Research on Information Hiding Technology based on Digital Watermarking

Xiaoxing Ma[1],
[1] Tianjin Hexi District Zhujiang Road 25# TianjinUniversity of Finance & Economics, 300222, Tianjin
[a]xxingl@163.com,

Abstract. The Internet is becoming more and more dependent on digital images and video. As a new technology to protect the information security, Information hiding provides a new direction for the research. Information hiding technology has important value for research and application in Internet hidden communication field, especially in the urgent need to solve copyright protection, information security and other aspects. This paper presents a comparative analysis of the algorithm to implement the information hiding technology; the algorithm based on DCT provides more security and data authentication compare to other digital watermarking approach.

Keywords: Information Hiding. Digital Watermarking. DCT.

Introduction

With the rapid development of communications network technology and the popularization of e-government and e-commerce, especially with the continuous increase of network bandwidth that support the development of the Internet, more and more multimedia files participate the development of the Internet for meet user's communication needs continuously. The Internet is becoming more and more dependent on digital images and video. As a new technology to protect the information security, information hiding provides a new direction for the research. Advanced information hiding technology makes hidden information not only able to withstand detection of human sensory organs and instruments, but also resists various artificial intentional attacks. The multimedia-based Information hiding technology has important value for research and application in Internet hidden communication field, especially in the urgent need to solve copyright protection, information security and other aspects.

Digital Watermarking

Watermarks are not printed watermarks, but digital watermarks-- Digital media like video and audio embedding a certain amount of information, digital watermarking is the behavior hide the relevant information within digital signal, such digital signals can be images, audio or video signals. An important application of watermarking is to authenticate object owners. Traditional protection of rights, usually add the protection of the rights of the label in each picture or song, after the development of digital watermarking technology, digital watermarking methods are usually used to replace the traditional copyrights protection methods by embedding copyrights protection contents to pictures and songs. For example, digital watermarking of a digital work, such as an image or video, can make this image or video coordinate very different to crack without sacrificing visual effects. Therefore, the research on digital watermarking is very valuable, especially in the applications related to copyright protection and infringement. Another application of digital watermarking is the tracking of transactions. In this case, the watermark is usually embedded in each copy of the place where the transaction took place, so as to implement the recording and tracing of transaction details. In this way, the application of transaction tracking can be implemented very simply and conveniently.

Copyright Protection. Digital watermark is divided into visible watermark and invisible watermark. Visible watermark achieves the purpose of protecting the copyright of the carrier. The embedded information enables people to effectively identify the copyright of digital media to possessor. The embedded watermark can not affect the commercial value of the carrier, and

watermark information can be extracted from the watermarked carrier signal when necessary, its main purpose is to identify copyrights and prevent illegal use. But more often, the watermark is invisible.

In recent years, copyright protection for multimedia files has become an increasingly important part of the development of the Internet. Therefore, how to ensure the copyright of digital images has become a new topic for watermark embedding algorithms. Up to now, over 95% of global network multimedia file information is processed using copyright protection technology among them; digital watermarking technology has become an indispensable basic technology. The encrypted watermark embedded in the original image without affecting the recognition by human eyes for the watermark technology is adopted, so for digital image copyright protection, digital watermark embedding has become an important technical measure for copyright protection of Internet multimedia files. The embedding of digital watermarks has become one of the most important techniques for copyright protection of multimedia files on the Internet.

Covert communication. Covert communication and encryption are different: encryption is to hide the contents of confidential communications; while concealment conceals that confidential communications are in progress, and it is a deeper level of confidentiality. Encryption algorithms garbled meaningful content and people can't understand it. However, people can't read it, and at the same time, it also prompts people that this is an "unusual thing," and takes a variety of cipher code cracking methods. In the Internet era, or the multimedia era, the data on the Internet is images, video, and audio. How to embed secret information into common images, videos, and audio in an imperceptible manner to covert communications is currently the mainstream of information encryption research. In order to avoid this hidden danger, network encryption technology came into being. However, technologies have transformed information into various garbled types; attract some challengers who want to seek stimuli. Faced with such problems, researchers have invented electronic information hiding technology to make those secret information and ordinary information look the same, to greatly enhance the security performance of the spread on the Internet.

Digital Watermarking Algorithm

Digital watermarking technology already can used to protect various intellectual property rights. It can mark multimedia data (including digital images, text documents, video and audio) and hide the secret information in data. This hidden information is invisible, so the appearance is the same as the original data. In addition, this hidden information can neither be deleted nor destroyed by other algorithms. Any watermarking technique should exhibit at least the following four desirable characteristics:

1) Readability: Watermarks should convey as much information as possible so that ownership and copyright can be implicitly determined.
2) Security: The watermark should be secret and must not be detected by unauthorized user.
3) Imperceptibility: The watermark should not introduce any perceptible original artifacts.
4) Robustness: Watermarks should not be removed after attack. It should be able to withstand various tests such as distortion, cropping, JPEG compression and various other geometric operations.

LSB Algorithm. The simplest covert communication method is the LSB (Least significant bits substitution) algorithm, replacing the least significant bit of the original image pixel with binary secret information. Assuming there are three pixels in the original image, the pixel values are 130, 123, and 117, respectively, their least significant bits are 0, 1, and 1; In order to hide the secret data 1, 0, 1, the pixel values may be modified to 131, 122, 117 so that the least significant bit of the modified pixel value is 1, 0, 1; After the image is transmitted over the Internet, the receiver extracts 1, 0, and 1 according to the least significant bits of 131, 122, and 117 to complete the covert communication.

The embedding of the watermark does not embed all the data information into the picture at one time, but divides the picture into blocks by size (a block is the three lines of the picture), at the same time the watermark data is also divided into the same number of blocks, so that the data

embedded in each part of the image is the same, increasing the difficulty of extraction. When embedding a watermark, we check whether the image (ie, the bearer) can load the embedded data first, if it can't indicate an error and exit message. If the first block is operated, the length of data to be load is coded first, this way is similar to the length encoding method in the Bit Mapping. After the encoding is completed, the length encoding is scrambled by CBF and embedded in the image. Whether it is the length code or the load data is followed the line draw algorithm, which selects certain data points in the data block according to the rule of drawing lines in the embedding process. After the length encoding is completed, the program will read the watermark data and continue to embed the CBF scrambled data into the image according to the line drawing algorithm, after a data block is embedded, the program will loop to the next data block to continue embedding the data until all the data is embedded.

DCT Algorithm. DCT (Discrete Cosine Transform) is currently the most studied digital watermark. DCT algorithm is a technique based on the transform domain algorithm, can embed large amounts of bit data without causing perceptible defects. It is characterized by strong robustness and good concealment. It is to select the middle and low frequency coefficients to superimpose the watermark information on the DCT transform domain of the image. The reason for choosing the medium and low frequency coefficients is that the perception of the human eye is mainly concentrated in this frequency band. In the process of destroying the watermark, the attacker will inevitably cause serious degradation of the image quality, and the general image processing process will not change this part of the data. Since the core of compression algorithms such as JPEG and MPEG is to quantize data in the DCT transform domain, the watermark can resist lossy compression by integrating the watermarking process and the quantification process skillfully. In addition, the statistical distribution of DCT transform domain coefficients has a better mathematical model, which can estimate the amount of watermark information theoretically.

1. DCT watermark embedding algorithm

The basic idea of the DCT watermarking algorithm is to first divide the original image into 8×8 sub-blocks, and perform discrete cosine transform on each sub-block separately to convert them into 64-bit DCT coefficients. The position of the DCT transform coefficients to be embedded is selected according to a certain principle, and embeds the watermark information by mathematical operations, then operate DCT inverse-transform in the sub-blocks embedded the DCT coefficients with the watermark information, and synthesized into the embedded watermark image. The DCT expression is:

$$Y(u,v) = a_0 c(u,v) \times \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} X(x,y) \cos\frac{(2x+1)u\pi}{2N} \cos\frac{(2y+1)v\pi}{2N} \quad (1)$$

Its IDCT (Inverse Discrete Cosine Transformation) expression is:

$$X(x,y) = a_1 \times \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} c(u,v) \cos\frac{(2x+1)u\pi}{2N} \cos\frac{(2y+1)v\pi}{2N} \quad (2)$$

2. Algorithms Based On Visual Cryptography Scheme.

Scholars design related optimization algorithms for digital watermark embedding based on Visual Cryptography Scheme (VCS). This scheme does not require any cryptographic calculations, encrypt the watermark image and embed a color concealment image, improve the security and robustness of the watermark image effectively. This digital watermarking scheme has high security, no pixel expansion, and strong anti-attack performance. The scheme divides the watermark image into two watermark sharing images, one watermark sharing image is embedded in the carrier image by DCT (Discrete Cosine Transform) transform, and the other is stored by the copyright owner. When the copyright is authenticated, the watermark-sharing image in the carrier image is extracted

by the IDCT (Inverse Discrete Cosine Transformation) transform and superimposed with the watermark saved by the copyright owner, and the original watermark image can be recovered.

In the (k,n) VCS, a secret image is divided into n parts shared images, each of which is a random, meaningless binary noise image. Superimposing any k or more shared images can restore the original secret image. However, if the number of shared images is less than k, then any information about this secret image cannot be obtained. In consideration of the characteristics of the human visual system (HVS), the watermark image is embedded in the blue portion of the color image, because human beings are the least sensitive to changes in the blue portion of the color image.

Watermark embedding steps are as follows:

(1) The image S to be protected is divided into two shared images S1, S2 by using the XOR operation based on VCS,

(2) Extract the blue part from the color image and decomposed into separate 8×8 sub-blocks,

(3) Operate the DCT transform on sub-blocks to obtain a DCT coefficient matrix.

(4) Embed S1 in the blue part,

(5) Restore the hidden watermark image from S2 to protect copyright,

(6) The color image is obtained by IDCT transform to the blue part embedded with the watermark.

This algorithm combines VCS and digital watermarking technologies to implement copyright protection efficiently. The algorithm has good practicality. The algorithm has highly robust and can resist common attacks such as JPEG compression and white noise. Compared with the traditional watermark technology, combining the visual cryptography technology to process the watermark is the innovation of this algorithm. The algorithm has high security; attacker extracts the share image with watermark and still cannot get any information about the watermark image. The algorithm uses XOR algorithm, so that the restored watermark image has good quality and no pixel expansion; this algorithm extends the application of digital watermarking technology and has a good development prospect.

Conclusion

From the research of many previous scholars, it is not difficult to see that although the above-mentioned means can be used to separate the frequency domain of useful images further; however, when it reaches a certain limit, the robustness and effectiveness of the watermark embedded image cannot be further improved. So in image processing and digital watermarking, scientists now study new algorithms for information hiding based on wavelet analysis, in order to achieve its discrete fast algorithm. Therefore, a more robust and effective digital watermarking algorithm is designed.

In the field of digital signal processing, there are many ways to accomplish the spatial-to-frequency conversion of the image. In the future, the kernel function in the wavelet will be adjusted appropriately; the image will be processed transform in the frequency domain. The digital watermarking algorithm has better performance for admission to Key through the transformation.

Information hiding technology has very precious application value and will have a broader future. However, it is still imperfect; researchers should clearly understand the advantages and disadvantages, and improve the information hiding technology continuously, so that they can serve the country, society and everyone more effectively.

References

[1] Wan X, Liu F. Study on audio digital watermarking technology based on DC component of DCT domain in military communication[J]. Modern Electronics Technique, 2017.

[2] Kong L J, Nie P. A holographic digital watermarking technology based on DWTDCT transform domain[J]. Journal of Optoelectronics·laser, 2016.

[3] Dong S, Li J, Liu S. Frequency domain digital watermark algorithm implemented in spatial domain based on correlation coefficient and quadratic DCT transform[C]// International Conference on Progress in Informatics and Computing. IEEE, 2017:596-600.

[4] Singh P, Agarwal S. A self recoverable dual watermarking scheme for copyright protection and integrity verification[J]. Multimedia Tools & Applications, 2017, 76:1-40.

[5] Al‐Maweri N A A S, Adnan W A W, Ramli A R, et al. A hybrid digital image watermarking algorithm based on DCT‐DWT and auto‐thresholding[J]. Security & Communication Networks, 2016, 8(18):4373-4395.

[6] Narula R, Chaudhary M M. Digital Image Watermarking[J]. Journal of Shanghai Jiaotong University, 2016, 1(5):1 - 6.

[7] Pardhu T, Perli B R. Digital image watermarking in frequency domain[C]// International Conference on Communication and Signal Processing. IEEE, 2016.

[8] Sharma P K, Sau P C, Sharma D. Digital image watermarking: An approach by different transforms using level indicator[C]// Communication, Control and Intelligent Systems. IEEE, 2016:259-263.

[9] Wang C. Research of, digital image watermarking algorithm based on DCT[C]// Eighth International Conference on Digital Image Processing. International Society for Optics and Photonics, 2016:1003333.