Received May 25, 2020, accepted June 4, 2020, date of publication June 9, 2020, date of current version June 22, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3000993

A Novel Coverless Information Hiding Method Based on the Most Significant Bit of the Cover Image

LINA YANG, (Member, IEEE), HAIYU DENG, AND XIAOCUI DANG
School of Computer, Electronics, and Information, Guangxi University, Nanning 530004, China

Corresponding author: Haiyu Deng (deng_haiyu@163.com)

This work was supported in part by the Natural Science Foundation under Grant 61862005, in part by the Guangxi Natural Science Foundation under Grant 2017GXNSFBA198226 and Grant 2018GXNSFAA138085, in part by the Scientific Research Foundation of Guangxi University under Grant XGZ160483, in part by the Higher Education Undergraduate Teaching Reform Project of Guangxi under Grant 2017JGB108 and Grant DD3070051008, and in part by the Guangxi Natural Science Foundation, under Grant 2018GXNSFAA138085.

ABSTRACT With the rapid development of information technology recently, information security has become the focus of public concern. Information Hiding (IH) technology is an effective method to tackle the problem of information leakage incidents. In this paper, a novel coverless information hiding method based on the Most Significant Bit (MSB) of cover image is proposed (CIHMSB). Firstly, the cover image is segmented into a number of fragments. Secondly, in order to use the MSB of cover image to represent the secret information, the average intensity of each fragment is calculated. Thirdly, a one-to-one mapping between the MSB of the image fragment and the secret information is established using the mapping sequence (denote as Km), decided by the sender and the receiver in advance. This process produces a mapping flag (denote as Kf), which is sent by the sender along with the stego image. The objective of the proposed work is to increase hiding capacity, curtail the distortion of the stego image to improve its quality and reduce the Bit Error Rate (BER) of stego image in the case of distortion. Experimental results show that the proposed method can conceal 2601 bits secret information per carrier with peak signal-to-noise ratio ($PSNR$) of ∞ dB. What's more, some stego image quality assessment parameters, such as structural similarity ($SSIM$) index and universal image quality index (Qi), are slightly better than existing information hiding methods. Furthermore, the proposed method has good performance against such as AGWN, salt & pepper noise, low-pass filtering and JPEG compression attacks.

INDEX TERMS Coverless information hiding, image fragments, the most significant bit (MSB), secret information, mapping.

I. INTRODUCTION

With the rapid development of the Internet, information technology plays an important role in economy, culture, military, medicine and many other fields [1]. The development of information technology leads to the explosive growth of data. A large amount of multimedia information is transmitted on the Internet, which contains personal privacy, trade secrets, military secrets and other secret information. If these secret information is intercepted by criminals and used for illegal activities, it will seriously harm the interests of the country and people. Therefore, the problem of information security has increasingly become an urgent problem to be solved [2]. In the early days, cryptography technology was widely used in information protection [3]. The main idea is to encrypt the secret information into ‘‘unreadable’’ ciphertext, and the receiver can only decrypt the ciphertext through the corresponding key. However, the ciphertext obtained after encryption is usually in the form of ‘‘garbled code’’, which is easy to attract the attention of attackers who attempt to decrypt it. Compared with encryption technology, information hiding turns ‘‘unreadable’’ information into ‘‘invisible’’ information, as shown in figure 1. As a covert communication technology, information hiding technology has been widely recognized by industry and academia [4].

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

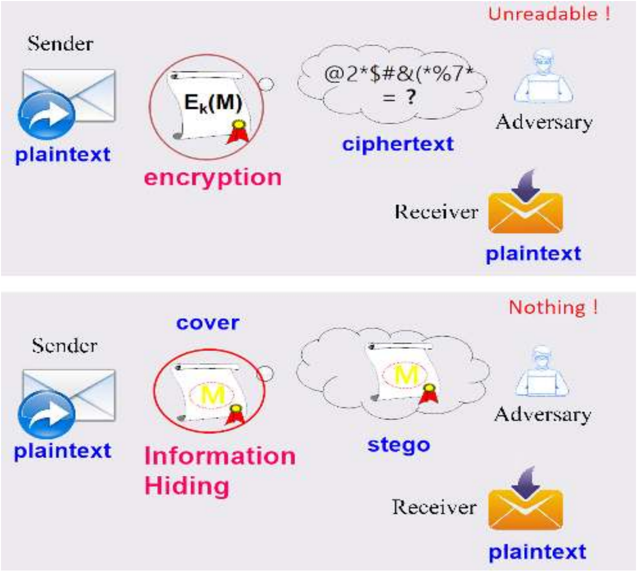


FIGURE 1. The difference between encryption and information hiding.

Traditional information hiding technologies are generally divided into spatial information hiding, frequency information hiding and adaptive information hiding [5]. LSB (Least Significant Bits) information hiding algorithm is a classical one based on spatial information hiding algorithm, which realizes the hiding of secret information by changing the least significant bit of image pixel [6]. In 2019, Aditya Kumar Sahu and Gandharba Swain improved two reversible data hiding (RDH) methods based on dual image least significant bit (LSB) matching and n-rightmost bit replacement (n-RBR) [7]. In their works, peak signal-to-noise ratio (*PSNR*) and embedding capacity (EC) were improved greatly. However, it still falls into the category of traditional information hiding, as it modifies the pixels of the stego image, leaving trace to steganographic analysis tools. In 2006, Ni *et al.* [8] first proposed an information hiding algorithm based on histogram translation. The basic idea based on histogram translation information hiding algorithm is to draw the histogram of each gray value, find the gray value with the most occurrence as the peak point P, and find the gray value with the least occurrence as the zero value point Z. Then it shifts the pixels between P and Z, making room for hiding information. In 2003, Tian [9] proposed the difference extension (DE) algorithm. It used the correlation between adjacent pixels to hide secret information. Although it is not easy to detected by eyes, when the spatial domain embedding mechanism performing the modification to cover image, the embedded information is sensitive to the image attacks. To settle this problem, many frequency domain information hiding algorithm have been proposed. It works by using some kind of reversible mathematical transformation, such as Discrete Fourier Transform (DFT) [10], Discrete Cosine Transform (DCT) [11] and Discrete Wave Transform (DWT) [12] to transform the spatial domain to the frequency domain, realizing the goal of information hiding by modifying some frequency domain coefficients. Adaptive steganography is a special case of spatial and frequency domain methods [13]. In [14], Jicang Lu improved an image content-adaptive steganography based on the pre-classification and feature selection to improve the accuracy and decrease the difficulty. Jung suggested a reversible information hiding (RIH) method based on the pixel value differencing (PVD) method, which is irreversible. However, Jung used the sub-block strategy to achieve reversibility when hiding secret information [15]. In terms of improving the quality of stego image and hiding capacity, Aditya Kumar Sahu and Gandharba Swain have done a lot of great work, which is superior to existing traditional information hiding methods [16-17]. In [16], Aditya Kumar Sahu improved dual imaging based reversible data hiding (RDH) technique, maintaining excellent peak signal-to-noise ratio (*PSNR*) of 51.30 dB when embedding 262,144 bits (when using the cover image of 256 × 256). In [17], Aditya Kumar Sahu and Gandharba Swain proposed a dual-layered reversible information hiding (RIH) method based on modified least significant bit (LSB), embedding 768,432 bits (when using the cover image of 256 × 256) of secret information with peak signal-to-noise ratio (*PSNR*) of 48.20 dB. Traditional information hiding techniques are widely used in various fields. However, the traditional information hiding technologies need to make some changes to the carrier more or less [18], causing some image distortion in the stego-image, especially when carry out a relatively large embedding rate. Since these modification traces will be left in the cover image, leaving the hidden danger that the steganographic analysis technology may detect sensitive information [19].

In order to address these above issue, this paper presents a novel coverless information hiding method based on the MSB of the cover image. First, the sender segments the cover image into a number of fragments of the same size. In order to facilitate the description of the method proposed by this paper, the fragment size is defined as $F_w * F_h$. Second, each fragment pixel values are averaged by the sender. Third, the secret information is converted into binary bits. Fourth, the secret information is mapped with the image fragments' MSB according to the mapping sequence (Km) decided by the sender and receiver. The result of the mapping is to get the mapping flag (Kf) and then it is sent along with the stego image to the receiver through the ordinary channel. The receiver can correctly extract the secret information from stego image using Km and Kf. The entire information hiding process does not make any modification to the cover image. In the other words, the cover image keeps the same as stego image. Therefore, the attacker can not find the secret information of stego image, even if the steganalysis tools are used.

Innovations of this paper:

- Compared with the traditional information hiding technology, this method does not modify the information carrier. This shows that the proposed method can obtain higher PSNR, SSIM and Qi. Therefore, the steganographic analysis tools can not detect the existence of secret information.

- Compared with the previous coverless information hiding technology, this method has higher security and robustness in improving the integrity of the secret information.
- This scheme can achieve higher hiding capacity compared with the existing coverless information hiding methods.

The arrangement of the paper: Section I introduces the shortcomings of traditional information hiding and proposes the solution. Section II overviews some frameworks for coverless information hiding algorithms. In section III, the method proposed by this paper is introduced. The experiments and analysis will be illustrated in section IV, and next is the conclusion and future work in section V. The last part is acknowledgement in section VI.

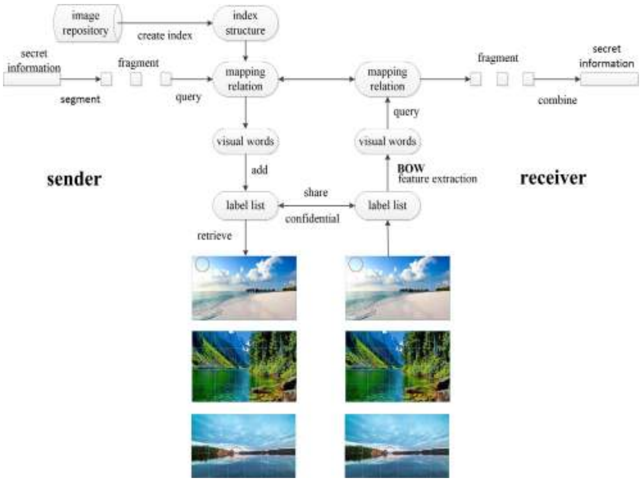


FIGURE 2. **The framework of the proposed method.**

II. RELATED WORK

In order to solve the problem that traditional information hiding technology is easy to be detected the secret information by the steganalysis tools. In August 2015, zhou *et al.* first proposed the concept of coverless information hiding at the first international conference, cloud computing and security [20]. Coverless information hiding technology can not mean it does not need carriers. Compared with traditional information hiding technology, it is directly driven by ''secret information'' to ''generate/obtain'' stego carriers [21].

Reference [22] proposed a coverless information hiding method based on the image bag-of-words (BOW) model [23]. This method extracts visual words (VW) by the BOW model to represent the secret information, so as to realize the purpose of hiding secret information in the image. In [22], the BOW model is used to extract the visual words of each image in the image set, and the dictionary of secret information segmentation is constructed. Then, it builds the mapping repository that maps the dictionary of secret information segmentation to visual words. Before the transmission of secret information, the sender searches the image repository for images containing visual words that have a mapping with the secret information, and then these images can be transferred as stego images. The algorithm framework based on the image bag-of-words(BOW) model is shown in figure 2. The core steps of their algorithm are:

Step 1: Divide the secret information S into n pieces of secret information, $S \to s_1, s_2, \ldots, s_n$.

Step 2: Select the first n tags from the image tag sequence shared by both parties to form the original image tag sequence $P_0 \to p_1, p_2, \ldots, p_n$. Then, P_0 is randomized using the hash sequence Hp decided by both parties in advance, obtaining the image label sequence used in this communication, $P_0 \to p'_1, p'_2, \ldots, p'_n$.

Step 3: Query the mapping relationship $L \to l_1, l_2, \ldots, l_n$, getting the VW set $W \to w_1, w_2, \ldots, w_n$, corresponding to the secret information fragment. Then, the maximum frequency of the overall stego image VW is constructed, denoted as $V \to v_1, v_2, \ldots, v_n$.

Step 4: Firstly, according to the search conditions (w, p',v), retrieve the first layer, obtaining the VW corresponding to the secret information fragment. Secondly, the second layer tag location corresponding to VW is retrieved to find the predetermined tag location p'; Thirdly, search for the maximum VW value of the whole image in the third layer, ensuring that v satisfies the increasing condition. Finally, one of the cover images that meet the conditions of (v, p', v) is selected as stego image for transmission.

In [22], although the multi-stage inverted index [24] method was used in the process of searching out qualified images from a large-scale database, the process is time-consuming. Meanwhile, the SHIFT features of the image is used as the visual words, it will cost a lot of time when extracting the SHIFT feature of the image.

Reference [25] proposed a coverless information hiding method for Chinese sentences based on the average pixel value of sub-images. First, cover image is divided into several sub-images $S_1, S_2, \ldots, S_m$, and then the average pixel value of each sub-image is calculated [26]. Second, according to the structure of the Chinese sentence, the sentence is divided into fragments $I_1, I_2, \ldots, I_n$, and then generate the dictionary $P_1, P_2, \ldots, P_n$. Third, generate hash sequences to represent the sentence fragments. The framework of [25] is shown in figure 3. The main idea of their algorithm is:

Step 1: First, the secret information of Chinese statements is divided into four parts: the subjects, the predicates, the objects and the prepositions, defined as I_1, I_2, I_3, I_4. Then, according to the Chinese dictionary W_1, W_2, W_3, W_4, the positions of these four parts are obtained as P_1, P_2, P_3, P_4.

Step 2: According to the mapping relationship and location information, the 20-bit hash sequence label is obtained, defined as L_1, L_2, L_3, L_4. Then, based on the hash array

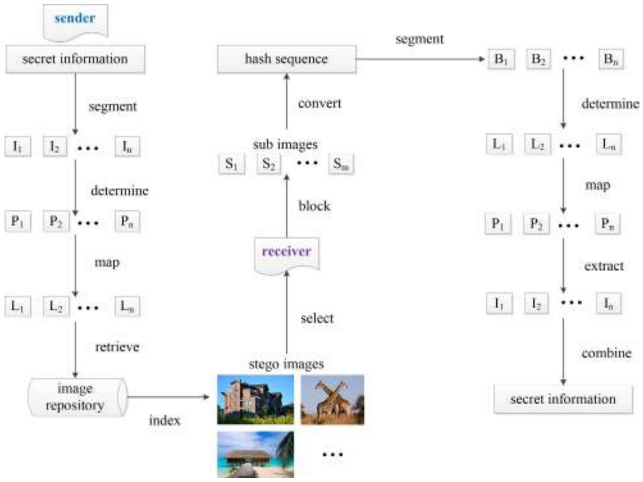


FIGURE 3. The framework of the proposed method.

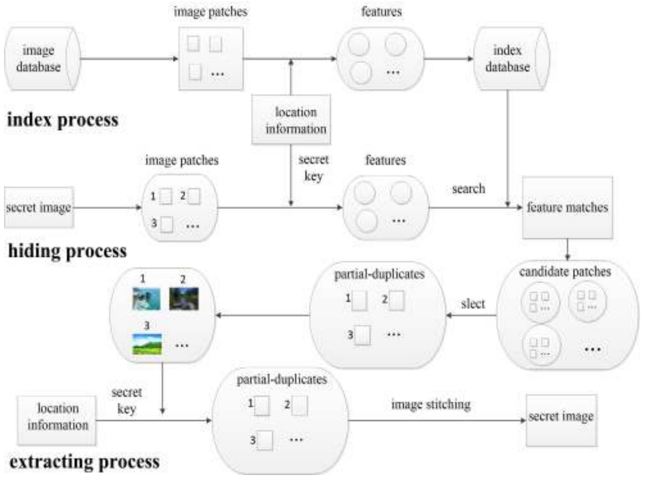


FIGURE 4. The framework of the proposed method.

$M \rightarrow M_1, M_2, M_3, M_4$, the corresponding 20-bit hash sequence B_1s, B_2s, B_3s, B_4s is obtained.

Step 3: According to L_1, L_2, L_3, L_4 and B_1s, B_2s, B_3s, B_4s, $image_1s, image_2s, image_3s, image_4s$ are retrieved from the image database, and the stego image are consisted of these images.

In [25], the average pixel value of sub-images is used to represent the Chinese sentences, which can reduce the time consumption for image feature extraction and improve the hiding capacity compared with [22]. However, the object of secret information is relatively single in [25], limiting to some regular Chinese sentences. It cannot hide the Chinese sentences without explicit sentence structure. Moreover, the hiding capacity of [25] is relatively low, which is 80 bits per carrier.

In 2018, zhou *et al.* proposed a steganographic algorithm based on partial-duplicate image retrieval [27]. It divides the images database into several image patches [28], which are then indexed by using features extracted from the image patches. In order to hide the secret image, the secret image also needs to be divided into several image patches, and then the partial-duplicate of the secret image is retrieved based on the similarity of image patches. The receiver can approximately recover the secret image from these partial-duplicate. The framework of [27] is shown in figure 4. The algorithm process is as follow:

Step 1: Divide the images of cover image database into a number of image patches. Then, with the participation of secret key, features were extracted from these image patches. Next, the layered quantization of features is done to obtain an indexed database.

Step 2: The secret image is segmented into several image patches *PB*, and feature extraction is performed for each image patches with the participation of secret key.

Step 3: Match secret image patches features with cover image patches features, searching for cover image patches that are similar to secret image patches.

Step 4: The sender send these cover images to the receiver as stego images, and the receiver can regenerate the secret image according to these stego image features with the participation of the secret key.

Although the hiding capacity of [27] is higher than those of the existing coverless image steganography methods, it still cannot overcome the shortcomings of time-consuming in feature extraction and inverted index structure construction. In addition, zhou was unable to extract the confidential images completely and accurately in [27].

Reference [29] proposed an algorithm framework similar to [27], but increasing the hiding capacity. The algorithms described above are the classical ones among the coverless information hiding algorithms. They are much better performance than the previous coverless information hiding algorithms in both the accuracy of extracting secret information and the robustness of the algorithm. However, the time-consuming and the low hiding capacity cannot be neglected.

Inspired by the above coverless information hiding algorithm, this paper proposes a novel coverless information hiding method based on the MSB of the cover image (CIHMSB). As the MSB of image fragment is used as the feature of cover image in this paper, it is simpler than the above algorithm in feature extraction and higher hiding capacity than the above algorithm. In addition, the coverless information hiding method proposed by this paper has greater robustness, which is better than CBZS method [30], CSD method [31], CBD method [32], Jia's method [33] and CBRI method [34]. Since the CIHMSB method proposed by this paper does not make any modification to cover image in the whole process, the CIHMSB method can resist the attacks of various steganalysis tools, making the adversary unable to detect the existence of the secret information.

III. THE PROPOSED SCHEME

In this section, we will specifically introduce how CIHMSB method realizes the process of information hiding and

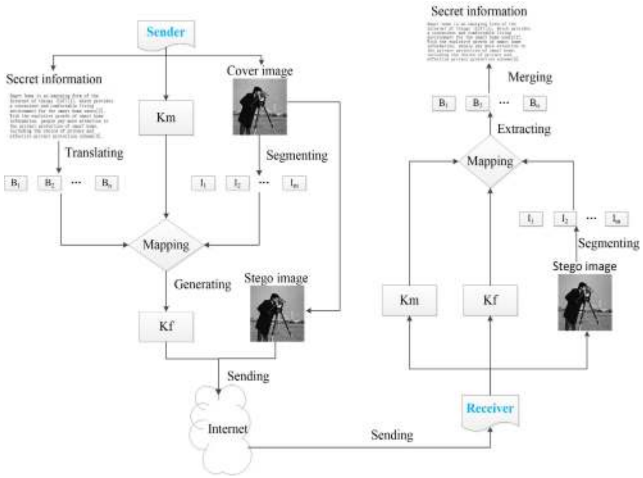


FIGURE 5. The framework of the proposed method.

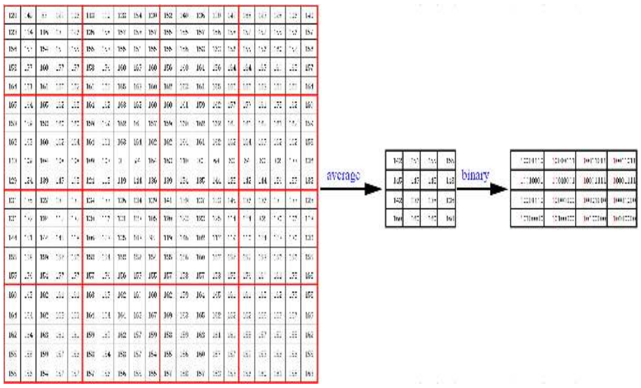


FIGURE 6. Preprocessing of cover image.

information extraction. Figure 5 is the framework of the CIHMSB method.

The purpose of CIHMSB method is for the transmission of text information. Before communication, the sender and receiver need to decided the Km in advance, and it is shared by the sender and receiver. Km is a set of random numbers, using to represent the serial number of the image fragments. The values of Km range from 1 to the largest serial number of the image fragment. In order to prevent the case that the Km value is greater than the serial number of the image fragment, the size of all cover images are stipulated in advance. As the carrier of information hiding, cover image can be any natural image. In order to facilitate the management of Km by both sides of communication, the size of cover image is defined as $I_w * I_h$. The secret information can be any character, Chinese text or English text.

In order to hide the secret information, firstly, the sender converts the secret information into the binary string, and segments the cover image into image fragments, which are used to represent the secret information. Secondly, according to the order of Km, the image fragments are used to map with the secret binary digits. After this mapping, Kf is generated, which realizes the process of information hiding. After receiving the Kf and stego image transmitted by the sender, the receiver segments the stego image into a number of image fragments, using the method that is same as the sender's. Then, the secret information in binary form is extracted from the fragment according to Km and Kf. Finally, the receiver merges the binary secret information to the text form of secret information. The following is a detailed introduction of the CIHMSB method to achieve information hiding and information extraction.

A. THE PROCESS OF INFORMATION HIDING

Pixels are the basic elements that make up digital images. They exist in computers as two-dimensional matrix elements. Pixel values range from 0 to 255, with "0" represents the brightest and "255" represents the darkest. The value of a pixel can be represented in eight-bit binary, where the left-most bit is the Most Significant Bit (MSB) and the right-most bit is the Least Significant Bit (LSB). In order to represent the secret information with cover image, the sender first segments the cover image into a number of image fragments $I_1, I_2, \ldots, I_m$, the size of which is $F_w * F_h$. The number of fragments can be calculated using Eq. (1).

$$Fm = \frac{\mathrm{I_w}}{\mathrm{F_w}} \times \frac{\mathrm{I_h}}{\mathrm{F_h}} \tag{1}$$

After the segmentation, each fragment is numbered to facilitate the search operation in the mapping process. Next, the pixel value of the fragments are averaged to $V_1, V_2, \ldots, V_m$, which are translated into eight-bit binary, as shown in figure 6. The MSB of each fragment is used to represent secret information. This process can be expressed as:

$$Cover\ image\ I \rightarrow I_1, I_2, \ldots, I_m \rightarrow V_1, V_2, \ldots, V_m \tag{2}$$

where $m = Fm$.

Before the secret information is transmitted, the sender converts each character of the secret information (T) into a seven-bit binary string $(B_1, B_2, \ldots, B_n)$, as shown in figure 7. For the secret information, if it is consisted of C characters, the number of bits can be calculated using Eq.(3).

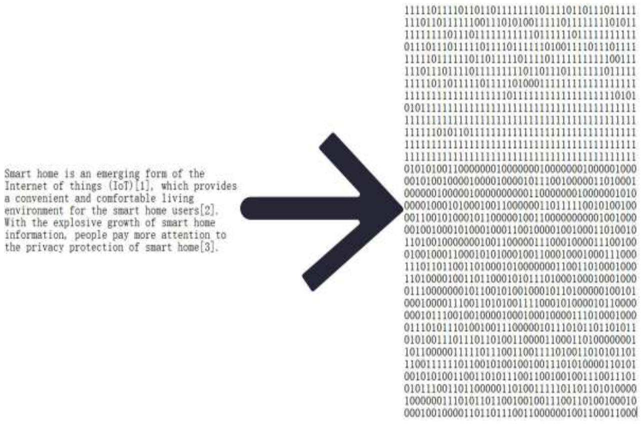
$$Cn = 7 \times C \tag{3}$$

The preprocessing of secret information can be expressed as:

$$T \rightarrow \ B_1, B_2, \ldots, B_n \tag{4}$$

where $n = Cn$.

In the process of mapping, the sender establishes a mapping between B_i and V_j according to the mapping sequence Km decided by both sides in advance. If B_i is same as the MSB of V_j, outputting "$Kf = 1$", in other word, the MSB of V_j represents B_i. If the MSB of V_j and B_i and are not equal, outputting "$Kf\ = 0$", which needs to be discussed in two cases:



Smart home is an emerging form of the Internet of things (IoT)[1], which provides a convenient and comfortable living environment for the smart home users[2]. With the explosive growth of smart home information, people pay more attention to the privacy protection of smart home[3].

```
1111101111011011011111111011110110110111111
1110110111111001110101001111101111111101011
1111111101110111111111110111111011111111111
0111011101111101111011111101001111011101111
1111101111110110111110111101111111111100111
1110111011110111111111011011101111111011111
1111101101111101111101000111111111111111111
1111111111111111111101111111111111111110101
0101111111111111111111111111111111111111111
1111111111111111111111111111111111111111111
1111110101101111111111111111111111111111111
1111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111
0101010011000000001000000010000000010000001000
00101001000010000100001011100100000011010001
0000001000000100000000000110000000010000001010
00001000101000100110000000110111110010100100
00110010100010110000010011000000000001001000
00100100010100010001100100001001000110100010
11010010000000010011000001110001000011100100
01001000110001010100010011000100010001110000
11101101100110100010100000001100110100001000
11010000100110110001010111010001000100001000
01110000000101100101001000101101000000100101
00010000111001101010011110001010000010110000
0001011100100100001000100010000111010001000
0111010111010010011100000101110101101101011
0101001110111011010011000011000110100000001
1011000001111101110011001111010011010101101
1100111111011001010010010011101010000110101
0010101001100110101110011001001001110011101
0101110011011000001101001111101101101010000
1000000111010110110010010011100110100100010
00010010000110110111001100000001001100011000
```

FIGURE 7. Preprocessing of secret information.

- If $V_{j_{MSB}}$ == "1", using "0" to represent B_i.
- If $V_{j_{MSB}}$ == "0", using "1" to represent B_i.

It is worth noting that the length of the secret information should not exceed the number of image fragments, $n \leqslant m$, otherwise overflow errors will occur.

$$Kf = \begin{cases} 1, & if\ B_i == V_{j_{MSB}} \\ 0, & if\ B_i \neq V_{j_{MSB}} \end{cases} \tag{5}$$

where $i = 1, 2, \ldots n; j = 1, 2, \ldots m; n \leqslant m$.

The sender sends the cover image to the receiver as the stego image along with Kf, realizing the process of information hiding. Since stego image and cover image are the same, so CIHMSB method can resist all the attack of steganalysis tools. The process of information hiding can be summarized as Algorithm 1.

In order to give a more intuitive understanding of the information hiding process, we present some simple examples to illustrate it. Suppose the secret information to be sent is converted into a binary string B_i = "1 0 1 1 0 0 1 0 1 1 1". A cover image is segmented into 9 image fragments, and the average pixel values of these 9 fragments are represented by 8-bit binary, as shown below.

① "**0** 0 1 1 0 0 1 1" ②"**1** 0 1 0 1 0 1 0" ③"**1** 0 0 0 1 1 1 0"
④ "**0** 1 1 0 1 1 0 0" ⑤"**0** 1 0 0 0 1 0 0" ⑥"**0** 1 1 0 0 0 1 1"
⑦ "**1** 0 1 0 0 1 1 0" ⑧"**0** 0 0 1 1 1 0 1" ⑨"**0** 1 1 0 0 1 1 1"

Suppose the mapping sequence Km = "9, 5, 4, 2, 1, 3, 6, 8, 7", as determined in advance by the sender and the receiver. According to Km, the 1st bit of secret information is mapped with the 9th image fragment, the 2nd bit of secret information is mapped with the 5th image fragment, and the 3rd bit of secret information is mapped with the 4th image fragment.... The 1st bit of secret information B_1 = "1" is not equal to $V_{9_{MSB}}$ = "0", according to Eq. (5), output Kf_1 = "0". The 2nd bit of secret information B_2 = "0" is not equal to $V_{5_{MSB}}$ = "0", according to Eq. (5), output Kf_2 = "1". The 3rd bit of secret information B_3 = "1" is not equal to $V_{4_{MSB}}$ = "0", according to Eq. (5), output Kf_3 = "0"... ..At last, Kf ="0, 1, 0, 1, 1, 0, 0, 1, 1" is obtain. The sender sends Kf to the receiver along with stego image.

```
Algorithm 1 Information Hiding
Input: Cover image $I$, Secret information $T$, Mapping sequence $Km$.
output: Stego image $I'$, Mapping flag $Kf$.
Step1. Preprocess the secret information using Eq. (4),the function of which is to convert secret information into a binary string. $T \rightarrow B_1, B_2, \ldots, B_n$.   (4)
Where $n = Cn$.
Step2. Preprocess the cover image using Eq. (2). The purpose of this step is to obtian the pixel average of each cover image fragment. Cover image $I \rightarrow I_1, I_2, \ldots, I_m \rightarrow V_1, V_2, \ldots, V_m$.   (2)
Where $m = Fm$.
Step3. Establish mapping and obtain the Mapping flag $Kf$ using Eq. (5). First, check whether the length of the secret information binary string is greater than the number of cover image fragments. If yes, report an error. Otherwise, perform the following procedure: Establish a mapping according to mapping sequence $Km$, if $B_i$ is the same as the MSB of $V_j$, output $Kf = 1$; Otherwise, output $Kf = 0$. $Kf = \begin{cases} 1, & ifB_i == V_{j_{MSB}} \\ 0, & ifB_i \neq V_{j_{MSB}} \end{cases}$   (5)
Where $i = 1, 2, \ldots n; j = 1, 2, \ldots m; n \leqslant m$.
Step4. Return mapping flag $Kf$ and stego image $I'$.
Step5. Information hiding process is done.
```

B. THE PROCESS OF INFORMATION EXTRACTION

Information extraction is the reverse process of information hiding. The extraction of secret information includes two processes: stego image preprocessing and mapping. After receiving the stego image, the receiver preprocesses the stego image and the preprocession is the same as the sender's, obtaining the binary bits $V'_1, V'_2, \ldots, V'_m$ using Eq. (6).

$$Stego\ image\ I' \rightarrow I'_1, I'_2, \ldots, I'_m \rightarrow V'_1, V'_2, \ldots, V'_m \tag{6}$$

where $m = Fm$.

In the process of establishing a mapping between Kf and image fragment, the receiver establishes a mapping between Kf and V'_j according to the Km. If Kf == 1, the MSB of V'_j is used to represent B_i. If Kf == 0, then it need to discuss with two different cases:

- If $V'_{j_{MSB}}$ == "1", using "0" to represent B_i.
- If $V'_{j_{MSB}}$ == "0", using "1" to represent B_i.

$$B_i = \begin{cases} V'_{j_{MSB}}, & if\ Kf == 1 \\ \text{“}1'', & if\ Kf == 0\ \&\ V'_{j_{MSB}} == \text{“}0'' \\ \text{“}0'', & if\ Kf == 0\ \&\ V'_{j_{MSB}} == \text{“}1'' \end{cases} \tag{7}$$

where $i = 1, 2, \ldots, n; j = 1, 2, \ldots, m; n \leqslant m$

After all the B_i are extracted, the B_i are merged into the text form of secret information Tsuing Eq. (8).

$$B_1, B_2, \ldots, B_n \rightarrow T \tag{8}$$

The process of information extraction can be summarized as Algorithm 2.

Algorithm 2 Information Extraction

Input: Stego image I', Mapping flag Kf, Mapping sequence Km.

output: Secret information T.

Step1. Preprocess the stego image using Eq. (6), which is used to get the pixel average of each stego image fragment.

$Stego\ image\ I' \rightarrow I'_1, I'_2, \ldots, I'_m \rightarrow V'_1, V'_2, \ldots, V'_m.$ (6)

Where $m = Fm$.

Step2. Establish a mapping according to mapping flag Kf and mapping sequence Km. This process can obtain the binary string $B_1, B_2, \ldots, B_n$ using Eq. (7). First, check whether the length of mapping flag Kf is greater than the number of stego image fragments. If yes, report an error. Otherwise, do the following process: Establish mapping according to mapping flag Kf and mapping sequence Km. If $Kf == 1$, assign the MSB value of stego fragment to B_i; Otherwise, if $Kf == 0$ and the MSB value of stego fragment is "0", let $B_i =$ "1″, if $Kf == 0$ and the MSB value of stego fragment is "1", let $B_i =$ "0″. Output the Binary string $B_1, B_2, \ldots, B_n$ at last.

$$B_i = \begin{cases} V'_{jMSB}, & if\ Kf == 1 \\ \text{“}1\text{″}, & if\ Kf == 0\ \&\ V'_{jMSB} == \text{“}0\text{″} \\ \text{“}0\text{″}, & if\ Kf == 0\ \&\ V'_{jMSB} == \text{“}1\text{″} \end{cases} \tag{7}$$

Where $i = 1, 2, \ldots, n; j = 1, 2, \ldots, m; n \leqslant m$.

Step3. Merge secret information using Eq. (8). In this step, the binary string $B_1, B_2, \ldots, B_n$ is merge to secret information T. $B_1, B_2, \ldots, B_n \rightarrow T$ (8)

Where $n = Cn$.

Step4. Return the secret information T.

Step5. Information extraction process is done.

In order to give a more visual understanding of the extraction process, the previous example will be used to illustrate it. Mapping sequence Km = "9, 5, 4, 2, 1, 3, 6, 8, 7", as determined in advance by the sender and recipient. In the previous assumption, the sender sends stego image and Kf = "0, 1, 0, 1, 1, 0, 0, 1, 1" to the receiver. The receiver segments the stego image into 9 image fragments using the method which is same as segmenting cover image by the sender. Since stego image has not been modified in any way, the 9 stego image fragments are the same as the previous 9 cover image fragments. The average pixel values of 9 stego image fragments are represented by 8-bit binary, as shown below.

① "**0** 0 1 1 0 0 1 1" ②"**1** 0 1 0 1 0 1 0" ③"**1** 0 0 0 1 1 1 0"
④ "**0** 1 1 0 1 1 0 0" ⑤"**0** 1 0 0 0 1 0 0" ⑥"**0** 1 1 0 0 0 1 1"
⑦ "**1** 0 1 0 0 1 1 0" ⑧"**0** 0 0 1 1 1 0 1" ⑨"**0** 1 1 0 0 1 1 1"

Since Kf_1 = "0", Km_1 = "9" and V'_{9MSB} = "0", according to Eq. (7), output B_1 = "1". Kf_2 = "1", Km_2 = "5" and V'_{5MSB} = "0", according to Eq. (7), output B_2 = "0". Kf_3 = "0", Km_3 = "4" and V'_{4MSB} = "0", according to Eq. (7), output B_3 = "1"… B_i = "1 0 1 1 0 0 1 0 1" is obtained finally.

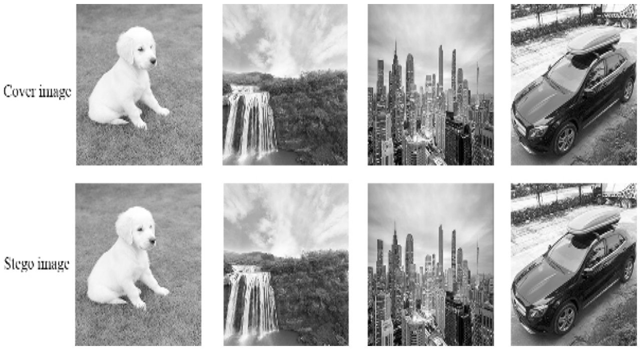


FIGURE 8. Cover image and stego image.

Kf and stego images need to be transmitted using common channels. During the transmission, Kf or stego images may lose, or both. If this happens, the receiver needs to ask the sender to resend the stego image or Kf or both, in order to extract the secret information.

IV. EXPERIMENTS AND ANALYSIS

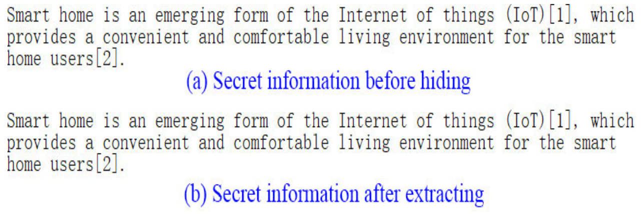
A. EXPERIMENT DEMO

In this experiment, an English sentence is used as the secret information, as shown in figure 9. The secret information is $C = 160$ characters in total. Any kind of grayscale image can be used as cover image. After hiding, the cover image is same as stego image, as show in figure 8. In this experiment, the cover image named "Car" is used as the cover image as mention in figure 8, and its size is $I_w * I_h = 256 * 256$. Before communication, the sender and receiver decide a mapping sequence Km in advance. The size of each image fragment is $F_w * F_h = 5 * 5$. After segmenting the cover image by the sender, 2601 image fragments are obtained using Eq. (1). After the secret information being preprocessed, 1120 bits are obtained using Eq. (3). According to the Km, the sender maps the binary secret information with the MSB of the image fragment, outputting Kf and Stego image, which are sent to the receiver later. With the participation of Km, Kf and stego image, the receiver can fully extract the secret information from the stego image, as shown in figure 9.

In order to prove the universality of the proposed method, we also use other forms of information as secret information for information hiding and extraction, as shown in figure 10.

B. SECURITY ANALYSIS

This section will analyze the security of the CIHMSB method in two aspects: the resistance to the steganalysis tool and the security to attacks.



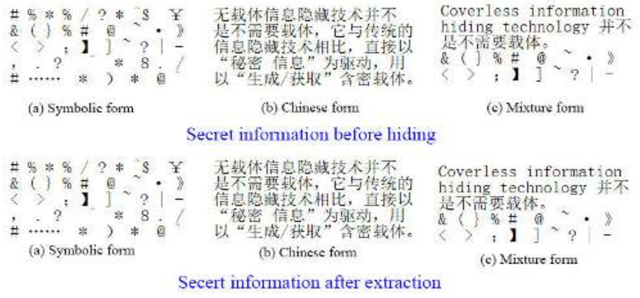
Smart home is an emerging form of the Internet of things (IoT)[1], which provides a convenient and comfortable living environment for the smart home users[2].

(a) Secret information before hiding

Smart home is an emerging form of the Internet of things (IoT)[1], which provides a convenient and comfortable living environment for the smart home users[2].

(b) Secret information after extracting

FIGURE 9. The result of information extraction.



```
# % * % / ? * `$ ￥
& ( } % #  @  ~  • 》
<  >  ; 】 ] ~ ? | -
, . ?       * 8 . /
# ……  *  )  *  @
```

(a) Symbolic form

无载体信息隐藏技术并不是不需要载体，它与传统的信息隐藏技术相比，直接以"秘密 信息"为驱动，用以"生成/获取"含密载体。

(b) Chinese form

Coverless information hiding technology 并不是不需要载体。

```
& ( } % #  @  ~  • 》
<  >  ; 】 ] ~ ? | -
```

(c) Mixture form

Secret information before hiding

```
# % * % / ? * `$ ￥
& ( } % #  @  ~  • 》
<  >  ; 】 ] ~ ? | -
, . ?       * 8 . /
# ……  *  )  *  @
```

(a) Symbolic form

无载体信息隐藏技术并不是不需要载体，它与传统的信息隐藏技术相比，直接以"秘密 信息"为驱动，用以"生成/获取"含密载体。

(b) Chinese form

Coverless information hiding technology 并不是不需要载体。

```
& ( } % #  @  ~  • 》
<  >  ; 】 ] ~ ? | -
```

(c) Mixture form

Secert information after extraction

FIGURE 10. Hiding and extracting other forms of confidential information.

1) THE RESISTANCE TO THE STEGANALYSIS TOOL

General information hiding tools rely on making some modification to cover image to hide the secret information, and these vulnerabilities will become the breakthrough of stego image being attacked by the steganalysis tool. Existing steganalysis tools generally implement steganographic analysis by detecting the modification traces of stego image [35]. An ideal information hiding tool is one that does not make any modification to the cover image, thus resisting all the attack of steganalysis tools. The information hiding method proposed in this paper is a coverless information hiding technology, which is not sensitive to all steganalysis tools. Because in the process of information hiding, this method merely use the cover image to establish a mapping with the secret information, and does not make any modification to the cover image. Therefore, the information hiding method proposed in this paper is an ideal information hiding method, which can resist all the attack of steganalysis tools without being detected.

2) THE SECURITY TO ATTACKERS

A safe and effective information hiding method must be largely resistant to the attack of the adversaries, even if stego image is completely exposed to the them. In this section, we will analyze the time cost of breaking the method proposed in this paper. We assume that stego image and *Kf* are fully accessible to adversaries. But *Km* is perfectly safe, unless one of the sender or receiver divulges *Km*. If the adversary can not access *Km* but wants to extract the secret information in stego image, he must use *Kf* and stego image to carry out violent attacks. Step back and assume that the adversary also knows the segmentation method to cover image. That is, the adversary knows how the cover image is segmented into the specified size image fragments. In this experiment, the grayscale image with the size of $I_w * I_h = 256 * 256$ is used as the cover image. If the size of the image fragment is $F_w * F_h = 5 * 5$, 2601 image fragments can be obtained after the operation of segmenting using Eq. (1). In other words, the length of *Km* is 2601. In this experiment, for example, supposing that the sender needs to transmit 1120 bits of secret information using Eq. (3). When the adversary needs to extract 1120 bits of secret information from the 2601 image fragments, he used violent attacks because of without knowing the *Km*. The violent attack methods can be calculated Eq. (9).

$$U = \frac{(\mathrm{Fm})!}{(\mathrm{Fm} - \mathrm{Cn})!} \tag{9}$$

In this experiment, the violent attack methods reach to $2601!/(2601 - 1120)! = 7.95 * 10^{3700}$using Eq. (9), but there is only one way to extract all secret information correctly. Assuming that an ordinary computer can perform 10 billion calculations per second, it would take $7.95 * 10^{3700}/(365 * 24 * 3600 * 10^{10}) = 2.52 * 10^{3683}$ years to extract the secret information correctly. If the image fragment size is increased to $F_w * F_h = 7 * 7$, the cover image is segmented into 1296 image fragments using equation (1). If it is necessary to send $Cn = 1120$ bits of secret information, it will take $1296!/(1296 - 1120)!/(24 * 3600 * 365 * 10^{10}) = 1.78 * 10^{3135}$ years to extract the secret information correctly. If the cover image is larger in size and the secret information to be transmitted is more, it will take longer to extract the secret information. From the above analysis, it can be known that the security performance of this scheme is high.

C. HIDING CAPACITY ANALYSIS

Increasing the capacity of hiding can increase the amount of secret information hidden in each cover image. In the test of hiding capacity in this paper, the number of bits per carrier ($bits * carrier^{-1}$) is used as the criterion to judge the capacity of information hiding [25]. In the experiment of this scheme, the cover image with a size of $I_w * I_h = 256 * 256$ is used for information hiding. Taking the image fragment sizes $F_w * F_h = 5 * 5$ and $F_w * F_h = 7 * 7$ as examples, each cover image is segmented into $256 * 256/(5 * 5) = 2601$ or $256 * 256/(7 * 7) = 1296$ image fragments using Eq. (1), each image fragment is used to hide 1 bit of secret information. The hiding capacity of this scheme is at least 1296 $bits * carrier^{-1}$. In fact, the hiding capacity of this scheme is not limited to 1296 $bits * carrier^{-1}$. If the communication parties adopt a larger size cover image or segment the cover image into smaller size image fragment, the hiding capacity will be higher. Table 1 shows the hiding capacity comparison of CIHMSB method, Zou's method [25], Zhou's method [27], Luo's method [29] and CBRI method [34]. It can be seen from table 1 that the hiding capacity of CIHMSB method is 72 times of CBRI method, 16 times of Zou's method, 3 times of Zhou's method and 1.6 times of Luo's method. It's obvious that CIHMSB is superior to the existing classical coverless information hiding methods in terms of hiding capacity.

TABLE 1. The hiding capacity comparison of CIHMSB method, Zou's method [25], Zhou's method [27], Luo's method [29] and CBRI method [34].

Methods	Capacity($bits * carrier^{-1}$)
CBRI method[34]	18
Zou's method[25]	80
Zhou's method[27]	384
Luo's method[29]	800
CIHMSB method($F_w * F_h = 7 * 7$)	**1296**
CIHMSB method($F_w * F_h = 5 * 5$)	**2601**

D. IMAGE QUALITY ASSESSMENT PARAMETERS ANALYSIS

Generally, the peak signal-to-noise ratio (*PSNR*) is used to analyze the distortion of stego image. The unit of *PSNR* is dB. The larger the value, the smaller the distortion level of the stego image. Therefore, we pursue the greatest possible *PSNR* value [36]. The *PSNR* can be calculated using Eq. (10).

$$PSNR = 10 \times log_{10}\frac{255^2}{MSE} \tag{10}$$

where, the mean square error (*MSE*) is used to measure the similarity between cover image and stego image. It can be found using Eq. (11).

$$MSE = \frac{1}{w \times h}\sum_{i=1}^{w}\sum_{j=1}^{h}\left(O_{ij} - P_{ij}\right)^2 \tag{11}$$

where O_{ij} and P_{ij} represent the pixel positions of cover image and stego image on coordinates (i, j). The width of the image is w, and the height of the image is h.

In the proposed method, no modification is made to the stego image when the secret information is hidden. In other words, cover image is the same as stego image, so $O_{ij} - P_{ij} = 0$, $MSE = 0$, and $PSNR = \infty$.

The structural similarity (*SSIM*) index is used to measure the similarity between cover image and stego image [37]. Its value ranges from -1 to $+1$. When cover image is the same as stego image, *SSIM* is equal to 1, which is also the optimal value of *SSIM*. It can be expressed by Eq. (12).

$$SSIM = \frac{(2\bar{p}\bar{q} + c_1)\left(2\sigma_{xy} + c_2\right)}{\left[(\bar{p})^2 + (\bar{q})^2 + c_1\right]\left(\sigma_x^2 + \sigma_y^2 + c_2\right)} \tag{12}$$

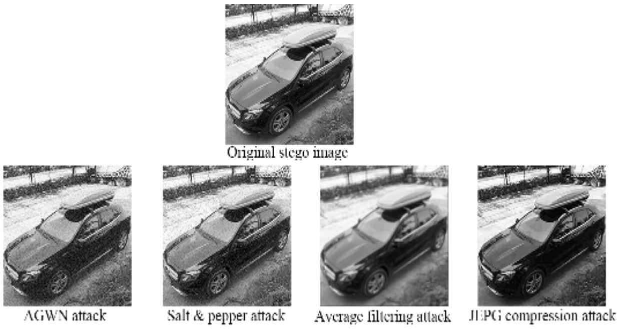
where, $\bar{p}$ and $\bar{q}$ represent the average pixel values of cover image and stego image. σ_x^2 and σ_y^2 represent the standard deviation of the cover image and the stego image, while σ_{xy} represents the covariance between the cover image and the stego image. Constant $c_1 = 2.55$, $c_2 = 7.65$.

The universal image quality index (*Qi*) is another important parameter to measure the similarity between the cover image and the stego image. When cover image is the same as stego image, *Qi* can get the optimal value of 1. The definition of *Qi* is as follows:

$$Q_i = \frac{4\sigma_{xy}\bar{p}\bar{q}}{\left(\sigma_x^2 + \sigma_y^2\right)\left[(\bar{p})^2 + (\bar{q})^2\right]} \tag{13}$$

TABLE 2. The hiding capacity, PSNR, SSIM and Qi comparison of CIHMSB method, Jung's method [15], Sahu's method [16], Sahu's method [17].

Methods	Hiding capacity($bits * carrier^{-1}$)	PSNR(dB)	SSIM	Qi
CIHMSB method	2601	∞	**1**	**1**
Jung's method[15]	288,369	44.06	0.9924	0.9913
Sahu's method[16]	262,144	51.30	0.9988	0.9965
Sahu's method[17]	768,432	48.20	0.9976	0.9950


Original stego image

AGWN attack

Salt & pepper attack

Average filtering attack

JPEG compression attack

FIGURE 11. After the attack, stego image became distorted.

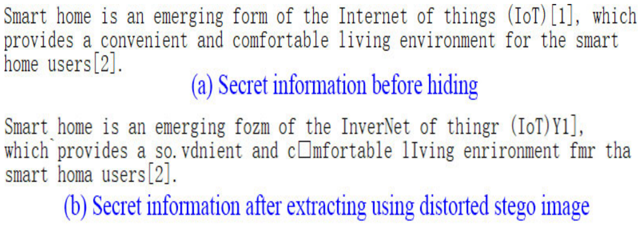
where, $\bar{p}$ and $\bar{q}$ represent the average pixel values of the cover image and the stego image. σ_x^2 and σ_y^2 represent the standard deviation of the cover image and the stego image, while σ_{xy} represents the covariance between the cover image and the stego image.

Table 2 gives the hiding capacity, *PSNR*, *SSIM* and *Qi* comparison for CIHMSB method, Jung's method [15], Sahu's method [16], Sahu's method [17]. As can be seen from Table 2, in terms of hiding ability, CIHMSB method is weaker than Jung's method and Sahu's method. However, the *PSNR*, *SSIM* and *Qi* of CIHMSB method all reach the optimal values, which are ∞, 1 and 1 respectively. Improving the hiding capacity is a direction for the future research on coverless information hiding.

E. ROBUSTNESS ANALYSIS

In this paper, gray image is used as the carrier of information hiding. Since stego image is transmitted through ordinary channels, various factors will interfere with stego image during transmission, such as defects of communication components and internal noise, resulting in image distortion, as shown in figure 11. Once the stego image is distorted, the extraction quality of the secret information will be affected, as shown in figure 12.

It is necessary to analyze the robustness of information hiding method. In this paper, Additive Gaussian White Noise (AGWN), salt & pepper noise, Low-pass filtering and JPEG compression are used to attack the CIHMSB method. The final results are averaged over multiple tests. In this paper, Bit Error Rate (*BER*) is used as the criterion to judge the



Smart home is an emerging form of the Internet of things (IoT)[1], which
provides a convenient and comfortable living environment for the smart
home users[2].

(a) Secret information before hiding

Smart home is an emerging fozm of the InverNet of thingr (IoT)Y1],
which provides a so.vdnient and c□mfortable lIving enrironment fmr tha
smart homa users[2].

(b) Secret information after extracting using distorted stego image

FIGURE 12. The quality of information extraction is affected by the use of the distorted stego image.

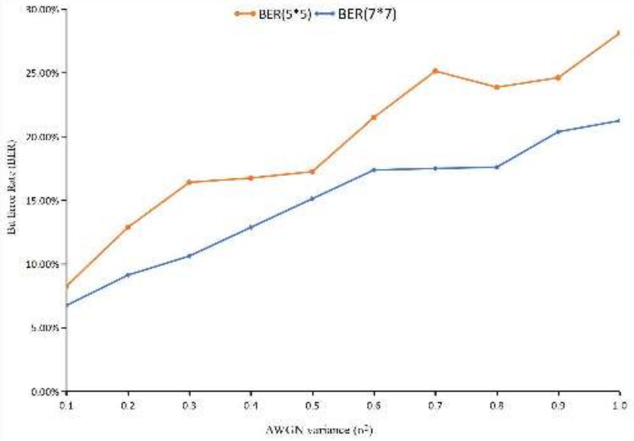


FIGURE 13. The *BER* tendency of CIHMSB method under different intensity AGWN attacks.

TABLE 3. The *BER* comparison of CIHMSB method, CBZS method [30], CSD method [31], and Jia's method [33] under different intensity AGWN attacks.

σ^2	CBZS	CSD	Jia	CIHMSB($F_w * F_h = 5 * 5$)	CIHMSB($F_w * F_h = 7 * 7$)
0.1	18%	14%	11%	**8.25%**	**6.75%**
0.2	19%	24%	17%	**12.88%**	**9.13%**
0.5	21%	25%	34%	**17.25%**	**15.13%**
0.6	21%	26%	35%	**21.50%**	**17.37%**
0.9	22%	31%	37%	**24.63%**	**20.38%**
1.0	22%	33%	37%	**28.12%**	**21.25%**

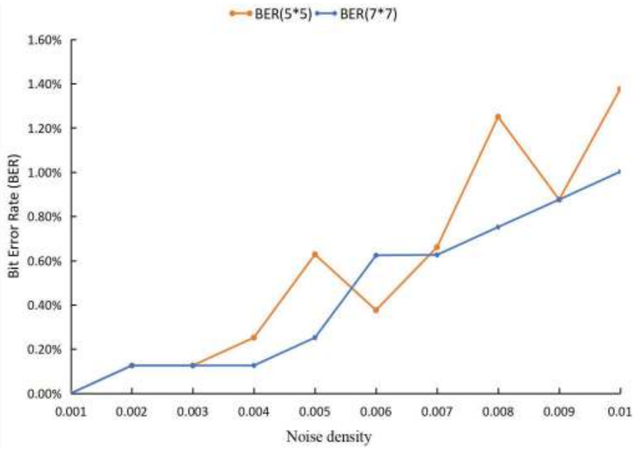


FIGURE 14. The *BER* tendency of CIHMSB method under different intensity salt & pepper noise attacks.

TABLE 4. The *BER* comparison of CIHMSB method, CSD method [31], CBD method [32] and Jia's method [33] under different intensity salt & pepper noise attacks.

Noise density	CBD	CSD	Jia	CIHMSB($F_w * F_h = 5 * 5$)	CIHMSB($F_w * F_h = 7 * 7$)
0.001	2.8%	2.6%	0%	**0%**	**0%**
0.003	4.0%	4.9%	0%	0.13%	0.13%
0.005	4.7%	6.2%	0%	0.63%	0.25%
0.007	5.9%	7.1%	0%	0.66%	0.63%
0.009	7.1%	8.2%	2.3%	**0.88%**	**0.88%**
1.0	22%	33%	37%	**1.38%**	**1.00%**

robustness performance [33]. *BER* is defined as:

$$BER = \frac{\mathrm{N_m}}{\mathrm{N_n}} \times 100\% \tag{14}$$

where, N_m represents the number of bits with errors when extracting secret information from stego image, and N_n represents the total number of bits of secret information to be hidden.

1) AGWN ATTACK

In the AGWN attack experiment, setting $\mu = 0, \sigma^2$ increases from 0.1 to 1.0. Figure 13 shows the *BER* tendency of CIHMSB method under different intensity AGWN attacks. As the show in figure 13, the *BER* increases with the increase of noise density. It is more effective against AWGN attacks when the image fragment size is $F_w * F_h = 7 * 7$ than the size of $F_w * F_h = 5 * 5$. Table 3 shows the *BER* comparison of CIHMSB method, CBZS method [30], CSD method [31], and Jia's method [33] under different intensity AGWN attacks. It is obvious that when the image fragment size is $F_w * F_h = 7 * 7$, the anti-AGWN performance of CIHMSB method is better than the other three methods.

2) SALT & PEPPER NOISE ATTACK

In the experiment of salt & pepper noise attack, the noise density increases from 0.01 to 0.1. Figure 14 shows the *BER* tendency of CIHMSB method under different intensity salt & pepper noise attacks. It is not difficult to find that the *BER* increases with the increase of noise density. It is more effective against salt & pepper noise attacks when the image fragment size is $F_w*F_h = 7*7$ than the size of $F_w*F_h = 5*5$. Table 4 shows the *BER* comparison of CIHMSB method, CSD method [31], CBD method [32] and Jia's method [33] under different intensity salt & pepper noise attacks. When the image fragment size is $7 * 7$, CIHMSB method has better performance in resisting the attack of salt & pepper noise than CBD and CSD method. In the case of low noise density, the performance of CIHMSB method is slightly worse than that of Jia's method. However, in the case of high noise density, CIHMSB method has better performance than Jia's method. In general, the performance of CIHMSB method in against salt & pepper noise attack is similar to Jia's method, but it is better than CBD and CSD method.

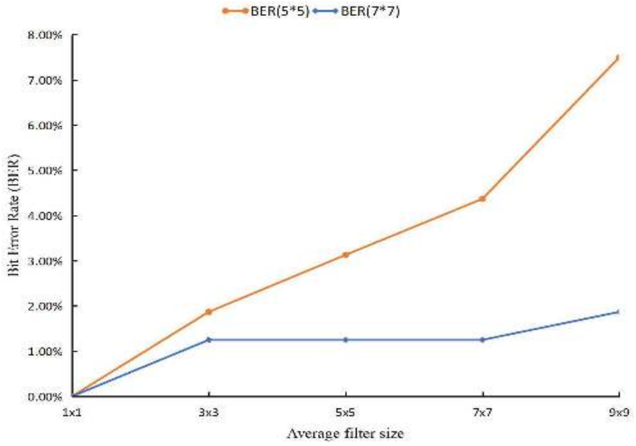


FIGURE 15. ***BER*** **of CIHMSB method under different average filtering attack.**

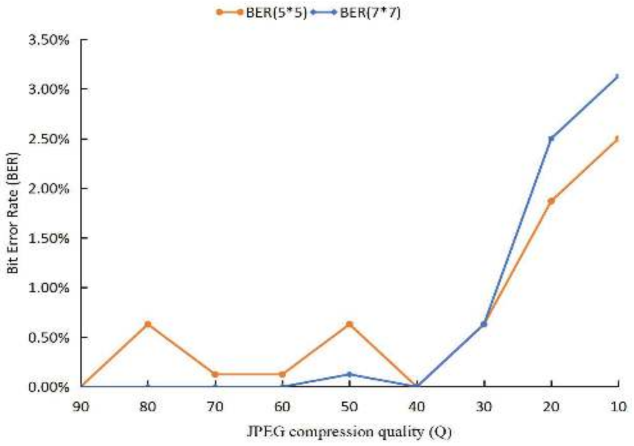


FIGURE 16. ***BER*** **of CIHMSB method under different** ***Q*** **of JPEG compression attack.**

TABLE 5. ***BER*** **comparison of CIHMSB method, CBZS method [30], CSD method [31] and Jia's method [33] under different average filtering attacks.**

Size	CBZS	CSD	Jia	CIHMSB($F_w * F_h = 5 * 5$)	CIHMSB($F_w * F_h = 7 * 7$)
3x3	7%	2%	6.25%	**1.87%**	**1.25%**
5x5	10%	3.5%	6.25%	**3.13%**	**1.25%**
7x7	12.5%	5.1%	12.5%	**4.37%**	**1.25%**
9x9	14%	6.8%	12.5%	7.5%	**1.87%**

TABLE 6. ***BER*** **comparison of CIHMSB method, CSD method [31], CBRI method [34] and Jia's method [33] under JPEG compression attacks with different** ***Q*****.**

Quality	CSD	CBRI	Jia	CIHMSB($F_w * F_h = 5 * 5$)	CIHMSB($F_w * F_h = 7 * 7$)
90	0.24%	0%	0%	**0%**	**0%**
80	0.4%	2.5%	0%	0.630%	**0%**
70	0.8%	7.5%	0%	0.125%	**0%**
60	1.8%	7.5%	0%	0.125%	**0%**
50	2%	7.5%	0%	0.630%	0.125%

3) LOW-PASS FILTERING ATTACKS

In the analysis of low-pass filtering attacks, the average filtering technique is selected in this test scheme. Average filtering technique is to take the average of the image brightness. The size parameters of the average filter range from 1 × 1 to 9 × 9, where 1 × 1 represents the minimum attack and 9×9 the maximum attack. Figure 15 shows the *BER* tendency of CIHMSB method under the average filtering attacks of different filtering sizes. As the filtering size increases, so does *BER*. In the same filtering size, when the image fragment is $F_w * F_h = 7 * 7$, the performance of resisting low-pass filtering attack is better than when the image fragment is $F_w * F_h = 5 * 5$. Table 5 illustrates the *BER* comparison of CIHMSB method, CBZS method [30], CSD method [31] and Jia's method [33] under different average filtering attacks. From table 5, it can come to a conclusion that the performance of ant-low-pass filtering attacks of CIHMSB is the best than other three methods no matter the size of the image fragment is $F_w * F_h = 5 * 5$ or $F_w * F_h = 7 * 7$.

4) JPEG COMPRESSION ATTACK

Although JPEG compression is lossy and the appearance of compressed images is poor, it is still used in many fields. If JPEG compression technology is used in the transmission of stego image, it may affect the secret information extraction quality for the receiver. Therefore, it needs to test the JEPG compression attack on CIHMSB method. The JPEG compression quality (Q) selected in this experiment range from 10 to 90, with a unit interval of 10. $Q = 10$ indicates a lower mass of compression, while $Q = 90$ indicates a higher mass of compression. Figure 16 shows the *BER* tendency of CIHMSB method under JPEG compression attack with different Q. As Q decreases, *BER* increases. In the case of high Q, the performance of against JPEG compression attack is better when the image fragment is $F_w * F_h = 7 * 7$ than when the image fragment is $F_w * F_h = 5 * 5$. However, in the case of lower Q, the situation is reversed. Table 6 shows the *BER* comparison of CIHMSB method, CSD method [31], Jia's method [33] and CBRI method [34] under the attack of JPEG compression with different Q. It can be seen from table 6 that CIHMSB method has a better performance of resistance to JPEG compression attack than CSD method and CBRI method, regardless of the size of the image fragment ($F_w*F_h = 5*5$ or $F_w*F_h = 7*7$). When the image fragment size is $F_w * F_h = 5 * 5$, the performance of CIHMSB method is slightly worse than that of the Jia's method. However, when the image fragment size is $F_w * F_h = 7 * 7$, the performance of CIHMSB method is similar to that of the Jia's method.

V. CONCLUSION AND FUTURE WORK

To solve the information leakage problem, this paper proposes a novel coverless information hiding method based on the Most Significant Bit of the cover image. In this scheme, the cover image is first segmented into a number of image fragments. After the preprocess of the secret information, the secret information is translated to binary form. Then, the mapping between the MSB of the image fragments and the binary form secret information is established according to the mapping sequence *Km*, outputting a mapping flag *Kf*. Using *Kf* and *Km*, the receiver can extract the secret information from the stego image. In the whole process of information hiding, no modification are made to the cover image. In other words, cover image and stego image are exactly the same. The proposed method can resist all the attack of steganalysis tools.

The experimental results show that the proposed method has higher hiding capacity than the existing coverless information hiding methods. What's more, the proposed method can conceal 2601 bits secret information per carrier with peak signal-to-noise ratio (*PSNR*) of ∞ dB, and the *SSIM* and *Qi* of the proposed method are better than existing information hiding methods. In addition, in terms of security, the method can resist all the attack of steganalysis tools. The proposed method can effectively resist such as AGWN, salt & pepper noise, low-pass filtering and JPEG compression attacks. Compared with the existing information hiding methods, the proposed method has higher robustness. In summary, the proposed method is more suitable for practical application than the existing coverless information hiding methods.

Stego image is transmitted through ordinary channels, and the channel noise will cause the distortion to stego image, causing the receiver to be unable to accurately extract the secret information. Therefore, part of our future works is to select more perfect image features, improving the robustness of the algorithm, reducing the *BER* when the receiver extracting secret information. At the same time, we will also work on increasing the hiding capacity.

ACKNOWLEDGMENT

The authors would like to thank to Dr. Lina Yang for her guidance of the scheme and experiment, and Dr. Xiaocui Dang for her careful help in writing the paper.

REFERENCES

[1] A. K. Sahu, G. Swain, and E. S. Babu, "Digital image steganography using bit flipping," *Cybern. Inf. Technol.*, vol. 18, no. 1, pp. 69–80, Mar. 2018.

[2] Y. A. Basallo, V. E. Senti, and N. M. Sanchez, "Artificial intelligence techniques for information security risk assessment," *IEEE Latin Amer. Trans.*, vol. 16, no. 3, pp. 897–901, Mar. 2018.

[3] M. G. V. Kumar and U. S. Ragupathy, "A survey on current key issues and status in cryptography," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Mar. 2016, pp. 205–210.

[4] Y. Ziqian, G. Zijie, and F. Hao, "An improved information hiding algorithm based on image," in *Proc. IEEE 15th Int. Conf. Softw. Eng. Res., Manage. Appl. (SERA)*, Jun. 2017, pp. 169–172.

[5] A. K. Sahu and G. Swain, "Pixel overlapping image steganography using PVD and modulus function," *3D Res.*, vol. 9, no. 3, pp. 40–54, Sep. 2018.

[6] H.-C. Wu, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," *IEE Proc.-Vis., Image Signal Process.*, vol. 152, no. 5, pp. 611–615, Oct. 2005.

[7] A. K. Sahu and G. Swain, "High fidelity based reversible data hiding using modified LSB matching and pixel difference," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 7, no. 4, pp. 1–15, Jul. 2019.

[8] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.

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

[10] R. T. McKeon, "Strange Fourier steganography in movies," in *Proc. IEEE Int. Conf. Electro/Inf. Technol.*, May 2007, pp. 178–182.

[11] L. Yuejun, S. Jing, and L. Feng, "Research on information hiding system based on DCT domain," in *Proc. 2nd Int. Conf. Comput. Model. Simulation*, Jan. 2010, pp. 11–14.

[12] J. Wang, T. Li, Y.-Q. Shi, S. Lian, and J. Ye, "Forensics feature analysis in quaternion wavelet domain for distinguishing photographic images and computer graphics," *Multimedia Tools Appl.*, vol. 76, no. 22, pp. 23721–23737, Nov. 2017.

[13] P. Schottle and R. Bohme, "Game theory and adaptive steganography," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 4, pp. 760–773, Apr. 2016.

[14] J. Lu, G. Zhou, C. Yang, Z. Li, and M. Lan, "Steganalysis of content-adaptive steganography based on massive datasets pre-classification and feature selection," *IEEE Access*, vol. 7, pp. 21702–21711, 2019.

[15] K. H. Jung, "Dual image based reversible data hiding method using neighbouring pixel value differencing," *The Imag. Sci. J.*, vol. 63, no. 7, pp. 398–407, 2015.

[16] A. K. Sahu and G. Swain, "Dual Stego-imaging based reversible data hiding using improved LSB matching," *Int. J. Intell. Eng. Syst.*, vol. 12, no. 5, pp. 63–73, 2019.

[17] A. K. Sahu and G. Swain, "Reversible image steganography using dual-layer LSB matching," *Sens. Imag.*, vol. 21, no. 1, pp. 1–21, Dec. 2020.

[18] Y. Ma, X. Luo, X. Li, Z. Bao, and Y. Zhang, "Selection of rich model steganalysis features based on decision rough set α-positive region reduction," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 2, pp. 336–350, Feb. 2019.

[19] 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, no. 28, pp. 299–326, Mar. 2019.

[20] Z. Zhou, H. Sun, R. Harit, X. Chen, and S. Xingming, "Coverless image steganography without embedding," in *Proc. Int. Conf. Cloud Comput. Secur.*, vol. 9483, 2015, pp. 123–132.

[21] J. Qin, Y. Luo, X. Xiang, Y. Tan, and H. Huang, "Coverless image steganography: A survey," *IEEE Access*, vol. 7, pp. 171372–171394, 2019.

[22] Z. L. Zhou, Y. Cao, and X. M. Sun, "Coverless information hiding based on bag-of-words model of image," *J. Appl. Sci.*, vol. 34, no. 5, pp. 527–536, 2016, doi: 10.3969/j.issn.0255-8297.2016.05.005.

[23] J. Yang, Y.-G. Jiang, A. G. Hauptmann, and C.-W. Ngo, "Evaluating bag-of-visual-words representations in scene classification," in *Proc. Int. Workshop Workshop Multimedia Inf. Retr. (MIR)*, 2007, pp. 197–206.

[24] X. Shi, Z. Guo, D. Zhang, and X. Fang, "Multiple features fusion based inverted multi-index for image retrieval," in *Proc. Int. Conf. Virtual Reality Vis. (ICVRV)*, Oct. 2015, pp. 148–153.

[25] L. Zou, J. Sun, M. Gao, W. Wan, and B. B. Gupta, "A novel coverless information hiding method based on the average pixel value of the sub-images," *Multimedia Tools Appl.*, vol. 78, no. 7, pp. 7965–7980, Jul. 2018.

[26] Y. Cao, Z. Zhou, X. Sun, and C. Gao, "Coverless information hiding based on the molecular structure images of material," *Comput., Mater. Continua*, vol. 54, no. 2, pp. 197–207, 2018.

[27] Z. Zhou, Y. Mu, and Q. J. Wu, "Coverless image steganography using partial-duplicate image retrieval," *Soft Comput.*, vol. 23, no. 2, pp. 1–12, Mar. 2018.

[28] X. Liao, J. Yin, S. Guo, X. Li, and A. K. Sangaiah, "Medical JPEG image steganography based on preserving inter-block dependencies," *Comput. Electr. Eng.*, vol. 67, pp. 320–329, Apr. 2018.

[29] Y. Luo, J. Qin, X. Xiang, Y. Tan, Q. Liu, and L. Xiang, "Coverless real-time image information hiding based on image block matching and dense convolutional network," *J. Real-Time Image Process.*, vol. 17, no. 1, pp. 125–135, Sep. 2019.

[30] M. Bilal, S. Imtiaz, W. Abdul, S. Ghouzali, and S. Asif, "Chaos based zero-steganography algorithm," *Multimedia Tools Appl.*, vol. 72, no. 2, pp. 1073–1092, Sep. 2014.

[31] J. Wu, X. Fei, and N. Wang, "Study on image zero steganography algorithm based on chaotic sequence and DCT transform," *Electron. Meas. Techn.*, vol. 40, no. 5, pp. 174–179, 2017.

[32] S. Singh and T. J. Siddiqui, "A security enhanced robust steganography algorithm for data hiding," *Int. J. Comput. Sci. Issues*, vol. 9, no. 3, pp. 131–139, 2013.

[33] Y. Jia, "Research and implementation of coverless information hiding algorithm based on image coding," M.S. thesis, College Phys. Sci. Technol., Central China Normal Univ., Wuhan, China, 2018.
[34] S. Zheng, L. Wang, B. Ling, and D. Hu, "Coverless information hiding based on robust image hashing," *Intell. Comput. Methodol.*, vol. 10363, pp. 536–547, Jul. 2017.
[35] A. Anjum and S. Islam, "LSB steganalysis using modified weighted stego-image method," in *Proc. 3rd Int. Conf. Signal Process. Integr. Netw. (SPIN)*, Feb. 2016, pp. 630–635.
[36] A. K. Sahu and G. Swain, "A novel n-rightmost bit replacement image steganography technique," *3D Res.*, vol. 10, no. 1, pp. 1–18, Mar. 2019.
[37] A. K. Sahu and G. Swain, "An optimal information hiding approach based on pixel value differencing and modulus function," *Wireless Pers. Commun.*, vol. 108, no. 1, pp. 159–174, Sep. 2019.

LINA YANG (Member, IEEE) received the B.S. degree in computer engineering from Shijiazhuang Railway University, Shijiazhuang, China, in 2005, the M.Eng. degree in computer science from the University of Malaya, Kuala Lumpur, Malaysia, in 2011, and the Ph.D. degree from the University of Macau, Macau, in 2015. She is currently a Lecturer with the School of Computer, Electronics, and Information, Guangxi University, Nanning, China. Her research interests include medical biometrics, machine learning, image processing, and information security.

HAIYU DENG received the B.S. degree in thermal energy and power engineering from Shandong University, Shandong, China, in 2015. He is currently pursuing the M.S. degree with the School of Computer, Electronics, and Information, Guangxi University, Nanning, China. His research interests include information security, image processing, and machine learning.

XIAOCUI DANG received the B.S. degree in computer science and technology from Jining University, Shandong, China, in 2017. She is currently pursuing the M.S. degree in computer science and technology with Guangxi University, Nanning, China. Her research interests include information security, image processing, machine learning, and bioinformatics.