Watermarking Algorithm Research and Implementation Based on DCT Block

Gengming Zhu, and Nong Sang

***Abstract*—**In this paper the watermarking programs based on the discrete cosine transform (DCT) domain DC component (DC) is adopted. Through adjusting the block DCT coefficient of the image the watermarks are hidden. And blocking the selected image according to 8×8 pixel, then dividing the selected image into four non-overlapped sub image blocks according to 4×4 pixel, and thus the watermarks are embedded through adjusting their DCT coefficient. The experimental results show that the method has strong robust.

***Keywords*—**Digital Watermark, DCT, Direct Current Component, JPEG.

I. Introduction

ALONG with with digital technology and Internet development, all kinds of multimedia digital products (image, video frequency and audio frequency) are released by network mode, and however, digital products' convenience and unreliability coexist. It is very urgent to protect digital products by many ways and so research of digital watermark technology is rapidly developed.

The paper adopts video frequency watermark proposal based on discrete cosine transform (DCT) domain DC component (DC). In DCT domain, DC component is more suitable to embed watermark than AC component (AC). Firstly, DC component has larger perceptual capacity, after embedding watermark, it doesn't cause obvious change for visual quality of original image; secondly, signal processing and noise interference have smaller influence for DC component than AC component.

II. Concept and Principle of Digital Watermark Technology

Digital watermark is to embed hidden marker in digital multimedia data by signal processing method, the marker is generally unobservable, which is only drawn by special detector or reader. The basic idea for digital watermark is to use human's insensitive perceptual organs and redundancy in digital signal and embed secret information in digital products, such as image, audio frequency and video frequency in order to easily record its copyright, and in addition, the embedded information survives after fighting back some attacks so as to reach copyright authentication and protection functions. Digital watermark doesn't change digital products' basic characteristic and using value.

A complete digital watermark system is composed of two parts, watermark creation, embedding and watermark picking up/inspection. Watermark embedding algorithm uses symmetric key or public key to embed watermark into original carrier information and then gets secret carrier. Watermark picking up/inspection algorithm uses corresponding key to inspect or recover watermark from secret carrier, without decryption key, attackers difficultly find and revise watermark from secret carrier. The watermark is composed of many models, such as random digital sequence, digital identification, text and image, etc.

A. Watermark Embedding Model

Before watermark signal embedding, with the consideration of robustness and safety, many watermark systems are always randomized and encrypted. Suppose that *I* is digital image, *W* is watermark signal, *K* is key and the processed watermark *W'* is defined by function *F*. As the (1):

$$W^{'} = F(I, W, K) \tag{1}$$

If watermark owner doesn't want others to know watermark, the function F should be irreversible, such as typical DES encryption algorithm, which is a general method combined watermark technology with encryption algorithm for the purpose of improving watermark reliability, safety and generalization. Suppose watermark embedding function *E*, original data *I* and watermark *W'* (*W'* is for (1)), I_w with watermark data objective is:

$$I_w = E(I, W^{'}) = E(I, F(I, W, K)) \tag{2}$$

Watermark embedding process is as Fig. 1, digital watermark embeds in original data to get watermark data through certain watermark embedding algorithm and key is used to improve watermark information safety.

Gengming Zhu is with the Institute for Pattern Recognition and Artificial Intelligence, Huazhong University of Science and Technology, Wuhan, Hubei Province,430074, P.R.China, and with Department of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, Hunan Province, China (phone: +86-13973205935; e-mail: gengmingzhu@gmail.com; hnustcs@163.com).

Nong Sang is with the Institute for Pattern Recognition and Artificial Intelligence, Huazhong University of Science and Technology, Wuhan, Hubei Province, China.

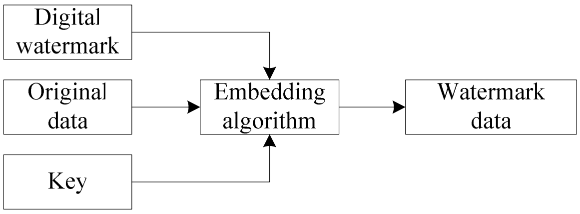

Fig. 1 Watermark embedding process

B. Watermark Picking up Model

For integrity confirmation and sophistication prompt application, accurately pick up the embedded watermark information to confirm multimedia data integrity through watermark integrity. For whether need original data while watermark picking up, watermark is divided into bright watermark and blind watermark. Suppose *W'* is the detected watermark, *D* is watermark picking up algorithm and $I_W^{'}$ is watermark carrier data after being attacked during transportation.

(1) Bright watermark: need original data for watermark picking up, through watermark picking up algorithm, the picked up watermark information can be got from watermark data and original data. W' can be expressed as:

$$W' = D(I'_W, I, K) \tag{3}$$

Bright watermark picking up process is as Fig. 2.

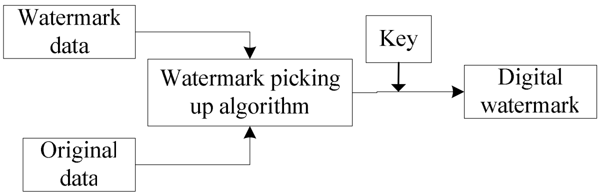

Fig. 2 Bright watermark picking up process

(2) Blind watermark: don't need original data for watermark picking up, through watermark picking up algorithm, directly get watermark information from watermark data, and *W'* is expressed as:

$$W' = D(I'_W, K) \tag{4}$$

Blind watermark picking up process is as Fig. 3.

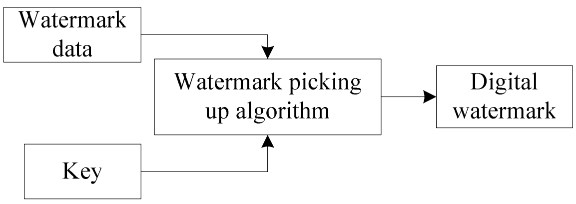

Fig. 3 Blind watermark picking up process

III. Watermark Embedding Based on Discrete Cosine Transform

Discrete Cosine Transform—DCT is a general orthogonal transform for digital image processing and signal processing, with such advantages, as high compression ratio, small bit error rate, good information integration ability and good synthetic effect of calculation complexity and it is one of central technologies of image encoding and technical base used for several standards of multimedia video frequency compression (H. 261, H. 263 and MPEG, etc.). Compression video frequency watermark algorithm based on DCT doesn't need additional transform to get spectrum distribution of video frequency, but effectively withstands influence of DCT coefficient quantification coding, so it has important research meaning and application foreground.

A. One-dimensional DCT

One-dimensional DCT definition is as (5) and (6):

$$F(0) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} f(x) \tag{5}$$

$$F(u) = \sqrt{\frac{2}{N}} \sum_{x=0}^{N-1} f(x) \cos\frac{2(x+1)u\pi}{2N} \tag{6}$$

Wherein, F (u) is No. u cosine transform coefficient, u is general frequency variable, u=1, 2, 3…., N-1; if f(x) is M sequence of time domain, x= 1, 2, 3,…, N-1, one-dimensional inverse discrete cosine transform is as (7):

$$f(x) = \sqrt{\frac{1}{N}} F(u) + \sqrt{\frac{2}{N}} \sum_{x=0}^{N-1} f(x) \cos\frac{2(x+1)u\pi}{2N} \tag{7}$$

B. Two-dimensional DCT

The definition of two-dimensional DCT is as (8):

$$f(x,y) = C(u)C(v) \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} F(u,v) \cos\left[\frac{(2x+1)u\pi}{2N}\right] \cos\left[\frac{(2y+1)v\pi}{2N}\right] \tag{8}$$

The definition of two-dimensional inverse discrete cosine transform is as (9):

$$F(u,v) = \frac{2}{N} C(u)C(v) \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y) \cos\left[\frac{(2x+1)x\pi}{2N}\right] \cos\left[\frac{(2y+1)y\pi}{2N}\right] \tag{9}$$

Where in, $C(\omega) = \begin{cases} 1/\sqrt{2} & \omega = 0 \\ 1 & \omega = 1,2,3,\cdots,N-1 \end{cases}$, *N* is horizontal and vertical pixel number of pixel block, generally N=8. If N is more than 8, efficiency is increased a little but complexity is increased many. 8*8 two-dimensional data block is changed to 64 transform coefficients after DCT, which have definite physical meaning. For example, when u=0 and v=0, F(0,0) is the average of 64 values, equal to DC component with good robustness; along with u and v increasing, corresponding coefficients are AC coefficients, respectively representing gradually increased horizontal space frequency and vertical space frequency components, that is, share size of the component in original image signal. And then DCT has a very important nature: after DCT, important visual information of the image is centralized in small par domain.

C. DCT Domain Coefficient Analysis

In DCT domain, different DCT coefficients have different influences for watermark robustness as watermark carriers. For good robustness of watermark, DCT coefficient embedding watermark should meet the following conditions:

(1) It is kept well after it has been processed by common signal and noise interference, i.e., these DCT coefficients are not changed much by signal processing and noise interference to ensure that watermark has good robustness after it has embedded in the image. If watermark image is attacked, if DCT coefficient with watermark is changed much, watermark will be possibly remained.

(2) With more perceptual capacity in order not to cause obvious change of visual quality of original image after it has embedded in the watermark, which is advanced for watermark non-visibility and robustness. More perceptual capacity means larger change amplitude under the precondition of unchangeable subjective visibility effect and it means to embed stronger watermark signal.

According to these requirements, low and medium frequency AC coefficient, as embedding watermark position, has been gradually used and cognized, such as Cox watermark method adopts low frequency AC coefficient. However, a neglected fact is that DC component is more suitable to embed watermark signal than any AC component, which has two reasons, □ comparable to AC coefficient, DC coefficient has much more amplitude. Embedding watermark in the image is regarded as iterating a weak signal under strong background. According to Weber law and visual system illumination coverage characteristic, the brighter the background is (the higher DC coefficient is), the higher the visible inspection threshold of embedding signal is, that is, the bigger DC coefficient (represent average brightness of image block) perceptual capacity is. DC coefficient is generally tens of multiplies and even hundreds of multiplies bigger than the biggest AC coefficient, the higher the space frequency is, the smaller the average frequency of coefficient is. Even though DC coefficient change proportion is less than AC coefficient, its absolute value is changed much more than AC coefficient. After they are adjusted with the same size, DC coefficient change is comparatively less, which means DC coefficient has bigger perceptual capacity than AC coefficient. □ According to signal processing theory, the image with embedding watermark the most possibly encounters signal processing processes, such as lossy compression, low-pass filtering, secondary sampling, interpolation, D/A and A/D conversion, which have smaller influence for DC component than AC component, and the watermark embedding DC component is more stable than the watermark embedding AC component.

Therefore, it is concluded that, in DCT domain, for robustness, DC component is more suitable for embedding watermark. Image embedding watermark is regarded as iterating a weak signal under strong background, according to human's visual system characteristic, only when iterative signal exceeds certain strength, it will be inspected by visual system. Visibility threshold of iterative signal is influenced by background illumination, background texture complexity, background and signal space frequency; the brighter the background is, the higher the visibility threshold is (illumination shield); the more complex the background texture is, the higher the visibility threshold is (texture shield); space frequency influence for visibility threshold is explained by contrast sensation function (CSF), which is called frequency masking.

IV. Watermark Proposal and Realization of DCT DC Component

A. Watermark Embedding Algorithm

Watermark embedding algorithm is described as follows:

Suppose original image is *X*, binary watermark image is *W* and the dimension for the selected watermark image *W* is 1/64 of host pixel, that is:

$$X = \{x(i,j), 0 < i, j < N\} \tag{10}$$

$$W = \{W(i,j), 0 < i, j < N/8\} \tag{11}$$

Wherein, *x (i, j)* is gray value of pixel point, $W(i,j) \in \{0,1\}$. Watermark embedding algorithm is:

(1) Firstly transform original image *X*, the paper chooses 256×256 standard image woman as the original image, pick up the decomposed similar component and get 128×128 image and the decomposed low frequency coefficient matrix is A(128×128).

(2) For the added watermark equally distributed in 128×128 image, matrix A is blocked by 8×8 size and then make DCT for each block, and choose the first value in the matrix composed of DCT transformed coefficient of each block as $F_n(1,1)$ $(1 \le n < 1024)$.

(3) Read binary watermark $(1 \le n < 1024)$. Firstly according to positive direction Z scanning (from left to right and from upper to lower), transform watermark image to the sequence $\{W_k\}$ as the length of N, create 0 ~ N-1 random sequence $\{r_j\}$ as random seed of key K and increase it to $\{W_k\}$ sequence to create new watermark sequence W_k. The new watermark is embedded in $F_n(1,1)$ for the following procedure.

Step 1: suppose $Z_n = F_n(1,1) \bmod Q$, *Q* is quantification value set in advance to adjust watermark embedding depth, *Q* is chosen related to original image and watermark image. If *Q* is less, embedding watermark robustness is worse; if *Q* is more, it drops using value of the original image, and therefore, *Q* is chosen properly according to detailed application condition of watermark.

$$Z_n \in \left[\frac{Q}{4}, \frac{3Q}{4}\right], \text{then } F_n(1,1) = F_n(1,1) + \frac{Q}{4} - Z_n;$$

$$\text{if } Z_n \in \left[\frac{3Q}{4}, Q\right], \text{then } F_n(1,1) = F_n(1,1) + \frac{5Q}{4} - Z_n$$

Step 2: when embedding bit W_k =0, if $Z_n \in \left[0, \frac{Q}{4}\right]$, $F_n(1,1) = F_n(1,1) + \frac{Q}{4} - Z_n$; if $Z_n \in \left[\frac{Q}{4}, \frac{3Q}{4}\right]$, $F_n(1,1) = F_n(1,1) + \frac{Q}{4} - Z_n$; if $Z_n \in \left[\frac{3Q}{4}, Q\right]$, $F_n(1,1) = F_n(1,1) + \frac{5Q}{4} - Z_n$.

$Z_n \in \left[\frac{Q}{4}, \frac{3Q}{4}\right]$, then $F_n(1,1) = F_n(1,1) + \frac{3Q}{4} - Z_n$; if $Z_n \in \left[\frac{3Q}{4}, Q\right]$, then $F_n(1,1) = F_n(1,1) + \frac{3Q}{4} - Z_n$

Step 3: when embedding bit W_k =1, if $Z_n \in \left[0, \frac{Q}{4}\right]$, $F_n(1,1) = F_n(1,1) - \frac{Q}{4} + Z_n$; if $Z_n \in \left[\frac{Q}{4}, \frac{3Q}{4}\right]$, $F_n(1,1) = F_n(1,1) + \frac{3Q}{4} - Z_n$; if $Z_n \in \left[\frac{3Q}{4}, Q\right]$, $F_n(1,1) = F_n(1,1) + \frac{3Q}{4} - Z_n$.

Step 4: repeat the above process until embedding all bits, and then IDCT for each 8×8 block to get low frequency coefficient matrix (low frequency image after adding watermark).

Step 5: IDWT transform for the changed coefficient, recompose and get the image I_w with watermark component as original image.

The watermark embedding algorithm as the above ensures that the coefficient with larger amplitude in original chart field corresponds to watermark image DCT coefficient with larger amplitude; secondly, since DCT coefficients are comprised watermark image low frequency information, if the information isn't lost or lost less, watermark image will be better recovered to improve algorithm's robustness and hidden.

B. Watermark Picking Algorithm

Use similar method with watermark embedding process for watermark picking up and the algorithm is as follows:

Step 1: first transform for embedding watermark image I_w to get low frequency coefficient matrix B (128×128).

Step 2: block division for matrix B according to 8×8 size, and then DCT for each block, choose the first value of the matrix composed of DCT transform coefficient of each bock as $F_n(1,1)$ ($1 \le n < 1024$), and then pick up watermark according to the method as follows. Calculate $Z_n = F_n(1,1) \bmod Q$, if $Z_n \in \left[0, \frac{Q}{2}\right)$, W_k =0; if $Z_n \in \left[\frac{Q}{2}, Q\right)$, W_k =1.

Step 3: recover original watermark sequence according to key K, according to reverse direction *Z* scanning (from lower to upper, and from left to right) to recover DCT coefficient of two-dimensional watermark image and make IDCT to get picking up watermark *W'*.

$$sim(W, W') = \frac{\sum_{i=1}^{n} (w_i \times w_i')}{\sqrt{\sum_{i=1}^{n} (w_i \times w_i')}} \qquad (12)$$

Step 4: use similarity formula, compare similarity between recovered watermark signal W' and original watermark signal W.

C. Algorithm MAPLAM Realization

Step 1: read original open image and watermark pattern to binary set I, J;

Step 2: divide the original open image I to uncovered image block (x, y), $1 \le$ x, y≤ 4, l=1,2,…,n×n/64, DCT transform for block(x, y) to get block_dec (x, y);

Step 3: chose the element J (p, q) of watermark image and embed to low frequency system of original open image block;

Step 4: IDCT change for image block embedding watermark information block_det (x, y) to get block(x', y');

Step 5: compound image block to get the image embedding watermark;

Step 6: JPEG compression for the image embedding watermark;

Step 7: watermark picking up from compressed image.

D. Test Result and Conclusion

Simulation test result is as follows:

TABLE I
TEST EMULATION RESULT

No Attack	*Sim(W, W')* = 0.9836	
Attack	Increase 0.02 Gaussian noise	Sim(W, W') = 0.8432
	5 * 5 median filter	Sim(W, W') = 0.8231
	Reduce 50% and then recover dimension	Sim(W, W') = 0.6277
	Motion Blur Processing	Sim(W, W') = 0.6022

It can be seen that the algorithm has good robustness for such attacks, as dimension transform, median filter, noise interference and image blurring.

V. CONCLUSION

For the digital watermark algorithm of the paper, DC component is more suitable to embed watermark than AC component on DCT domain, but embedding is less if only embedding on DC component. Further consider for watermark embedding of DC component and AC component to improve watermark embedding.

Along with more and more mature of digital watermark technology, the copyright authentication system based on digital watermark technology has more and more function for general domains, including digital library, electronic commerce, video-on-demand, remote education and training, digital camera and scanner. As a new thing of digital information security domain, digital watermark technology will be more and more useful. Therefore, it is believed that digital watermark technology might have long-range development foreground and gestate great commercial potential.

ACKNOWLEDGEMENT

It is a project supported by National Natural Science Foundation of China (50775070) and Provincial Natural Science Foundation of Hunan (04JJ30048).

REFERENCES

[1] J. Abbate, "Inventing the Web", *Proceedings of the IEEE*, 1999, 87(11):1999-2002.
[2] K.Tanaka, Y.Nakamura, Matsuik, "Embedding secret information into a dithered multilevel image", *Proceeding of 1990 IEEE Military Commune*, Conf, 1990: 216-220.
[3] G.T.Ramkin, "Electronic watermark", *Proceedings of Dicta*, 1993: 666-672.
[4] R.Anderson, "Information Hiding", *Lecture Notes in Computer Science*, Berlin, New York, Springer-Verlag, 1996(1174).
[5] Lu Zhe-Ming, Wu Hao-Tian, Liu Zhong-Ren, Sun Sheng-he, "A Multipurpose Color Image Watermarking Algorithm for Copyright Notification and Protection", *Acta Electronic Sinica*, 2006, 32(5):778-781.
[6] Chuntian Zhang, "New Technologies in the Information Security Fields-Digital Watermarking", *Tianjin Science & Technology*, 2002(6):45.
[7] Zhang Jing, Zhang Chuntian, "Overview of Digital Watermarking Techniques for Binary Images", *Computer Engineering*, 2005(3): 1-4.
[8] Niu Xinxin, Yang Yixian, Wu Zhijun, "Study on the Basic Theory and Technology of Information Hiding", *Telecommunications Science*, 2004(12): 28-31.
[9] Dong Gang, Zhang Liang, Zhang Chun-tian, "A semi-fragile digital image watermarking algorithm", *Journal of China Institute of Communications*, 2003, 1(24):33-38.
[10] Yi Kai-xiang, Sun Xin, Wang Dao-shun, Shi Jiao-ying, "New Content-Based Semi-Fragile Watermarking", *Acta Simulate Systematica Sinica*, 2002, 9(14): 1201-1204.