Fingerprint Watermark Embedding by Discrete Cosine Transform for Copyright Ownership Authentication

Chi-Man Pun and Ioi-Tun Lam

***Abstract*—** In respect to the issues on protecting intellectual property, particular for artistic works in electronic form, some sorts of techniques could be put on a copyright material image to ensure its ownership authentication. In this paper, signatories' biometric fingerprint watermark message in digital format will be embedded into a copyright material image by Discrete Cosine Transform (DCT) for copyright ownership authentication. During the embedding process, copyright material image and the fingerprint watermark message will be adaptively partitioned and then DCT method will be applied to each partition for embedding and extracting the watermark message. Experimental results from our prototype system show that the proposed method is successfully tested for message embedding and extraction. In case that the watermarked image has been attacked, the embedded digital fingerprint watermark message can still be extracted with a certain degree of tolerance.

***Keywords*—** Intellectual property, ownership authentication, discrete cosine transform, digital fingerprint.

I. Introduction

Copyright is a form of intellectual property and, like physical property, it can be bought and sold, inherited or otherwise transferred. These rights start as soon as the material is recorded in writing or in any other way including those uploaded to the internet web servers. The rights cover: copying; adapting; distributing; communicating to the public by electronic transmission; renting or lending copies to the public; and, performing in public. However, copyright is automatic in the UK and most of the rest of the world and thus there is no official registration system.[1] In case that their work has been distorted or mutilated, the authors are responsible for taking legal action and submitting evidences to identify the ownership rights on their work for the suits. This is a question concerning not about the authentication against the genuineness and integrity of the material, but rather the property ownership. How can the authors prove that the work is original from them?

Traditionally, they may deposit copies of their work with a bank or solicitor; or send copies to themselves by special delivery which gives a clear date stamp on the envelope, leaving the envelope unopened when it is returned to them. Either of these methods could help to prove that their work existed at a certain time. But nowadays, globalization and use of internet make these traditional methods impractical. An electronic copy can be easily obtained by just a simple click and its creation time stamp can be adjusted by some sorts of applications. Facing these technical challenges, how can we protect our copyright materials from being unauthorized downloaded or even distributed? Adopt an instant download permission key to open a copied multimedia file and on-line database? Embed a visible security overlay in a duplicated electronic artistic works? But these methods can merely increase the difficulties on the access to the material. In respect to the ownership authentication of a copyright material, hiding some invisible personalized information as an authentication key can be a considerable method.

Covert Channels, Steganography, Anonymity and Copyright Marking are some of the Information hiding[2] techniques. Digital watermarking is one of the types from Copyright Marking and is a process of embedding information into a digital media such as image materials (binary, gray scale or color), audio and video. If the media is copied, then the hidden information is also carried in the copy.

Considering the high uniqueness and imitation difficulty on human fingerprint, and the hiding features of digital watermarking, a thought of embedding a digital fingerprint as a watermark ownership authentication message inside a copyright material emerges. By this way, ownership authentication will rely on the matching between the digital fingerprint extracted from the watermarked copyright material and the digital fingerprint data previously archived in the system or the fingerprint captured immediately during the process. Can this idea be implemented? Which digital watermarking methods should be adequate to apply? How is it got done? What will be the performance? Are there any limitations? This research will focus on answering all of these queries.

This work was supported in part by the Research Committee of University of Macau under the Grant: RG056/08-09S/PCM/FST.

C.-M. Pun and I.-T. Lam are with the Department of Computer and Information Science, University of Macau, Macau S.A.R., China. (e-mail: {cmpun, ma26255}@ umac.mo).

II. Proposed Method

Generally speaking, digital data watermarking techniques[2] can be grouped into two classes: Spatial Domain and Transform Domain. Transform Domain[3] [4] such as [5] [6] [7] [8] [9]transforms the original text document into frequency components and then embeds message into particular frequency regions. Discrete Cosine Transform (DCT) is one of the commonly implemented methods in this domain. Spatial Domain[3] [4] such as [10] [11] [12] [13] [14] modifies pixel value directly and Flipping method is one of its implementing methods. Theoretically, Flipping and DCT methods can be applied to embed a watermark message in a grey or color digital document. But in practice, due to the discreteness features, Flipping is less favorable since its discrete flipping values may not be capable for applying to the gradual changing color spectrum compared with the continuous frequency transformation values in DCT. Moreover, the embedded document from DCT method is more robust and has higher visual quality than that from Flipping. Therefore, DCT methods are normally selected for watermarking a message to a grey and color document even though their complicated computation algorithm on frequency transformation involves larger overhead than in Flipping. Based on these advantages, DCT will thus be chosen as the proposed method for ownership authentication. This method had been studied by a few scholars: In 1996, Adrian G. Borg and Ioannis Pitas [7] proposed modifying DCT coefficients to fulfill a block site selection constraint. In 1996, Weili Tang, Aoki, Y. [8] proposed DCT algorithm to implement the middle band embedding. In 1997, Bo Tao and BTadley Dickinson [9] proposed an adaptive watermarking technique in DCT domain.

Discrete Cosine Transform

Discrete Cosine Transform (DCT) is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers to orderly express finitely data points in terms of a sum of cosine functions oscillating at different frequencies. DCT is equivalent to DFT of roughly twice the length, operating on real data with even symmetry, where in some variants the input and/or output data are shifted by half a sample[15]. There are few types of DCT variants such as DCT-I, DCT-II, DCTIII-VIII and the most common one is the type DCT-II. Its definition for an input image A and output image B is

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N},$$

$$0 \le p \le M-1$$

$$0 \le q \le N-1$$

$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p=0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \qquad \alpha_q = \begin{cases} 1/\sqrt{N}, & q=0 \\ \sqrt{2/N}, & 1 \le q \le M-1 \end{cases}$$

where M and N are the row and column size of A, respectively. If one applies the DCT to real data, the result is also real. The DCT tends to concentrate information, making it useful for image compression applications.[16]

Formula (1) below is used to compute the coefficient of the watermarked image which is denominated as $I'w$. Where, Iw is the coefficient of the copyright material image and Ww is the coefficient of the fingerprint watermark message.

$$I'w = Iw(1 + \alpha Ww) \quad (1)$$

Formula (2) is used to compute the coefficient of the embedded fingerprint watermark message which is denominated as $\overline{W}w$. Where, $\overline{I}w$ is the coefficient of the watermarked image and Iw is the coefficient of the copyright material image.

$$\overline{W}w = 1/\alpha[\overline{I}w / Iw - 1] \quad (2)$$

The following steps in (Fig.1) are the DCT algorithm to embed a fingerprint watermark message into a copyright material image:

1. Based on the pre-test results in (Fig.5), partition the copyright material image and fingerprint watermark message into 32x32.
2. Transform a partitioned copyright material image to obtain its coefficients (Iw).
3. Transform a partitioned fingerprint watermark message to obtain the message's coefficients (Ww).
4. Apply formula (1) to each partition to compute the coefficient ($I'w$) for the watermarked image.
5. The coefficients of the watermarked image computed for each partition are sorted by ascending order.
6. Inversely transform the watermarked image.
7. Reconstruct the watermarked image.

The following steps in (Fig.2) are the DCT algorithm to extract the embedded fingerprint watermark message from a watermarked image:

1. Transform the partitioned watermarked image to obtain its coefficients ($\overline{I}w$).
2. Transform the partitioned copyright material image to obtain its coefficients (Iw).
3. Apply formula (2) to each partition to compute the coefficient ($\overline{W}w$) for the embedded fingerprint watermark message.

4. The coefficients of the embedded fingerprint watermark message computed for each partition are sorted by ascending order.
6. Reconstruct the extracted fingerprint watermark message.
7. Inversely transform the extracted fingerprint watermark message.
8. Combine the fingerprint watermark message.

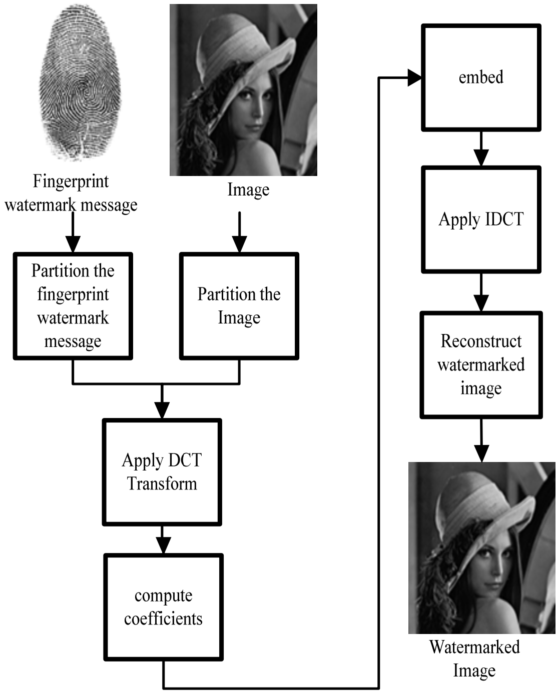

Fingerprint watermark message
Image
Partition the fingerprint watermark message
Partition the Image
Apply DCT Transform
compute coefficients
embed
Apply IDCT
Reconstruct watermarked image
Watermarked Image

Fig. 1. Embed a fingerprint watermark message to copyright material image using DCT.

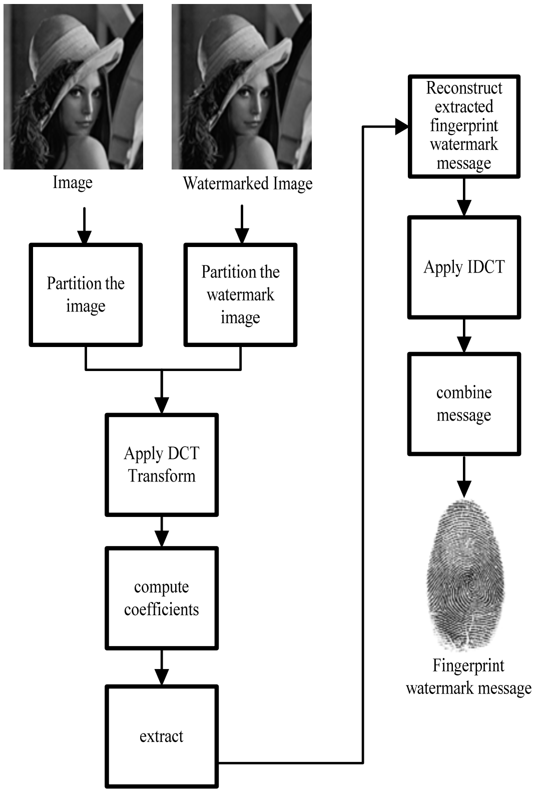


Fig. 2. Extract an embedded fingerprint watermark message using DCT.

III. Experimental Results and Discussions

In this research, three experiments will be performed: embedding a gray level fingerprint watermark message into a gray level copyright material image; extracting an embedded fingerprint watermark message from a watermarked image; and robustness of the watermarked image against simulated interferences like shrinking and enlarging the image, pasting an overlay logo on the image and cropping the image.

For having a better difference invisible effect on a watermarked image, a 512x512 Lena portrait (Fig.3) and a 128x128 digital fingerprint (Fig.4) will be chosen as the copyright material image and the watermark message for the experiment. Based on the pre-test PSNR results (Fig.5) in different α values on different image partition settings, α=0.003 and 32x32 partition setting will be applied to both copyright material image and fingerprint watermark message for all the experiments except for the robustness experiment against image cropping, where no partition will be applied.

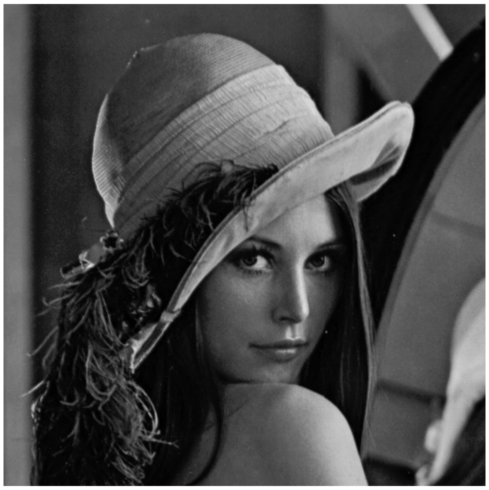


Fig. 3. Lena Portrait – copyright material image (512x512)

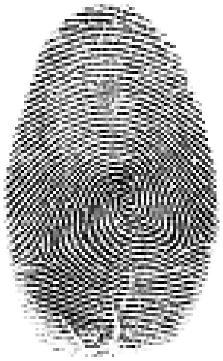


Fig. 4. Fingerprint watermark message (128x128). This image is from http://forensicfact.wordpress.com

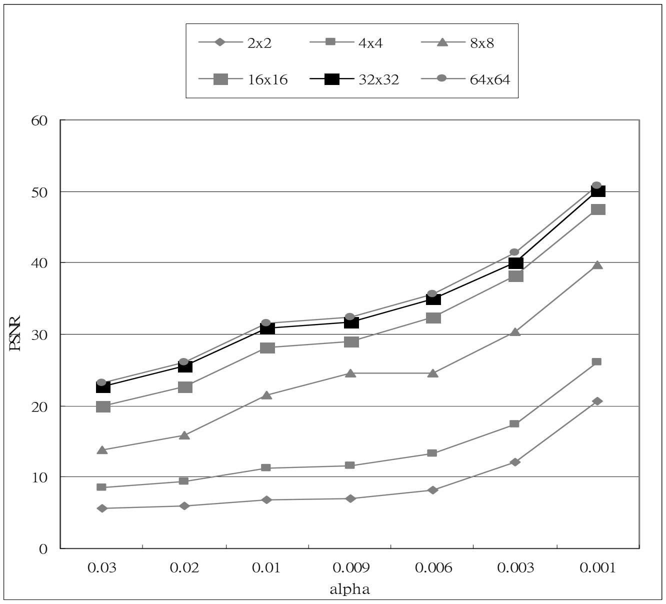


Fig. 5. PSNR vs different α values on different image partition settings

3.1 Embedding Fingerprint watermark message

After applying the above mentioned watermark message embedding procedure, a watermarked image (Fig.6) is produced. Comparing it to the original copyright material image (Fig.3), it can be seen that the difference between them is almost invisible. The requirement of invisibility after embedding a fingerprint watermark message into an image is successfully proven, and thus DCT method can be applied for watermarking.

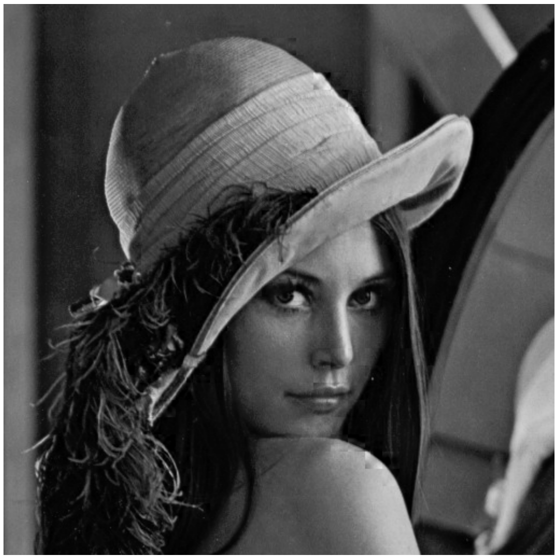


Fig. 6. Watermarked image (α = 0.003, 40.08dB)

3.2 Message extraction from a watermarked Image

In this experiment, the watermarked image (Fig.6) is used for the extraction. After applying the above procedure for extracting an embedded watermark message, a fingerprint watermark message (Fig.7) will be extracted from the watermarked image. Comparing it to the original fingerprint watermark message (Fig.4.), it can be seen that the difference between them is almost invisible. Therefore, DCT method can be applied for extracting an embedded fingerprint watermark message which can be used for ownership authentication.

For the above watermark message embedding and extraction experiments, different α values and different image partition settings can be chosen, for example, values from (Fig.5). According to DCT, smaller α values will yield a better difference invisible results (copyright material image vs watermarked image and fingerprint watermark message vs the extracted fingerprint watermark message). However, the robustness against interference attacks will become lower with smaller α values. Due to this contradictory effect on α value, a balanced choice fit to both difference invisible result and robustness should be considered, and thus α=0.003 is selected for this research.

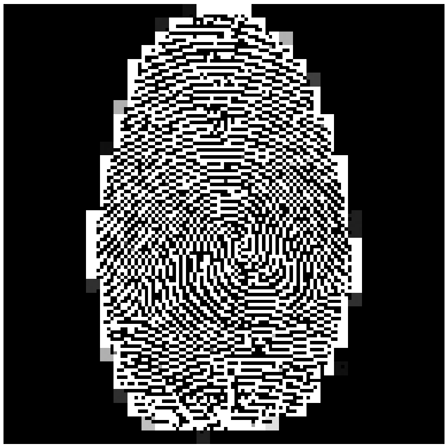


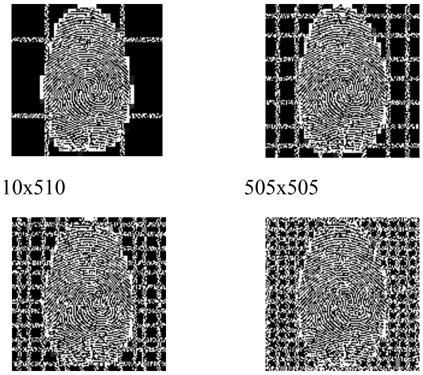
Fig. 7. Extracted fingerprint watermark message

3.3 Robustness on watermarked image being attacked

All interference attacks, namely resizing the watermarked image, pasting an overlay logo on the image and cropping the image, are used to simulate the behaviors which infringers may apply to the copied image in order to obscure his copyright infringement activity.

(1). Resizing the watermarked image:

Experimental results indicate that enlargement on the watermarked image will not affect the embedded fingerprint watermark message extraction, whereas shrinkage the image will affect its extraction. (Fig.8) shows that extracted fingerprint watermark messages can still be recognized as the shrinkage is no more than 495x495. However, comparing the extracted fingerprint watermark message from an unattacked watermarked image (Fig.7.), all extracted images contain some sorts of distortion. Therefore, the ownership authentication by matching the extracted fingerprint watermark message against the captured digital fingerprint will not be fully done, but is still considered workable as we can accept a certain degree of tolerance (as soon as the shrinkage is kept small).



510x510 505x505

500x500 495x495

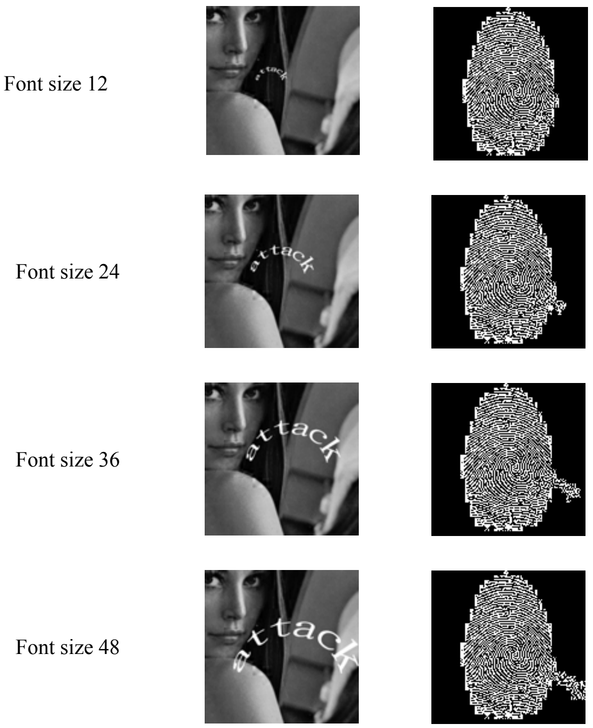
Fig. 8. attack simulated by shrinking the watermarked image

(2). Pasting an overlay logo “attack” on the watermarked image:

Experimental results (Fig.9) indicate that extracted fingerprint watermark messages can still be recognized even an overlay logo has been put on the watermarked image. However, comparing the extracted fingerprint watermark message from an unattacked watermarked image (Fig.7.), all extracted images contain some sorts of distortion and the distortion will become larger as the overlay logo area increases. Therefore, the ownership authentication by matching the extracted fingerprint watermark message against the captured digital fingerprint will not be fully done, but is still considered workable as we can accept a certain degree of tolerance (as soon as the size of overlay logo is kept small).

(3). Cropping the watermarked image:

In this experiment, the watermarked image is cropped by 10, 20 and 30 pixels from the image top margin and by 30 pixels from all four side margins. With an assumption that there is an application to adjust the cropped image position so that it can be shifted to fully match the uncropped watermarked image position, experimental results (Fig.10) indicate that extracted fingerprint watermark messages can still be recognized even though some parts of watermarked image have been cropped. However, comparing the extracted fingerprint watermark message from an unattacked watermarked image (Fig.7.), all extracted images contain some sorts of distortion and the distortion will become larger as the cropping area increases. Therefore, the ownership authentication by matching the extracted fingerprint watermark message against the captured digital fingerprint will not be fully done, but is still considered workable as we can accept a certain degree of tolerance (as soon as the cropping area is kept small).



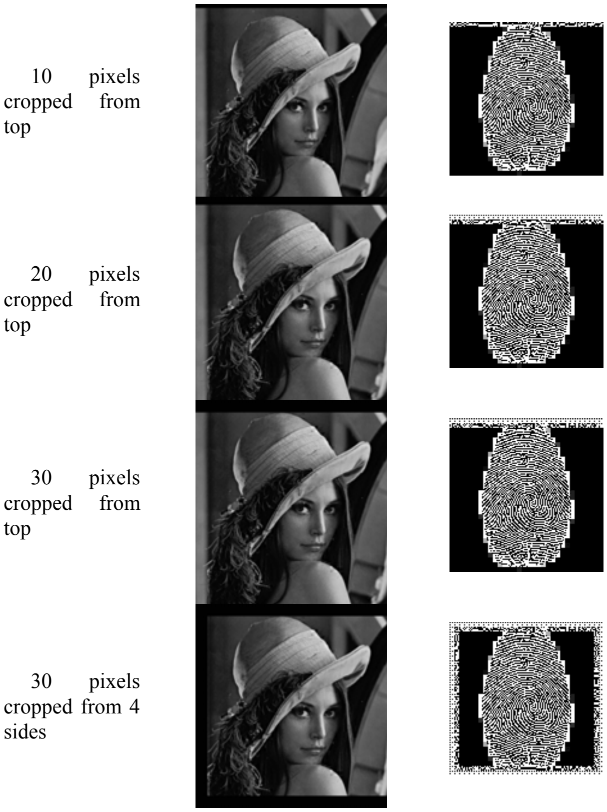
Font size 12

Font size 24

Font size 36

Font size 48

Fig. 9. attack simulated by pasting an overlay logo on the watermarked image



10 pixels cropped from top

20 pixels cropped from top

30 pixels cropped from top

30 pixels cropped from 4 sides

Fig. 10. attack simulated by cropping the watermarked image

3.4 Performance Comparison Between DCT and DWT Methods

Both Discrete Cosine Transform (DCT) method and Discrete Wavelet Transform (DWT) method are the digital watermarking techniques coming from Transform Domain category, therefore, they have some features in common. For example, they transform cover media into frequency components and embed the watermark message into particular frequency regions and thus can generate continuous frequency transformation values to embed watermark message in a wide range of cover mediae such as those in audio, video, color and gray text document image; the visibility quality and the robustness capability of the watermarked media are inversely affected by the value of the functional parameter α in DCT and (α, β) in DWT algorithm. That is, smaller functional parameter value yields higher visibility but less robustness, on the contrarily, lower visibility and stronger robustness with larger parameter value. However, they have some characteristics different from each other. For instance, document image and watermark message can be partitioned into smaller areas and DCT algorithm will be applied to each partitioned area in order to have a better quality watermarked document image. But in DWT, both images will not be partitioned but the algorithm will be iteratively applied in order to have a better watermarking result; DCT algorithm requires only one functional parameter α for watermark message embedding and extraction while DWT requires both α and β functional parameters. Will these differences produce significant performance disparity between two Transform Domain methods? A simple performance comparisons based on watermark message embedding computation efficiency, imperceptibility on the watermarked document image, visibility on the extracted watermark message and robustness capability of the watermarked document image have been reviewed, and the results are as follows:

Computation Efficiency

The comparison will be done by calculating the time required for embedding the fingerprint watermark message to produce the watermarked document images and the time consumed for extracting the embedded message images respectively. In order to have a comprehensive comparison, both watermarked document images produced from the two methods have a close dB value and the time stamp is recorded at the same starting and ending point in the algorithm processes. The results show in (Table.1) below.

Compared items	DCT	DWT
dB value	38.37dB	38.09dB
Time consumed for getting watermarked document images	10.295 s	13.182 s
Time consumed for extracting the embedded watermark message .	10.383 s	12.199 s
Total time consumed for watermark message embedding and extraction	20.678 s	25.381 s

Table.1. Time consumed for watermark message embedding and extraction

From (Table.1), DCT algorithm requires less time for the processes of watermark message embedding and extraction than DWT algorithm. Therefore, one can view that DCT method has faster computation efficiency algorithm than DWT method in generating the watermarked document image and in extracting the embedded watermark message.

Imperceptibility and Visibility

Having close dB values and computational time figures shown in (Table.1) as the presetting background conditions to generate the pairs of watermarked document images and extracted watermark message for performing the imperceptibility and visibility quality comparisons, the watermarked document image (Fig.34) from DWT method seems to be little more imperceptible than the one (Fig.26) from DCT method. Compared the extracted watermark message (Fig.27) from DCT method with the one (Fig.35) from DWT, both images have similar visibility quality. As a whole, both methods yield a similar imperceptibility and visibility quality outcomes.

Robustness capability

Comparison is done by observing the visibility of the extracted fingerprint watermark message images whose watermarked document images have been interfered by imitating attacks Gaussian White Noise, JPEG Compression and Low-Pass Filter with equal degree of its associated interfering parameter Variance, favorable parameter Quality and interfering parameter Sigma. Observation on the above three sets of paired figures leads a conclusion that the all extracted fingerprint watermark message images from DCT method are more visible than those from DWT method. In other words, the watermarked document images generated by DCT method algorithm are more robust against attack than by DWT method.

To this instance, Discrete Cosine Transform method has higher computation efficiency and stronger robustness capability, similar visibility but less imperceptibility than Discrete Wavelet Transform method. Thus, one may consider that Discrete Cosine Transform method has better watermarking performance than Discrete Wavelet Transform method. Bearing in mind that the comparison here is just for this particular instance, one cannot treat this conclusion as a general fact for these two methods. More performance comparisons on different watermarked document images and different interfering attacks should be tested in order to obtain a more general conclusion. However, doing these experiments is out of the scope of this thesis, and thus will not be performed here but could be left for future studies.

IV. Conclusion

In this paper, the proposed Discrete Cosine Transform (DCT) method can successfully embed a gray level fingerprint watermark message into a copyright material image. The watermarked image is shown to be difference invisible against the original copyright material image. Moreover, the same method can be applied to extract the embedded fingerprint watermark message from a watermarked image. The same conclusion but with certain degree of tolerance can still be obtained if some sort of attacks simulated by resizing, pasting an overlay logo and cropping the watermarked image have been applied.

Moreover, an appropriate α value and image partition settings should be wisely selected while applying DCT method so that a balanced outcome between difference invisible effect and robustness and a better computational efficiency as applying DCT method can be obtained. Generally speaking, we can conclude that the DCT method can be considered a useful technique for data hiding which can be used for copyright material ownership authentication purposes.

Based on our prototype system, ownership authentication can be implemented by comparing signatory’s fingerprint captured immediately during the process against the fingerprint watermark message extracted from the watermarked image which had been archived in data centre. However, the authentication veracity will be affected as the watermarked image has been attacked by some sorts of interferences like resizing, pasting overlay logo and cropping the watermarked image. But the fingerprint watermark message matching can still be done but with certain degree of tolerance. The tolerance may not be acceptable as the interferences become larger. Therefore, further studies on other digital watermarking techniques and improvements on the current DCT Transform method to minimize the degree of tolerance even in larger interferences should be continued in the future.

References

[1] I. P. Office, "Copyright Basic facts," pp. http://www.ipo.gov.uk/c-basicfacts.pdf.

[2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," Proceedings of the IEEE, vol. 87, pp. 1062-1078, 1999.

[3] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," in Signal Processing Magazine. vol. 17, 2000, pp. 20-46.

[4] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," Proceedings of the IEEE, vol. 86, pp. 1064-1087, 1998.

[5] D. Kundur and D. Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition," in Acoustics, Speech and Signal Processing, 1998. Proceedings of the 1998 IEEE International Conference on, 1998, pp. 2969-2972 vol.5.

[6] D. Taskovski, S. Bogdanova, and M. Bogdanov, "Digital Watermarking In Wavelet Domain," in First IEEE Balkan Conference On Signal Processing, Communications, Circuits, And Systems, Istanbul, Turkey, 2000.

[7] A. G. Bors and I. Pitas, "Image watermarking using DCT domain constraints," in Image Processing, 1996. Proceedings., International Conference on, 1996, pp. 231-234 vol.3.

[8] T. Weili and Y. Aoki, "A DCT-based coding of images in watermarking," in Information, Communications and Signal Processing, 1997. ICICS., Proceedings of 1997 International Conference on, 1997, pp. 510-512 vol.1.

[9] B. Tao and B. Dickinson, "Adaptive watermarking in the DCT domain," in Acoustics, Speech, and Signal Processing, 1997. ICASSP-97., 1997 IEEE International Conference on, 1997, pp. 2985-2988 vol.4.

[10] T. Amano and D. Misaki, "A feature calibration method for watermarking of document images," in Document Analysis and Recognition, 1999. ICDAR '99. Proceedings of the Fifth International Conference on, 1999, pp. 91-94.

[11] W. Min and B. Liu, "Digital watermarking using shuffling," in Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference on, 1999, pp. 291-295 vol.1.

[12] W. Min, E. Tang, and B. Lin, "Data hiding in digital binary image," in Multimedia and Expo, 2000. ICME 2000. 2000 IEEE International Conference on, 2000, pp. 393-396 vol.1.

[13] Q. Mei, E. K. Wong, and N. Memon, "Data Hiding in Binary Text Documents," in Proc. of SPIE, 2001, pp. 369-375.

[14] W. Min and L. Bede, "Data hiding in binary image for authentication and annotation," Multimedia, IEEE Transactions on, vol. 6, pp. 528-538, 2004.

[15] Wikipedia, "Discrete cosine transform," http://en.wikipedia.org/wiki/Discrete_cosine_transform.

[16] I. The MathWorks, "2-D discrete cosine transform,", www.mathworks.com/access/help desk/help/toolbox/images/dct2.html

Chi-Man Pun received the B.Sc. and M.Sc. degrees from the University of Macau in 1995 and 1998 respectively, and Ph.D. degree in Computer Science and Engineering from the Chinese University of Hong Kong in 2002. He currently is an associate professor at the Department of Computer and Information Science of the University of Macau. His research interests include Content-Based Image Indexing and Retrieval, Digital Watermarking, Pattern Recognition, and Computer Vision.