 sub-images are marked as Q_{LL_2}, Q_{LH_2}, Q_{HL_2}, and Q_{HH_2} respectively. According to *Rule2*, singular value decomposition Q_{LH_2} is carried out to obtain the set D_{LL_2}, D_{LH_2}, D_{HL_2} and D_{HH_2} of singular value difference. According to *Rule3*, the singular value difference of carrier region LH_2 and HL_2 is encoded to generate bit sequences C_{LH_2} and C_{HL_2}. When processing the carrier image, the stability of SVD can ensure that the secret information can still be extracted from the image with small changes, which ensures the robustness of the algorithm. When the image is damaged slightly, the change of singular value of image matrix is very small, that is, it will not change obviously, which enhances the invisibility of the algorithm.

Step4. The secret image G is transformed by single-layer wavelet transform, and four wavelet sub-band coefficient matrices of LL_1, LH_1, HL_1 and HH_1 are obtained. The single-layer wavelet transform is used to sparse the secret image to get the sparse transform vector, which can reduce the storage and transmission cost of the signal in the transmission process.

Step5. Using a sparse basis $\boldsymbol{\Psi}$ and Bernoulli distribution random observation matrix $\boldsymbol{\varphi}$ (the number of observations is small and the reconstruction performance is good) to observe the secret information, the measured value matrix $\boldsymbol{Y}_G$ is obtained, and the original secret image is compressed. In the stage of secret information preprocessing, the secret information is directly observed sparsely and then compressed and sensed, which can effectively avoid the problem of weak security caused by the preprocessing of scrambling algorithm, thus improving the anti-attack ability of secret information.

$$\boldsymbol{Y}_G = \boldsymbol{\varphi}\boldsymbol{G}_1 \tag{17}$$

Step6. The secret information measured value matrix $\boldsymbol{Y}_G$ is processed by singular value decomposition to obtain the singular value G_2, orthogonal matrices $\boldsymbol{U}_{Y_G}$and $\boldsymbol{V}^T_{Y_G}$, and a diagonal matrix $\boldsymbol{S}_{Y_G}$. The sequence value $G_2$of the watermark information to be embedded is normalized to the [0, 1] interval by (19), and the normalized value G_2' is obtained. When the image suffers slight damage, the change of the singular value of the image matrix is very small, that is, it will not change obviously, which enhances the invisibility of the algorithm. When the carrier image is processed, the unique stability of singular value decomposition is used to ensure that the extraction of secret information will not be affected when the image undergoes slight changes, which ensures that the secret carrier can still be completely extracted after being transmitted through the open channel and enhances the robustness of the algorithm.

$$\boldsymbol{G}_2 = \boldsymbol{U}_{Y_G} \bullet \boldsymbol{S}_{Y_G} \bullet \boldsymbol{V}_{Y_G}^T \tag{18}$$

$$G_2' = \frac{G_2 - G_2^{\min}}{G_2^{\max} - G_2^{\min}} \tag{19}$$

In which $G_2^{\min}$ is the minimum value of G_2, and $G_2^{\max}$ is the maximum value of G_2.

Step7. Large-capacity secret information is segmented according to *Rule1* in information hiding rules, 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 classifications, different secret information is embedded in heterogeneous carriers, and the same secret information is embedded in multiple similar carriers, which improves the robustness of the algorithm. When extracting information, the length of large-capacity secret information is combined according to the order from small to large, to avoid missing part of secret information, ensure the integrity of secret information and realize safer secret transmission.

Step8. Segmented secret information is scrambled by Logistic map chaos. As shown in (20), the scrambling parameter μ and the initial value x_k are determined, and the bit sequence of the segmented secret information after scrambling is $G_{IN}^x = (b_1^x, b_2^x, \ldots, b_{n-1}^x, b_n^x)$. The logistic map encryption and scrambling processing for the segmented secret information to be embedded increases the complexity of the algorithm and enhances the anti-analysis ability of the algorithm.

$$x_{k+1} = \mu x_k(1 - x_k), \quad x_k \in (0, 1) \tag{20}$$

Step9. Optimal adjustment by genetic algorithm. The number of G_{IN}^x and C_{LH_2}, G_{IN}^x and C_{HL_2} corresponding to the same number is represented by F_{LH_2} and F_{HL_2} respectively. Optimize x_{k1} and x_{k2} to make F_{LH_2} and F_{HL_2} as large as possible. The optimization model is shown in (21), and the optimal solutions y_1 and y_2 are obtained. By optimizing parameters x_{k1} and x_{k2}, the number F_{LH_2} and F_{HL_2} corresponding to the secret information sequence to be embedded and the embedded position bit sequence of the carrier image are as large as possible, which reduces the modification of the carrier image, ensures the maximum matching degree between the embedded information and the embedded position, and improves the invisibility and robustness of the algorithm.

$$F(y) = \max F(x_k) = \max \sum (t_n \bar{\oplus} b_x^n) \tag{21}$$

Step10. Substituting y_1 and y_2 into G_{IN}^x, the optimal hiding bits $C_{IN}^{y1} = (b_1^{y1}, b_2^{y1}, \ldots, b_{n-1}^{y1}, b_n^{y1})$ and $C_{IN}^{y2} = (b_1^{y2}, b_2^{y2}, \ldots, b_{n-1}^{y2}, b_n^{y2})$ are obtained. G_{IN}^{y1} and G_{IN}^{y2} are cross-hidden in LH_2 and HL_2 according to the order of knight parade traversal, and the singular value is modified according to *Rule3*. The singular value represents the energy information of the image, which has certain stability. Using the stability of singular value to embed secret information can reduce the difference between the carrier image and the secret image and further enhance the robustness of the algorithm. At the same time, the rotation invariance of singular values makes the secret information hiding area more robust and anti- analysis.

Step11. The verification data R^L, optimal scrambling parameters x_{k1}, x_{k2} and μ of secret information are hidden in LL_2 part. The verification data R^H is hidden in HH_2 part. The LL_2 part is the most robust, whereas the HH_2 part is the most vulnerable in the second-order component. By embedding the above data and parameters in these two parts, the receiver can quickly judge whether the encrypted image has been tampered with by the comparison of R^L and R^H, which is helpful to judge and recover the hidden information that may be damaged during transmission in the secret information extraction stage, and improves the robustness of the algorithm while ensuring the perceived tampering of the algorithm.

Step12. Carry out GHM inverse transformation on the image once to obtain a dense image Q'.

D. INFORMATION EXTRACTION

In the stage of secret information extraction, the secret information extracted from the images of similar secret carriers is compared, and the secret information with complete meaning is selected to be retained. The different secret information obtained by different carriers is arranged and combined in sequence to obtain complete secret information, which ensures the safe transmission of large-capacity secret information, ensures the tamper-sensing ability of the algorithm, and further improves the security and robustness of the algorithm. The extraction of secret information is the inverse process of embedding, which is divided into the following steps.

Step1. According to *Step1-Step4* of the secret information embedding process, the secret image carrier set is processed to obtain LH_2 and HL_2 singular value difference sets D_{LH_2} and D_{HL_2}, and parameters b_1, b_2, b, μ, x_{k1}, x_{k2}, R^L and R^H are extracted from LL_2 and HH_2.

Step2. Judge R^L extracted from LL_2 and R^H extracted from HH_2. If $R^L = R^H$, it means that it is not attacked, then extract hidden information from LH_2 and HL_2. If $R^L \neq R^H$, it means that it has not been attacked or modified, then continue.

Step3. Determine the secret sequence. According to *Rule3*, the singular value difference set is encoded to generate bit sequence, and the watermark sequence information G_s' is obtained.

For the watermark sequence extracted from the same carrier, the receiver judges whether the comparison information is attacked by the outside world in the transmission process by comparing multiple watermark sequence information G'_s extracted from the images of the same carrier. If the two are consistent, the information is transmitted safely. If the two are inconsistent, check the length of the sequence. If it is complete, it means it has not been attacked. If it is obviously short, it means it has been damaged or tampered with by an attack, and it will be discarded. At this time, the complete sequence in multiple copies of watermark sequence information G'_s is selected as the final extracted secret sequence.

For the watermark sequence information extracted by heterogeneous carriers, calculate the length of each segmented watermark sequence information, and sort and combine them according to *Rule1* in the information hiding rules to obtain complete secret information.

Step4. The singular value diagonal matrix $\boldsymbol{S'}_{Y_G}$ extracted from the secret image and the $\boldsymbol{U}_{Y_G}$ and $\boldsymbol{V}^T_{Y_G}$ orthogonal matrices obtained by singular value decomposition after observing the secret image is used to reconstruct the observed value $\boldsymbol{Y'}_G$ of the secret image.

$$\boldsymbol{Y'}_G = \boldsymbol{U}_{Y_G} \cdot \boldsymbol{S'}_{Y_G} \cdot \boldsymbol{V}^T_{Y_G} \tag{22}$$

Step5. The observed value $\boldsymbol{Y'}_G$ of the secret image is reconstructed by using the RAMP algorithm to obtain G'_1.

Step6. Finally, the secret image G' is obtained by inverse wavelet transform.

IV. PERFORMANCE ANALYSIS AND EXPERIMENTAL COMPARISON

A. ALGORITHM PERFORMANCE ANALYSIS

1) INVISIBILITY ANALYSIS

In terms of invisibility, the algorithm completes the embedding of secret information through small changes in the image singular value. First, the secret image is processed by compressed sensing, which reduces the amount of secret information embedded. Secondly, the algorithm uses GHM multiwavelet transform to process the carrier image and selects the LH_2 and HL_2 regions with the middleweight as the hidden regions, so that the whole algorithm has better concealment. Third, the unique stability of singular value decomposition ensures that the carrier image will not change significantly when the secret information is embedded. Finally, the genetic algorithm is used to optimize the scrambling parameters of the secret information to improve the matching degree of the secret information and the carrier information, so that the amount of changes to the carrier image is as small as possible. The above four points not only consider the laws of human vision but also reduce the degree of modification of the carrier image so that the proposed algorithm has good invisibility.

2) ROBUSTNESS ANALYSIS

In terms of robustness, multi-carrier information hiding is more robust than single-carrier information hiding. First, the algorithm fully considers the carrier image energy and color relevance to classify and preprocess the image carrier set, and embed the scrambled segmented secret information into multiple types of image carriers for transmission. Secondly, the algorithm uses the energy distribution characteristics of the GHM multiwavelet transform to select the robust middle region (LH_2 and HL_2) for combined embedding. Third, the stability of the singular value is used to embed secret information to reduce the difference between the carrier image and the dense image. At the same time, the rotation invariance of the singular value makes the hidden area more robust. Finally, the image is scrambled through the knight parade to make the secret information evenly distributed in the carrier image. The above four points can effectively ensure that the secret carrier can still extract complete secret information when encountering malicious attacks such as rotation attacks, compression attacks, and shear attacks, and fully guarantees the robustness of the algorithm.

3) ANALYSIS OF PERCEPTUAL TAMPERING

In the aspect of the perception of tampering, firstly, the verification data R^L and R^H is hidden in a robust part LL_2 with the highest energy and vulnerability identification part HH_2 with the lowest energy. Through the comparative judgment in the secret information extraction stage, the algorithm can quickly determine whether the secret image has tampered. Secondly, the algorithm embeds the same secret information in the same carrier. If the secret information extracted from the image of the same kind of carrier is significantly different from other secret information, it indicates that the image of the carrier containing secret information is attacked in the transmission process, which further ensures the algorithm has the ability of perceptual tampering.

4) RESISTANCE ANALYSIS

In the aspect of anti-analysis, the algorithm uses the GHM multiwavelet theory and processes the carrier image, takes the region with the middle energy weight value to embed the information, and the information hiding area is relatively hidden, which avoids steganalysis in essence. Compressed sensing and Logistic mapping scrambling make the secret information chaotic and irregular, even if the secret information is extracted, it is difficult to recover the correct secret information through analysis. The pre-processing of multi-carrier image classification, GHM multiwavelet transform, normalization processing, and small change of image singular value can further enhance the anti-analysis ability of the algorithm by increasing the complexity of the algorithm.

5) EMBEDDED AMOUNT ANALYSIS

In the aspect of embedded information analysis, the traditional pre-processing process is to scramble the secret

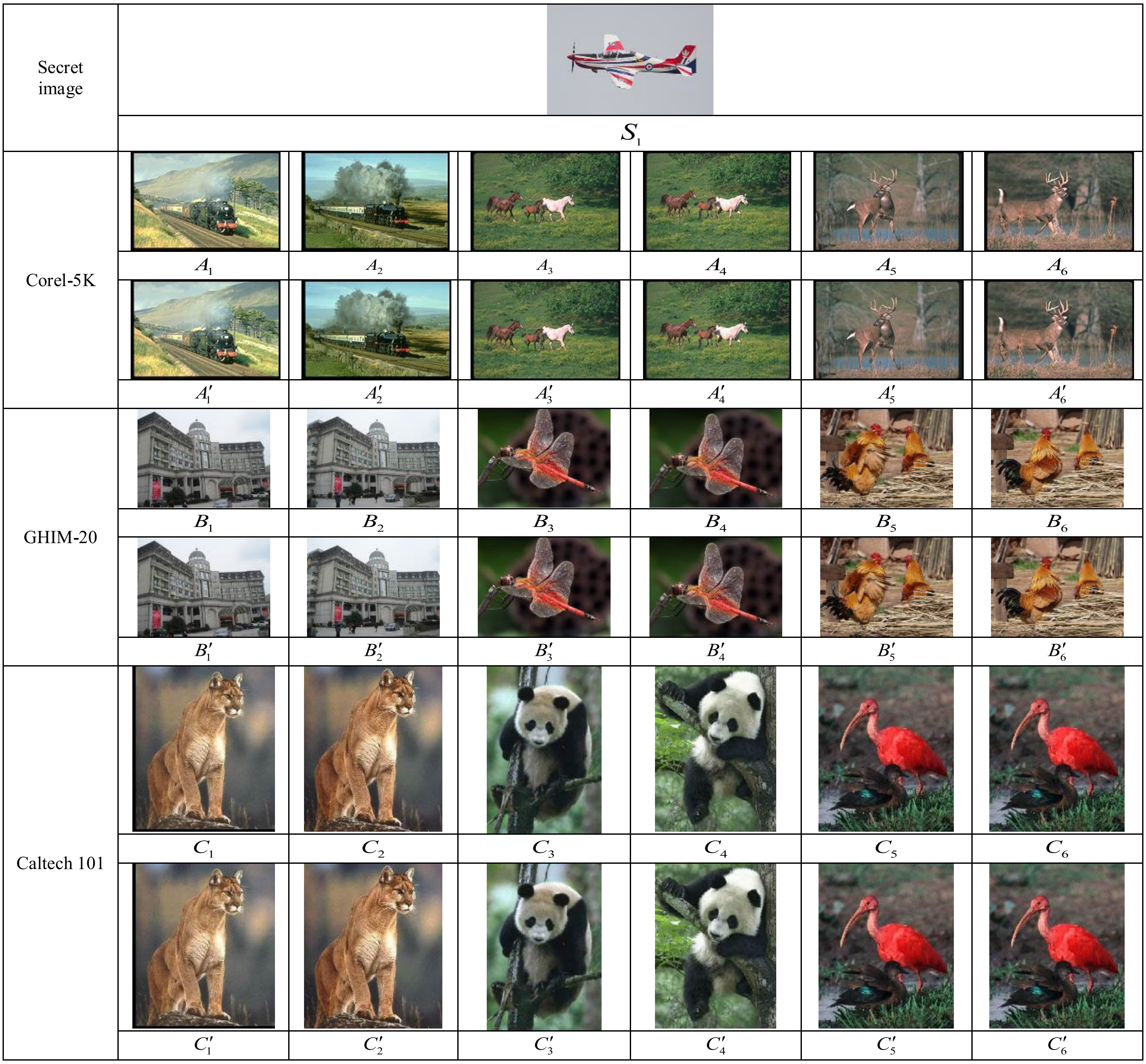
Secret image
S_1
Corel-5K
A_1 A_2 A_3 A_4 A_5 A_6
A_1' A_2' A_3' A_4' A_5' A_6'
GHIM-20
B_1 B_2 B_3 B_4 B_5 B_6
B_1' B_2' B_3' B_4' B_5' B_6'
Caltech 101
C_1 C_2 C_3 C_4 C_5 C_6
C_1' C_2' C_3' C_4' C_5' C_6'

FIGURE 4. The original carrier and secret carriers after embedding secret information through our proposed method.

information and embed the information according to different embedding algorithms. It is easy to cause a large number of redundant information to be embedded into the carrier image, which reduces the embedding of effective information. The algorithm in this paper uses compressed sensing theory to perform sparse sampling of information numbers to reduce redundant information in secret information, reduce the density of secret information in carrier information, and increase the amount of information embedded in secret information. At the same time, the algorithm constructs a large capacity and low-density embedding environment. The same kind of carrier images embeds the same secret information, and the segmented secret information is embedded into the heterogeneous carrier images, which effectively increases the embedding capacity of the algorithm.

B. EXPERIMENTAL COMPARISONS

The transmitted image carrier may be subject to various damages and attacks by the third party during the actual communication process. The experimental environment is Matlab7.0, Python 3.4.6, and the carrier set comes from Corel-5K, GHIM-20, Caltech 101. The algorithms proposed in [18], [25], [26], and [27] are selected as the experimental references.

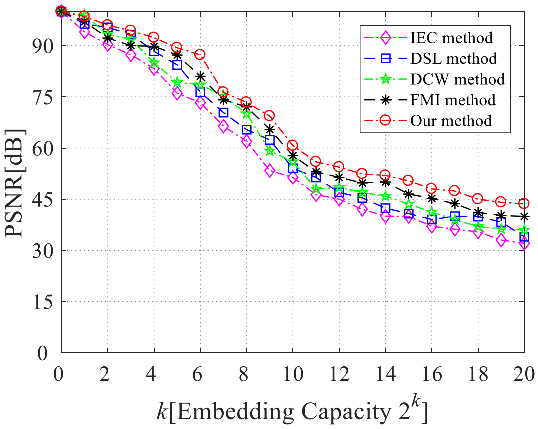

FIGURE 5. Invisibility comparison experiment results with exiting information hiding algorithms.

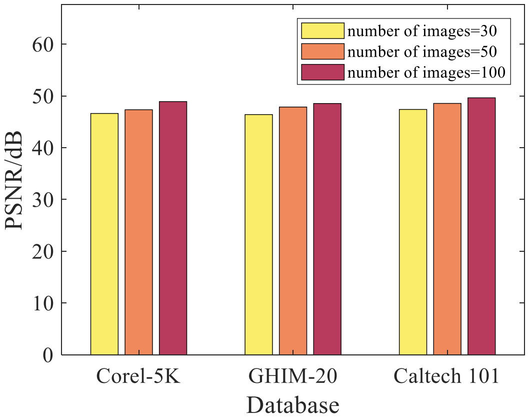

FIGURE 6. Invisibility experimental results of PSNR(dB) after different amount secret images within different image databases.

1) ANALYSIS OF PERCEPTUAL TAMPERING

In this paper, the sampling rate of the reconstruction algorithm is 0.7, and the experimental results are given by taking the secret image S_1 stored in three categories of six images in each image carrier set of Corel-5K, GHIM-20, and Caltech 101 as examples. The carrier image, secret information, and encryption effect are shown in Fig. 4, where S_1 is the secret image, A_1-A_6 and A'_1-A'_6 are the original carrier image and the encryption image in the Corel-5K image data set, B_1-B_6 and B'_1-B'_6 are the original carrier image and the encryption image in GHIM-20 image data set, C_1-C_6 and C'_1-C'_6 are the original carrier image and the encryption image in the Caltech 101 image data set. Comparing the original carrier image and the secret carrier image in Fig. 4, it is difficult to see the difference in image vision, which satisfies the imperceptibility of human vision, indicating that the algorithm has good invisibility.

The proposed algorithm is compared with the algorithms proposed in [18], [25], [26], and [27]. The invisibility comparison experiment results are shown in Fig. 5. It can be seen from Fig. 5 that when $k>9$, the PSNR of the algorithm is higher than that of other comparison algorithms. At the same time, as the embedding capacity increases, the PSNR tends to be stable. When $k = 18$, compared with the algorithm proposed in [18] (IEC), the algorithm proposed in [25] (DSL), the algorithm proposed in [26] (DCW), and the algorithm proposed in [27] (FMI), the average PSNR of the algorithm in this paper is increased by 27.05%, 12.73%, 21.58%, and 9.46% respectively, which shows that the algorithm in this paper has high invisibility.

Randomly select 30, 50, and 100 images in the three image databases of Corel-5K, GHIM-20, and Caltech 101 for information hiding according to the algorithm proposed in this paper, and calculate their PSNR value. It can be seen from Fig. 6 that as the number of test images in each image database in-creases, the PSNR of the algorithm also increases. When 100 images of Corel-5K, GHIM-20, and Caltech 101 image databases are selected respectively, the average PSNR can reach 49.0273dB, indicating that the algorithm in this paper is invisible and has a certain degree of stability.

2) ROBUSTNESS EXPERIMENT

Robustness reflects the degree of integrity of the secret information after processing and attacking the secret image, and it is processed and attacked to different degrees. The integrity of the secret information can be expressed with corresponding values, that is, the robustness can be quantified. In this paper, the Normalized Correction (NC) [34] is used for the quantitative evaluation of robustness, as shown in (23). When the NC value is higher, the robustness of the algorithm is stronger, otherwise, the robustness of the algorithm is lower.

$$NC = \frac{\sum_{m,n} \omega(m,n)\hat{\omega}(m,n)}{\sqrt{\sum_{m,n}(\omega(m,n))^2}\sqrt{\sum_{m,n}(\hat{\omega}(m,n))^2}} \tag{23}$$

Among them, $\omega(m, n)$ is the pixel value of the corresponding coordinate point of the secret information, and $\omega(m, n)$ is the pixel value of the corresponding coordinate point of the extracted secret information.

a: SINGLE ATTACK EXPERIMENT

When the encrypted image carrier is transmitted in the open channel, it is often vulnerable to attacks such as compression, cutting, rotation, and noise addition. Taking the encrypted image A'_1 as an example, the algorithm of this paper is compared with IEC, DSL, DCW, and FMI algorithms to perform single attack experiments of compression attack, cutting attack, rotation attack, and noise addition attack. The comparison results are shown in Fig. 7, Fig. 8, Fig. 9, as shown in Fig. 10 and Table 3.

It can be seen from the experimental data of compression attack in Fig. 7 that when the compression ratio is 40%, the NC value of secret information extracted by this algorithm is 75.43, and the NC values of IEC, DSL, DCW, and FMI are 63.29, 67.63, 72.45, and 61.14, respectively. Compared with IEC, DSL, DCW, and FMI, the robustness NC value of

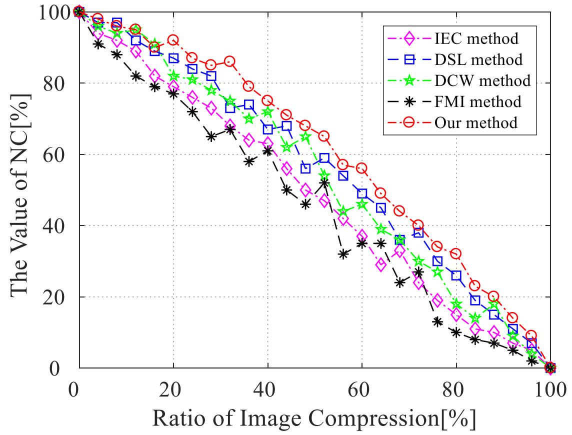

FIGURE 7. Compression attack comparison experimental results.

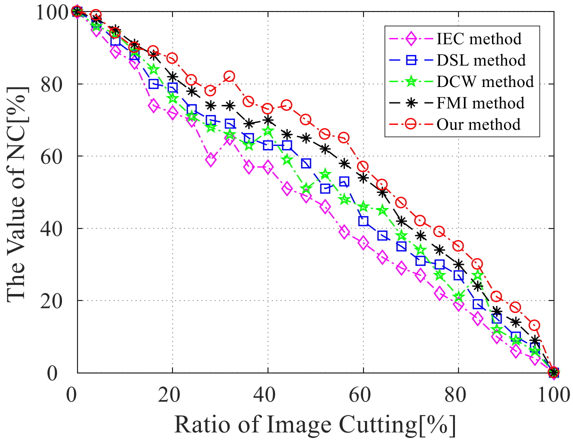

FIGURE 8. Cutting attack comparison experimental results.

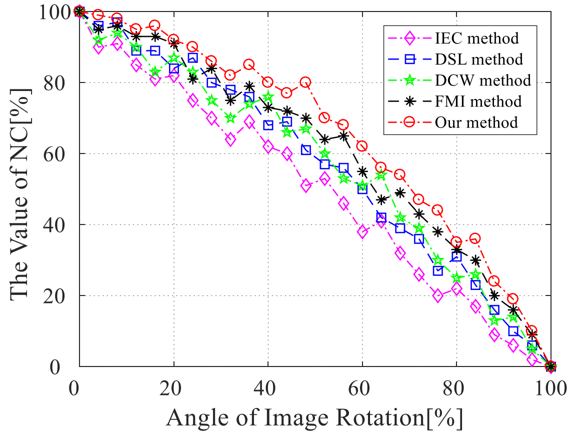

FIGURE 9. Rotation attack comparison experimental results.

this algorithm is improved by 19.18%, 11.53%, 4.11%, and 23.37%, respectively.

As shown in Fig. 8, when the cutting rate reaches 35%, the robustness NC values of the algorithm, IEC, DSL, DCW, and FMI are 79.25, 60.71, 66.91, 64.38, and 72.38, respectively, which means that the robustness NC values of the proposed algorithm are 30.84%, 18.44%, 23.10%, and 9.49% higher than those of IEC, DSL, DCW, and FMI, respectively.

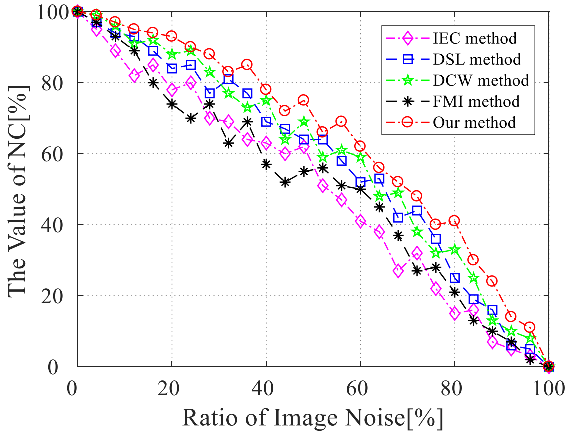

FIGURE 10. Noise attack comparison experimental results.

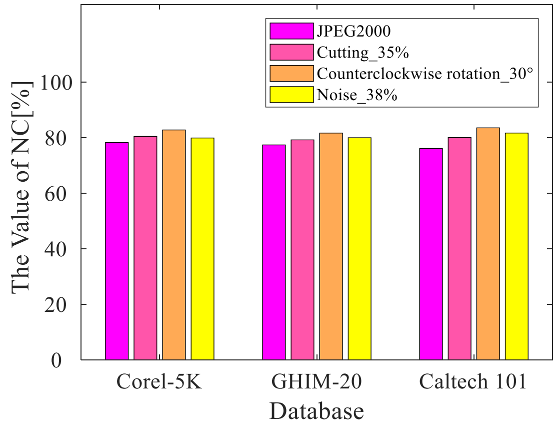

FIGURE 11. Single attack experimental results of NC(%) after different attacks within different image databases.

As shown in Fig. 9, when the counterclockwise rotation is 30°, the NC value of the algorithm is 83.42, IEC, DSL, DCW and FMI are 79.25, 60.71, 66.91, 64.38, and 72.38, respectively. Compared with IEC, DSL, DCW, and FMI, the NC values of our algorithm are increased by 23.06%, 4.41%, 13.02%, and 7.49% respectively.

It can be seen from Fig. 10 that when the noise adding rate is 38%, the NC value of secret information extracted by our algorithm is 80.50, and the NC value of IEC, DSL, DCW, and FMIS are 63.54, 70.83, 74.07, and 65.48, respectively. Compared with IEC, DSL, DCW, and FMIS, the NC value of this algorithm is increased by 26.91%, 13.65%, 8.68%, and 22.94% respectively.

At the same time, 100 images from Corel-5K, GHIM-20, and Caltech 101 image databases were randomly selected for the same JPEG2000 compression, 35% cutting, anti-clockwise 30° rotation, and 38% noise adding single attack experiments. The experimental results are shown in Fig. 11. As can be seen from Fig. 11, based on the images in Corel-5K, GHIM-20, and Caltech 101, the algorithm performs JPEG2000 compression, 35% cutting, 30° counterclockwise rotation, and 38% noise adding attacks, respectively, the NC values can reach 77.29, 79.94, 82.69 and 80.54, respectively, which indicates that the algorithm can be robust

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

Experiment number		The carrier with secret information						PSNR/dB
		A_1'	A_2'	B_1'	B_2'	C_1'	C_2'	
Experiment 1	Attacks type	*Cut*	/	/	/	/	/	44.4872
Experiment 2		/	/	*Com*	/	/	/	45.2187
Experiment 3		/	/	/	/	*Noi*	/	43.6874
Experiment 4		/	/	/	/	/	*Rot*	44.2587
Experiment 5		/	*Com*	*Cut*	/	/	/	43.1589
Experiment 6		*Noi*	/	/	*Com*	/	/	41.6257
Experiment 7		/	/	/	/	*Rot*	*Com*	42.4325
Experiment 8		/	/	*Cut*	/	/	*Noi*	41.8542
Experiment 9		*Cut*			*Rot*	/	/	42.0237
Experiment 10			*Rot*	*Noi*	/	/	/	39.9947
Experiment 11		*Com*	/	/	*Noi*	*Cut*	/	40.1147
Experiment 12		/	*Cut*	/	*Com*	/	*Rot*	40.4721
Experiment 13		/	*Rot*	/	*Cut*	/	*Noi*	39.8631
Experiment 14		/	*Com*	*Rot*	/	*Noi*	*Cut*	38.2104

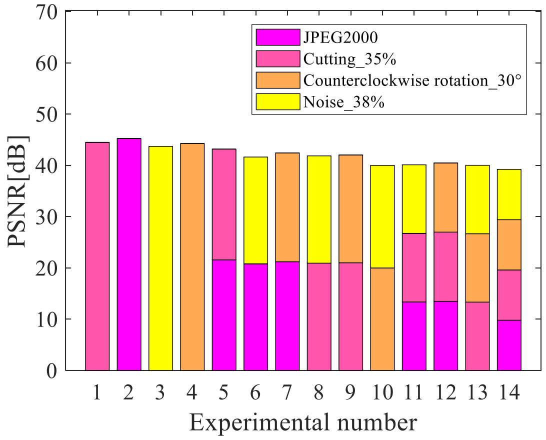

FIGURE 12. Compound attack experimental results after different attacks within different image databases.

against single attacks such as compression, cutting, rotation and noise addition when facing different image carrier databases.

b: COMPOUND ATTACK EXPERIMENT

In fact, in the actual open channel transmission, the dense image carrier will not only suffer compression attack, cutting attack, rotation attack, and noise adding attack, but also may encounter the compound attack of the above single attack. For this algorithm, we carry out the compound attacks of JPEG2000, 35% cutting, 30° counterclockwise rotation, and 38% noise adding. Table 3 shows the experimental data under 14 composite attacks, in which *Cut*, *Com*, *Rot*, and *Noi* represent 35% cutting, JPEG2000 compression, 30°counterclockwise rotation, and 38% noise respectively.

It can be seen from Table 3 and Fig. 12 that the PSNR of the algorithm can reach 43.1589dB when facing the combined attack of JPEG2000 compression and 35% cutting at the same time. The PSNR of the algorithm is 40.4721dB in the face of 35% cutting, JPEG2000 compression, and 30° counterclockwise rotation. The PSNR of the algorithm can reach 38.2104dB in the face of 35% cutting, JPEG2000 compression, 30° counterclockwise rotation, and 38% noise, which shows that the algorithm can effectively resist high-intensity composite attacks and has good robustness. All of the above show that the algorithm can effectively resist high-intensity composite attacks, and the algorithm has good robustness.

3) PERCEPTUAL TAMPERING EXPERIMENT

Compared with the IEC algorithm in [18], the DSL algorithm in [25], the DCW algorithm in [26], and the FMI algorithm in [27], the perceptual tampering is a unique characteristic of this algorithm. When a secret-containing image carrier is transmitted on an open channel, a third party may likely attempt to influence or damage the secret-containing behavior. The unique perceptual tampering ability of the proposed algorithm can effectively detect the tampering of the secret carrier during the transmission process, and help the receiver of the secret information to obtain complete and correct secret information. We randomly selected 200 images and used this algorithm to hide information, and compared the verification data of LL_2 and HH_2.

When the attack type and intensity are JPEG compression ratio of 2%, cutting rate of 5%, rotation 1°, mean filtering ([3, 3]), white noise (0, 0.003), and salt and pepper noise ($d = 0.05$), the detection rate is shown in Table 4, and the average detection rate reaches 96.20%, which indicates that the algorithm in this paper has a keen perception of tampering.

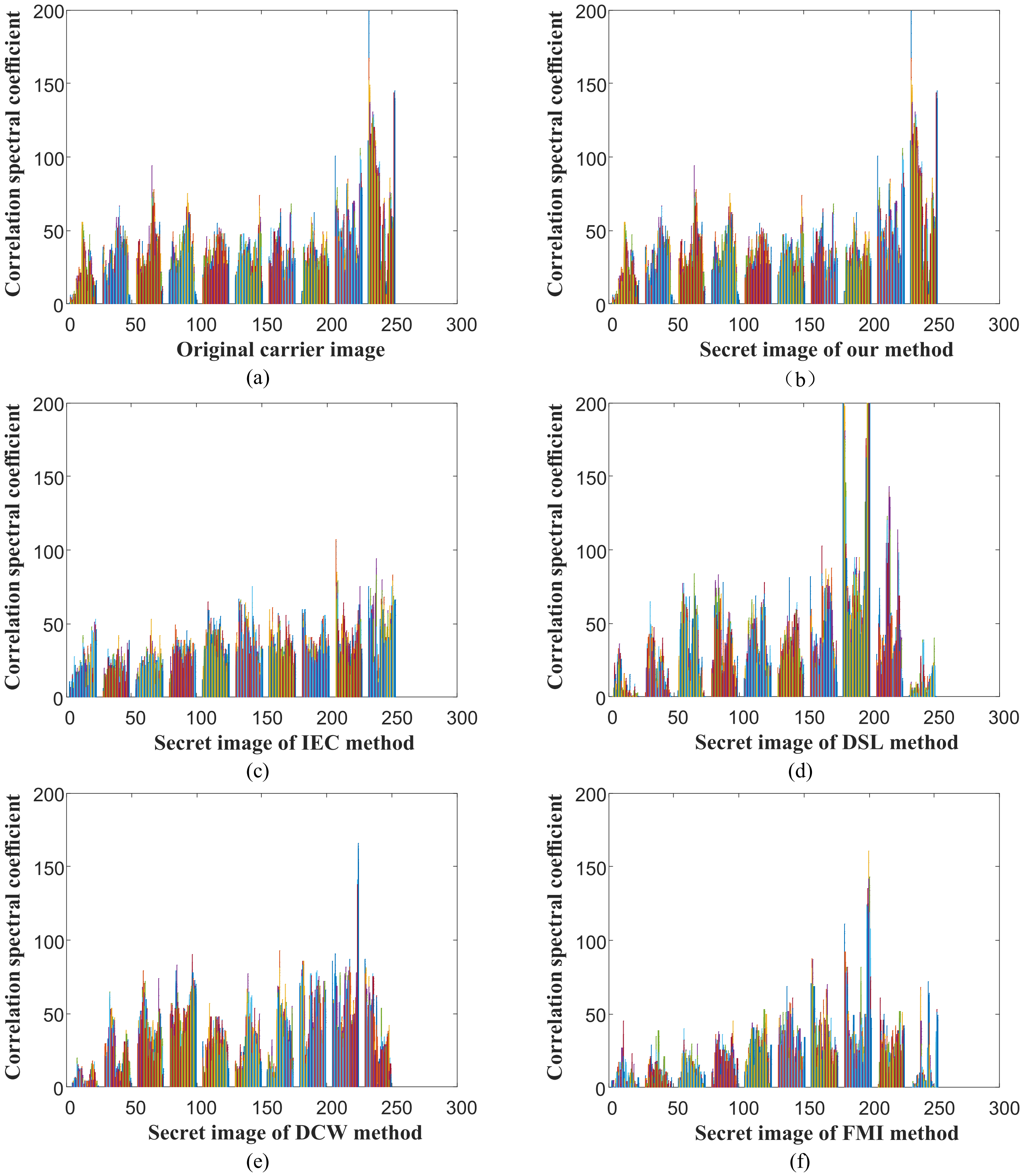

FIGURE 13. Anti-analysis comparison experiment results. (a) The original carrier image. (b) The secret image of our method. (c) The secret image of IEC method. (d) The secret image of DSL method. (e) The secret image of DCW method. (f) The secret image of FMI method.

4) ANTI-ANALYSIS EXPERIMENT

In information hiding, anti-analysis is the macro-control of the performance of an algorithm. Only under the premise of ensuring the invisibility, robustness, and certain capacity of the algorithm, can there be strong resistance to analysis. As a reverse analysis technology as opposed to image steganography, steganalysis technology detects the existence of hidden information by analyzing the statistical characteristics of the image carrier and the secret data. Common steganalysis methods include χ^2 detection, RS detection method, DIH

TABLE 4. The detection rate of perceptual tampering for various attacks.

Image processing	Detection rate of perceived tampering
JPEG 2000 compression	94.57%
Cutting	99.12%
Rotation	95.71%
Filtering	95.22%
White noise	98.14%
Salt pepper noise	97.46%

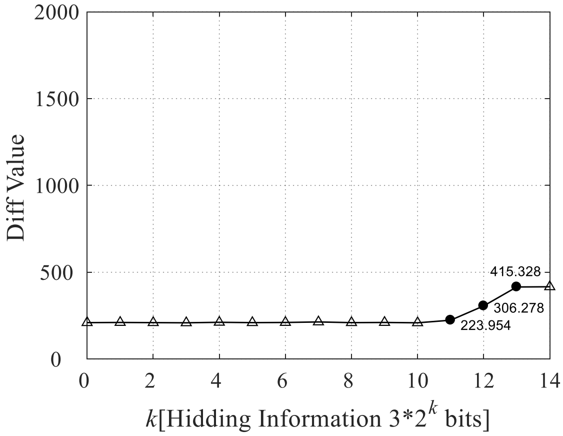

FIGURE 14. The histogram changes based on the proposed algorithm.

detection method, histogram feature analysis method, high-order statistics detection method, and gray image analysis detection method. We adopt the gray image analysis detection method, histogram feature analysis method, and high-order statistics detection method to conduct anti-analysis experiments respectively.

a: GRAY IMAGE ANALYSIS AND DETECTION METHOD

Gray image feature steganalysis detects the change of the gray value of image pixels and measures the anti-analysis ability of the algorithm based on the change degree of image pixels. The smaller the change of image pixels, the closer to the original image, the stronger the anti-analysis ability of the algorithm. On the contrary, the larger the change of image pixels, the weaker the anti-analysis ability of the algorithm. In this paper, the gray image A_1 containing dense carrier is selected for anti-analysis detection. The experimental data of the gray image correlation spectrum coefficient of the original carrier image and the comparison algorithm are shown in Figs. 13(a)-(e).

Comparing the pedigree data of each object in Fig. 13, it can be seen that the gray distribution of the dense vector image contained in the algorithm in this paper is basically consistent with the original image, with minimal difference. However, the gray distributions of the dense carrier images of the IEC, DSL, DCW, and FMI algorithms are quite different, so it can be shown that the algorithm in this paper is more resistant to analysis than the comparison algorithm.

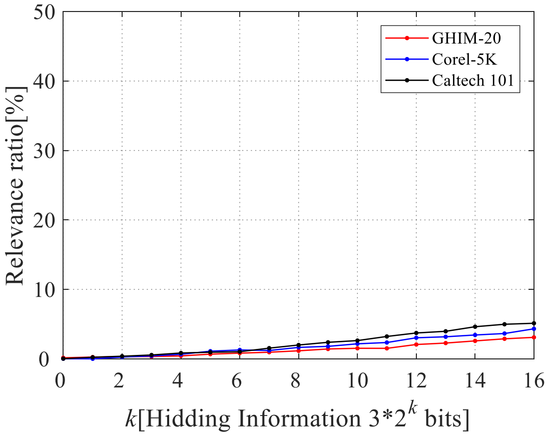

FIGURE 15. The detection rate based on histogram feature analysis method.

b: HISTOGRAM FEATURE ANALYSIS

The histogram is an effective image analysis method that reflects color information. In the algorithm of this paper, after the HSV color space quantization of the carrier image, the carrier image is classified according to the ASD feature vector of the image. In the process of embedding the secret information, it is inevitable to modify the color information of the carrier image. We conduct anti-analysis experiments on the algorithm in this paper based on the histogram feature analysis method. Fig. 14 is the variation curve of the feature description quantity Diff based on histogram analysis from 0 to 2^{14} and the corresponding detection rate.

It can be seen from Fig. 14 that as the amount of information hidden increases, Diff tends to increase. The growth rate is extremely small in $k \in [0, 10)$, and the growth rate slightly increases in $k \in [10, 13]$, but not enough to be a clear feature of analysis. As shown in Fig. 15, 1000 random images are used for testing, the detection rate is lower than 5.127%, and the main detection is above $k = 11$, which indicates that the algorithm has strong analysis resistance to the method based on histogram feature analysis.

c: HIGHER-ORDER WAVELET STATISTICS DETECTION METHOD

The high-order wavelet statistics analysis algorithm [35] utilizes the first-order and second-order characteristics of the image and is a general detection algorithm based on statistics. Using the high-order wavelet statistics detection method to detect and analyze the algorithm proposed in this paper, the experimental results are shown in Fig. 16.

In 100 random pictures, it is impossible to find one or more thresholds before and after hiding, indicating that the algorithm in this paper can effectively resist such detection and analysis. It can be seen from Fig. 17 that using 1000 random images for detection, the maximum detection rate is 9.036%, which proves that the algorithm is highly resistant to analysis.

By comparing the detection rates of the histogram feature analysis method and higher-order statistics detection analysis method in Fig. 15 and Fig. 17 for three different image

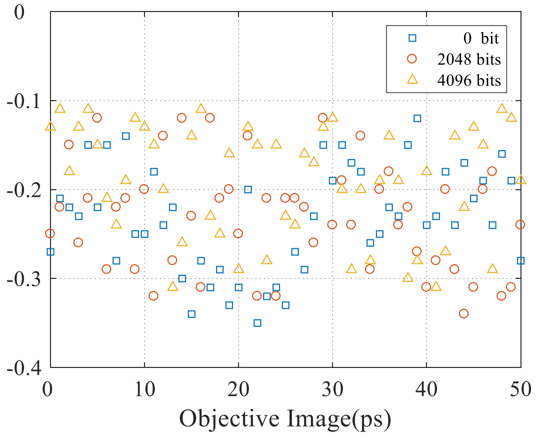

FIGURE 16. The detection and analysis results of higher-order wavelet statistics.

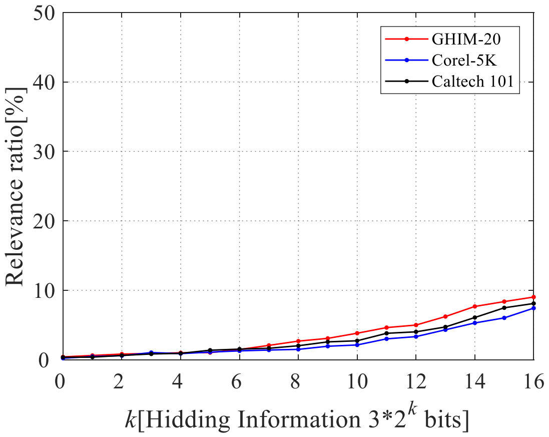

FIGURE 17. The detection rate based on higher-order wavelet statistics detection analysis method.

databases, we can see that the detection rate of the proposed algorithm with the above two steganalysis scopes is lower, which shows that the proposed algorithm has a good and stable anti-analysis performance. As the detection method of high-order statistics is sensitive to wavelet coefficients, the detection rate of detection and analysis based on high-order statistics is higher than that of histogram analysis on the whole. Compared with Caltech 101 image database, the correlation between image carriers in GHIM-20 and Corel-5k image databases is stronger. Therefore, when histogram analysis is used for steganalysis, the detection rate of Caltech 101 image database is higher than that of GHIM-20 and Corel-5k image databases.

V. CONCLUSION

This paper proposes an identifiable tampering multi-carrier image information hiding algorithm based on compressed sensing, which effectively solves the security problem of secret information preprocessing existing in previous image information hiding algorithms, and breaks the limitation of single-carrier image information hiding algorithm in capacity and robustness. The algorithm considers the internal correlation of the carrier images comprehensively, and reduces the redundancy of the secret information embedding by using the sparse sampling of compressed sensing, and distributes the secret information on multiple carriers by small changes of the image singular value. The simulation results show that the proposed algorithm has strong robustness and invisibility in the process of secret information transmission and extraction, and can resist the common JPEG compression, cutting, rotation, and noise attacks, as well as the composite attacks of these common attacks, and has a strong sense of tampering and anti-analysis. In the following research work, we will further explore the organization mode of multi-carrier images based on the carrier image features and secret information allocation embedding process, to maintain the internal correlation among multiple image carriers as far as possible, and further improve the efficiency of information embedding, and achieve the secure transmission of large-scale secret information.

REFERENCES

[1] S. Xiang and X. Luo, “Reversible data hiding in homomorphic encrypted domain by mirroring ciphertext group,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 11, pp. 3099–3110, Nov. 2018.

[2] S. Li and X. Zhang, “Toward construction-based data hiding: From secrets to fingerprint images,” *IEEE Trans. Image Process.*, vol. 28, no. 3, pp. 1482–1497, Mar. 2019.

[3] Z. Wang and X. Zhang, “Secure cover selection for steganography,” *IEEE Access*, vol. 7, pp. 57857–57867, May 2019.

[4] Z. Yin, Y. Xiang, and X. Zhang, “Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding,” *IEEE Trans. Multimedia*, vol. 22, no. 4, pp. 874–884, Apr. 2020.

[5] M. Huang, H. He, and F. Chen, “Separable reversible data hiding in encrypted image against ciphertext-only attack,” *J. Comput. Aided Design Comput. Graph.*, vol. 32, no. 6, pp. 874–882, Apr. 2020.

[6] A. D. Ker, “A capacity result for batch steganography,” *IEEE Signal Process. Lett.*, vol. 14, no. 8, pp. 525–528, Aug. 2007.

[7] A. D. Ker, “Locally square distortion and batch steganographic capacity,” *Int. J. Digit. Crime Forensics*, vol. 1, no. 1, pp. 29–44, Jan. 2009.

[8] A. D. Ker, “The square root law does not require a linear key,” in *Proc. 12th ACM Workshop Multimedia Secur. (MM&Sec)*, New York, NY, USA, 2010, pp. 213–224.

[9] A. D. Ker, “Batch steganography and pooled steganalysis,” in *Proc. 8th Int. Conf. Inf. Hiding*, Alexandria, VA, USA, 2006, pp. 265–281.

[10] A. D. Ker, “Batch steganography and the threshold game,” in *Proc. 9th Secur., Steganography, Watermarking Multimedia Contents*, San Jose, CA, USA, Feb. 2007, pp. 650504–650517.

[11] A. D. Ker, “Steganographic strategies for a square distortion function,” *Electron. Imag.*, vol. 6819, no. 13, pp. 43–55, Feb. 2008.

[12] A. D. Ker, “Perturbation hiding and the batch steganography problem,” in *Proc. 10th Int. Conf. Inf. Hiding*, Santa Barbara, CA, USA, 2008, pp. 45–59.

[13] A. D. Ker and T. Pevny, “Batch steganography in the real world,” in *Proc. Multimedia Secur. (MM&Sec)*, New York, NY, USA, 2012, pp. 1–10.

[14] X. Liao and J. Yin, “Two embedding strategies for payload distribution in multiple images steganography,” in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Calgary, AB, Canada, Apr. 2018, pp. 1982–1986.

[15] 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, Jun. 2018.

[16] Y. Huang and L. Shao, “Multi-carrier secret image sharing scheme with embedding,” *J. Image Graph.*, vol. 23, no. 8, pp. 1108–1130, Aug. 2018.

[17] X. Liao, J. Yin, M. Chen, and Z. Qin, “Adaptive payload distribution in multiple images steganography based on image texture features,” *IEEE Trans. Depend. Sec. Comput.*, early access, Jun. 24, 2020, doi: 10.1109/TDSC.2020.3004708.

[18] J. Yang and X. Liao, “An embedding strategy on fusing multiple image features for data hiding in multiple images,” *J. Vis. Commun. Image Represent.*, vol. 71, pp. 102822–102828, Aug. 2020.

[19] E. J. Candes, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489–509, Feb. 2006.

[20] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[21] R. Huang, K. H. Rhee, and S. Uchida, "A parallel image encryption method based on compressive sensing," *Multimedia Tools Appl.*, vol. 72, no. 1, pp. 71–93, Sep. 2014.

[22] L. Bao and Y. Zhou, "Image encryption: Generating visually meaningful encrypted images," *Inf. Sci.*, vol. 324, pp. 197–207, Dec. 2015.

[23] Y. Zhang, J. Zhou, F. Chen, L. Y. Zhang, K.-W. Wong, X. He, and D. Xiao, "Embedding cryptographic features in compressive sensing," *Neurocomputing*, vol. 205, pp. 472–480, Sep. 2016.

[24] D. Xiao, Y. Chang, T. Xiang, and S. Bai, "A watermarking algorithm in encrypted image based on compressive sensing with high quality image reconstruction and watermark performance," *Multimedia Tools Appl.*, vol. 76, no. 7, pp. 9265–9296, Apr. 2017.

[25] J. Chen, Y. Zhang, L. Qi, C. Fu, and L. Xu, "Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression," *Opt. Laser Technol.*, vol. 99, pp. 238–248, Feb. 2018.

[26] Q. Xu, K. Sun, S. He, and C. Zhu, "An effective image encryption algorithm based on compressive sensing and 2D-SLIM," *Opt. Lasers Eng.*, vol. 134, pp. 106178–106190, Jun. 2020.

[27] Z. Wang, Z. S. Hussein, and X. Wang, "Secure compressive sensing of images based on combined chaotic DWT sparse basis and chaotic DCT measurement matrix," *Opt. Lasers Eng.*, vol. 134, pp. 106246–106257, Nov. 2020.

[28] X. Chai, J. Bi, Z. Gan, X. Liu, Y. Zhang, and Y. Chen, "Color image compression and encryption scheme based on compressive sensing and double random encryption strategy," *Signal Process.*, vol. 176, pp. 107684–107762, Nov. 2020.

[29] 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.

[30] D. L. Donoho, Y. Tsaig, I. Drori, and J.-L. Starck, "Sparse solution of underdetermined systems of linear equations by stagewise orthogonal matching pursuit," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 1094–1121, Feb. 2012.

[31] Y.-X. Liu, R.-Z. Zhao, S.-H. Hu, and C.-H. Jiang, "Regularized adaptive matching pursuit algorithm for signal reconstruction based on compressive sensing," *J. Electron. Inf. Technol.*, vol. 32, no. 11, pp. 2713–2717, Nov. 2010.

[32] S. Ren, T. Zhang, D. Mu, W. Hu, and D. Zhang, "A new and better information hiding algorithm based on GHM multiwavelet transform and adaptive color transfer," *J. Northwestern Polytechnical Univ.*, vol. 28, no. 2, pp. 264–269, Apr. 2010.

[33] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans. Multimedia*, vol. 4, no. 1, pp. 121–128, Mar. 2002.

[34] M. Tagliasacchi, G. Valenzise, and S. Tubaro, "Hash-based identification of sparse image tampering," *IEEE Trans. Image Process.*, vol. 18, no. 11, pp. 2491–2504, Nov. 2009.

[35] H. Farid and S. Lyu, "Higher-order wavelet statistics and their application to digital forensics," in *Proc. Conf. Comput. Vis. Pattern Recognit. Workshop*, Madison, WI, USA, Jun. 2003, pp. 94–102.

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.

TAO ZHANG received the Ph.D. degree in control theory and engineering from Northwestern Polytechnical University, Xi'an, China, in 2012. She is currently an Associate Professor with the School of Electronic and Control Engineering, Chang'an University. Her research interests include multimedia information hiding and tampering detection and location technology, power vision and privacy protection technology, unstructured power big data processing technology, and data processing technology of power depth vision.

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.