Journal of Computer and Communications, 2019, 7, 17-27
http://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

# Research on a Watermarking Algorithm for Remote Sensing Images Resist Screen Capture Attacks in Urban Planning Information Management

**Xiao Wang, Jiangang Xu, Yiming Yin**

School of Architecture and Urban Planning, Nanjing University, Nanjing, China
Email: 523445957@qq.com

**How to cite this paper:** Wang, X., Xu, J.G. and Yin, Y.M. (2019) Research on a Watermarking Algorithm for Remote Sensing Images Resist Screen Capture Attacks in Urban Planning Information Management. *Journal of Computer and Communications*, **7**, 17-27.
https://doi.org/10.4236/jcc.2019.77003

**Received:** April 18, 2019
**Accepted:** July 7, 2019
**Published:** July 10, 2019

## Abstract

Remote Sensing data, as an essential urban basic information in urban planning, has the characteristics of large information capacity, real time, high update speed and accuracy. Because of urban spatial information involving multi-faceted public and public interests, its data security is very important. The use of digital watermarking technology can effectively protect the security of urban planning basic data. In practical applications, the "screen capture" poses a great threat to the security of remote sensing image. In order to resist the screen capture attacks, the QR code watermark information is encoded and converted, and combined with a circular angle template watermark, a digital watermarking algorithm for remote sensing images in urban planning information management is proposed. And the proposed algorithm is experimentally verified. Experiments show that the algorithm is robust against screen capture attacks, and provide security guarantee for urban construction and management.

## Keywords

Remote Sensing Image, Digital Watermarking Technology, Screen Capture Attack, Circular Angle Template Watermark

## 1. Introduction

Remote Sensing data, one of the sources of geospatial information, has the characteristics of large information capacity, real time, high update speed and accuracy. It plays an important basic and strategic position in national geographic information resources [1]. As an efficient technical method, remote sensing technology provides an effective data foundation for urban planning, so that cities can be planned efficiently, rationally and scientifically, and ur-

ban land planning can be coordinated to realize urban ecological, healthy and sustainable development [2]. At present, remote sensing image is widely used in urban planning, mapping drawing, land use dynamic assessment and environmental monitoring. For example, obtaining multi-sequence image data at different time periods can visually describe the process of urban spatial expansion and urban land use change [3]. In addition, comparing the orthophoto map with the planning scheme can not only reflect the relationship between urban status and urban planning, but also verify the rationality and operability of the planning scheme [4]. However, in the process of using remote sensing data, its data security issues have also become increasingly prominent. It is extremely urgent to protect the security of remote sensing images.

As a kind of information security technology, digital watermarking technology uses a specific algorithm to hide the watermark information in the original data to determine the copyright owner, track the infringement behaviors, content authentication and data source. Digital watermarking technology can effectively deter and track the leakers, it provides a feasible technical method for the protection of remote sensing images.

With the development of digitalization and the popularity of smart phones, screen capture is relatively simple and common. For example, in the process of distribution of confidential remote sensing images, it is difficult to protect the data copyright information if a person who is exposed to confidential data leaks the data through a screen capture. How to protect data copyright against screen capture is a problem that needs to be solved.

There are few researches on watermarking algorithms against screen capture attacks at home and abroad, and the construction of such watermarking algorithms can depend on other watermarking algorithms which can be robust against print-scan and print-cam attacks. Some research results of digital watermarking algorithms against print-scan are as follows. Chen [5] proposed a watermarking algorithm based on polarized DCT coefficients by considering the properties of DCT coefficients under print scan attack and modifying the polarities of DCT domain coefficients. Amiri [6] proposed a robust watermarking against print and scan attack based on DWT and DCT domains. And the appropriate location of the watermark was determined by analyzing the effects of the modeling algorithm. Xie [7] proposed a double transform domain holographic watermarking algorithm, which can effectively resist print scanning attacks. Liao [8] presented a robust blind watermarking scheme based on uniform log-polar mapping and perceptual band decomposition of Fourier domain.

Also, there are a few viable print-cam robust watermarking methods. Lee [9] proposed a watermarking algorithm suitable for printing photographs by comparing the order of average DCT values in the RGB color model system. Gourrame [10] focused on the main attack caused by perspective distortion printing, using perspective transformation for geometric correction and com-

bining DFT to propose a watermarking algorithm against print-cam. Pramila [11] encoded the watermark information into a square angle tem-plate with periodicity and directionality, and completed the watermark embedding in the form of block. The watermark extraction was realized by detecting the angle feature. This algorithm can effectively resist the print photo attack.

In this paper, we encoded and converted the watermark information in combination with a circular angle template. A digital watermarking algorithm based on QR Code and circular angle template is proposed. It provides a practical technical approach to the protection of basic data in urban planning.

## 2. Proposed Method

The proposed method encodes the watermark information into angle information, and embeds the watermark information by constructing a circular angle template watermark. The watermark embedding rule is realized by changing the JND values of the original remote sensing image. And by detecting the hidden angle information in the circular angle template, the corresponding watermark information will be obtained.

The key technologies of the proposed method mainly include: 1) Positioning and correction of screen capture data, 2) Watermark information preprocessing, 3) Angle watermark detection. The whole procedure of the algorithm is depicted in **Figure 1**.

### 2.1. Watermark Generation

#### 2.1.1. Circular Angle Template Construction

1) Generate a periodic and directional template watermark randomly

Firstly, a basic template watermark block is randomly generated. Then, the basic template watermark block is repeated in the vertical direction and the horizontal direction according to Formula (2.1). Finally, a basic template watermark with periodicity and directivity is generated.

The formula is as follows:

$$\begin{cases} W_1(x+N_0,y)=W_0(x,y) \\ W_1(x,N_1+y)=W_0(x,y) \end{cases} \quad N_0 \geq 1, N_1 \geq 1 \tag{2.1}$$

where $N_0$ and $N_1$ refer to the number of repetitions in the horizontal direction and the vertical direction.

2) Generate a basic circular template watermark

Converting the basic square template watermark $W_1(x,y)$ into the basic circular template watermark $W(x,y)$ by finding the inscribed circle method.

3) Generate a circular angle template watermark

According to the angle information $\theta$ encoded by the watermark information, the basic circular template watermark $W(x,y)$ is rotated to generate a circular angle template watermark with angular features $W^{\theta}(x,y)$. Then, according to the size of the embedded block, the radius of the circular angle template watermark can be adjusted to adapt to the embedding of the

subsequent watermark information.

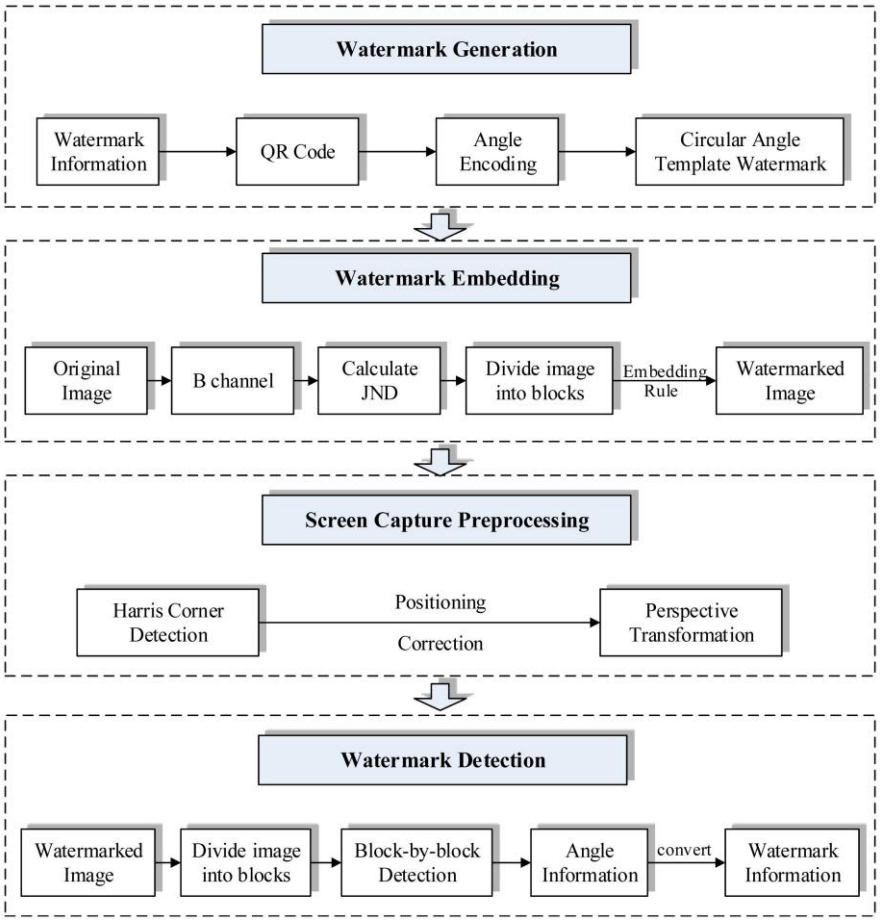



**Figure 1.** The proposed algorithm framework.

Compared with the square angle template watermark [11], the circular angle template watermark constructed in this paper has the following two advantages:

a) In the aspect of changing the pixel value of the carrier image, compared with the square angle template watermark, the circular angle template is used as the watermark information to embed, and only the pixel value covered by the square inscribed circle is changed. The change range of pixel value is small. It makes the pixel value of the whole carrier image change less.

b) In the aspect of watermark information detection, the data obtained after the screen capture has the largest change in the edge portion pixel value. When a square angle template watermark is used, the pixel values of the data edges participate in watermark detection. The distortion of the edge image makes the pixel value change greatly, which affects the detection result. However, for the circular angle template watermark, the edge pixel value does not participate in the detection during the watermark detection, which has a small impact on the detection results and is helpful to obtain accurate detection results.

#### 2.1.2. Watermark Generation

In order to enhance watermark robustness, the image is preprocessed. The main procedures are as follows:

1) Meaningful textual information is fetched.

2) Textual information is converted to a QR code based on the generating rules for the latter.

3) Convert the QR code into its corresponding binary sequence by the progressive raster scanning method.

4) The binary sequence is encoded every four bits, and the encoded watermark information is converted into circular angle template watermark with angle information.

### 2.2. Watermark Embedding

The detailed watermark embedding procedure is stated below.

1) Get the B channel pixel value

Read the remote sensing image, then get its blue channel pixel value $B(x,y)$, $M$ and $N$ are the length and width of the remote sensing image.

2) Calculate JND (Just Noticeable Distortion)

Calculate the JND value of remote sensing image, the JND value is obtained by the luminance model and the texture model.

3) Divide the remote sensing into blocks

According to the number $l_1$ of embedded template watermark blocks, the remote sensing image is $\frac{M}{l_1}\times\frac{N}{l_2}$ divided to ensure that each circular angle template watermark $W^{\theta}(x,y)$ can be embedded into the remote sensing image sub-pixel matrix block.

4) Rules for embedding watermark information

The circular angle template watermark is embedded into the remote sensing image to obtain the watermarked remote sensing image, and the embedding rule is as shown in Formula (2.2).

$$\begin{aligned} B_i'(x,y) = B_i(x,y) + 10*\delta_1*JND(x,y)*W^{\theta}(x,y) \\ +\delta_1*(1-JND(x,y))*W^{\theta}(x,y) \end{aligned} \tag{2.2}$$

where, $B_i(x,y)$ is the i-th block B channel pixel value, $B_i(x,y)$ is the i-th block B channel pixel value after embedding the watermark. $\delta_1$ is the embedding strength, $W^{\theta}(x,y)$ is the circular angle template watermark.

### 2.3. Screen Capture Preprocessing

1) Positioning

The four corner points of the data to be detected are obtained by Harris corner detection for data positioning, and redundant information such as background is removed according to the positioning point.

2) Correction

By using perspective transformation to eliminate the distortion caused by factors such as shooting angle, and thus less distortion and effective data information can be obtained.

### 2.4. Watermark Detection

The traditional detection of watermark information involves the opposite processes to watermark embedding. In the paper, the original watermark information is obtained by detecting the hidden angle information in the circular angle template.

The main procedures are as follows:

1) Get the B channel pixel value

Read the data to be detected after preprocessing, and obtain its B channel pixel value.

2) Block-by-block watermark information detection

First of all, the winner filter is performed to remove the noise that may be added; then, the autocorrelation function is calculated to generate a large autocorrelation peak point; thirdly, the gradient point is used to sharpen the peak point; what's more, add morphological knowledge—expansion and corrosion to make peak points more visible; finally, the line angle is detected by Hough transform to obtain angle information.

3) Convert Angle information to watermark information

According to the angle range of detection angle, the watermark in-formation is obtained.

4) Text watermark information is decoded by QR code

The extracted sequence of watermark information is converted to a QR code. The latter is then scanned to obtain the textual information contained within.

## 3. Experimental Results and Analysis

In order to verify the effectiveness and practicability of the algorithm, experiments were carried out from two aspects: imperceptibility and anti-screen capture attack capability. In this experiment, two remote sensing images were selected as experimental data, as shown in **Figure 2**. Test 1 is an aerial image with a spatial resolution of 0.2 m; test 2 is a satellite image with a spatial resolution of 2.5 m. The experimental data size is 1000 × 1000, and the data format is .tif. The QR code generated is shown in **Figure 3** with the scanning result of "Urban planning copyright protection", which is generated by Version 3, Grade M for error correction, and has the dimensions of 58 × 58.

**Figure 2.** Original remote sensing images. (a) Test 1; (b) Test 2.

Urban planning copyright protection

**Figure 3.** QR code and scan result.

In this experiment, under the premise that the experimental data and watermark information are known, the number of remote sensing image blocks is set to 10 × 10, and the watermark embedding intensity $\theta$ is set to 12. At this time, the watermark information capacity of the algorithm can be embedded up to 400 bits. It can meet the actual application requirements of watermark information capacity.

### 3.1. Analysis of Imperceptibility

A good digital watermarking algorithm can protect the security of re-mote sensing image data without affecting the later use of the data. Imperceptibility is the criterion for verifying whether the watermarking algorithm affects the later use of the data. In order to verify the imperceptibility of the algorithm, this study will be illustrated from two aspects: subjective visual analysis and objective quantitative evaluation.

The watermarked remote sensing images and extracted QR code are shown in **Figure 4** and **Figure 5**, respectively.

1) Subjective visual analysis

Comparing **Figure 1** and **Figure 3**, it can be found from the subjective visual that there is no visible difference between the remote sensing images before and after embedding the watermark. The experimental analysis proves that the algorithm has good invisibility.

2) Objective quantitative evaluation

The objective evaluation index of imperceptibility are shown in **Table 1**.

As can be seen from **Table 1**, the $\bar{G}$, Std and Entropy of the two remote sensing images before and after embedding the watermark are 0.1565, 0.0860, 0.1534 and 0.1150, 0.04383, 0.0139, respectively. The change of evaluation indexes is small, which indicates that the pixel values of watermarked and original remote sensing images do not change much. The PSNR reached 38.5857 and 40.1457, respectively, which was much greater than the

experiential threshold value of 28. The objective evaluation indices adequately illustrated that there is no significant reduction in image quality after embedding of a watermark that is generated using the proposed algorithm.

### 3.2. Analysis of Screen Capture Attacks

There are a variety of screen capture devices. In this paper, mobile phones were used for screen capture, and desktop computer monitors were used for electronic screen equipment. The parameter settings for screen capture are shown in **Table 2**.

**Figure 4.** Watermarked remote sensing images. (a) Watermarked test 1; (b) Watermarked test 2.

Urban planning copyright protection

**Figure 5.** Extracted QR code and scan result.

**Table 1.** Objective quantitative evaluation.

| image | evaluation index | Original remote sensing image | Watermarked remote sensing image |
|---|---|---|---|
| (a) test 1 | $\bar{G}$ | 108.1237 | 108.2802 |
| | *Std* | 66.0863 | 66.1723 |
| | *Entropy* | 7.8158 | 7.6624 |
| | *PSNR* | 38.5857 | |
| (b) test 2 | $\bar{G}$ | 144.8084 | 144.6934 |
| | *Std* | 46.7114 | 46.7597 |
| | *Entropy* | 7.5155 | 7.5016 |
| | *PSNR* | 40.1457 | |

**Table 2.** Screen capture parameter setting.

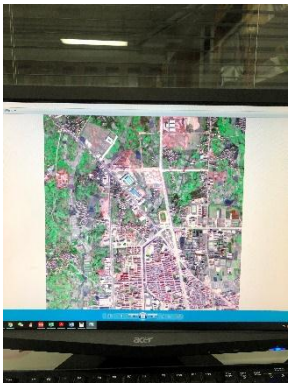
| | |
|---|---|
| Display screen | acer desktop monitor (1920 × 1080) |
| Screen capture device | iphone 8 plus |
| Screen capture distance | 20 cm |

| Screen capture mode | Adjust the shooting angle to minimize the Milo Moire |
|---|---|

According to the parameter setting in **Table 2**, screen capture attacks are done on the two watermarked remote sensing images in **Figure 3**. The experimental results are shown in **Table 3**.

Comparing the photos taken by the mobile phone after screen capture with the original watermarked remote sensing image, it can be found that not only the data volume, data format and size are changed, but also the color and brightness of the image are greatly changed. Besides, the data size has increased

**Table 3.** Experimental results after Screen capture attacks.

| Test data | **Figure 1(a)** | **Figure 1(b)** |
|---|---|---|
| Watermarked image size and format |  1000 × 1000 (.tif) |  1000 × 1000 (.tif) |
| Screen capture photo size and format |  3024 × 4032 (.jpg) |  3024 × 4032 (.jpg) |
| Preprocessed photo size and format |  2493 × 2494 (.jpg) |  2174 × 2156 (.jpg) |
| $NC$ | 1 | 1 |
| $BER$ | 0 | 0 |

| | | |
|---|---|---|
| Extracted QR code |  |  |
| Scanning result | Urban planning copyright protection | Urban planning copyright protection |

from the original 1000 × 1000 to 3024 × 4032, and the data format has changed from .tif to .jpg. Then, the positioning and correction preprocessing of the screen capture is performed, and the amount of data is further reduced to 2493 × 2494 and 2174 × 2156. At this point, it can be intuitively seen that the screen capture by the mobile phone has made a great damage to the remote sensing image.

For all that, using the proposed algorithm, the extracted QR code could still be correctly identified. The NC between the extracted and original watermark information is 1, so that the BER is always 0. This indicates that lossless extraction of the watermark information could be carried out after the screen capture attack. The experimental analyses proved that the proposed algorithm has a high level of fidelity and robustness, and can effectively resist screen capture attack.

## 4. Conclusions

Remote sensing technology provides effective basic information for urban planning, and digital watermark technology provides security for urban planning. In order to resist the screen capture attacks, the watermark information is encoded and converted, and combined with a circular angle template watermark, a digital watermarking algorithm based on QR Code and circular angle template is proposed. The algorithm replaces the binary sequence watermark information with the circular angle periodic pattern watermark, and the watermark information is embedded with the JND value of the remote sensing image. Before the watermark information detection, Harris corner detection and perspective transformation are used to preprocess the detected data. In the process of watermark information detection, the angle in-formation is detected by steps such as winner filtering, calculating autocorrelation function, sharpening peak point, expansion and erosion, and Hough transform, and then the watermark information is obtained. The experimental results show that the proposed algorithm can effectively resist the attacks caused by screen capture and provide technical support for data security. At the same time, the algorithm has strong imperceptibility and practicability.

The combination of urban planning with new technology such as remote sensing technology, digital watermark technology, will help to improve the level of informatization and modernization of urban planning. What's more,

multi-technology fusion can help to plan cities with high efficiency, rationality and science, so as to realize the intelligent development of urban planning information management. In the future research work, a more practical digital watermarking algorithm can be designed to protect data security for the specific application scenarios of urban planning information management.

## Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

## References

[1] Wang, J.Y. (2004) Spatial Information System Theory. Science Press, Beijing.

[2] Han, P.P. (2018) Application Analysis of Remote Sensing Information Technology in Urban Planning. *Urban Construction Theory Rereaearch*, No. 17, 77.

[3] Cui, L.N., Gong, W.P. and Hao, H. (2012) Study the Result of Remote Sensing Monitoring Supported Urban Planning Supervision. *Urban Studies*, **19**, 140-144.

[4] Kan, M.Z., Li, W. and Liu, J.G. (2012) An Overview of the Application of High Resolution Satellite Remote Sensing Technique in Urban Planning and Management. *Geomatics & Spatial Information Technology*, No. S1, 100-102.

[5] Chen, C.H., Tang, Y.L. and Hsieh, W.S. (2013) Print-and-Scan Resilient Watermarking through Polarizing DCT Coefficients. *IEICE Transactions on Information and Systems*, **96**, 2208-2214.

[6] Amiri, S.H. and Jamzad, M. (2014) Robust Watermarking against Print and Scan Attack through Efficient Modeling Algorithm. *Signal Processing Image Communication*, **29**, 1181-1196. https://doi.org/10.1016/j.image.2014.07.004

[7] Xie, Y., Tan, H.H., Wang, K.L., *et al.* (2016) Color Image Watermark Algorithm Robust to the Print-and-Scan Process. *Packaging Engineering*, No. 13, 151-156.

[8] Liao, T. and Li, Z.J. (2016) Adaptive Print-Scan Resilient Image Watermarking Based on Fourier Transform. *Journal of Applied Sciences—Electronics and Information Engineering*, **34**, 309-316.

[9] Lee, M.L., Ting, P.Y. and Wu, T.S. (2015) Photograph Watermarking. *Multimedia Tools & Applications*, **75**, 16173-16189. https://doi.org/10.1007/s11042-015-2925-6

[10] Gourrame, K., Douzi, H., Harba, R., *et al.* (2016) Robust Print-Cam Image Watermarking in Fourier Domain. *International Conference on Image and Signal Processing*, Springer, Cham, 356-365. https://doi.org/10.1007/978-3-319-33618-3_36

[11] Pramila, A., Keskinarkaus, A. and Seppänen, T. (2012) Toward an Interactive Poster Using Digital Watermarking and a Mobile Phone Camera. *Signal Image & Video Processing*, **6**, 211-222. https://doi.org/10.1007/s11760-011-0211-2