PAPER • OPEN ACCESS

Comparison of the Schemes in Digital Image Watermarking Techniques

To cite this article: Yongqiang Ma *et al* 2020 *J. Phys.: Conf. Ser.* **1617** 012096

View the article online for updates and enhancements.

Comparison of the Schemes in Digital Image Watermarking Techniques

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. With the rapid developing of network techniques and multimedia technology, the data security becomes an important and challenging research topic. The emergence of digital image watermarking technology provides an effective way for multimedia copyright protection, which embeds specific information. This paper analyses the characteristics of digital watermarking technology firstly, then studies some important digital image watermarking algorithms, finally compares the schemes in digital image watermarking techniques. The work aims to compare the differences of the schemes in digital image watermarking techniques and improve the performance of digital image watermarking.

1. Introduction

The rapid development of computer technology and multimedia technology has speeded up the arrival of digital new age. The storage and transmission of digital media contents such as text, graphics, images, audio and video have become very convenient. Digital multimedia security problem has become a very important and challenging research topic. In this background, digital image watermarking technology has got high attention by the international academia and the business community, and become one of the fastest growing hot technologies in information security field [1-3].

The earliest method used for copyright protection of multimedia content is the password authentication technology. We should encrypt the content before sending it, and distribute the key encryption only to the users who have purchased a legal copy of the content. In this way, after being distributed through the Internet, although pirates can obtain the encrypted file, but there is no correct key encryption, this file is also useless.

However, the use of cryptographic technology alone cannot completely solve the problem of copyright protection. Password technology can only protect data during the transmission of data from the sender to the receiver, but it cannot help the seller to monitor how legitimate users handle decrypted multimedia. In this way, the software pirates can purchase products and use keys to obtain unprotected copies of content, and then continue to issue illegal copies. In other words, cryptography can only protect the content in transmission, and once the content is decrypted it no longer works. In order to solve the deficiencies of cryptographic technology in multimedia protection, a new effective digital copyright protection and data security maintenance technology that called digital watermark technology has been developed.

We know that the Digital watermarking technology embedded the special watermark information into the multimedia information, the watermarking information will not be eliminated in the general multimedia content using process. Even after the processes of encryption, decryption, compression, digital-to-analog conversion, and changing the file format, the digital watermark can still exist.

The huge hidden danger is information security, especially the copyright of digital image works. As a means of information hiding, digital watermarking technology can provide copyright protection for digital multimedia works. In the case of copyright disputes, we can identify the copyright owner and track the infringement, verify the integrity of the multimedia data, authenticate the authenticity of multimedia data, and provide effective legal basis for the identification of infringement, so as to deter illegal users and reduce infringement. As a result, this technology has become a commercial tool for digital works protection [4].

2. Discrete Cosine Transform(DCT)

One of the famous transformation technique is the Discrete Cosine transform (DCT). We usually use the 2D-DCT in image processing. 2D-DCT transform instantly converts 2D images from spatial domain to frequency domain.

The discrete cosine transform can be defined as follows [5]:

$$C(u,v) = \frac{2}{\sqrt{mn}} \alpha(u)\alpha(v) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \cos\frac{\pi(2x+1)u}{2m} \cos\frac{\pi(2y+1)v}{2n} \tag{1}$$

Where M and N represent the image size.

The mathematical expression of the inverse 2D-DCT is:

$$f(x,y) = \frac{2}{\sqrt{mn}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \alpha(u)\alpha(v) C(u,v) \cos\frac{\pi(2x+1)u}{2m} \cos\frac{\pi(2y+1)v}{2n} \tag{2}$$

Where $C(u,v)$ and $f(x,y)$ are respectively the pixel values in the discrete cosine transform coefficients and the spatial domain. The block size is represented as the m m and n.

$$\alpha(u)\alpha(v) = \begin{cases} \dfrac{1}{\sqrt{2}} & if\,(u,v)=0 \\ 1 & else \end{cases} \tag{3}$$

3. Discrete Wavelet Transform(DWT)

We all know that the Discrete Wavelet Transform is a new generation standard of JPEG-2000, which is a compression coding of static digital graphics. The basic idea of the digital image watermarking algorithm based on Discrete Wavelet Transform is to decompose the digital graphics into multiple sub-images of different frequencies, and then embed the watermark information according to the characteristics of each sub-image.

The multi-resolution analysis of wavelet is consistent with the Human Visual System (HVS). Compared with DCT that is needed to find the low and medium frequency regions, the discrete wavelet transform naturally divides the carrier graphics into high frequency regions and low frequency regions, which can better select the embedded position of watermark information.

The discrete wavelet transform can be described as the following [6]

$$W_\phi\left[j_0,k\right] = \frac{1}{\sqrt{M}} \sum_n x[n]\phi_{j_{0,k}}[n] \tag{4}$$

$$W\psi[j,k] = \frac{1}{\sqrt{M}} \sum_n x[n]\psi_{j,k}[n] \tag{5}$$

Where the approximation coefficients are expressed as $W_\phi\left[j_0,k\right]$, the detail coefficients can be show by $W\psi[j,k]$, so the IDWT is defined as

$$x[n] = \frac{1}{\sqrt{M}} \sum_k W_\phi[j_0,k]\phi_{j_{0,k}}[n] + \frac{1}{\sqrt{M}} \sum_{j=j_0}^{J} \sum_k W_\psi[j,k]\psi_{j,k}[n] \tag{6}$$

Where M represent the number of samples to be transferred$= 2^J$, and J means the number of transfer levels, $\{\phi_{j,k}[n]\}$ and $\psi_{j,k}[n]$ are two foundation functions, the $\phi[n]$ represents the scaling function, the wavelet function can be expressed as $\psi[n]$.

4. Two-dimensional Discrete Fourier Transform

The discrete Fourier transform is very important in image processing and two-dimensional discrete Fourier Transform is the most ordinary. [6].

The two-dimensional Discrete Fourier Transform can be described as the below

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) e^{-j(2\pi/M)xu} e^{-j(2\pi/N)yv} \tag{7}$$

Where $u = 0,1,...,M-1; v = 0,1,...,N-1$, M and N represent the image size.

And the two-dimensional discrete Fourier Inverse Transform is defined as

$$f(x,y) = \frac{1}{MN}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F(u,v) e^{j(2\pi/M)xu} e^{j(2\pi/N)yv} \tag{8}$$

Where M and N mean the image size and $x = 0,1,...,M-1; y = 0,1,...,N-1$.

The main characteristics of the Discrete Fourier Transform can be expressed in figure 1.

Characteristics	Frequency Domain	Spatial Domain
Principle of Addition	$F(u,v)+G(u,v)$	$f(x,y)+g(x,y)$
Principle of Displacement	$e^{-j2\pi(au+bv)}F(u,v)$	$f(x-a,y-b)$
Principle of Similarity	$\dfrac{1}{\|ab\|}F\left(\dfrac{u}{a},\dfrac{v}{b}\right)$	$f(ax,by)$

Figure 1. The main characteristics of the Discrete Fourier Transform.

5. Basic process of digital image watermarking

The generation of watermarking, embedding location selection, embedding method design are important factors in the process of digital image watermarking. Digital image watermarking algorithms generally include three steps: generation of watermark image, digital watermarking embedding and digital watermarking extraction [7]. We can divide the digital watermarking basic process into three stages.

5.1. Generation of watermark image

According to the watermark content, digital image watermarking can be divided into meaningless watermarking and meaningful watermarking. The meaningless watermarking is usually a pseudo-random sequence, and the meaning watermarking means that the watermark itself is also a binary image or other images.

For meaningless watermarking, it is usually only possible to detect whether there is a watermark in the image, and meaningful watermarks can be extracted from the image by the detection algorithm and confirmed by observation.

Meaningless watermarking can be generated by a random text generator. For meaningful watermarking, it is common to use some pre-processing methods to encrypt the original watermark graphics, such as image scrambling or spread spectrum.

5.2. Watermarking embedding

Digital image watermarking embedding process can be given by

$$W' = F(O, K, W) \tag{9}$$

Where digital image can be described as O, K means the key of the embedding method, F represents the embedding method.

The image information W that represented the copyright of the carrier is combined with the carrier by the F method to obtain a new carrier W'.

Only the image watermarking algorithm designer can know the key of the embedding method and the embedding method. Once the image was theft, if somebody who wants to steal the important information but he has not the key of the embedding method, so he could not find the watermarking embedding method. In this way we can improve the confidentiality and security[8][9].

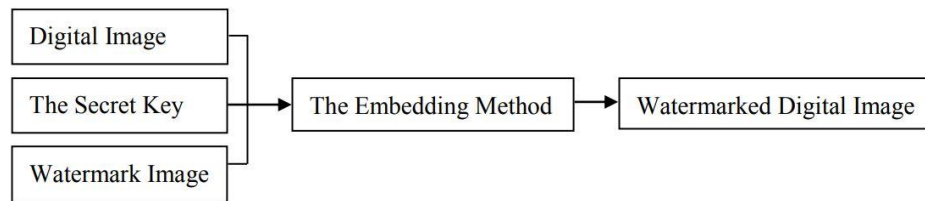The watermarking embedding can be expressed in figure 2.

Figure 2. Watermarking embedding.

5.3. Watermarking detection

According to the location of watermarking embedding, image watermarking embedding algorithm can be divided into two categories: spatial domain technology and transform domain technology. The spatial domain technology is relatively simple to implement, while the transform domain technology is more robust. Watermarking detection is usually used for meaningful watermarking information. The original watermark image is usually a binary image that contains the copyright owner's information, so it can be detected to indicate the owner of the protected image.

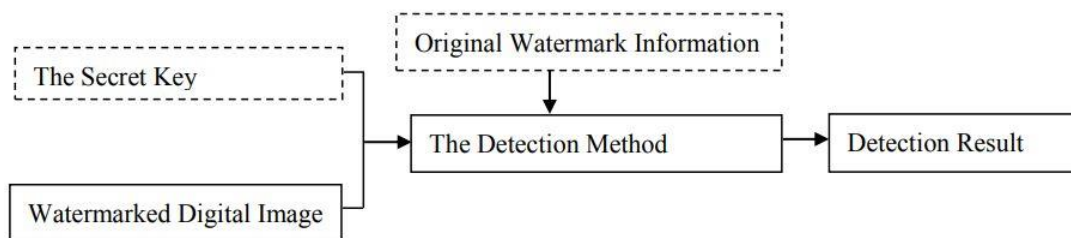Watermarking detection can be expressed in figure 3.

Figure 3. Watermarking detection.

6. Conclusion

Digital image watermarking technology is a research hotspot for copyright protection of digital multimedia works. The digital image watermarking technology not only has practical applications, it also has considerable economic value.

Different digital image watermarking algorithms have different characteristics. In practical applications, the advantages of digital image watermarking technology are fully utilized to meet different needs. There are still many deficiencies in the digital watermarking algorithm, which needs to be constantly improved in the development.

With the wide application of digital image watermarking technology, many researchers begin to regard it as an important research direction in the field of information security, but some problems still remain unsolved. For example, the comprehensiveness of the anti-attack ability of the watermarking system, the security of tampering detection in content authentication and so on.

Research on key techniques in digital image watermarking field has theoretical and practical significance.

Acknowledgments

References

[1]   Gu Y.F. (2009) Research on Digital Watermarking in Image Transform Domain.Zhejiang University Publishing, HangZhou.

[2]   Cox I, Miller M, Bloom J, Fridrich J, Kallker T.(2007) Digital watermarking and steganography. Morgan Kuafmann, San Mateo

[3]   Rosa A Asmara, Reza Agustina, Hidayatulloh.(2017) Comparison of Discrete Cosine Transforms(DCT), Discrete Fourier Transforms(DFT), and Discrete Wavelet Transforms(DWT) in Digital Image Watermarking. International Journal of Advanced Computer Science and Applications, 8:245-249.

[4]   Mohamed Hamidi, Mohamed El Haziti, Hocine Cherifi, Mohammed El Hassouni. (2018) Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform. Multimedia Tools and Applications., 77:27181-27214.

[5]   Yang L. (2019) Research on Digital Image Watermarking Based on Pubic Key Encryption. China University of Geosciences Publishing, Wuhan.

[6]   Kehtarnavaz, N. (2008) Digital Signal Processing System Design, 2nd ed. Elsevier: Cambridge, MA, USA.

[7]   Sun J, Yang J.Y, Fu D.S. (2011) Watermarking Algorithm for Color Images Based on Quaternion Frequency Modulation. Computer Science, 38:123-126.

[8]   Chang C.C, Lu T.C., Zhu Z.H, et al. (2018) An effective authentication scheme using DCT for mobile devices. Summetry, 10: 4–16.

[9]   Lai J, Deng R.H, Guan C. (2013) Attribute-based encryption with verifiable outsourced decryption. IEEE Transactions on Information Forensics & Security, 8: 1343–1354.