Comparative and Analysis of spatial domain and frequency domain digital image watermarking algorithm

Yongqiang Ma, Shunli Wang, Jinping Song, Yandong Yu, Wei Sun, Jing Bian

School of Computer Science, Jining Normal University, Wulanchabu, Inner Mongolia, 012000, China

Corresponding author’s e-mail: nsd-myq@126.com

Abstract. Digital image watermarking belongs to the branch of information hiding discipline, the study of the digital watermarking will play an invaluable role in the integrity of business transactions and the protection of personal privacy. This paper introduce the embedding process of digital watermarking technology and the extraction process of digital watermarking technology. We analyze the characteristics of digital image watermarking and juxtapose the basic principle of the Least Significant Bits algorithm and the basic principle of the Quaternion Fourier Transform algorithm. Finally, According to analysis and comparison, we summarize the advantages of the frequency domain method.

1. Introduction

With the development of computer and network technology, we can download and use any graphic images music or videos through relevant devices in anytime and anywhere. However, people don’t know the origin and authenticity of the data they used, the data has been falsified and forged freely. How to protect the security of multimedia data such as pictures and how to verify its effectiveness is becoming one of the hotspots in scientific research.

The problems of copyright attribution and product certification that brought by the massive use of multimedia data have not been solved by traditional cryptography techniques [1]. As an extension of traditional cryptography, digital watermarking provides a good solution to the problems of copyright protection and malicious tampering of multimedia such as images audio and video.

Digital watermark belongs to the branch of information hiding discipline. It embeds hidden information in multimedia products such as images, can protect the copyright of digital products and can track piracy. Studying digital watermarks will play an invaluable role in the integrity of business transactions and the protection of personal privacy. Therefore, the digital watermark as a research direction not only has important scientific research value, but also can bring economic and social benefits, it can achieve the purpose of protecting collective and personal information, and has far-reaching social impact.

2. The basic principle of digital watermarking technology

The digital watermarking technology can be described as a technique for selecting a suitable watermark embedding method to embed copyright information into the digital multimedia directly, and it does not affect the visual effect of the digital product but can achieve protection, which mainly includes the watermarking embedding and the watermarking extraction.
In order to detect whether the multimedia information is damaged, the data represented the copyright information is detected, and the difference between the extracted information and the previously embedded watermark information is sought to determine whether it changes, and if the change occurs, we should know the degree of damage and then effectively improve its algorithmic flaws and study watermarking algorithms with better robustness and imperceptibility.

2.1 The embedding process of digital watermarking technology

We should define a digital product \( O \), the key of the Embedding method can be represented by \( K \). \( F \) represents the embedding method. Then, the data information \( W \) that represented the copyright of the carrier is combined with the carrier by the \( F \) method to obtain a new carrier \( W' \), and the process is represented by

\[
W' = F(O, K, W)
\]

The watermark embedding function \( F \) and the key \( K \) are known only by the designer who designs the embedding algorithm [2]. Therefore, even if the destroyer steals the multimedia product, the key cannot be obtained without cracking the embedding algorithm, and it is difficult to destroy or obtain the copyright of the multimedia digital product. The embedding process of digital watermarking technology is shown in figure 1.

2.2 The extraction process of digital watermarking technology

The extraction operation of watermarking scheme is mainly divided into two types: non-blind extraction and blind extraction. The non-blind extraction watermark refers to the process of extracting watermark information with the help of the original carrier and the digital product embedded with watermark. On the contrary, blind extraction means that the original image is not needed. Both of the two methods, the key of the embedded method needs to be recorded in advance, and the embedded information is extracted by using the extraction scheme and the recorded key, the selected method is recorded as \( E \) and the extracted watermark \( W'' \) can call it \( W' \), and it is given by

\[
W'' = E(I, W', K)
\]

The extraction process of digital watermarking technology is shown in figure 2.

2.3 The characteristics of digital image watermarking

Nowadays, digital watermarking technology has become a hot field for the security certification and protection of multimedia digital products. In order to protect multimedia digital products, digital watermarking as color image digital watermarking must have some features, the characteristics of digital image watermarking is shown in table 1.
Firstly, Invisibility is the basic characteristics of the digital watermarking. After the watermark information is embedded in the multimedia product, the embedded watermarked multimedia product will not produce large distortion, and on the other hand, the embedded watermark information is difficult to be discovered by the human eye, and a better visual effect is achieved. Some products used in life require embedded watermark information to be visible, but most digital products require better invisibility, so watermarking technology requires invisibility [3].

Secondly, Robustness refers to the fact that when the product is embedded with other information, the obtained watermarked multimedia product is subjected to various attacks, and the extracted watermark information can still prove the copyright of the digital product. In contrast, after the damage, the correct watermark information cannot be extracted, that is, the watermark embedded product has no value.

Security means that the information to be combined with the carrier data must have the ability to protect it, it must meet the security requirements. Therefore, when we select the embedding algorithm, the watermark needs to be encrypted, so that when the digital product is extracted, if the embedded algorithm is known without knowing the key, the complete digital product cannot be stolen.

The characteristics of digital image watermarking are shown in table 1.

| The characteristic | The description |
|--------------------|----------------|
| Concealment        | Not perceived by the observer |
| Integrity          | Only authorized users can separate the watermark |
| Robustness         | Robust watermark: Requires the system to accept general information processing attacks and geometric attacks |
|                     | Fragile watermark: Requiring any minor changes will cause the extraction operation to fail |
| safety             | Unauthorized extraction of information |
| Availability       | Authorized entities can obtain verification services at any time |
| Controllability    | Security monitoring data to prevent illegal use |

3. The watermark classification according to embedding position

In the field of digital image processing, watermarks are a set of data representing image, video, and audio copyright information. Correspondingly, the watermark information can be divided into many types according to different classifications.

The watermarking embedding process modifies the pixel values in the spatial domain, or transforms them from the spatial domain to the frequency domain, and then modifies the frequency domain pixel values and finally restores them to the spatial domain. According to embedding position, we can divide the digital image watermark into spatial domain watermark and frequency domain watermark. The watermarking algorithm LSB [4] (Least Significant Bits) originally proposed achieves the goal of modifying the lowest element pixel value when embedding the watermark. This watermarking algorithm is less robust than the frequency domain algorithm, thus generating another kind of watermarking called frequency domain algorithm.

The spatial domain algorithm has poor visibility and good robustness. In order to take advantage of the advantages of the two algorithms, many algorithms combining spatial and frequency domains are gradually proposed to achieve the equalization effect of watermark invisibility and robustness.

3.1 The basic principle of the LSB algorithm

The Least Significant Bits abbreviated as LSB is a common method, we can divided it into two categories. LSB replacement is the first one and LSB matching is the other one. In the LSB substitution, the LSB(s) of cover image pixels are replaced by bits of the confidential message. In the LSB matching, the pixel bit of cover image is incremented or decremented randomly according to the secret bits [5].
Implement LSB is very easy to us, and a large size of secret data can be embedded. Hidden data can be recovered easily. However, LSB has a low robustness, because the secret information can be destroyed by easy statistical attacks. In addition, The Least Significant Bits is considered to be insecure, because the suspected media can be analyzed to find a clue to the secret message, and then is easily recognize the presence of the secret message [6].

Through experiments, we find that the implementation of the LSB algorithm is simple and can guarantee the invisibility of the digital image watermarking, but the watermark has some blur.

3.2 The basic principle of the QFT algorithm
The advantage of processing color image with quaternion theory is that three color channels of the image are treated as a whole. Color host image is described as a quaternion matrix. We can get its frequency domain information, using Quaternion Fourier Transform (QFT). The watermarking information is embedded into the frequency domain information of the host, using Arnold transform[7].

Thus, we can get a color image containing watermarking information, using inverse quaternion Fourier transform of the host frequency domain information we get before. Information hiding is enabled. Each steps are reversible here, so the watermarking extraction process is oppose to the above process.

The quaternion is a number in a four-dimensional space that has a real part and three imaginary parts. Where q represents the quaternion, and we defined it as
\[ q = a + bi + cj + dk \]  
\[ i^2 = j^2 = k^2 = ijk = -1 \]  
\[ ji = -k, kj = -i, ik = -j \]  

The Quaternion Fourier Transform (QFT) can be given by
\[ F(u, v) = \frac{1}{\sqrt{MN}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} e^{-\frac{2\pi mu}{M} M} e^{-\frac{2\pi nv}{N} M} f(m, n) \]  
\[ f(m, n) = \frac{1}{\sqrt{MN}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} e^{\frac{2\pi mu}{M} M} e^{\frac{2\pi nv}{N} N} F(u, v) \]

In the RGB color space, any color can be represented by a three-dimensional vector [8], so each pixel can be represented by a pure quaternion imaginary number. The three components of RG andB are used as the coefficients of i j and k, respectively, and the color image can be represented by a quaternion matrix. By this way we can treat the color image as a whole.

4. Conclusion
According to analysis and comparison, the frequency domain method has many advantages.

The embedded watermark signal energy can be distributed to all pixels in the spatial domain, which is beneficial to ensure the invisibility of the watermark.

Certain features of the vision system can be more easily incorporated into the watermark encoding process.

Frequency domain method is compatible with international data compression standards.

Acknowledgments
We would like to thank professor WANG and professor SONG for stimulating discussions with respect to the topic of this paper. This work was supported by Research Program of Science and technology at Universities of Inner Mongolia Autonomous Region (NJZZ20246).

Author
MaYongqiang is an associate professor of Jining Normal University, China.
His main research interests include computer-aided instruction and multimedia technology application.
References
[1] Petitcolas F.A.P., Anderson. R.J., Kuhn, M.G. (1999) Information hiding-A survey. Proceedings of the IEEE, 87:1060-1080
[2] Liu, F.M., Zhai, H.C., Yang, X.P. (2003) Kinoform-based iterative random phase encryption. Acta Phys. Sin, 52:2462-3465.
[3] Cui, S.B. (2013) Digital Watermarking Algorithm for Color Image Based on Quaternion Fourier Transform. Jiling Publishing, ChangChun
[4] Xu, C.C., Yang, Q.M., Yin, F.C. (2019) Image Encryption Based on Digital Watermarking Technology. Computer & Digital Engineering, 47:252-255.
[5] Tong, X.A., Zhang, N., Yuan, K.H. (2019) Design and Implementation of RGB Image Dual Watermarking Based on 3D-DCT. Science Technology and Engineering, 23:15-20.
[6] Feng Wei, Hu Bo. (2010) Novel Color Image Registration Algorithm Using Quaternion Phase-only Correlation. Systems Engineering and Electronics, 32: 183-187.
[7] Chen, S.X, Feng, Y.B. (2014) Double Zero-watermarking Algorithm Based on Quaternion and for Color Images. Computer Applications and Software, 31: 263-267.
[8] Sun, J, Yang, J.Y. (2012) Quaternion Based Holistic Color Images Watermarking Algorithm. Journal of Electronics & Information Technology, 34: 2389-2395.