A copyright protection watermarking algorithm for remote sensing image based on binary image watermark

Peng Zhu a,*, Fei Jia b, Junliang Zhang c

a Department of Information Management, School of Economics and Management, Nanjing University of Science and Technology, Nanjing 210094, China
b Division of Education Affairs, Nanjing Forest Police College, Nanjing 210046, China
c School of Management, Xinxiang Medical University, Xinxiang 453003, China

A R T I C L E   I N F O

Article history:
Received 22 July 2012
Accepted 12 December 2012

Keywords:
Digital watermarking
Copyright protection
Binary image
Remote sensing images

A B S T R A C T

As the internet keeping developing, copyright protection of the remote sensing image has become more and more important. This paper designs the algorithm that protects remote sensing image’s copyright by using the binary digital watermark technology, and analyzes security and imperceptibility of the algorithm. As the experiment result shows, the algorithm put forward in this paper has better security, imperceptibility and anti-attack robustness, and thus it can meet the requirements in protecting copyright of the digital remote sensing image in an effective manner.

© 2013 Elsevier GmbH. All rights reserved.

1. Introduction

As the computer network technology rapidly develops, it becomes increasingly common to see public data transmission channel, public information publication platform, shared data and easily copying of digital data [1]. All of these factors have helped improve quality of information service, but these also cause the potential data insecurity at the same time [2]. The rapid development of aviation and aerospace technology promotes remote sensing images gradually become the main source of space-based information for civilian services [3]. The problem of copyright ownership for the digital remote sensing images and data integrity has become one of the key technology problems in providing reliable spatial information service [4]. In addition, the digital watermarking technology, as an effective technology for copyright protection, has been studies and applied in the fields such as image, audio and video [5]. As a result, the digital watermarking technology of the remote sensing images is a good solution which can solve copyright protection problem of the remote sensing images.

The rest of the paper is organized as follows. In Section 2, we present a brief survey on the watermarking methods recently introduced in the remote sensing image. Section 3 describes the proposed scheme. Experimental results are reported in Section 4 and conclusions are drawn in Section 5.

2. Related work

At present, quite a number of scholars have devoted to studying how to apply the digital watermarking technology into copyright protection of the digital remote sensing images.

Serra-Ruiz et al. [6] propose a semi-fragile forensic watermarking scheme for remote sensing image. They propose to embed a mark into remote-sensing image applying a tree-structured vector quantization approach to the pixel signatures, instead of processing each band separately. The signature of the multi or hyperspectral image is used to embed the mark into it in order to detect any significant modification of the original image. The image is segmented into three-dimensional blocks and a tree-structured vector quantizer is built for each block. These trees are manipulated using an iterative algorithm until the resulting block satisfies a required criterion which establishes the embedded mark. The method is shown to be able to preserve the mark under lossy compression, but it detects possibly forged blocks and their position in the whole image.

Ren et al. [7] propose a semi-blind watermarking algorithm for high-resolution remote sensing image. The algorithm firstly analyzes the characteristics of high-resolution remote sensing images, then proposes the key matrix to save the matching result whether the highest significant bit value of image pixel value equal with the watermark value or not. In the watermark extraction stage, a key matrix is used to extract the spread spectrum watermark.
After extracting the spread spectrum watermark information, the original watermark is employed as the template and in accordance with the template matching methodology is used to extract the region with the maximum correlation coefficient as the extracted watermark information.

Melgani et al. [8] propose to adapt a state-of-the-art spread spectrum method found to be particularly powerful for real-world images to make the watermark insertion process near-lossless while preserving most of its effective robustness capability. This is done by embedding the watermark in the middle-frequency range of the discrete cosine transform (DCT) domain instead of the low-frequency range. The exact position is determined by a numerical root-finding method, targeted to achieve a user-specified minimum level of robustness against a given ensemble of attacks. In this way, an optimal trade-off can be obtained between quality and robustness.

Kumari and Rallabandi [9] propose a modified patchwork-based watermarking (MPW) scheme in the spatial domain. The proposed MPW algorithm is capable of embedding a watermark with minimal manipulation of the original image pixel values. The watermark contains information about the provider and the intended recipient of the data. The MPW watermark embedding process does not create any visual artifacts and is imperceptible. The watermark retrieval process operates with the help of a key and does not require the original image.

Jing et al. [10] propose a robust zero-watermarking method that constructs watermarks from the host data instead of embedding watermark into that data. The proposed method constructs two watermarks from host image. One is constructed from low-frequency coefficients in discrete wavelet transform domain of the host image, and the other is constructed from that of the log-polar mapping image of the host image.

In fact, digital remote sensing images are mostly binary images consisting of two strong contrast colors [11], however, the digital watermarking algorithm in the above-mentioned studies consider the characteristics of the binary image less. In this regard, this paper presents a new digital watermarking algorithm based on the binary image technology to protect the copyright of remote sensing image. The basic procedure of this algorithm is to divide the digital remote sensing image into different blocks, and then to embed the watermark signal into the image by modifying parity of the white pixel in the image block. By doing so, the watermark signal can be extracted by using parity of the white pixel in the image block.

3. Proposed scheme

Digital watermarking technology mainly refers to embed the watermark information into digital images covertly, and the watermark information is to prove as copyright basis. The basics of digital watermarking can refer to reference [12]. Before the watermark information is embedded, it is required to perform the scrambling encryption operation to the watermark information first, with the purpose of enhancing security of the embedded watermark. In this paper, the improved Arnold transformation is used for the scrambling encryption.

3.1. Watermark embedding algorithm

The watermark embedding procedure is a procedure which embeds the digital watermark information into host image (this article refers to the remote sensing image) by using certain rules and methods. Before describing the watermark embedding procedure, we should define several variables first:

- I: means original host image, i.e. digital remote sensing image; its size is \( I_I \times I_w \);

![Fig. 1. Watermark embedding process.](image)

\( W \): means watermark information, i.e. copyright identification image or pseudo random code, it is the \( W_I \times W_w \) binary image in this paper;

- \( a, b, c, d, \text{ chaos}_n \): means parameters of image scrambling. In this paper, \( a, b, c, d \) means parameters of the improved Arnold transformation and \( \text{chaos}_n \) means the scrambling times;

- \( \text{clm} \): means the location transformation structure matrix which records the location transformation caused by improved Arnold transformation of the watermark image;

- \( K_1 \): means the key matrix to encrypt host image, it is a random binary matrix.

- \( K_2 \): means the key matrix to encrypt watermark image, it is a random (0,1) binary matrix;

After the definition, this paper designs the watermark embedding algorithm of the digital remote sensing image by using binary feature of the image, as shown in Fig. 1:

The watermark embedding procedure is described as below:

Step 1: Read the host image \( I \) (the digital remote sensing image) and the watermark image \( W \) (the copyright identification image) respectively.

Step 2: Enter \( a, b, c, d \) and \( \text{chaos}_n \) to scramble the watermark image \( W \), and save the location transformation structure matrix \( \text{clm} \).

Step 3: Divide \( I \) into non-overlapping image blocks with size of \( W_I \times W_w \), and then record it as \( I_{ij}(1 \leq i \leq I_I, 1 \leq j \leq I_w/W_w) \).

Step 4: Encrypt the image blocks \( I_{ij} \) via \( K_1 \):

\[
I_{ij} = I_{ij} \oplus K_1
\]  

Step 5: Encrypt the scrambled watermark \( W \) via \( K_2 \):

\[
W = W \oplus K_2
\]

Step 6: Calculate \( \text{sum}(I_{ij}) \) of \( I_{ij} \) (image block) and then apply the \( \text{sum}(I_{ij}) \) to do \( \text{sum}(I_{ij}) \mod 2 \) operator. If the \( W(i,j) \) is equal to the \( \text{sum}(I_{ij}) \), do not make any change; otherwise, select any pixel in \( I_{ij} \) and apply the formula to get the inverse value:

- Step 7: Decrypt \( I_{ij} \) via \( K_1 \);

- Step 8: Repeat steps 4 and 7 until all image blocks are embedded successfully.

3.2. Watermark extraction algorithm

The watermark extraction refers to the procedure that extracts the watermark in the digital remote sensing image to be checked, the watermark extraction algorithm is the reverse procedure of the watermark embedding algorithm. The embedded watermark information is an identity image, so the copyright of the remote sensing image can be determined visually through the watermark image is extracted. The paper designs the watermark extraction procedure by combining with the detection model as shown in Fig. 2.

The steps of the watermark extraction algorithm are described as below:
Step 1: Divide \( I' \) (the remote sensing image to be detected) into different blocks \( I'_{i,j} \) according to the sub-block method in step 3 of the watermark embedding process;

Step 2: Encrypt the image block \( I'_{i,j} \) via \( K_1 \):
\[
I'_{i,j} = I'_{i,j} \oplus K_1
\]  

Step 3: Calculate \( \text{sum}(I'_{i,j}) \) of \( I'_{i,j} \) and then apply the value of the \( \text{sum}(I'_{i,j}) \) to do \( \text{sum}(I'_{i,j}) \mod 2 \) operator and mark the value as \( W'(i,j) \);

Step 4: Repeat steps 2 and 3 until all information in the image blocks are extracted, then \( W' \) (the possible watermark information) is generated.

Step 5: Decrypt \( W' \) via \( K_2 \):
\[
W'' = W' \oplus K_2
\]  

Step 6: Perform the reverse scrambling to the decrypted \( W'' \) via the location transformation structure matrix (clm) and obtain the extraction watermark information \( W'' \).

Step 7: Compare the similarity between the extraction watermark information \( W'' \) and the original watermark image \( W \).

If the watermark can be extracted successfully and the similarity between \( W' \) and \( W \) is high, it means people obtain the remote sensing image’s copyright license; if it cannot, it means people do not. As a result, this method serves as an important reference for the remote sensing image’s copyright ownership.

### 3.3. Algorithm analysis

#### (1) Security analysis

Security in protecting the remote sensing image copyright is required to be high, so the security requirement on watermark embedding algorithm is also very high. The watermark embedding algorithm uses \( K_1 \) and \( K_2 \) to encrypt the remote sensing image for protection and the watermark image. If you want to extract the watermark correctly, you shall have to estimate values of \( K_1 \) and \( K_2 \). However, \( K_1 \) and \( K_2 \) are binary random matrices with size of \( W_l \times W_w \) and their values can be as many as \( 2^{W_l \times W_w} \). Besides that, the watermark image needs to be restored correctly, therefore \( a, b, c, d, \text{chaos} \_n \) should be estimated as an accurate value, or clm needs to be obtained. Because \( a, b, c, d \) belongs to the positive integer set that meet the requirement of “\( ad - bc = 1 \)”, it is more difficult to estimate the value. In addition, only copyright owner of the remote sensing image can provide clm.

#### (2) Imperceptibility analysis

Due to the fact that the remote sensing image of the copyright protection still needs to be used in a wide range, and the watermark image is embedded in the remote sensing image, so it is required to reduce the impact to the original image as much as possible during the watermark embedding process, or the location of modified pixel is a randomly distributed state when the watermark is embedded. By doing so, the imperceptibility of the watermark can be guaranteed and the quality of the remote sensing image should be good. The image block is \( W_l \times W_w \) in size; it is assumed that possibility of each image block \( (I_i,j) \) which needs to modify the pixel is \( P \times M \); then, the number of pixels \( (N) \) for which the whole image needs to be modified is:
\[
N = P \times \frac{I_l \times I_w}{W_l \times W_w}
\]

During the procedure when the watermark is embedded, the location of the modified pixels is randomly selected in the image block, so it is required that the location of the modified pixels should be in the randomly distributed state.

### 4. Experimental results

#### 4.1. Experiment design

To verify the validity of the algorithm, watermark security, imperceptibility and anti-attack robustness, we conducted several experiments such as water embedding and extraction, general signal processing and geometric attack. In the experiments, we let the remote sensing image (with size of \( 512 \times 512 \)) which needs to be protected by copyright as the host image (as shown in Fig. 5(a)) and
the binary image (with size of $32 \times 32$) as digital watermark image (as shown in Fig. 3(a)).

During the experiment, the key $K_1$, $K_2$ as the binary matrix that is generated via random function and same as the size of digital watermark image, and we adopt the PSNR value (the difference between the original image and the changed image) to show relationship of the similarity between the original watermark image and the scrambled watermark image, as well as the modification measurement to the embedded remote sensing image compared with the original remote sensing image (the host image).

In order to enhance the security and robustness of the proposed algorithm, we have done scrambling processing to the original watermark image. Fig. 3 shows the scrambling effect diagrams of the original watermark image (Fig. 3(a)) which has been undergone with Arnold transformation and improved Arnold transformation for a number of times. Among all figures, Fig. 3(b)–(d) are effect diagrams for which the scrambling is implemented for one, five and ten times respectively based on Arnold transformation; Fig. 3(d)–(f) are effect diagrams for which the scrambling is implemented for one, five and ten times respectively based on improved Arnold transformation in which the parameter settings are as follows: $a = 3, b = 2, c = 4$ and $d = 3$.

The PSNR value of the scrambled watermark image base on Arnold transformation and improved Arnold transformation are as shown in Fig. 4. As is shown in Fig. 4, the relativity between the scrambled image which has been undergone with Arnold transformation and the original watermark image is small, but the relativity between the scrambled image which has been undergone with improved Arnold transformation and the original one is smaller than the previous one. In this case, in order to enhance security of the embedded watermark, we should perform the improved Arnold transformation operation first before the watermark image is embedded.

4.2. Result analysis

Fig. 5 shows the effect diagram before and after the watermark is embedded in the remote sensing image. Fig. 5(a) is the original remote sensing image, Fig. 5(b) is the watermarked remote sensing image which the scrambled watermark Fig. 4(g) been undergone with improved Arnold transformation from original watermark Fig. 4(a) has been embedded in. Judging by the visual effect, we cannot see existence of the watermark and the discrimination of the two images, which means that the algorithm in this article has good imperceptibility.

Fig. 6 shows the extraction result of the experiment. If the watermarked remote sensing image suffers no alterations, the watermark extracted correctly as shown in Fig. 6(a) is exactly the same as the original one. However, if a wrong extract method is used, the extracted watermark as shown in Fig. 6(b) looks like random noise. This proves that security of the watermark content is guaranteed because of the randomness of $K_1$, $K_2$ and the difficulties in valuation the value of $a$, $b$, $c$, $d$, chaos and $clm$.

In the experiment, we also test the visual effects of the original host image by embedding different capacity of watermark through PSNR. Table 1 shows the diversification of PSNR when different capacity of watermark is embedded into the host image. As is shown in this table, different capacity of watermark can produce different effects to the host image: the more the capacity of embedded watermark is, the greater the effects brought to the host image. In this article, the capacity of watermark in the proposed algorithm is $32 \times 32$ which can meet the requirements on security and imperceptibility of copyright protection.

In order to test the robustness of the algorithm, we conduct an experiment to the watermarked remote sensing image Fig. 5(b) which includes extracting the watermark after JPEG compression which has the Q-factors of 90, 70, 50 and 30, respectively, extracting the watermark after median filtering and low-pass filter respectively, extracting the watermark after adding random noise and salt and pepper noise respectively, and extracting the watermark after shearing part of the watermarked image. Analysis results are shown in Table 2, both in terms of PSNR and NC [13].

<table>
<thead>
<tr>
<th>No.</th>
<th>Capacity of the watermark</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$16 \times 16$</td>
<td>99.2311</td>
</tr>
<tr>
<td>2</td>
<td>$32 \times 32$</td>
<td>83.1312</td>
</tr>
<tr>
<td>3</td>
<td>$64 \times 64$</td>
<td>69.7843</td>
</tr>
<tr>
<td>4</td>
<td>$128 \times 128$</td>
<td>55.6317</td>
</tr>
</tbody>
</table>
Table 2
Evaluation the robustness of watermark.

<table>
<thead>
<tr>
<th>No.</th>
<th>Attacks</th>
<th>NC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>JPEG compression (Q-factors: 90)</td>
<td>0.9658</td>
</tr>
<tr>
<td>2</td>
<td>JPEG compression (Q-factors: 70)</td>
<td>0.9636</td>
</tr>
<tr>
<td>3</td>
<td>JPEG compression (Q-factors: 50)</td>
<td>0.9307</td>
</tr>
<tr>
<td>4</td>
<td>JPEG compression (Q-factors: 30)</td>
<td>0.9169</td>
</tr>
<tr>
<td>5</td>
<td>Median filtering</td>
<td>0.8433</td>
</tr>
<tr>
<td>6</td>
<td>Low-pass filter</td>
<td>0.9798</td>
</tr>
<tr>
<td>7</td>
<td>Random noise</td>
<td>0.9579</td>
</tr>
<tr>
<td>8</td>
<td>Salt and Pepper noise</td>
<td>0.8847</td>
</tr>
<tr>
<td>9</td>
<td>Shearing part of the image (Upper left 1/4)</td>
<td>0.5637</td>
</tr>
<tr>
<td>10</td>
<td>Shearing part of the image (Middle 1/4)</td>
<td>0.3864</td>
</tr>
<tr>
<td>11</td>
<td>Rotation (Five degrees)</td>
<td>0.4521</td>
</tr>
<tr>
<td>12</td>
<td>Enlarge 1 times</td>
<td>0.5134</td>
</tr>
<tr>
<td>13</td>
<td>Shrink 1/2</td>
<td>0.4026</td>
</tr>
</tbody>
</table>

The experiment result shows the algorithm has good robustness in terms of JPEG compression, general filter operation and handling of the added noise, but it does not perform well in geometric attacks such as cutting.

5. Conclusions

This article based on the requirements of the copyright protection of digital remote sensing images, proposes a binary image based digital watermarking copyright protection algorithm, describes the watermark embedding and watermark extraction algorithm in detail, and analyzes security and imperceptibility of the algorithm. As the experiment result shows, the algorithm put forward in this paper has better security, imperceptibility and anti-attack robustness, and thus it can meet the requirements in protecting copyright of the digital remote sensing image in an effective manner. In future, we will further study this solution with practices, trying to fix the algorithm defects and improve the watermark embedding robustness. In this way, the binary image watermark technology can better protect copyright of the remote sensing image.

Acknowledgments

This research was supported by Ministry of Education of the People’s Republic of China, Humanities and Social Sciences project (No. 12YJC870036).

References