92

SUSTech EE326 project Proposal Report

Topic: Digital Watermarking

Author: 11911521钟新宇

Project: The Proposal Report of Project for Digital Image Processing

1. Introduction

文中引用参考文献 -2

Information hiding technology, also known as steganography, is to hide secret information in another public information (carrier information) to form a hidden carrier, and then transmit the hidden information through the transmission of the hidden carrier, making it difficult for potential attackers to judge whether the secret information exists from the public information and intercept the hidden information, so as to achieve the purpose of ensuring information security.

Digital watermark is an important application of image steganography, and is one of the important methods to carry out copyright protection and information hiding at present. Digital watermarking technology has been developed for more than thirty years, and many kinds of watermarking algorithms have been born.

2. Basic Model of Digital Watermarking

The basic model of digital watermarking system contains three main steps: generating, embedding, and extracting. The figure below shows the basic model of watermarking system.

Fig.1 —

最好再加简单说明.

下图 -2

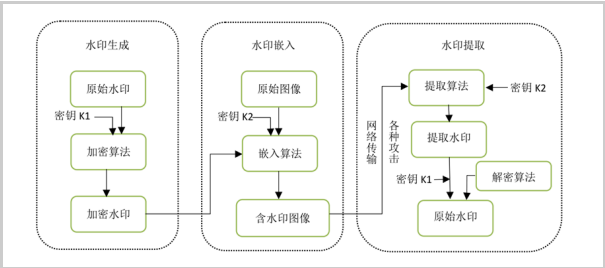


Fig.1 xxxx

2.1 Encryption Algorithm

The scrambling technique is a process of replacing the spatial domain of a digital image, or modifying the parameters of the transform domain of a digital image to change the generated image into a scrambled image, which is a nonlinear transformation process, and thus can be achieved by performing an invertible 2D transformation within a 2D matrix.

In the history of disorder technology, scholars have proposed several algorithms based on mathematical transformation techniques, including Arnold transform, FASS curve, phantom square transform, Gray code, life model, etc., which are effectively used in the pre-processing and post-processing of digital image information security processing. Among all reversible two-dimensional chaotic mappings, the performance of baker mapping is the best, so using baker mapping can have a good hiding effect.

The Baker mapping stretches the image in the width direction and compresses it in the length direction. It transforms a horizontally aligned image into a vertically aligned image. A continuous Baker map B(x, y) can be described as

$$B(x,y) = \begin{cases} (2x, \frac{y}{2}), & 0 \le x < \frac{1}{2} \\ (2x-1, \frac{y}{2} + \frac{1}{2}), & \frac{1}{2} \le x < 1 \end{cases} \tag{4}$$

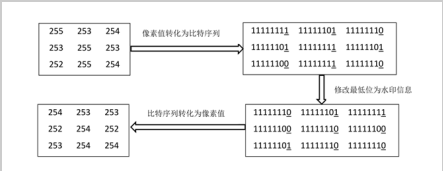
2.2 Embedding Algorithm

Digital watermarking techniques can be divided into transform domain-based watermarking techniques and spatial domain-based watermarking techniques.

2.3 Spatial Domain-Based Watermarking Techniques

Spatial domain based watermarking technique is to directly change the intensity value of the image pixels. The simplest and representative spatial domain-based watermarking scheme is the LSB algorithm.

First we binarize the watermark and at the same time convert the intensity value of the carrier image pixel into a binary bit sequence. Since the range of grayscale values is from 0 to 255, we can represent the intensity value of each pixel point with 8 bits. Then let the value of the binarized watermark replace the value of the least significant bit (LSB) in the 8-bit sequence of the carrier image. In the process of information extraction, we only need to focus on the values of the least significant bits of the image, and extracting them all and recombining them is the hidden information.

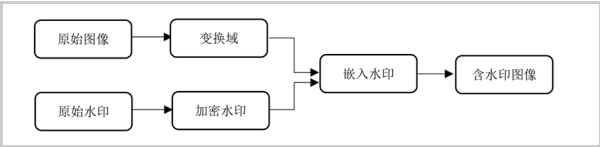


The LSB algorithm is very widely used and can be found in almost all image steganography algorithms. Besides, most of the common steganography software on the Internet also uses the LSB algorithm or the LSB derivative algorithm. Since it uses the least important pixel bits of the image, the LSB algorithm is less robust and the embedded information is easily attacked by operations such as filtering, image quantization, geometric distortion and noise addition.

2.4 Transform Domain-Based Watermarking Techniques

Digital watermarking based on transform domain has the advantages of better invisibility, robustness and larger amount of embedded watermark information.

Firstly, we transform the carrier image into the transform domain, and then embed the watermark in the corresponding frequency band, such as modifying, replacing and swapping the coefficients of the frequency band.



We can choose the embedding bands according to the actual requirements. In general, the low frequency band of the transform domain contains the main information of the image and the distortion is not large, but it will affect the invisibility of the watermark. The high frequency band is the part of the human eye visual system is not sensitive, so embedding the watermark in this region can ensure a good invisibility of the watermark. However, the high frequency region is also the part that is often rejected by compression techniques, so the robustness is poor.

Watermarking algorithms based on transform domain mainly include discrete cosine transform (DCT) domain, discrete wavelet transform (DWT) domain, discrete Fourier transform (DFT) domain and so on.

- Discrete Cosine Transform (DCT)

  The discrete cosine transform is often used for lossy data compression of images. The discrete cosine transform has energy concentration property, most of the energy of natural signal is concentrated in the low frequency part after discrete cosine transform.

- Discrete Wavelet Transform (DWT)

  Wavelet transform is a time-frequency analysis method based on Fourier transform and Gabor transform, which not only inherits the good properties of Fourier analysis, but also solves many shortcomings of Fourier analysis. When analyzing the high frequency part of the signal, wavelet analysis shows a lower frequency resolution; when analyzing the low frequency part of the signal, wavelet analysis shows a higher frequency resolution.

3. Attack Methods

Then we need to evaluate the performance of the system. The most important performance evaluation metrics are: Peak Sign-to-Noise Ratio (PSNR), and Normalization Coefficient (NC).

3.1 Peak Sign-to-Noise Ratio (PSNR)

The Peak Signal-to-Noise Ratio is used to measure the distortion between the embedded watermarked image and the original image. The larger the PSNR value, the less distortion and the better the invisibility of the watermark. The PSNR value ranges from [0,100]. When the PSNR value is greater than 30, the human eye visual system cannot perceive the difference between the watermarked image and the original image.

The definition of PSNR is as below.

$$
\begin{aligned}
&10 \times \lg\left(\frac{MAX^2}{MSE}\right) \\
&MSE = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n}[f(i,j) - g(i,j)]
\end{aligned}
\tag{5}
$$

where `f(x,y)` is the original image, `g(x,y)` is the image with watermark, and `MAX` is the maximum value of image pixels.

3.2 Robustness

3.2.1 Normalization Coefficient (NC)

The Normalized Correlation Coefficient (NC) is used to measure the similarity between the original watermark information and the extracted watermark information, and its value range is [0,1].

The larger the NC value, the higher the similarity between the original watermark and the extracted watermark, and the stronger the robustness of the watermarking algorithm; Conversely, the smaller the NC, the lower the similarity between the original watermark and the extracted watermark, and the weaker the robustness of the watermarking algorithm.

The definition of NC is as below.

$$
\mathrm{NC} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\left(w(i,j) \times w'(i,j)\right)}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}[w(i,j)]^2}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}[w'(i,j)]^2}}
\tag{6}
$$

where `w` is the original watermark, `w'` is the extracted watermark, `m` and `n` are the number of rows and columns of the watermark image matrix, respectively.

3.2.2 Non-Geometric Attack

The Non-Geometric Attack is a common signal processing attack. The attacker modifies the pixel values of the image. Common geometric attack methods include adding noise to the image, compressing, filtering, and enhancing.

3.2.3 Geometric Attacks and Other Attacks

The Geometric Attack takes operations such as occlusion, translation and rotation to change the position of pixels, which can result in incomplete or unextractable watermark information. The common geometric attacks include clipping attack, rotation attack, row offset attack and scaling attack.

In addition, the attacker can also use non-geometric attacks and geometric attacks at the same time. There are also mosaic attacks and other methods

Review 很好.

4. Objective of the Project

计划工作有点欠缺. -4

The goal for the project is to design a complete digital watermark system. The specific objectives are as follows.

- Design a watermarking system based on baker mapping and LSB with carrier and watermark as grayscale image.
- Try other embedding algorithms such as DCT and DWT.

5. Reference

- 王树梅.(2022). 数字图像水印技术综述. 湖南理工学院学报 (自然科学版)(01),31-36+68. doi:10.16740/j.cnki.cn43-1421/n.2022.01.006.
- 马玲 & 覃亮成.(2021). 基于 DCT-DQFT 变换和 QR 分解的彩色图像盲水印算法. 信息网络安全 (09),25-31.
- 王玉莹，关虎，黄樱，张树武 & 牛保宁.(2020).DWT-DCT 联合变换域上的文本图像水印方案. 计算机工程与设计 (06),1676-1682. doi:10.16208/j.issn1000-7024.2020.06.029.
- 谢建全 & 阳春华.(2008). 大容量的信息隐藏算法. 计算机工程 (08),167-169.
- 张华熊，仇佩亮.(2001). 置乱技术在数字水印中的应用. 电路与系统学报 (03),32-36.
- 钮心忻，杨义先.(2000). 基于小波变换的数字水印隐藏与检测算法. 计算机学报 (01),21-27.
- 叶绍鹏，张天骐，柏浩钧 & 刘鉴兴.(2021). 基于 Baker 映射与时空混沌相结合的 CT-QR 域双彩色鲁棒盲水印算法. 信号处理 (05),843-853. doi:10.16798/j.issn.1003-0530.2021.05.018.
- 數位浮水印. (2021, November 22). Retrieved from 维基百科，自由的百科全书: https://zh.wikipedia.org/w/index.php?title=%E6%95%B8%E4%BD%8D%E6%B5%AE%E6%B0%B4%E5%8D%B0&oldid=68767272
- 隐写术. (2020, December 26). Retrieved from 维基百科，自由的百科全书: https://zh.wikipedia.org/w/index.php?title=%E9%9A%90%E5%86%99%E6%9C%AF&oldid=63439708