Research on Image Digital Watermarking Algorithm Based on Matlab

Jialin Chen¹, Jun Sun¹, Lu Ye¹, Peng Zhan¹, Shiwen Zhao²

¹State Grid Hubei Information Telecommunication Co, Ltd., Wuhan, 430077, China, ²Nari Group Corporation Information & Communication Technology Co., Ltd, Nanjing, 210003, China

Abstract. Digital watermarking technology provides an effective protection method for copyright protection and information security. This paper uses MATLAB's powerful image digital watermarking function to realize the embedding and extraction of digital image information based on DCT transform domain. The algorithm also effectively attacks the embedded digital image information.

1. Introduction

In this era of big data, the widespread use of computers and the smooth transmission of the Internet make it easy to read and store large amounts of information. People can more easily consume, read, and communicate around the world. However, such an information life the method has also brought a lot of problems. The security of personal information is being concealed. The network transmission makes it possible for everyone's information and works to be copied and profited by others without the permission of the author. Sometimes they even look for there is no source of infringement. Therefore, it is especially important to protect intellectual property rights and maintain information security changes.

2. Digital watermarking system general model

Intuitively, digital watermarking technology embeds a signal that is not easily noticed and has no regularity to be embedded in the digital structure of the multimedia domain. It is a so-called digital watermarking algorithm. Its principle is human vision. The system resolution is used as the basis for the watermark display. If the embedded signal coefficient is weak, the visibility is reduced in a carrier with a strong signal until it is lower than the lowest resolution limit of the human eye. The existence of the watermark signal is not noticeable, and usually the standard value of the human visual system has a certain stability, so the reprocessing of the sample image is performed without disturbing the normal visual effect of the person.

The watermark signal A, the host signal B, and the key C are three necessary inputs of the watermark embedding device. The watermark signal M refers to digital information in which the original watermark modulated in a certain mode is embedded in the host signal S. The host signal B is the original information after embedding the watermark. The function of the key C is to improve the overall security of the watermark. The key information is independent of the host signal. The key has two types: a private key and a public key. The former means that the attacker is when the watermark embedding method is clear, it cannot be destroyed or stolen, and the attacker does not know the key. The latter means that the key is not confidential and can be used as a public key when the attacker is not interested in the host signal.
3. DCT domain algorithm model

![Diagram 1](image1.png)

**Figure 1.** Algorithm embedded model based on DCT domain

![Diagram 2](image2.png)

**Figure 2.** Algorithm for extracting detection based on DCT domain

4. Algorithm implementation process

The current mainstream watermarking algorithm in the academic world is the transform domain algorithm. The following two algorithms have the highest degree of recognition: DCT and DWT. This paper mainly uses the former DCT domain transform, and its principle is similar to DFT. In the DTFT Fourier series expansion, if the expanded function is a real function, then the Fourier series contains only the cosine term, and then the DFT is derived from the cosine transform. The digital watermarking algorithm based on the DCT domain uses certain methods, such as random sequences, chaotic sequences, scrambling, etc. The watermark signal is preprocessed, then embedded into the components of the image sub-block DCT transform, and similar correlation functions are used to detect and extract the watermark information.

In order to better make the stable human visual system have a good signal superposition effect under different conditions, the control of the numerical strength of the signal needs to be differentiated and standardized. For example, the image is in different light. In the environment of sensitivity, there are different average gray scales and irregular textures. This requires that the sample images be segmented according to the division of these different intensities, so that the superposition effect is the most reasonable. HVS has the weakest perception of changes in pixel values. In the case, it usually occurs in high average gray scale and complex pattern texture. Conversely, when low average gray scale and smooth texture appear, the sensitivity of HVS will increase. At this time, the intensity of the superimposed watermark is in the weakest state.

The DCT transform domain watermarking algorithm is a kind of watermarking algorithm which is widely used in image processing for its versatility and practical operation. It has a large amount of bit data embedded in the image and ensures that the processing is not observed. Come out and be welcomed. The specific steps of the DCT domain algorithm: firstly perform DCT transform on the original image, then use the statistics of the image coefficients to select an appropriate frequency segment to embed the watermark, and then perform DCT inverse transform on the image, and finally obtain an image with
embedded watermark. In the frequency band selection of the image, we must avoid the low frequency band of the image that covers almost all the content and is easily perceived by people. We also avoid the high frequency band that covers the image content but is vulnerable to attack, so we are choosing when the position of the watermark is embedded, the mid-range is often compromised. It is well known that the advantage of the transform domain watermarking algorithm is that the image produced is not easily detected by people, so the robustness of the mid-band is ensured.

5. Image block DCT
The DCT transform domain watermarking algorithm is divided into an overall transform algorithm and a block transform algorithm. COX et al. first proposed the DCT domain watermarking algorithm, which was applied to the operation of the entire image, but with the development of the times, people deal with complex images. The idea of dividing the original image into 8×8 partitions is derived, and the whole part of the block is DCT transformed, converted into 64-bit DCT coefficients, and then the intermediate frequency coefficients in each block are selected. Frequency and other methods modify the band coefficient, which not only reduces the complexity of image operations but also greatly improves the accuracy of image processing.

The method is as follows: first input the image into a matrix, then divide the image into K identical image blocks \( f_x(x', y'), x' \geq 0, y' < 8, k = 0, 1, \ldots, K - 1 \), that do not coincide with each other, and then perform DCT transformation on the \( f_x(x', y') \) to obtain \( F_x(u', v') \), and the equation is:

\[
F(u, v) = \frac{2}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cos \left( \frac{(2x+1)\mu\pi}{2N} \right) \cos \left( \frac{(2y+1)v\pi}{2N} \right) (1)
\]

\[
F(u, v) = \frac{2}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cos \left( \frac{(2x+1)\mu\pi}{2N} \right) \cos \left( \frac{(2y+1)v\pi}{2N} \right) (2)
\]

6. Scattering of watermark signals
Usually, before doing the work of embedding the watermark image, it is necessary to perform scrambling. Image scrambling has two functions. The first one is encryption. That is, if you do not know the scrambling method, there is no way to directly remove the scrambled image. Extracting the correct watermark pattern. The second is to spread the information of the original watermark information data to the new watermark data information, so as to ensure that even if the image is partially damaged, it can still be partially or completely restore the watermark pattern. This article uses the Arnold scrambling method, the specific block diagram and the experimental effect diagram are listed below. The block diagram is as follows:

![Figure 3. Scattering of watermark images](image)

7. Watermark extraction and detection
The extraction of the watermark means that in the system containing the water signal, the embedded watermark signal is accurately extracted by a certain method. The good evaluation of a certain watermark data is generally confirmed by the integrity of the extracted watermark. When the watermark we extracted locally changes, the best way is to find the location where the original data is modified by
changing the position of the watermark. Watermark detection uses correlation detection technology, and
the difference between the image to be tested and the original image is:

\[ e(x, y) = f^*(x, y) - f(x, y) = \sum_{k=0}^{K-1} e_k(x', y'), x' \geq 0, y' < 8 \]  

(3)

Perform a DCT transform on the \( e_k(x', y') \), and then use the following equation to extract the
watermark sequence:

\[ x_i = \left( \frac{F'_k(u', v')}{F'_k(u', v')} \right) / \alpha \]  

(4)

The extractable sequence to be tested is obtained:

\[ W^* = \{ x_i^*, 0 \leq i < n \} = \sum_{k=0}^{K-1} W_k^* \]  

(5)

Calculation of similarity:

\[ \rho(W^*, W) = \frac{1}{\sqrt{\sum_{i=0}^{n-1} (x_i^*)^2}} \sum_{i=0}^{n-1} (x_i^* x_i) \]  

(6)

The criterion for digital watermarking is the comparison of numerical values. The value of the
similarity is calculated to distinguish whether the image watermark contains unknown information,
which has the effect of protecting the intellectual property rights of the right holder. First, set the
threshold \( T \), if the similarity is calculated. \( \rho > T \), which concludes that there is a watermark signal \( W \)
in the sample image, and vice versa. Not only that, but in addition to the intuitive data calculation, it
also needs to consider the false alarm probability and the missed alarm probability behind the threshold.
For example, the sample there is no appearance of the watermark in the image, but the detection result
of the machine shows the probability of the watermark trace. This case is called the false alarm
probability. The other kind of false alarm probability is that there is an obvious watermark in the sample
image. At the same time, the probability of false alarm is reduced. If the newly acquired watermark
signal \( W^* \) has no correlation with the original data \( W \), the probability coefficient of the similarity \( \rho \)
greater than the threshold \( T \) will be more than \( T \) times the mean value of the random variable \( X \) with
the Gaussian distribution sequence. The block diagram is divided into two steps, the first step is the
inverse transformation:
Figure 4. DCT inverse transformation

8. Summary
This paper proposes a programming using MATLAB. The author uses MATLAB's powerful and simple operation design program to realize DCT discrete cosine transform, completes the watermark embedding and extraction of the digital image, and effectively attacks the embedded watermark information. The results of the attack experiment can still detect the existence of watermark information, which shows that the algorithm has good concealment and robustness.

References
[1] IJ Cox, J Kilian, T Leighton, T Shamoon. Secure Spread Spectrum Watermarking for Images, Audio and Video. Proceedings of the 1996 IEEE International Conference in Image Processing. CA: IEEE, Los Alamitos, 1996, 3: 243 - 246.
[2] IJ Cox, J Kilian, T Leighton, T Shamoon. Secure Spread Spectrum Watermarking for Multimedia [J]. IEEE Transactions on Image Processing. 1997, 6 (12): 1673 - 1687.
[3] Hui-Yu Huang, Cheng-Han Yang, and Wen-Hsing Hsu. A Video Watermarking Technique Based on Pseudo-3-D DCT and Quantization Index Modulation. IEEE transactions on information forensics and security, 2016, 5, (4): 625 - 637.