2011 Fourth International Joint Conference on Computational Sciences and Optimization

# The Research of Image Watermarking Encryption Algorithm

Shanshan Zhang, Xiaohong Wang, Shizheng Zhou
Department of Computer Sciences, Communication university of China
Beijing, 100024, China
E-mail: shanshan3692008@126.com

*Abstract*—**The image watermarking technology is an important aspect about multimedia authentication and copyright protection, in order to enhance its reliability and security, this paper proposes an encryption algorithm based on color image watermarking in security DCT domain. By processing the color watermark image's R, G, B pixels, that is, converts the pixel value matrix into binary one-dimensional sequence, then get the one-dimensional sequence as the watermark embedding the carrier images, overcame the traditional understanding defects about the DCT domain can only be embedded two value image. Furthermore, through setting the key to strengthen the security and prevent unauthorized watermark recovery and repair. Finally use the MATLAB/SIMULINK and the Embedded MATLAB™ to build the watermark embedding and detection system model, quickly and intuitively verify the correctness of the watermark encryption algorithm. Experimental results demonstrate that its robustness is good and computational complexity is low, basically achieve non-destructive extraction.**

***Keywords- watermarking; image encryption; DCT; simulink***

## I. INTRODUCTION

With the development of network technology, network information security becomes increasingly prominent. Online trading and transmission of multimedia data, there are two key technical issues need to be resolved: Firstly, multimedia data transmission access control and security; second one is the protection of multimedia data. For the first question, the traditional encryption technology can handle it. The second problem consists of two main parts: copyright protection and content integrity protection, then the traditional encryption technology can do anything [1] [2]. Recent development of digital watermarking technology can solve this problem. Through embedding the secret information in the original media – watermark to verify the ownership of the data and ensure data integrity. This watermarked image can't be perceived by the human eyes, only through professional testing can detect the existence of watermark, and also need the key to crack the watermark information, enhance the reliability.

Digital image watermarking algorithm includes four categories: time-domain (e.g. LSB, Patchwork algorithm), compressed domain (e.g. JPEG compressed domain, MPEG compressed domain), transform domain (e.g. DCT domain, DWT domain) and spread spectrum watermarking [3]. Where, the DCT domain watermark algorithm has good hidden effect, can not only withstand loss JPEG compression, filtering, signal processing, but also subject to the general geometric transformation, such as cropping, scaling, translation and rotation operations. Its robustness is good and computational complexity is low.

The research of Image watermarking technology in DCT domain is generally based on the binary image, each pixel value is either 1 or 0, not exist intermediate pixel values. It has many limitations in the actual applications about copyright protection and multimedia authentication, and not has very well visual effects in matching process.

Simulink is a graphical simulation tool for dynamic system modeling, simulation and comprehensive analysis. It can call MATLAB powerful function library, save a lot of duplicate codes writing work, and the user can immediately see the results of the simulation system.

In this paper, I propose an encryption algorithm based on color image watermarking in security DCT domain. By setting the key to prevent recover and repair the watermark in the unauthorized situation. Finally, through using the MATLAB/SIMULINK modules and write custom modules (Embedded MATLAB function) [4] [7].To build the color image watermark embedding and detection algorithm. The results fast and intuitively show that this algorithm is correctly and feasibly, and then lays the foundation for the hardware implementation in the next step.

## II. ANALYSIS OF IMAGE WATERMARKING ENCRYPTION SYSTEM

According to the traditional encryption technology and the digital watermarking technology features, this paper proposes an encryption algorithm of embedding the color image watermark information into the color image in the DCT domain. The watermark encryption algorithm mainly includes the carrier image 8x8 piecemeal DCT algorithm, choosing embedding region, producing watermark sequence, embedding watermark sequence and setting key.

### *A. Image block DCT transform*

2D-DCT can concentrate the main image information into the least low frequency coefficients, and cause smallest image blocking effect, thus achieves good compromise between centralized information and computational complexity. Moreover, 2D-DCT is real transformation. It has good energy compression ability, goes to the related ability and well compatibility with the international compression standard. It's a good choice about using the 2D-DCT transform to implement the watermark embedding and extraction .I divide the color image into not-cover 8×8 block mutually, then each sub block do the 2D-DCT transform.

978-0-7695-4335-2/11 $26.00 © 2011 IEEE
DOI 10.1109/CSO.2011.282

## B. *Choose the watermark embedded region*

According to the humanity vision system degree of the illumination and texture hides characteristic, it is possible to know: background brightness is higher, the texture is more complex, and the human vision is more insensitive to its slight transformation [5]. Here, I use sub block's variance to weigh the complex degree of the sub block texture. When $\sigma^2$ value is small, think the block is quite smooth, otherwise, the block is containing more complex texture or edge. The formulas to compute the sub blocks' picture element average value (m) and the variance ($\sigma^2$) are as follows:

$$m = \frac{1}{n^2}\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} x(i,j) \quad (1)$$

$$\sigma^2 = \frac{1}{n^2}\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} [x(i,j) - m]^2 \quad (2)$$

Through experiment we can get a conclusion: if embedding too much more watermark information into the image smooth region, which is easy to cause the blocking effect phenomenon, and cause the quality of image dropping; to the contrary, if embedding into the texture complex sub block of the image, basically does not have the visual difference. Therefore, I embed image watermark information into the texture complex region. Namely, I embed the watermarking information into the variance value quite big sub-blocks.

## C. *Producing and embedding the watermarking sequence*

In SIMULINK model, the carrier image's coefficient matrix uses 64 bit double date type to express after 2D-DCT, the range of value is [0,1]. For preventing produce the block effect, the value of colored watermark image's picture element matrix need to be transformed into 1-D sequence which range is from 0 to 1.

What the watermark telescoping uses is one kind based on the DCT intermediate frequency digital watermark technology. Because the human's eyes are very relatively sensitive to the low frequency partial noises; if the watermark information embeds into the high-frequency unit, it's easy to loss information for quantification and low-pass filtering processing, and affects the robustness of the watermark. Therefore, I choose embedding the watermark information into the intermediate frequency region of 8×8 sub-block, that is, diagonal line 8 positions.

## D. *Detecting watermarking image*

Theoretically speaking, the watermark detection is the inverse procedure of the watermark embedding, but because the image after DCT transform coefficient matrix is the double decimal, will have more or less deviation, we need to establish the appropriate threshold value to converse the watermark data into unit8, then recover watermark image.

## E. *Setting key*

The key is the data which the user establishes independently and directly, then the key and the watermark sequence do 'XOR' operation before embedding watermark information, when detecting watermark sequence do 'XOR' operation again with the key, just can restore the original watermark image sequence. Thus, even if knows the watermark encryption, does not know the key, also cannot recover the original watermark image, strengthened the security.

## F. *Watermarking embedding algorithm and detecting algorithm flow chart*

### 1) *Watermark embedding system*

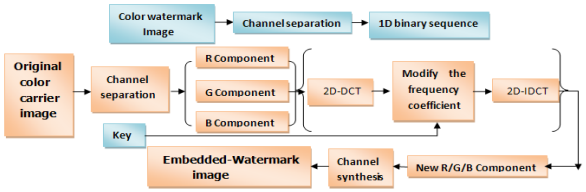


Figure 1. Watermark embedding diagram.

### 2) *Watermark detecting system*

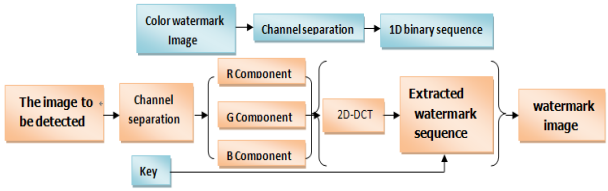


Figure 2. Watermark detecting diagram.

According to the sizes of the image and the watermark image what choose, the embedding information content is different, the embedding model will have the difference slightly. For instance, the carrier image's size is M×N, according to 8×8 piecemeal, sub block quantity C= (M/8) * (N/8); the watermark image's size is S×T, then the sequence length is l=S×T. If C> l, the sub block will embed 8bit watermark information, otherwise, needs to embed more. But to ensure the watermark information is embedded in the texture region and the DCT coefficient intermediate frequency, the size of the watermark image should not choose too big. This paper chooses carrier image is 640×640 Lena color image, watermark image is 70×70 the color Communication university of China's logo image.

# III. AUTHENTICATION THE IMAGE WATERMARK ENCRYPTION BY SIMULINK

## A. *Top module diagram shows as following:*

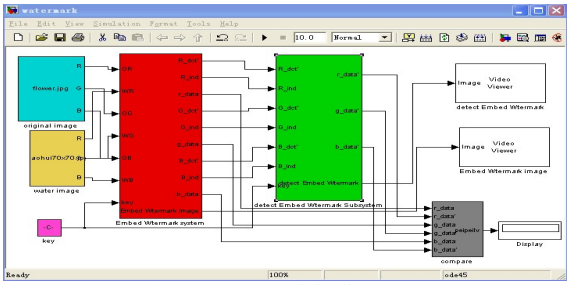

Figure 3. Top module diagram.

The above module, the blue color module is the original image, the yellow is the color watermark image module, the purple is the set key, red is the watermark embedding system, the green is the watermark detection system, the gray module is the compare system which achieve the original watermark and extracted watermark sequence comparison, the white module is used to display image and data.

### B. *Watermark Embedding subsystem*

I embed the color watermark image R, G, B components into the carrier image's R, G, and B component respectively, so I take the R component embedding process for example:

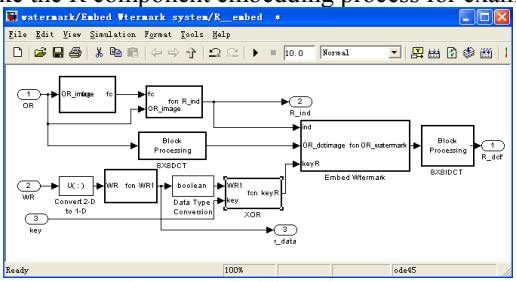


Figure 4. Embedding subsystem.

Mark the 640 × 640 color vector image is O, 70 × 70 color image watermark image is W, detail embedding process is as follows:

*a)* OR is the R component pixel matrix of the color carrier image (after channel separation ), OR is divided into 8×8 sub-blocks which are not covered with each other, (sub-block number C = (640 / 8) * (640 / 8) = 6400), calculate every sub-blocks' variance (fc), and order sequence from large to small, record the location of block in the original image after sorting, the resulting sequence is denoted R_ind, where fc and R_ind are the C × 1 matrix;

*b)* Do 2D-DCT transform for each 8 × 8 sub-block, the transformed coefficient matrix denoted OR_dctimage;

*c)* WR is the R component pixel matrix of color watermark image W, convert 2D WR into 1D sequence, calculate the length of one-dimensional sequence l, then convert the WR into a two-dimensional matrix WR' which size is l × 8, that is, each pixel WR' value represents by 8 bit binary number;

*d)* Setting key, the key and WR do the 'XOR' operation, get a new watermark matrix is keyR;

*e)* Taking R_ind former l item, namely, the former l bigger variance sub-block, taking the WR' by line, each sub-block embedded 8bit watermark information. I modify 8 frequency coefficients in each diagonal realization of OR_dctimage by the formula to achieve embedding, the formula 1:

$$OR\_dctimage(x, y) = rr * keyR(l, k). \quad (3)$$

Where, rr is the embedding strength, through an experiment, I selected rr = 0.002; WR (l, k) is the watermark sequence values, OR_dctimage '(x, y) is the modified coefficient, x, y is the relative coordinate which are calculated based on R_ind, l □ [1,4900], k□ [1,8]. It is difficult to determine the pixels' elative coordinate in the watermark block in the carrier the image according to the R_ind.

*f)* OR_watermark does 2D-IDCT operation, to generate a new red component;

Do the same operation with the G, B components of carrier image, then R, G, B components do channel synthesis, generates the color watermark-embedded image O', lastly, video viewer displays the watermark image.

### C. *Watermark detecting system*

It's similar with the watermark embedding system, also take the R for example to show the watermark detection process:

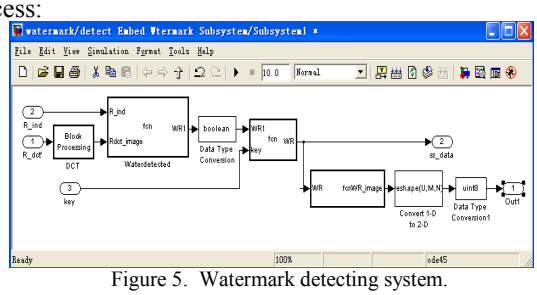


Figure 5. Watermark detecting system.

Color embedded-watermark image is denoted by O'. The detailed detection process is as follows:

*a)* After channel separation to get the red component R' component, dividing the image matrix R_dct into 8X8 sub-blocks which are not covered with each other, then do the 2D-DCT transform, record results as Rdct_image;

*b)* According to the sequence of R_ind which is obtained after sorting of the original image's variance to determine the location of the block where once embedded watermark;

*c)* According to the block position to calculate the blocks' starting coordinates in the original carrier image ;

*d)* Select R'_DCT (k) diagonal 8 data, and according to the formula to extract the R component watermark information from R_dct':

$$WR'(l, k) = Rdct\_image'(x, y) / rr. \quad (4)$$

For the WR' □ [0, 1], is double type, through set the threshold to get the nearly watermark sequence, had many observation and experiment, Threshold k = 0.5 is the most suitable, that is, if k>0.5, set WR'= 1, otherwise, WR'= 0.

*e)* Do XOR operations between WR' and key respectively, and key, restore the watermark sequence WR;

*f)* Converse WR to 2D matrix, the date type is unit8;

Lastly, the watermark information R, G, B component do channel synthesis, generating color image watermark W', and use the video viewer display.

### D. *Compare system*

The following system is seeking R, G, B three-component matching and averaging matching, in the paper way N approximately equal to 1.

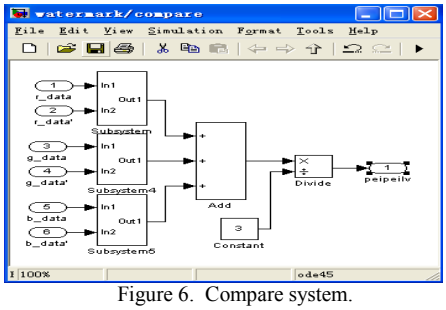

Figure 6. Compare system.

## IV. DISPLAY RESULTS ANALYSIS

Select the 640×640 lean as the carrier image(figure 7), the70×70 Communication University of China logo as watermark image information(figure 8),directly see embedded-watermark image(figure 9)and extracted-watermark (figure 10)through video viewer module as below:

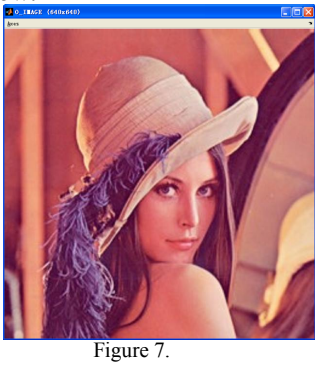
Figure 7.

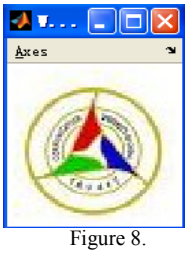

Figure 8.

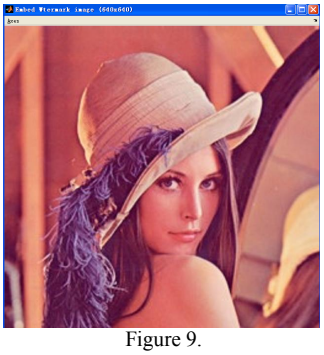
Figure 9.

Figure 10.

By comparing, it can be found that the embedded-watermark image and extracted-watermark are have little different with the original, also completely extract out of the embedded watermark image. Embedded-watermark image relative to the original image in the R \ G \ B peak signal to noise ratio (PSNR) [6] of each component are 61.61/66.69/59.97dB,all greater than 35dB, whether from subjectively or objectively point, good results Watermarking that the carrier did not significantly decrease the image quality; watermark image and extracted-watermark image sequence matching N = 1, PSNR = ∞, basically achieve non-destructive extraction, realize the expected goals.

## V. CONCLUSIONS

This paper proposes that select the color Communication University of China Logo image as meaningful watermark embed into Lena carrier image's 2D-DCT domain (intermediate frequency component), by setting the appropriate threshold and embedding strength, and ultimately realize the color watermark embedding and non-destructive extraction, pull in key to enhance security to prevent unauthorized watermark recovery and repair. In terms of subjective or objective, and have achieved good results. By simulink and Embedded MATLAB ™ module modeling the proposed watermark embedding algorithm and detection algorithm, fast and conveniently verify the correctness of the algorithm, and then lay the theoretical foundation for the next step hardware implementation.

## ACKNOWLEDGMENT

This work is supported by the Communication University of China "211 Project" third key discipline construction project (phase).

## REFERENCES

[1] W.F. Xie, "Research on Realization of Digital Watermarking Algorithm", Xian university of science and technology master degree theses,pp.6-7,Apr 2009.

[2] D.L. Zhu, "New Application of Digital Watermarking in Information Security", CHINA INFORMATION SECURITY ,2009.

[3] G.Y. Xiao, C.Y. Jiang, L. Ma, "The Application of Digital Watermarking", Journal of Chongqing Electric Power College, 2009(1).

[4] Y.Y. Sun, J. Liu, "Realization of Similarity Based on Embedded MATLAB Function Blocks", Computer&Digital Engineering 2010.

[5] S.R. Xi, C.P .Liu and Q. Wang. "Digital Image Processing and Analysis", Beijing: Tsinghua University Press, july 2006.

[6] X.D. Zhu, "The research for watermarking technique",Jilin University,Apr 2004.

[7] X.H. He, Y.Y. Zhou, J.Y. Wang and H. Zhou, "MATLAB 7.X Image Processing", Beijing: Posts & Teleco Press, Nov 2006.