A Novel Improved Reversible Visible Image Watermarking Algorithm Based on Grad-CAM and JND

Jiasheng Qu, Wei Song, Xiangchun Liu, Lizhi Zhao, and Xiaobing Zhao

1School of Information Engineering, Minzu University of China, Beijing, China
2National Language Resource Monitoring and Research Center of Minority Languages, Minzu University of China, Beijing, China

Correspondence should be addressed to Wei Song; songwei@muc.edu.cn

Received 2 November 2020; Revised 21 December 2020; Accepted 8 January 2021; Published 25 January 2021

Copyright © 2021 Jiasheng Qu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the rapid access convenience of content brought by 5G technology, the integrity protection of content becomes more important. The reversible visible watermarking algorithm has attracted more attention due to its effective content protection. In this paper, a novel improved reversible visible image watermarking scheme based on gradient-weighted class activation mapping (Grad-CAM) and the just noticeable difference (JND) model has been presented. The proposed region of interest (ROI) selection strategy is used to locate the main protected body of images for watermark embedding. Divide the watermark and ROI into nonoverlapping blocks in the same way and then embed the classified two types of watermark blocks into corresponding ROI blocks with the JND model. The optimal bit positions for watermark embedding can be selected adaptively with JND threshold and achieve the tradeoff between the watermark visibility and watermarked image quality. For lossless image recovery and watermark extraction, the recovery information is reversibly hidden into watermarked image. In the experiments, the same process of grayscale images is used to each channel separately for color images watermarking. Besides, there are six aspects in this paper to estimate the proposed scheme; with the comparison to other reversible visible watermarking schemes, experimental results demonstrate the effectiveness of our proposed scheme.

1. Introduction

Nowadays, the rapid development of 5G technologies is benefiting all aspects of our lives; at the same time, the multimedia data in the networks are becoming larger and larger. The security of multimedia data deserves more attention. Also, the digital images, as one of the most important carriers in the network information transmission, its security and privacy need more concerns from researchers. The visible watermarking technique which can embed copyright information into cover images has developed rapidly. There are two categories of visible watermarking: reversible and irreversible. In the past, many irreversible visible watermarking schemes have been proposed [1–4], but the original cover image can hardly be recovered. On the other hand, the reversible visible watermarking schemes can recover both the original image and the watermark perfectly. This paper focuses on the latter.

Many reversible visible watermarking schemes are proposed in the past [5–10]. Hu and Jeon [5] proposed a scheme by modifying one significant bit plane of the pixels to achieve watermark visibility. Then, they compressed the altered bit plane values as recovery information which was embedded into the nonwatermarked image region for lossless recovery. However, the watermarked image often distorts rather significantly compared with the original image. In [6], the reversible watermarking scheme based on deterministic one-to-one compound mappings of image pixel values has been proposed. Chen et al. [7] proposed a scheme based on the conventional difference expansion technique. In this scheme, the cover image is divided into nonoverlapping blocks and each block is embedded with one watermark bit. But unfortunately, there is a large amount of overflowing or underflowing pixels in the watermarked image. Once exceeded, the watermarked image cannot be recovered perfectly. In the scheme of [8] by Mohammad
et al., the pixel circular shift operation is utilized to embed the watermark into the block truncation coding-compressed (BTC-compressed) image. According to the parity of the bit plane, the watermark signal can be extracted reversibly. In the abovementioned reversible visible watermarking schemes, the watermark embedding region is specified, which is generally the center of the cover image. In [9], Qi et al. proposed a reversible visible scheme based on the human visual system (HVS) and region of interest (ROI) selection. For watermark embedding, HVS is adopted to modify the pixel values so as to get a better effect of watermark visibility. And, the ROI selection strategy is designed to find the flat regions with low or high luminance for watermark embedding. The chosen flat regions usually do not contain abundant information which can be easily cropped but without affecting the whole information of images. However, to maintain the copyright of the images better, the visible watermark should be embedded into the subject region of the image which contains the most important image information. Hence, the selected ROI for watermark embedding in [9] may be not suitable. To select the subject region of images, we proposed a novel ROI selection strategy based on Grad-CAM [11] for visible watermark embedding. With this novel ROI selection strategy, the visible watermark can be embedded in the subject region to protect the copyright of images. However, the visible watermark into the subject region can degrade the watermarked image quality. The key to solving this problem is to balance the watermark visibility and the watermarked image quality, which means the embedded watermark should not be so significant that the watermarked image details have been covered too much [2, 3]. Motivated by the scheme proposed by Yao et al. [10], the enhanced JND model [12] has been utilized in this paper to obtain the tradeoff between watermark visibility and watermarked image quality.

Generally, a reversible visible watermarking technique is used to protect and maintain the copyright. The region of visible watermark embedding is vital. Assuming that the watermark embedding region is not the subject of an image, it can be easily modified or cropped for malicious use. However, there is no scheme proposed in the past to select the main body region as ROI for visible watermark embedding.

In this paper, we have proposed an improved reversible visible watermarking scheme. In the proposed scheme, we concentrate on the novel ROI selection strategy to locate the subject region for watermark embedding and apply the JND model to balance between the watermark visibility and the marked image quality. To achieve reversibility, the reversible data hiding algorithm to embed the recovery information into the watermarked image is utilized so that the image can be recovered losslessly and the watermark can be extracted perfectly.

In conclusion, the contribution of the proposed algorithm is listed as follows:

1. A novel ROI selection strategy to locate the subject region of the image for watermark embedding is proposed.
2. Watermark embedding positions can be adaptively selected for the balance between watermark visibility and the marked image quality.
3. It can be lossless and perfect for image recovery and watermark extraction.

The rest of the paper is organized as follows. In Section 2, the gradient-weighted class activation mapping (Grad-CAM) for ROI selection strategy is presented. The proposed method is described in Section 3. In Section 4, the performance of the proposed framework is reported. Finally, Section 5 concludes the paper and discusses possible future work.

2. The Gradient-Weighted Class Activation Mapping

For most images, it contains at least one subject, which must belong to a certain category. By locating the class region, we can select the subject area as ROI for watermark embedding. Grad-CAM uses the gradients of a target concept which means the name of the class here, e.g., ‘wood rabbit’ and flow the feature maps into the final convolutional layer. Finally, the coarse localization map is obtained in which the subject region of the concept is highlighted [11]. And, we can obtain the ROI for watermark embedding by processing the coarse localization map.

With a specific class name and a cover image as input, we can obtain the coarse localization map \( L_{\text{Grad-CAM}} \in \mathbb{R}^{u \times v} \) of width \( u \) and height \( v \) for class \( c \) with the class subject region highlighted. Figure 1 shows the network structure in detail. The gradient information flows into the last convolutional layer of the convolutional neural network (CNN) by assigning importance values to each neuron to locate the class. And, the feature map importance weights \( \alpha^c_k \) for class \( c \) can be calculated by

\[
\alpha^c_k = \frac{1}{Z} \sum_i \sum_j \left( \frac{\partial y^c}{\partial A^c_{i,j}} \right),
\]

where \( k \) means the \( k \)-th feature map; \( y^c \) is the score for class \( c \) before softmax; \( A^c \) is the feature map activations at the position \( (i, j) \) of the feature map; \( \text{GAP} \) means global average pooling; \( \text{GB} \) means gradients via backprop; and \( Z \) is a constant used through the global average pooling.

The weight \( \alpha^c_k \) which represents a partial linearization of the deep network downstream from \( A \) can capture feature map \( k \) which means ‘important’ for the target class \( c \). To obtain the coarse localization map \( L_{\text{Grad-CAM}} \in \mathbb{R}^{u \times v} \), the weighted combination of forwarding activation maps is combined with function \( \text{ReLU} \). LC is the linear combination.
3. Proposed Scheme

The improved reversible visible image watermarking scheme proposed in this paper includes four parts: the novel ROI selection, watermark embedding, reversible data hiding, and last, watermark extraction and image recovery. The flow chart of our proposed scheme is shown in Figure 3. With the original cover image I, we propose a novel ROI selection strategy to locate the subject region for watermark embedding via Grad-CAM. Then, embed the visible binary watermark W into ROI using the JND model for balancing between the watermark visibility and the marked image quality, and also, we can obtain the recovery information D and watermarked image Iw meanwhile. To achieve the reversibility, the encoded recovery information Dc for compressing the bits of D should be embedded into the watermarked image Iw to obtain the reversible watermarked image Iw'. When receiving the reversible watermarked image Iw', the extracted watermark WE and the recovered image IR can be obtained losslessly and perfectly with the extracted recovery information from Iw'. To improve the security of this scheme, we use logistic mapping to generate pseudo-random sequences of [0, 1] with the secret key for watermark embedding and recovery information encryption. And, the original image cannot be recovered if the secret key is wrong. For our proposed reversible visible image watermarking scheme, the novel ROI selection strategy is discussed in Section 3.1. Section 3.2 presents the watermark embedding in detail. The reversible data hiding of recovery information is described briefly in Section 3.3. Finally, Section 3.4 shows the process of watermark extraction and image recovery.

3.1. The Novel ROI Selection Strategy. The region of watermark embedding also called ROI should cover the subject of images to the greatest extent. And, the image subject heatmap can be obtained via Grad-CAM with the dataset ImageNet [13]. The heatmap is quantized based on jet color; that is, for some regions, the redder, the closer to the subject. Hence, we can get the information on ROI by only processing the R channel of the subject localization heatmap. By binarizing the R channel, the connected region that approximates the main protected body of the image is obtained, shown in Figures 2 (c1), (c2), and (c3). Choose the connected region with the maximum area as the selected ROI processing region. When there is more than one salient subject in the image, the maximum ROI means more important and needs primary protect. To get the ROI for watermark embedding, we should obtain the watermark size and at least one coordinate in the cover image for embedding. Also, we can get the geometric center coordinate (x_o, y_o) of the connected area meanwhile. For cover images from ImageNet [13], we do not specify the watermark size because of themselves varying in size. Considering a cover image I with the size of H × W, we can obtain the watermark size by

\[ h = w = \min \left( \left[ \frac{H}{(r \cdot 2^l)} \right], 2l \right) \left[ \frac{W}{(r \cdot 2^l)} \right], 2l), \quad r = 2, 3, 4, \]

where \( h \times w \) is the watermark size, \( r \) is the ratio of watermark size respect to cover images, \( l \) is the divided block size of ROI for watermark embedding, and \( [\cdot] \) is the ceiling operator. For convenience, we use the top-left coordinate of watermark embedding in cover images calculated by

\[
\begin{align*}
x_w &= x_o - \frac{h}{2}, \\
y_w &= y_o - \frac{w}{2},
\end{align*}
\]

with the watermark size \( h \times w \) and the coordinate \((x_w, y_w)\), and the novel ROI for watermark embedding is denoted by

\[
\text{ROI} = \{(i,j)|x_w \leq i \leq x_w + h - 1, y_w \leq j \leq y_w + w - 1\},
\]

where \((i,j)\) is the position in the cover image I. Figures 2 (d1), (d2), and (d3) show the ROI in the heatmap with \( r = 2 \), which can cover the subject of images.
3.2. Watermark Embedding. In this section, the watermark embedding strategy will be discussed in detail. Figure 4 shows the framework of watermark embedding. With the embedding information, the resized watermark is embedded into the ROI of the image. The bit planes of the original image need to be substituted with corresponding watermark values for visibility. To obtain the tradeoff between the watermark visibility and the watermarked image quality, the enhanced JND model is utilized. Just noticeable difference (JND) usually means the limit threshold of the human visual system (HVS). And, HVS can only notice the image content change which is larger than the JND threshold. There are many efficient JND models proposed in the past [12, 14, 15]. The enhanced JND model with pattern complexity proposed by Wu et al. [12] is utilized for watermark embedding in this paper. Through the JND model, we can obtain the threshold.
of each pixel in the image. Figure 5 shows the cover image and its JND map for better understanding; more details of this JND model can be seen in [12]. And, to improve the security of this scheme, we use the logistic mapping to generate pseudorandom sequences with the secret key for watermark embedding. It is defined as

$$x_{n+1} = \lambda x_n(1 - x_n),$$  
(6)

where $n$ is the iteration times of chaotic sequences and $\lambda$ is the control parameter of the logistic mapping system.

For any $x_0 \in (0, 1)$, the logistic mapping has chaotic characteristics when $3.99 < \lambda < 4.00$[16, 17]. With the natural sequence $S_n$ as input, a pseudorandom sequence $S_r$ can be obtained using (6). Then, the pseudorandom sequence of $\{0, 1\}$ for watermark embedding is generated by

$$S_w = \text{mod}(S_r, 2).$$  
(7)

For instance, with $x_0 = 0.4, \lambda = 3.991$, a natural sequence whose length value is 9, $S_n = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, and $S_r = \{5, 6, 2, 0, 7, 3, 1, 8, 4\}$ can be obtained using (6), and finally the pseudorandom sequence for embedding $S_w = \{1, 0, 0, 0, 1, 1, 0, 0\}$ can be generated with (7).

Considering a binary watermark $W$ with the size of $h \times w$, which is equal to ROI, we divide $W$ and ROI into nonoverlapping blocks in the same way, and both of them are corresponding to each other denoted by

$$\Omega_W = \left\{ W_k | k = 1, 2, \ldots, \left[ \frac{h}{T} \right] \cdot \left[ \frac{w}{T} \right] \right\},$$  
$$\Omega_R = \left\{ R_k | k = 1, 2, \ldots, \left[ \frac{h}{T} \right] \cdot \left[ \frac{w}{T} \right] \right\},$$  
(8)

and then we classify watermark blocks into two types as black block and white block using

$$t = \begin{cases} 1, & \text{if } \phi(W_k) \geq l^2, \\ 0, & \text{else,} \end{cases}$$  
(9)

where $t$ means the type of binary watermark block, which refers to white block if the value is 1 and means black block if the value is 0. $\phi(W_k) = \sum_p S_w(p, q)$, where $W_k(p, q)$ is the watermark value at $(p, q)$ of this block which is 0 or 1 in a binary watermark. The embedding of the visible watermark is essentially the change of the pixel value of the cover image according to the watermark bits. Given a pixel $p_{i,j}$ at $(i, j)$ in the original cover image $I$, we can obtain the changed pixel $\hat{p}_{i,j} (\theta)$ after embedding the watermark bit value $\delta_{x,y} = \{0, 1\}$ into $p_{i,j}$ by

$$\hat{p}_{i,j} (\theta) = \begin{cases} p_{i,j} - b_{i,j} (\theta) \cdot 2^\theta + \delta_{x,y} \cdot 2^\theta, & \text{if } d_{i,j} = 1, \\ p_{i,j} - b_{i,j} (\theta - 1) \cdot 2^{\theta-1} + \delta_{x,y} \cdot 2^{\theta-1}, & \text{if } d_{i,j} = 0, \end{cases}$$  
(10)

where $b_{i,j} (\theta) = \text{mod}([p_{i,j} / 2^\theta], 2)$, $\theta = 1, 2, 3, \ldots, 7, \theta$ is the watermark embedding position of original pixel bit planes, $d_{i,j}$ is the pseudorandom $\{0, 1\}$ generated from logistic mapping, and $[\cdot]$ is the flooring operator. Noticed that the coordinate in watermark $W$, $(x, y)$ has a relationship with the position of the cover image $I$, $(i, j)$ as follows:

$$\begin{cases} x = i - x_w + 1, \\ y = j - y_w + 1. \end{cases}$$  
(11)

Considering the $k$-th ROI block $R_k$, its visual distortion caused by watermark bit embedded can be calculated by

$$D_{R_k}(\theta) = \frac{1}{I \times I} \sum_{p_{i,j} \in R_k} (\hat{p}_{i,j} (\theta) - p_{i,j})^2.$$  
(12)

For a binary watermark, only a level needs to be visible usually, which depends on the owner’s choice. The white...
region of the binary watermark using in this paper needs to be visible, while the black region should be invisible. The selected position of bit planes for watermark embedding can affect both watermark visibility and the watermarked image quality. To balance these two conflicting factors, we operate two types of blocks of watermark separately. For a watermark block $W_k$ embedding into a corresponding cover image block $R_k$, the optimal embedding position is obtained by

$$\begin{align*}
\text{OP1: minimize } & D_{R_k} (\theta) \\
\text{subject to } & \theta = 1, 2, 3, \ldots, 7,
\end{align*}$$

where

$$g(x) = \begin{cases} 
0, & \text{if } |x| \leq 1, \\
1, & \text{if } |x| \geq 10, \\
\log_{10}|x|, & \text{else}.
\end{cases}$$

In (13), $T_{\text{IND}}(p_{i,j})$ is the JND threshold at $(i,j)$ in the cover image and $\alpha$ and $\beta$ are tuning parameters to adjust the visibility of watermark. Simply speaking, the process of watermark embedding is to let the black block embedded with the least distortion while the white block is embedded with the least distortion but meeting the condition of visibility first. Also, the optimal watermark embedding positions set $\Theta = \{\theta_k | k = 1, 2, \ldots, [(h/l)] \cdot [(w/l)]\}$ can be constructed using (13). For reversibility, the optimal embedding positions $\theta_k$ and its corresponding pixel bit value $b_{i,j}(\theta_k)$ need to be saved as a part of recovery information. Through the operations of watermark blocks embedding into corresponding cover image blocks, we can obtain the watermarked image $I_w$ with the tradeoff between the watermark visibility and the marked image quality. The recovery information $D$ which should be reversibly hidden in $I_w$ consists of four parts as follows:

1. The top-left coordinate $(x_w, y_w)$ of watermark embedding which needs $\lceil \log_2 H \rceil + \lceil \log_2 W \rceil$ bits
2. The size of the watermark $h \times w$ which needs $\lceil \log_2 H \rceil + \lceil \log_2 W \rceil$ bits
3. The optimal watermark embedding positions $\Theta = \{\theta_k | k = 1, 2, \ldots, [(h/l)] \cdot [(w/l)]\}$ which need $3 \cdot [(h/l)] \cdot [(w/l)]$ bits
4. The corresponding substituted pixel bits $B = \{b_{i,j}(\theta_k) | (i,j) \in n \Omega_{g,h}, h \theta_k \in x\theta\}$ of the embbeding positions which need $h \times w$ bits

3.3. Reversible Data Hiding. For the reversibility of this scheme, the pairwise prediction-error expansion (PPE) for efficient reversible data hiding proposed by Ou et al. [18] is utilized in this paper. Compared with other reversible data hiding (RDH) schemes based on PEE [19–21], Ou et al. [18] consider the correlations among prediction-errors and use the sequence and the resulting 2D prediction-error histogram to make the RDH scheme more efficient.

Noticed that, the size of the total bits of the recovery information is $2 \cdot \lceil \log_2 H \rceil + 2 \cdot \lceil \log_2 W \rceil + 3 \cdot [(h/l)] \cdot [(w/l)] + h \times w$, which the selection positions and the original bit values are the most. Hence, before RDH, to reduce the size of recovery information, the simple arithmetic coding is utilized to encode the positions and the original bits; as a result, the encoded recovery information $D_e$ is obtained. Next, we use the EXCLUSIVE-OR operator to encrypt the encoded recovery information with the pseudorandom sequence generated by (6) and (7). Finally, using RDH to reversibly hide the information into a watermarked image $I_w$, the reversible watermarked image $I_w'$ is obtained. Details of the data hiding and extraction procedures can be seen in [18].

3.4. Watermark Extraction and Image Recovery. The original cover image can be losslessly recovered by removing the watermark with the correct keys. In addition, the binary watermark can also be extracted perfectly through the process. The procedures of watermark extraction and image recovery can be simply described as follows.

**Step 1.** Extract the encrypted encoded recovery information from the reversible watermarked image $I_w'$ via the RDH
algorithm [18], and also the watermarked image $I_w$ is obtained meanwhile.

**Step 2.** Decrypt the encoded information $D_e$ with the correct encryption key.

**Step 3.** Obtain the recovery information $D$ including the watermark embedding coordinate $(x_w, y_w)$, the watermark size $h \times w$, the selected positions $\Theta$, and the original bit values $B$ by decoding the encoded information $D_e$.

\[
p_{i,j}(\theta_k) = \begin{cases} \bar{p}_{i,j}(\theta_k) + b_{i,j}(\theta_k - 1) \cdot 2^{\theta_k - 1} - \omega_{x,y} \cdot 2^{\theta_k - 1}, & \text{if } d_{i,j} = 0, \\ \bar{p}_{i,j} + b_{i,j}(\theta_k), & \text{if } d_{i,j} = 1, \end{cases}
\]

\[
\omega_{x,y} = \begin{cases} \text{mod} \left( \frac{\bar{p}_{i,j}}{2^{\theta_k - 1}}, 2 \right), & \text{if } d_{i,j} = 1, \\ \text{mod} \left( \frac{\bar{p}_{i,j}}{2^{\theta_k - 1}}, 2 \right), & \text{if } d_{i,j} = 0, \end{cases}
\]

where $d_{i,j}$ is the pseudorandom number of $\{0,1\}$ generated by the watermark embedding key using (6) and (7).

4. **Experimental Results and Performance Analysis**

In this section, we conduct a series of analyses and take the schemes proposed by Hu and Jeon [5], Chen et al. [7], and Mohammad et al. [8] for comparison to demonstrate the effectiveness of our proposed scheme. In the experiments of our proposed scheme, all the subject localization heatmaps are generated via Grad-CAM with off-the-shelf pretrained VGG-16 [22], and the dataset for training and testing is ImageNet [17]. Also, the cover images in this scheme are from ImageNet [13] which are RGB color type; to be simple to describe the algorithm, we operate the grayscale images of themselves first, and then the same operation is used to each channel of RGB separately for color images. There are six aspects to estimate the proposed scheme: the novel ROI selection performance, the watermark visibility analysis with tuning parameters $\alpha$ and $\beta$, the reversible watermarked images quality estimation by the metrics of PSNR and SSIM [23], watermark robustness, original image recovery and watermark extraction with the security discussion, and last, the performance on color images.

As shown in Figures 6 and 7, the binary watermarks [24], deer and horse, and the cover images, wood rabbit, tabby, and partridge, are used in the experiments. A detailed description of the cover images and the watermarks is given in Table 1. And, the watermark can be resized for embedding according to the size of cover images $H \times W$ and the ratio $r$ using (3). Besides, the nonoverlapping block size $l \times l$ is $3 \times 3$.

Step 4. Recover the original image and extract the binary watermark losslessly with the recovery information $D$ and watermark embedding key.

Using the embedding coordinate $(x_w, y_w)$ and the watermark size $h \times w$, we can restore the watermark embedding region in the watermarked image $I_w$. Given the pixel $p_{i,j}$ at $(i, j)$ in watermarked image $I_w$, the optimal embedding positions $\theta_k$, and the corresponding original bit values $b_{i,j}(\theta_k)$, we can recover the original image and extract the binary watermark using (15) and (16) which denotes $I_R$ and $W_E$, respectively.

4.1. **ROI Selection Performance.** As discussed in Section 3.1, the ROI for visible watermark embedding should cover the image subject to the greatest extent. With the novel ROI selection strategy based on Grad-CAM, the watermark embedding information can be obtained. Table 2 shows the ROI information including the watermark size $h \times w$ and embedding coordinate $(x_w, y_w)$ under different proportion $r$ with the method proposed by Qi et al. [9] and ours. To intuitively perform our selected ROI which is the subject of the image, Figure 8 shows the watermarked images with different proportion values; besides, the parameters $\alpha = 1$ and $\beta = 1$ here. From Figure 8, we can see that the watermark can be embedded into the main body of the images whatever the size is. Figure 9 shows the ROI selection with different methods. For Qi et al. [9], the ROI is the region which not contains abundant main information of images that can be easily cropped and tampered for malicious use so that the effect of watermark for protecting the copyright is degraded. On the contrary, the ROI for watermarking by ours approximates that the image subject can protect the main body information and copyright better.

4.2. **Parameters of Watermark Visibility Analysis.** The parameters $\alpha$ and $\beta$ in (13) can adjust the watermark visibility and the watermarked image quality. From the definition of (13), the parameter $\beta \in [0, 1.0]$, and in our scheme, we set $\alpha \in [0.5, 1.0]$. To understand the tuning parameters how to affect watermark visibility and marked image quality, we make the line chart of $\alpha \in [0.5, 1.0]$ and $\beta \in [0, 0.5]$ with step 0.1 each, shown in Figure 10. According to Figure 10, the PSNR values of the reversible watermarked image $I''_w$ are getting lower and lower with the increase in tuning parameters $\alpha$ and $\beta$. The tuning parameters can control the bit
Figure 6: Watermark images used in the experiments: (a) deer and (b) horse.

Figure 7: Cover images used in the experiments: (a1) wood rabbit, (a2) tabby, (a3) partridge, (b1) grayscale wood rabbit, (b2) grayscale tabby, and (b3) grayscale partridge.

Table 1: Description of test images in detail.

<table>
<thead>
<tr>
<th>Image</th>
<th>Type</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wood rabbit</td>
<td>Color</td>
<td>675 × 477</td>
</tr>
<tr>
<td>Tabby</td>
<td>Color</td>
<td>500 × 357</td>
</tr>
<tr>
<td>Partridge</td>
<td>Color</td>
<td>750 × 500</td>
</tr>
<tr>
<td>Deer</td>
<td>Binary</td>
<td>693 × 703</td>
</tr>
<tr>
<td>Horse</td>
<td>Binary</td>
<td>315 × 266</td>
</tr>
</tbody>
</table>

Table 2: Watermark embedding information for cover images.

<table>
<thead>
<tr>
<th>Cover image</th>
<th>Proportion $r$</th>
<th>Watermark size</th>
<th>Coordinate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Proposed</td>
</tr>
<tr>
<td>Wood rabbit</td>
<td>2</td>
<td>240 × 240</td>
<td>(70,191)</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>162 × 162</td>
<td>(109,230)</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>120 × 120</td>
<td>(130,251)</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>180 × 180</td>
<td>(91,222)</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>120 × 120</td>
<td>(121,252)</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>90 × 90</td>
<td>(136,267)</td>
</tr>
<tr>
<td>Tabby</td>
<td>2</td>
<td>252 × 252</td>
<td>(90,272)</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>168 × 168</td>
<td>(132,314)</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>126 × 126</td>
<td>(153,335)</td>
</tr>
</tbody>
</table>
Figure 8: Embedding the watermark deer into ROI of cover image wood rabbit with different proportion $r$: (a) original cover image, (b) $(r) = 2$, (c) $(r) = 3$, and (d) $(r) = 4$.

Figure 9: ROI selection with different strategies: (a1), (a2), and (a3) Qi et al. [9] with $(r) = 2, 3,$ and $4$, respectively; (b1), (b2), and (b3) proposed strategy with $(r) = 2, 3,$ and $4$, respectively.

Figure 10: PSNR values of reversible watermarked image wood rabbit with watermark deer embedded with different tuning parameter combinations: (a) PSNR values versus $\alpha$ and (b) PSNR values versus $\beta$. 
position selection, with the larger $a$ and $\beta$, the higher position is selected, and result in the increase in watermark visibility, and the decrease in watermarked image quality. Also, these two factors for tuning, parameter $\alpha$ is coarse, while parameter $a$ is precise. With the change of $a$ and $\beta$, we can adjust the watermark visibility and the watermarked image quality to obtain the tradeoff between these two factors. Figure 11 shows some reversible watermarked image with all $a = 1$ and different values of $\beta$.

4.3. Reversible Watermarked Image Quality. In Section 4.2, we have discussed the effect of parameters $a$ and $\beta$ on watermark visibility. From reversible watermarked images with different combinations of parameters $a$ and $\beta$, we choose the one $a = 0.6$ and $\beta = 0.5$ as the representative of our proposed scheme in the experiments. Figure 12 shows the reversible watermarked image with $a = 0.6$ and $\beta = 0.5$ comparing to other schemes by Hu and Jeon [5], Chen et al. [7], and Mohammad et al. [8]. The watermark visibility among all the images in the scheme proposed by Hu and Jeon [5] is the most obvious by modifying one significant bit plane of the pixels. However, the distortion of the watermarked image is too much, and the details of the cover image are almost covered by the watermark. The result of Mohammad et al. [8] does not show the watermark background, but it still has a lot of distortion. Noticed that, the reversible watermarked images of our scheme have the same level as Chen et al. [7] on watermark visibility in general. However, for reversible watermarked image quality, the detail of Chen et al. [7] performs worse than ours, especially when the region of watermark embedding is rough instead of smooth, which can be seen in Figure 13, zooming in the region of watermark embedding. Also, to objectively assess the reversible watermarked image quality, the values of PSNR and SSIM are shown in Tables 3 and 4. Overall, almost all the values of these two metrics of our proposed scheme are higher than others. For cover image wood rabbit, the values of PSNR are much larger than those of others, e.g., when $r = 2$, with watermark horse embedded, the value of PSNR is 18.5095 dB, 24.3761 dB, 21.919 dB, and 25.3271 dB corresponding to the schemes proposed by Hu and Jeon [5], Chen et al. [7], Mohammad et al. [8], and ours. And, the larger $r$ is, the higher difference of PSNR and SSIM is. For cover image tabby with the watermark horse embedded, though the value of PSNR of our scheme, 23.9950 dB, is not so much higher than that of Chen et al. [7], 23.9406 dB, the value of SSIM is much larger than that of Chen et al. [7] and Mohammad et al. [8], where ours is 0.9402 while Chen et al. [7] is 0.8702 and Mohammad et al. [8] is 0.8787. For cover image partridge, though the PSNR value is less than the value of Chen et al. [7] when $r = 2$, the SSIM value is much higher. And, with the smaller $r$, the PSNR and SSIM values are both higher than others.

Also, more images with their grayscale are tested in this experiment, showing in Figure 14. The 100 cover images are randomly selected from the dataset ImageNet with different categories, like lion, goldfinch, and cicada, and the watermark is deer. From Figure 14, most images’ PSNR and SSIM values are higher than other schemes, especially the SSIM. And, for the averages of PSNR and SSIM, the proposed scheme is 26.9895 dB, Hu and Jeon [5] is 18.3870 dB, 24.4509 dB is from Chen et al. [7], and Mohammad et al. [8] is 21.6282 dB. Besides, 0.9520, 0.8232, 0.8746, and 0.8771 are the SSIM averages, respectively. The results demonstrate the stability of our proposed scheme.

Therefore, from Figures 12–14 and Tables 3 and 4, we can conclude that our proposed scheme performs more excellent than other schemes in most cases on watermark visibility and watermarked image quality.

4.4. Watermark Robustness. The reversible visible watermark is a sign of the copyright. Watermark robustness is an important property for the reversible visible watermark. In order to test the watermark robustness, some common attacks are used in the experiment, like histogram equalization, mean filtering, Laplacian sharpening, noise addition, and JPEG compression. The results are shown in Figure 15 by taking the cover image wood rabbit embedded horse as an example. From Figure 15, the visible watermark can be recognized clearly and the watermark can survive suffered after attacks. So, we can conclude that the proposed visible watermarking algorithm is robust against common signal processing attacks.

4.5. Image Recovery and Watermark Extraction with Security Discussion. The original image recovery and the watermark extraction can be achieved losslessly and perfectly in our proposed scheme with the RDH algorithm proposed by Ou et al. [18]. Three groups of image recovery and watermark extraction are shown in Figure 16; besides, the recovered images and extracted watermarks are the same as the original cover images and watermarks.

In our proposed scheme, security including watermark embedding security and recovery information security is taken into account. During the process of watermark embedding, the pseudorandom number of $[0, 1]$ generated by the logistic mapping is utilized. Without the embedding secret key, even though the selected bit positions $\Theta$ are right, you cannot figure it out that the changed position $\theta_k$ is the current bit plane or the next. Moreover, the encrypted encoded recovery information cannot be decrypted correctly without the right encryption key. Hence, $\Theta$, $B$, and other information cannot be correct, not mention recovering the image and extracting the watermark. In this experiment, the secret key including $x_0$ and $\lambda$ are uniform in these two security protections, but the generated pseudo-sequences are different because of their different length, which is $l \times l$ and the other depending on the length of encoded information. Figure 17 shows the results of the recovered image and extracted watermark with the correct and wrong secret key, respectively.

4.6. Performance on Color Images. The watermark can be embedded into each channel of RGB to obtain the color reversible watermarked image. As mentioned before, to
simply describe the algorithm, the grayscale images are used in the experiments above. In this subsection, the color reversible watermarked images performance will be discussed. And, the adopted measurement PSNRc [10] will be used to assess the color reversible watermarked image quality which is defined as

$$\text{PSNRc} = 10 \log_{10} \left( \frac{255^2}{MSE} \right),$$

$$MSE = \frac{1}{3 \cdot H \cdot W} \sum_{k=1}^{3} \sum_{i=1}^{H} \sum_{j=1}^{W} (p_{i,j,k} - \bar{p}_{i,j,k})^2,$$

where $p_{i,j,k}$ is the pixel value at $(i, j)$ in the $k$-th color channel of the original cover image and $\bar{p}_{i,j,k}$ is the corresponding reversible watermarked pixel value. Figure 18 shows the results of different reversible visible watermarking schemes. And, for reversible watermarked image wood rabbit embedded with the watermark deer, the PSNRc values of Hu and Jeon [5], Chen et al. [7], Mohammad et al. [8] and our proposed scheme are 18.4826 dB, 24.3150 dB, 21.9525 dB, and 26.2173 dB. For tabby with deer, the PSNRc values are 19.0718 dB, 23.9677 dB, 21.5469 dB, and 25.2189 dB. Among all these PSNRc values for these two cover images, the scheme proposed by ours is the largest. Although for image partridge with deer, the PSNRc of Chen et al. [7] which is

![Figure 11: Reversible watermarked image wood rabbit embedded watermark deer with different parameter $\alpha$ and $\beta$, all $\alpha = 1$: (a) original cover image, (b) $\beta = 0.3$ (PSNR = 34.6251 dB), (c) $\beta = 0.5$ (PSNR = 25.6902 dB), and (d) $\beta = 1.0$ (PSNR = 24.0495 dB).](image1)

![Figure 12: Reversible watermarked images with watermark horse embedded using different reversible visible watermarking schemes: (a1) Hu and Jeon [5]; (b1) and (b3) Chen et al. [7]; (c1), (c2), and (c3) Mohammad et al. [8]; (d1), (d2), and (d3) proposed scheme with $\alpha = 0.6$ and $\beta = 0.5$.](image2)
Figure 13: Zoom in the reversible watermarked image tabby with watermark horse embedded using different reversible visible watermarking schemes: (a) Hu and Jeon [5], (b) Chen et al. [7], (c) Mohammad et al. [8], and (d) proposed scheme with $\alpha=0.6$ and $\beta=0.5$.

Table 3: PSNR and SSIM values of reversible watermarked images with watermark deer and $\alpha=0.6$ and $\beta=0.5$

<table>
<thead>
<tr>
<th>Cover image</th>
<th>Proportion</th>
<th>PSNR</th>
<th></th>
<th>SSIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wood rabbit</td>
<td>2</td>
<td>18.4266</td>
<td>24.3363</td>
<td>22.1769</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>21.7123</td>
<td>26.9410</td>
<td>25.0400</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>24.3560</td>
<td>29.1749</td>
<td>27.0238</td>
</tr>
<tr>
<td>Tabby</td>
<td>2</td>
<td>18.9791</td>
<td>24.0190</td>
<td>21.8911</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>22.4079</td>
<td>27.7339</td>
<td>25.1256</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>25.0841</td>
<td>30.3175</td>
<td>26.9989</td>
</tr>
<tr>
<td>Partridge</td>
<td>2</td>
<td>19.3492</td>
<td><strong>25.3639</strong></td>
<td>23.0163</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>22.5405</td>
<td>27.4809</td>
<td>26.3797</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>24.8129</td>
<td>29.1759</td>
<td>28.6298</td>
</tr>
</tbody>
</table>

Table 4: PSNR and SSIM values of reversible watermarked images with watermark horse and $\alpha=0.6$ and $\beta=0.5$

<table>
<thead>
<tr>
<th>Cover image</th>
<th>Proportion</th>
<th>PSNR</th>
<th></th>
<th>SSIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wood rabbit</td>
<td>2</td>
<td>18.5095</td>
<td>24.3761</td>
<td>21.9190</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>21.8731</td>
<td>26.7856</td>
<td>24.9474</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>24.4574</td>
<td>29.2036</td>
<td>26.8982</td>
</tr>
<tr>
<td>Tabby</td>
<td>2</td>
<td>19.1799</td>
<td>23.9406</td>
<td>21.5767</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>22.5918</td>
<td>27.5535</td>
<td>24.6448</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>24.9722</td>
<td>30.0688</td>
<td>26.8721</td>
</tr>
<tr>
<td>Partridge</td>
<td>2</td>
<td>19.4780</td>
<td><strong>25.3601</strong></td>
<td>22.8416</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>22.6364</td>
<td>27.4272</td>
<td>26.0996</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>24.9065</td>
<td>29.1831</td>
<td>28.4580</td>
</tr>
</tbody>
</table>
Figure 14: PSNR and SSIM values within 100 randomly grayscale cover images and watermark deer using different reversible visible watermark schemes.

Figure 15: Watermark robustness against common attacks: (a) without attacks, (b) histogram equalization, (c) 3×3 mean filtering, (d) Laplacian sharpening, (e) Gaussian noise addition, and (f) JPEG compression with QF = 50.
25.2949 dB is larger than ours, 25.0240 dB, and the difference is only 0.2709 dB. According to the analysis of the grayscale image in Section 4.3, the color reversible watermarked image quality performing best can be explained using the following equations:

\[
D_{\text{min}} = \left\{ \sum_{i} \sum_{j} \left[ R' (i, j) - R(i, j) \right]^2 + \left[ G' (i, j) - G(i, j) \right]^2 + \left[ B' (i, j) - B(i, j) \right]^2 \right\}_{\text{min}},
\]

\[
C_{\text{min}} = \left\{ \sum_{i} \sum_{j} \left[ C' (i, j) - C(i, j) \right]^2 \right\}_{\text{min}},
\]

\[(18) \quad (19)\]
where $C(i, j)$ is the original pixel value at $(i, j), C'(i, j)$ is the corresponding changed pixel in a channel, and $C$ means the channel of RGB. In other words, the minimum distortion of color images, which means the shortest Euclidean distance in RGB space, is equivalent to the shortest distance or the least distortion in each channel. Hence, we can obtain the least distorted reversible watermarked color images by processing each RGB channel as the grayscale separately.

 Noticed that, in Figure 18 (b1), for the result of Chen et al. [7], the embedded watermark is kind of ‘purple’, which leads to great color distortion. To make the watermark visible, the scheme proposed by Chen et al. [7] sets a threshold for watermark embedding, which causes the lighter grayscale image to have the shadow watermark embedded while the darker grayscale image has the brighter one. And in the experiment, the channel G of the color image has the shadow watermark embedded while R and B channels are contrary, shown in Figure 19. For tabby and partridge embedded watermark deer, all channels have the bright watermarks, but as discussed in subsection C, the details of each watermarked image channel perform are not good enough, resulting in poor performance of the final color image details, shown in Figures 18 (b2) and (b3).

5. Conclusions and Future Work

To embed the watermark into the subject in cover images for protecting the copyright better, the novel ROI selection strategy based on Grad-CAM is proposed in this paper. To obtain the tradeoff between the watermark visibility and the
reversible watermarked image quality, the JND model is utilized for watermark embedding to select the optimal bit positions of the image pixel. And, the efficient RDH algorithm is used in this paper for reversibility, with the extracted recovery information, the original cover image can be recovered losslessly, and the embedded watermark can be extracted perfectly. According to the watermark visibility and the reversible watermarked image quality with less distortion, the proposed scheme performs much more excellent compared with other reversible visible watermarking schemes.

In the proposed scheme, the visible watermark can survive against common attacks. However, image recovery and watermark extraction cannot be achieved reversibly. In the future, enhancing the watermark robustness for reversibility and designing a general metric of watermark visibility to choose the most suitable tuning parameters deserve further investigation.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Science Foundation Project of P. R. China (52071349 and 61701554), Cross-Discipline Research Project of Minzu University of China (2020MDJ08), State Language Commission Key Project (ZD1135-39), and Promotion Plan for Young Teachers’ Scientific Research Ability of Minzu University of China, MUC 111 Project, First Class Courses (Digital Image Processing KC2066).

References

