Region of Interest Fragile Watermarking for Image Authentication

Yiping Chu, Yin Zhang, Sanyuan Zhang and Xiuzi Ye
College of Computer Science, State Key Lab of CAD&CG, Zhejiang University, 310027 Hangzhou, PR China
hzcyp@yahoo.com.cn

Abstract

Digital watermarking plays an important role in image verification and copyright protection. A watermarking scheme for authenticating ROI (region of interest) of image has been proposed in the paper. To embed the watermark in the interior of ROI, Poisson matting technique is introduced to extract the region of interest of image. The color foreground obtained by Poisson matting is converted to the binary image as reference mask. According to principles of wavelet, we construct watermark embedding function and accurately embed watermark in the interior of ROI. Exploiting watermark extraction function, we extract the watermark from watermarked image. Differentiating the values between embedding watermark and extracted watermark can detect whether ROI of image was tampered, and where was tampered. Experiment results have demonstrated that the presented watermarking scheme can detect tamper in the interior of ROI for image authentication.

1. Introduction

Digital watermarking [1] plays an important role in image verification and copyright protection. Many different watermarking schemes have already been proposed that can be divided in two general categories: those, which are robust watermarking [2], are robust for image processing operations and malicious attacks, and the others, are fragile watermarking schemes [3,4,5,6,7,8], which are very fragile to image tamper. For having a better understanding of what has already been proposed, we can also review more extensive surveys published [9, 10].

The watermarking schemes as mentioned above have not reported to be able to watermark for local image authentication and copyright protection. In some applications, we may need local watermarking scheme, such as copyright owner may permit unimportant region of the image tampered by others. In this paper, we present a new scheme for embedding watermark, which allows copyright owner to select a region of image, called region of interest (ROI), to embed watermark. Editing in the exterior of the ROI of watermarked image will not give rise to watermarking alarm.

We organize the rest of this paper as follows: in next section we will review the previous work of fragile watermarking scheme and approaches to extract foreground for images. In section 3, we use Poisson matting and binary image morphology filtering to produce the binary reference mask image for watermark embedding and watermark extraction function. Our watermarking schemes, including watermark embedding scheme, watermark extraction and tamper detection scheme, will be given then. Section 4 discusses how to choose parameters and shows the experiment results. We attack the watermarked images by tamper in the interior of the ROI and tamper in the exterior of the ROI respectively. JPEG compression tolerance of the scheme is also tested in our experiment. Finally in section 5, we give our conclusion.

2. Related work

2.1. Fragile watermarking Schemes

Fragile watermarking schemes have been proposed to authenticate the integrity of images. Techniques that embed hidden information in the spatial domain are more straightforward than the ones using transforms method [7, 11]. However, the schemes using transform domain offer a higher degree of robustness [12]. Nowadays, Many Fragile watermarking schemes are based wavelet transform since it allows the highest degree of robustness to simple image processing operations [13].

Kundur et al. [14] present a fragile watermarking technique which embeds a watermark in the discrete wavelet domain by quantizing the corresponding
coefficients. Their approach allows tamper detection in localized spatial and frequency regions, therefore, making possible the identification of specific modified frequencies in an image. They define a Tampering Assessment Function as a measurement for tamper proofing.

In [11], the authors propose a novel technique for content authentication of digital images by the use of wavelet packets. It is able to detect and localize malicious image alterations while offering a certain degree of robustness to image compression. These semi-fragile watermarking system also adopts the human visual system for enhance invisibility of watermarked image.

Wu et al. [15] present a secure semi-fragile watermarking for image authentication, which is based on integer wavelet transform, they also use the technique presented by Liu et al. [2] to embed the watermark in the spatial domain of the original image. Ding et al. [3] propose a semi-fragile watermarking scheme, which is a wavelet-based chaotic semi-fragile watermarking scheme with more JPEG compression tolerance.

2.2. Foreground extraction

The GVF snake [16, 17] was used to retrieve the contour of foreground because it has two significant advantages over the traditional snake formulation. First, the GVF snake can fit into concavities, and second, the GVF snake can fit itself to objects exploiting both expansion and contraction of the snake. But GVF snake fails to retrieve the contour of foreground when background of image is very complex.

Sun et al. [18] present a matting approach to obtain foreground from complex background by solving Poisson PDE equations. Boundary condition is important for Poisson matting to extract foreground, user need carefully specify the exterior boundary and the interior boundary, which are related to background and foreground, respectively.

In [19], authors present the system GrabCut to extract foreground for images, which is an iterative image segmentation technique based upon the Graph Cut algorithm [20]. Compared with Poisson matting, selection of foreground for GrabCut is simple. While background is complex, Poisson matting and GrabCut have their respective advantages over each other. In the paper, we adopt Poisson matting to extract foreground.

3. Proposed scheme

Fig.1 shows the diagram of watermark embedding scheme and diagram of watermark extraction and tamper detection scheme, which denote embedding watermark in the interior of ROI and detecting malicious temper inside ROI, respectively. We adopt technique of Poisson matting [18] to obtain ROI as foreground of original image, and then generate the binary reference mask image. The approach that produces the binary reference mask image will be described in following subsection.

To get diagonal detail coefficient $LL_k$ of original image, we make use of 2D discrete wavelet decomposition. Since the $LL_k$ sub-band is the coarse resolution image corresponding to original image with its $1/4^k$ size [21], we obtain the binary reference mask image with respect to $LL_k$ by resizing it with $1/4^k$ times the size of original image. We use $K$ as random seed to yield binary pseudo random sequence $W$, and embed $W$ in sub-band $LL_k$ of original image according the binary reference mask image.
between two watermarks illustrates the location of tamper in watermarked image.

3.1. Reference mask generation

To determine whether the color pixels belong to interior of ROI of image, we generate a binary reference mask image corresponding to original image. Binary reference mask is a binary image the same size as original image with 1's outside the ROI and 0's inside.

In order to produce the binary reference mask image, copyright owner adopt Poisson matting \[18\] to obtain the image $RIM$ which consists of the ROI of original image as foreground and blue color (or other colors) background. By interactive means, copyright owner can extract suitable ROI image $RIM$ just as Fig.2 (a). Generating binary image $BI$ from $RIM$ is relatively simple. Create a binary image with 0's for all pixels, and set 1's to pixels when corresponding pixels in $RIM$ are blue color. Fig.2 (b) is the binary image $BI$ constructed from the ROI image $RIM$. Some noises blobs with small size inside ROI in Fig.2 (b) are removed after the morphology filtering. Therefore binary reference mask image $BI'$ is yielded.

![Fig. 2. Reference mask image generation for Lena (a) ROI image obtain by using passion matting; (b) Binary image converted from (a); (c) Morphology filtering result of (b).](image)

To obtain another binary reference mask image $BM$, which indicates the location of ROI in $LL_k$ of wavelet domain, we resize the binary reference mask image $BI'$ with $1/4^k$ times the size of original image. $BM$ is a binary image the same size as $LL_k$ of original image with 1's outside the ROI of $LL_k$ and 0's inside.

3.2. Watermark embedding

To ensure that only ROI of image is embedded by watermark, we adopt the method described above to produce the binary reference mask image $BM$. After obtain $BM$, We choose parameter $K$ as random seed to generate pseudo-random sequence $W$ over GF(2) with the same size as $LL_k$.

We get watermark $W'$ by using logical operate between $W$ and $BM$, such as, let $W'(i,j) \leftarrow 0$, if $BM(i,j) =1$; else let $W'(i,j) \leftarrow W(i,j)$. We adopt 2D discrete wavelet to decompose the original image, and embed $W'$ in the coefficients of $LL_k$ by using watermark embedding function. Finally, watermarked image is yielded by wavelet synthesis. Our watermark embedding function is similar to one presented by Kundur et al. \[14\]. Firstly, we define a quantization function for our watermark embedding function. Quantization function $Q_\delta$ is given by.

$$Q_\delta = \begin{cases} 0 & \text{if } \frac{f}{\delta^2 h} \text{ is even} \\ 1 & \text{if } \frac{f}{\delta^2 h} \text{ is odd} \end{cases}$$

where $\delta \in \mathbb{Z}^+$ is the quantization magnitude, and $[\cdot]$ is floor function. Our watermark embedding function is defined as follows:

$$f(y,w) = \begin{cases} g(x) & \text{if } Q_\delta(y) \neq w \\ y & \text{if } Q_\delta(y) = w \end{cases}$$

(1)

where

$$g(x) = \begin{cases} x - \delta 2^h & \text{if } x > 0 \\ x + \delta 2^h & \text{if } x \leq 0 \end{cases}$$

$x \in R, \delta \in \mathbb{Z}^+, h \in \mathbb{Z}^+$

Watermark embedding procedure:

**Step1:** Obtain diagonal detail coefficient $LL_k$ by $k$ th-level 2D discrete wavelet decomposition on the original image, choose parameters $K$, where $K$ is random seed to generate binary pseudo random sequence $W$;

**Step2:** Copyright owner select the ROI of original image and adopt Poisson matting to extract foreground, then generate binary reference mask image $BI'$;

**Step3:** Compute $BM$ according to $BI'$, generate binary watermark $W'$ by using following method: if $BM(i,j) =1$, then $W'(i,j) \leftarrow 0$; else $W'(i,j) \leftarrow W(i,j)$;

**Step4:** Exploit watermark embedding function $f(y,w)$ to generate watermarking:
for $\forall l(i, j) \in LL_k$ , compute $l(i, j) \leftarrow g(l(i, j), W'(i, j))$;

Step5: Use Inverse discrete wavelet transform on the marked wavelet coefficient $LL_k$ and other wavelet coefficients to produce the watermarked image.

After watermark embedding, copyright owner need preserve $BM$ and $K$ for watermark detection.

### 3.3. Watermark detection

Before watermark detection, copyright owner use binary reference mask image $BM$ that was preserve in the step of watermark embedding and the same parameter $K$ as random seed to retrieve binary image watermark $W'$. On the other hand, we can extract another watermark $W''$ by wavelet decomposition of watermarked image, and calculated by following formula

$$W'_r(i, j) = Q_\delta(l(i, j)) \quad l(i, j) \in LL_k \quad (2)$$

Because $W'_r$ include the watermark information in exterior of ROI, so we need eliminate it by following process: for $\forall W'_r(i, j)$, if $BM(i, j) = 1$, then $W'(i, j) \leftarrow 0$; else $W'(i, j) \leftarrow W'_r(i, j)$. In this way, we get two watermarks $W'$ and $W''$, we define the tamper detection matrix

$$T = |W' - W''| \quad (3)$$

If $W' = W''$, then $T = 0$, it means that there's no tamper inside ROI of watermarked image. Otherwise, the $1$'s in the tamper detection matrix denote the pixels that were tampered. Notes that tamper detection matrix is the same size as the $LL_k$, which is about $1/4^k$ of the original image. Thus one element denotes a corresponding $4^{k-1} \times 4^{k-1}$ block in the ROI of original image.

Tamper detection procedure:

Step1: Use $K$ as random seed to generate binary watermark $W'$;

Step2: Use $BM$ and generate binary watermark $W'$ by following method: if $BM(i, j) = 1$, then $W'(i, j) \leftarrow 0$; else $W'(i, j) \leftarrow W(i, j)$;

Step3: Use wavelet decomposition of watermarked image, and then calculate extracted watermark

$W'_r(i, j)$ by the formula

$$W'_r(i, j) = Q_\delta(l(i, j)) \quad l(i, j) \in LL_k$$

Step4: Calculate $W''$ by using following method: if $BM(i, j) = 1$, then $W''(i, j) \leftarrow 0$; else $W''(i, j) \leftarrow W'_r(i, j)$;

Step5: If $W' = W''$, then the tamper detection matrix $T = 0$, which means no tamper in ROI of watermarked image. Otherwise, the $1$'s in the tamper detection matrix denote the pixels that were tampered.

### 4. Experiments and results

256×256 images Lena and Airplane are adopted to check the validity of our scheme. The binary watermark is pseudo random sequence generated by pseudo random generator. To generate high quality pseudo random number, we considered a generator implemented by means of an LFSR (Linear Feedback Shift Register) in our experiments. For such a generator characterized by $K$ degree primitive polynomial over GF(2) [22].
image, we introduce the normalized cross-correlation [3]

\[ NC = \frac{\sum \sum \tilde{W}(i,j) \cdot \tilde{W}'(i,j)}{\sum \sum |\tilde{W}'(i,j)|^2} \]

where \( \tilde{W}' \subseteq W' \) and \( \tilde{W}'' \subseteq W'' \) are corresponding to the values of in interior of the ROI. The PSNR and NC of watermarked image are influence each other while \( h \) varying. In our experiments, we found that \( h = 4 \) provide a good trade-off between invisibility and accuracy.

Let parameters \( k = 2, h = 4, \delta = 1, K = 21 \), in our experiments. Fig.3 (a) and (b) are original image and watermarked image respectively. It explains that our watermarking scheme has good invisibility for watermarked image when suitable parameters are specified.

### TABLE I

<table>
<thead>
<tr>
<th>ROBUSTNESS AGAINST JPEG COMPRESSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena(NC)</td>
</tr>
<tr>
<td>0.95 0.92 0.87 0.79 0.67 0.59</td>
</tr>
<tr>
<td>Airplane(NC)</td>
</tr>
<tr>
<td>0.94 0.87 0.83 0.77 0.68 0.61</td>
</tr>
<tr>
<td>JPEG Compression</td>
</tr>
<tr>
<td>92% 83% 75% 67% 58% 50%</td>
</tr>
</tbody>
</table>

We attack image by tamper in interior of ROI and in exterior of ROI for checking the validity of our scheme. In our experiment, the figure of Lena is ROI designated by us. In Fig.4 (a), the interior of ROI of watermarked image is tampered. A flower is added to the cap of Lena, and some words is added onto the airplane. As a result, the embedding watermark \( \tilde{W}' \) is different to the extracted watermark \( \tilde{W}'' \) from watermarked image. By computing its tamper detection matrix \( T \), the tamper locations in ROI of watermarked image are revealed in Fig. 4 (d).

Figure 4. (a) Tamper inside ROI; (b) Embedding watermark \( W' \); (c) Extracted watermark \( W'' \); (d) Tamper location inside ROI revealed by \( T \)

In Fig.5 (a), watermarked image was tampered in the exterior of ROI, which is permitted by the copyright owner. A frame is added to outside figure of Lena, also some words is added to outside airplane. In this case, the embedding watermark \( \tilde{W}' \) and the extracted watermark \( \tilde{W}'' \) are the same. Fig.5 (d) shows the image of \( T = 0 \) that means ROI was not tampered. It will not give rise to watermarking alarm.

Figure 5. (a) Tamper in the exterior of ROI; (b) Embedding watermark \( W' \); (c) Extracted watermark \( W'' \); (d) \( T = 0 \), no alarm occurred.
5. Conclusion

A secure watermarking for ROI of image authentication based on foreground extraction has been presented. To make sure that embedding watermark in the interior of ROI, we produce a binary reference mask image according to extracted foreground for ROI of image. Our watermarking embedding function and watermarking extraction function perform well for only authenticating ROI of image. Experiment results have demonstrated that the proposed scheme is capable of detecting tamper in the interior of ROI and tolerating tamper exterior of ROI.

Acknowledgment

The authors would like to thank the support from the China NSF under Grant #60473106, #60273060 and #60333010, China Ministry of Education under Grant#20030335064, Education Office of Zhejiang Province under Grant #G20030433.

References