Advances in Social Science, Education and Humanities Research, volume 234
3rd International Conference on Education and Development (ICED 2018)

Application of Digital Watermarking Technology on Copyright Protection of Library Digital Resources

Feng-Mei WU
Library of Jiangsu University of Science and Technology, Zhengjiang, 212003, China
wufm65@163.com,416199207 @qq.com

Keywords: Digital Watermarking, Digital Library, Copyright Protection.

Abstract. In recent years, with the development of Digital Library and network technology, the reproduction of digital Resources of books and materials, such as the use of communication network, has become more and more popular. The copyright protection of digital library has also been paid more and more attention by the academic circle. In this paper, a robust watermarking technique based on DCT transformation is introduced to illustrate the application of digital watermarking technology in copyright protection of library digital resources. The experimental results show that using digital watermarking technology can protect copyright and information security and solve the copyright protection problem of digital library.

Introduction

Digital library is a library that stores and processes documents of various kinds of pictures, texts and audio-visual materials. It is also a distributed information system made by multimedia, including processing, storage, retrieval, transmission and utilization of information resources. It is built on the basis of network environment. It can realize cross regional and object oriented network query and communication without the limitation of time and space. It relieves the contradiction between the literature service of University Library and the information demand of readers. Because of the rapid development of computer technology and network technology, the copying, downloading and piracy of digital works have become easier. The problem of intellectual property protection is more complex and prominent than traditional paper documents. This requires a kind of technology to effectively protect copyright and security. Digital watermarking technology just solved this problem. It is mainly used for copyright protection of digital products and authentication of authenticity and integrity. It is one of the fastest developing hot technologies in the field of multimedia information security.

Digital watermarking technology is to embed some identification information (digital watermarking) into the data carrier (such as image, sound, video, document, software and other digital media), and does not change the appearance of the original information, and does not affect the normal use of the original data. These digital watermarks are hidden in the original information and are not easy to be detected and modified to protect data security, copyright authentication, anti-counterfeiting traceability purposes [1].

Digital watermarking technology is a kind of information hiding technology, which is used to mark and identify the digital works, instead of protecting the digital works from unauthorized access, which belongs to the post protection means [2]. The secret information can be copyright identification, user serial number or product related information. In order to prevent the normal data manipulation technology from destroying the hidden information, the digital watermarking

technology should have the characteristic that it is not easy to be destroyed by the normal data manipulation. The characteristics of digital watermarking as fellow [1, 2]:

(1) Concealment. Also known as insensibility, that is, under normal circumstances, digital watermarking is invisible. After embedding watermark, the quality is not degraded without affecting the visual effect.

(2) Robustness. Digital watermarking must be difficult to remove, and any attempt to destroy or eliminate watermark will cause the carrier to be seriously degraded and unusable.

(3) Anti-tampering. After embedding digital watermark into the carrier, it is difficult for attackers to alter or forge it.

(4) Watermark capacity. Watermarking capacity refers to the information capacity of a digital carrier that can be embedded without pre-distortion. In the field of covert communication, the capacity of watermark is very large.

(5) Security. Digital watermark information should be secrecy and security, and at the same time, it has a low false detection rate. When the original data is change, the digital watermark should also change, so as to detect the change of original data.

According to the implementation technology of watermarking, watermark can be also divided into two categories: spatial domain algorithm and frequency domain algorithm. The spatial algorithm is to modify the pixel value directly and embed the watermark information in the brightness or color band of the image. The typical algorithm is the minimum effective bit (LSB) algorithm. The advantages of this method are large in information and have good invisibility. Amit Singh et al. Proposed an improved LSB algorithm. The frequency domain algorithm uses some mathematical transformations to represent the image in the transform domain. By changing some transform coefficients of the image, the watermark is embedded, and the inverse transform is used to generate the image containing the watermark. At present, the existing methods mainly focus on discrete wavelet transform (DWT), discrete cosine transform (DCT), discrete Fourier transform (DFT), and so on. This kind of method has good robustness and can resist a certain intensity of attack. It is suitable for the copyright protection of Digital Library's digital works. It has high robustness [3-9] while ensuring the transparency and security of digital watermarking. Li, Yongzhong and so on, proposed an adaptive blind watermarking algorithm [1]. A digital watermarking algorithm for block image wavelet transform was proposed, and Okkyung Choi et al [6]. Proposed a DCT domain watermarking algorithm for anti geometric attack [8]. Li Yongzhong and so on proposed a multi-resolution digital watermarking algorithm based on DWT. The following is an example of robust watermarking algorithm based on DCT domain to illustrate the embedding and extraction process of digital watermark.

Watermark Preprocessing

Before insertion process, the watermark signal should be preprocessed(image disorder) at first for increasing the security of the watermarking system as well as enhancing the robustness against some geometric attacks such as image cropping operation. Arnold transformation is chosen to disorder the water-mark here due to its good disorder effect and simple theory. For a $N \times N$ digital image with coordinates $x, y \in \{0,1 \cdots N-1\}$, Arnold transformation can be described as [1, 9]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\, N) \tag{1}$$

where $(x, y)^T$ and $(x', y')^T$ are the input and output coordinates respectively. We define $n(n = 0,1,2..)$ as the iterative frequency, and the iteration process can be re-presented symbolically by [9]:

$$P_{xy}^{n+1} = AP_{xy}^{n} (\mathrm{mod}\, N) \tag{2}$$

where $P_{xy}^{0} = (x, y)^T$, $A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$.Watermark preprocessing is finished when all the coordinates are covered in this iteration process. System safety will be surely increased as the secret key ($key = n$) is used in watermark extraction.

Watermark Embedding and Extraction

Watermark Embedding

Step-1: Divide the host image (M×M) into disjoint 8×8 blocks.

Step-2: Calculate the 64 DCT coefficients in each block by DCT. All these coefficients are then further quantized to integers d_{ijk} using q_{ij} :

$$d_{ijk} = R\left(\frac{c_{ijk}}{q_{ij}}\right) \tag{3}$$

where R denotes the integer round operation and c_{ijk} is the ij^{th} DCT coefficient of the k^{th} block

Step-3: Arrange the quantized coefficients in zigzag manner denoted by $Z_k(i), 0 \le i \le 63, k = 1,..., B$, where B is the number of the total blocks [1]. Let $i0$ be the embedding position in the coefficient block. We define the embedding unit as M (presented in Fig.1) and gain M_1 by setting M in ascending order.

8×8 DCT block 1 $Z_1(i0)$	8×8 DCT block 2 $Z_2(i0)$
8×8 DCT block 3 $Z_3(i0)$	8×8 DCT block 4 $Z_4(i0)$

Figure 1. An embedding unit

$$M = [Z_1(i0), Z_2(i0), Z_3(i0), Z_4(i0)] \tag{4}$$

We also define a normalized masking set as follows

$$M_\alpha = \{\alpha_j(i0),\ j \in 1,2,3,4\} \tag{5}$$

where $\alpha_j(i0)$ is the normalized masking .

Step-4: A single bit w is embedded as follows: First find p to meet $M_1(p) = Z_1(i0), 1 \le p \le 4$, then

While $w=1$, $Z_1^*(i0) = \max\{\bar{M} + \alpha_1(i0), Z_1(i0) + \alpha_1(i0)\}$, where $\bar{M} = (Z_2(i0) + Z_3(i0) + Z_4(i0))/3$, $Z_j(i0)$ and $\alpha_j(i0)$ have been presented in eq.(4)and eq.(5) separately.

If $p \neq 4$, find a set of $Z_j(i0)$ when $Z_j(i0) = M_1(p^*), p^* = p+1, \cdots, 4;$

Then $Z_j^*(i0) = Z_j(i0) - \alpha_j(i0), j \in 2,3,4$.

Else $p=4$, no more modification is needed.

While $w=0$, $Z_1^*(i0) = \min\{\bar{M} - \alpha_1(i0), Z_1(i0) - \alpha_1(i0)\}$

If $p \neq 1$, find a set of $Z_j(i0)$ when $Z_j(i0) = M_1(p^*), p^* = 1, \cdots, p-1;$

Then $Z_j^*(i0) = Z_j(i0) + \alpha_j(i0), j \in 2,3,4$

Else $p=1$, no more modification is needed.

Step-5: Replace $Z_j(i0)$ with $Z_j^*(i0)$, $j=1,2,3,4$. Then apply the above procedure to all the four adjacent blocks orderly, and the watermarked image can be obtained by IDCT at last.

Watermark detection

The first three steps are exactly the same as that in the embedding procedure. Suppose that I^* is the attacked water-marked image and $\bar{M}'$ is calculated from M' (Fig.1) in the same way as in step-4. Then the watermark w can be extracted according to the following rule [1, 9]:

If $Z_1'(i0) > \bar{M}'$, then $w=1$; else ($Z_1'(i0) \le \bar{M}'$), $w=0$.

To check the similarity between the embedded watermark (W) and the extracted one (W^*), a correlation measured between them can be found using [1, 6]

$$\rho(W, W^*) = \frac{W \cdot W^*}{\sqrt{W^* \cdot W^*}} \tag{10}$$

where $W \cdot W^*$ is the scalar product between these two vectors.

Experimental and Results

The watermark signals are 32×32 two-value images (shown in Fig.2) and the original gray images are of 512×512×8bit. The embedding positions $i0$ mentioned below are all in zig-zag manner. The results of "Lena" in Fig.3 with embedding position $i0=14$.

Figure 2. Signatures watermark image

Figure 3. Original images (left), watermarked images (middle) and its watermark signal (right)

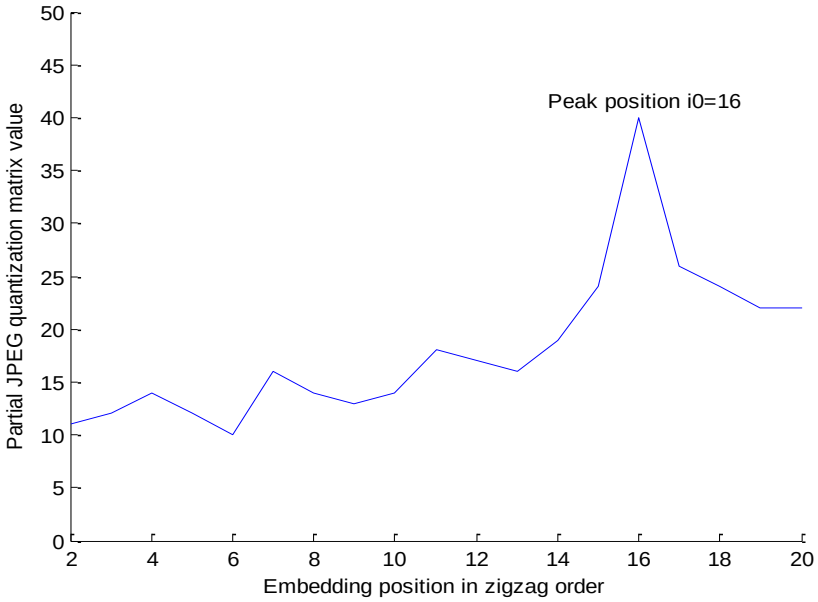

Figure 4. Partial JPEG quantization matrix

The quantized values of low frequency components using JPEG QM are usually larger than that of mid-frequency ones. So the normalized masking is affected differently when $i0$ is selected from these two areas respectively. This also implies that the system performance is close relative to JPEG QM (partially plotted in Fig.4). Fig.5 shows the PSNR of "lena", "plane", "man" and "couple" with no attack as $i0$ alters from 2 to 20.

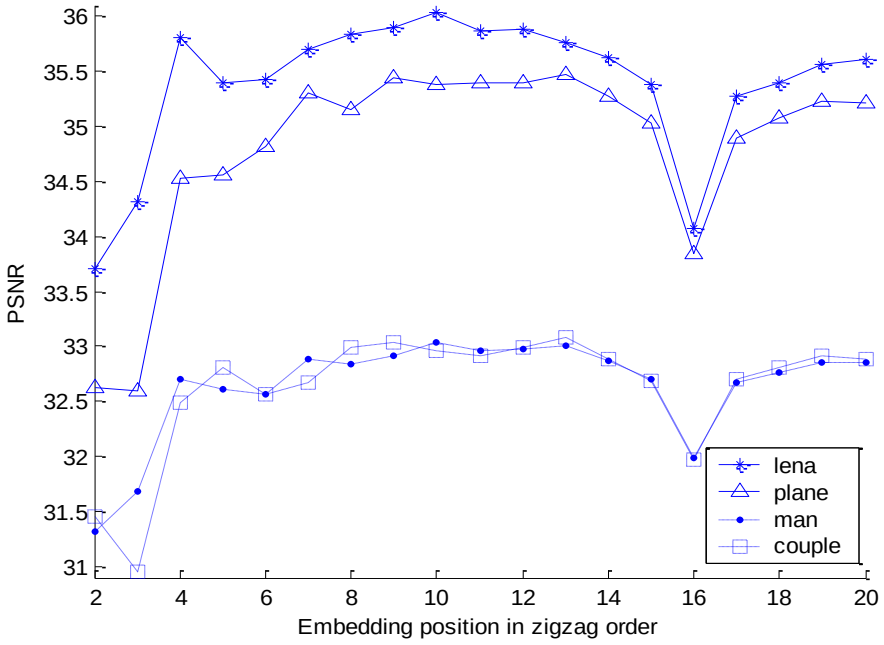

Figure 5. PNSR with different embedding positions

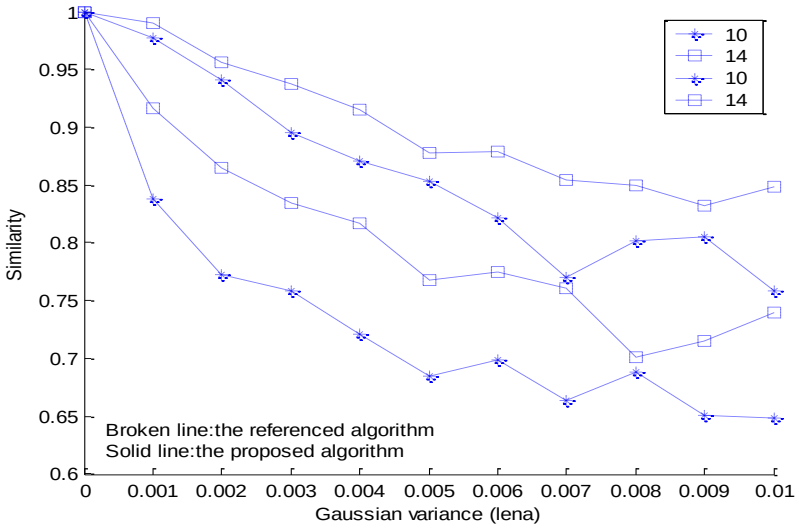

Figure 6. Comparison of Gaussian noise with different variance. Embedding positions are 10 and 14 (lena)

Embedding intensity can be maximized according to the characters of HVS and the host image. This allows more than one block (in four-adjacent-blocks) to insert the normalized masking along with the actual condition of M (Fig.1). This brings obvious robustness improvement against common attacks such as Gaussian noise and JPEG, etc. Fig.6 present the robustness comparison of Gaussian noise between the proposed algorithm and reference [9] with different inserting positions and different Gaussian variance respectively. Solid and broken lines denote the presented and referenced strategy separately. It is clearly that no matter

changing the embedding position or Gaussian variance, robustness of the proposed system is apparently higher than that of the referenced. JPEG robustness comparison with different JPEG quality factor (Q) is shown in Fig.7 and obvious improvement to JPEG compression is also be easily found (particularly when Q is less than 30).

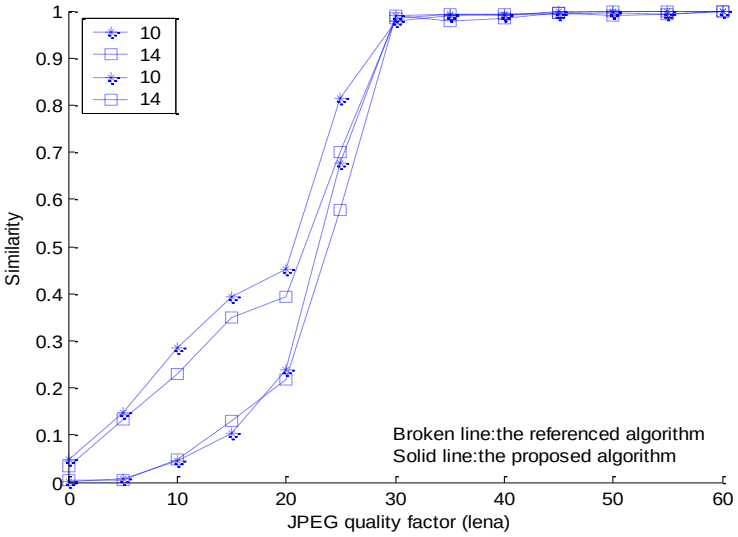

Figure 7. PNSR with different embedding positions

Robustness Performance

Table Ⅰ gives PSNR/similarity of watermarked images with none and different attacks. The mark for "lena" and "man" is Mark1, and that for "couple" is Mark2 (see Fig.2). The first row of Table denotes the case without any attack, the 2-4th and 5-6th row present three typical filters and two different noise separately. The 7th row corresponds to JPEG compression (Q=30), and the last three rows give the results with respect to histogram equalization, gamma enhancement and 1/4 cropping respectively. All the extracted watermarks from Lena are shown in Fig.8.

Table 1. PSNR of watermarked images under various attack

Attacks	Test Image/Watermark Signal			
	Lena/ Mark1	Man/ Mark1	Couple/ Mark2	Lax/ Mark 2
none	35.62/1.00	32.87/1.00	32.93/1.00	28.48/1.00
Mean filter 3×3	34.12/0.95	30.56/0.96	29.34/0.95	24.97/0.92
Median filter ***3×3***	34.96/0.95	31.48/0.94	30.16/0.95	25.26/0.90
Sharpen filter	22.80/0.90	22.60/0.90	22.66/0.89	21.96/0.89
Gaussian noise Var=0.005	21.37/0.89	21.25/0.88	21.20/0.86	20.51/0.85
Salt &Pepper D=0.025	32.96/0.98	30.00/0.97	29.90/0.97	25.54/0.97
JPEG Q=30	23.34/1.00	20.64/1.00	19.82/0.99	16.66/0.99
Histogram equalization	15.73/0.99	12.48/0.99	13.78/0.99	8.57/0.98
Gamma enhancement	14.24/1.00	13.57/1.00	13.90/0.99	12.53/1.00
1/4 cropping	12.41/0.75	9.93/0.75	12.00/0.76	9.09/0.75

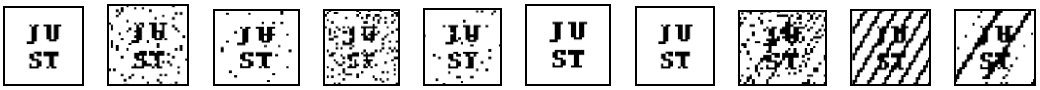

Figure 8. Detected watermark images of Lena under various attacks listed in Table Ⅰ

Note: The detected watermark images of Lena, from left to right correspond to no attack, 3×3 mean filtering, 3×3 median filtering, sharpen filter, Gaussian noise (variance=0.005); 2-th line from left to right correspond to salt & pepper (D=0.025), JPEG compression (Q=30), histogram equalization, gamma enhancement, and 1/4 cropping.

Conclusion

Digital watermarking plays an important role in the big data times. It can provide copyright protections of digital library resources. In this paper, we propose a compressed DCT domain watermarking algorithm based on four-adjacent-blocks. Computation is simplified by using the deduced normalized masking and embedding position is selected according to the JPEG quantization matrix. Experimental results indicate that the proposed scheme is resistant to common image processing operation (such as mean filter, median filter, etc) and especially performs higher robustness to Gaussian noise and JPEG compression than that of the referenced method. Moreover, the presented method does not require access to the original image during extraction process, and can be extended to video watermarking.

Acknowledgement

This research was financially supported by Jiangsu provincial university fund project (13KJD52004) and Jiangsu postgraduate research innovation project (CXLX13_70, KYCX17_1845).

References

[1] Yongzhong Li, Hua Zhu, Ruiqing Yu. An Adaptive Blind Watermarking Algorithm Based on DCT and Modified Watson's Visual Model, 2008 International Symposium on Electronic Commerce and Security (ISECS 2008), Guangzhou, China, 4-5 August 2008

[2] Feng Deng-Guo, ZHANG Min, Li Hao . Big Data Security and Privacy Protection, Chinese Journal of Computer, Vol.37, pp.246-2553, Jant, 2014

[3] Zekeriya Erkin, Gene Tsudi, Private computation of spatial and temporal power consumption with smart meters, in: Applied Cryptography and Network Security, Springer, Berlin, Heidelberg, 2012, pp. 561–577.

[4] Arezou Soltani Panaha, Ron van Schyndel, Timos Sellis. Towards an asynchronous aggregation-capable watermark for end-to-end protection of big data streams, Future Generation Computer Systems, 72 (2017) 288–304

[5] Chetna, "Digital Image Watermarking using DCT," A Monthly Journal of Computer Science and Information Technology, Vol.3, Issue.9, pages 586–591, September 2014.

[6] Yang-Wai Chow, Willy Susilo, Joseph Tonien and Wei Zong, "A QR Code Watermarking Approach based on the DWT-DCT Technique," 22nd Australasian Conference on Information Security and Privacy, 2017.

[7] B. Tao and B. Dickinson, "Adaptive watermarking in the DCT domain", in IEEE International Conference on Acoustics, Speech, and Signal Processing, pp.2985-2988, April.21-24, 1997.

[8] C. Y. Lin and S. F. Chang, "A robust image authentication method distinguishing JPEG compression from malicious manipulation", in IEEE Transactions on Circuits and Systems for Video Technology, pp.153-168, Feb, 2001.

[9] W.Luo, G.L.Heileman and C.E.Pizano,"JPEG domain watermarking", Proc. SPIE, Vol.4684, pp.980-985, May, 2002.