การทำภาพพิมพ์ลายน้ำดิจิตอลโดยใช้วิธีกระจายแถบความถี่

ธำรงรัตน์ อมรรักษา [1] พงษกร จิระกุลสวัสดิ์ [2] และ บัณฑิต ทิพากร [1]

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี บางมด ทุ่งครุ กรุงเทพฯ 10140

บทคัดย่อ

บทความฉบับนี้นำเสนอกระบวนการทำภาพพิมพ์ลายน้ำดิจิตอลโดยใช้เทคนิคการกระจายแถบความถี่ในการระบุตำแหน่งในภาพต้นฉบับเพื่อฝังสัญญาณลายน้ำดิจิตอลใช้เทคนิคการกระจายแถบความถี่แบบความถี่กระโดด ในขณะที่การเพิ่มความทนทานของสัญญาณลายน้ำใช้เทคนิคการกระจายแถบความถี่แบบอันดับโดยตรง กระบวนการที่นำเสนอมีข้อได้เปรียบเหนือกว่ากระบวนการทำภาพพิมพ์ลายน้ำโดยใช้เทคนิคการกระจายแถบความถี่แบบดั้งเดิมคือ ในภาพต้นฉบับจะมีสัญญาณลายน้ำอยู่ในปริมาณที่ต่างกัน เพื่อที่จะให้คุณภาพของรูปภาพผลลัพธ์เสียหายน้อยที่สุด นอกจากนี้ในการใส่สัญญาณลายน้ำดิจิตอล ได้ทำการเลือกกลุ่มบิตขึ้นมาจากกลุ่มพิกเซลที่กำหนดไว้เพื่อใช้ในการใส่สัญญาณลายน้ำ การประเมินประสิทธิภาพของกระบวนการทำภาพพิมพ์ลายน้ำจะใช้ค่า Peak Signal to Noise Ratio (PSNR) ผลจากการทดลองได้แสดงให้เห็นว่า กระบวนการที่ได้นำเสนอให้ค่า PSNR ที่ดีกว่า ขณะเดียวกันยังสามารถใช้ฝังสัญญาณลายน้ำในปริมาณที่มากกว่าลงในรูปภาพต้นฉบับได้อีกด้วย

[1] *อาจารย์ประจำ ภาควิชาวิศวกรรมคอมพิวเตอร์*

[2] *นักศึกษาระดับบัณฑิตศึกษา ภาควิชาวิศวกรรมคอมพิวเตอร์*

Digital Watermarking using Spread Spectrum Techniques

Thumrongrat Amornraksa [1] Pongsakorn Jirakulsawad [2]
and Bundit Thipakorn [1]

King Mongkut's University of Technology Thonburi, Bangmod, Toongkru, Bangkok 10140

Abstract

A digital watermarking scheme, based on the spread spectrum techniques, is proposed in this paper. The scheme uses the frequency hopping spread spectrum technique to determine positions for watermark embedding in the original image, while the direct sequence spread spectrum technique is used to provide robustness to the watermark signal. This scheme has an advantage over the existing spread spectrum watermarking schemes, that is, various levels of watermark signal can be embedded into the original image in order to minimize the quality degradation of the watermarked image. To embed the watermark signal, the selected bits of selected pixels are used to carry the watermark signal. The performance of the watermarking scheme is evaluated by using the Peak Signal to Noise Ratio (PSNR). The experimental results indicated that the proposed scheme gained higher PSNR and, simultaneously, more watermark bits could be embedded into the original image.

[1] *Lecturer, Department of Computer Engineering.*

[2] *Graduate Student, Department of Computer Engineering.*

1. Introduction

The rapid development and deployment of new IT technologies have improved the ease of access to digital information. Since digital data can be reproduced infinitely without any loss of quality, it is therefore difficult to differentiate the illegal copies from the original one. The copyright protection for multimedia data is then needed to counteract the piracy. Several techniques in digital signal processing have been studied and emerged to provide copyright owners with the desired degree of protection and to act as a disincentive to data piracy, for example, digital signature, digital fingerprint, and digital watermarking. However, digital watermarking techniques have been widely used as a solution for protecting the copyrighted data [1].

Digital watermarking is a method for embedding hidden data that contains copyright related information into the digital object. This provides an ownership identification of the object, and possibly other information that conveys conditions of use. Therefore, watermarking enables identification and tracing of different copies of distributed data. Watermark embedding can generally take place either in a spatial domain or in a transformed domain. In spatial domain watermarking, the watermark signal is directly embedded into the value of each pixel in an image, while in frequency domain watermarking, the watermark signal is embedded into the coefficients of the transformed image. Several techniques have been proposed to embed the watermark signal into various kinds of data such as text, audio, images and video. Digital watermarks can be either a visible or an invisible "seal" placed over an image to identify the copyright owner.

The requirements on digital watermarking are number of desirable characteristics that a watermark should exhibit. Since different applications have different requirements, there is no unique set of requirements that all watermarking techniques must satisfy. Some of the desirable properties are :

- Imperceptibility : the watermark should not be noticeable to the viewer nor should it degrade the quality of the content.

- Robustness : the watermark should not be removed or destroyed without degrading the quality of the image. It should be robust to common signal processing methods. Thus, the major challenge in watermarking is to ensure both imperceptibility and robustness. It is obvious that this requirement conflict with each other.

- Unambiguousness : Retrieval of the watermark should unambiguously identify the owner of the content.

- Universality: the same digital algorithm should be appropriated for all media under consideration. This allows audio, still image or video watermarking to be done on common hardware.

2. Literature Review

Nowadays, large numbers of watermarking technique have been proposed, and the survey on those vital techniques is described as follows. A watermarking based on Discrete Cosine Transform (DCT) method, in which the watermark signal was embedded into the middle-frequency range of DCT coefficients of the transformed original image was proposed by Rekocevic *et al* [2]. The DCT coefficient was constants after transforming the image from spatial domain into spectral domain. However, when the watermarked image was compressed by JPEG (Joint Photographic Experts Group) with high compression ratio, the watermark embedded in the middle-frequency range of DCT coefficients was destroyed. Alternatively, an efficient method which embedded the watermark into the image by modifying 1000 largest DCT coefficients of the image was proposed by Cox *et al* [3]. However, modification of these spectral components resulted in severe image degradation. In this method, the watermark signal was prepared by spread spectrum technique, the information was firstly spread and then modulated with pseudo random noise before being embedded. The experimental results showed that the watermark could be effectively extracted, even if the watermarked image had been significantly degraded through several common geometric and signal processing attacks.

In 1999, Ng *et al* [4] proposed a Pixel Position Shifting (PPS) watermarking method. This method was started by calculating the summation of all 64 values in each 8x8 pixel-block, then the result was divided by 16 to obtain the remainder. This remainder was used to calculate the starting point for embedding the watermark in the DCT coefficients. Moreover, the hamming code (8, 4) was employed to detect and correct the error. However, the disadvantage of this method was that the watermark was not robust against the low-pass filter and medianpass filter. Hsu and Wu [5] proposed a multi-resolution watermark embedding algorithm, in which lower resolution watermark was embedded into the lower frequency components of the image, while the higher frequency watermark resided in the higher frequency components of the image.

A watermarking scheme, based on direct sequence spread spectrum technique, was proposed by George *et al* [6]. In this scheme, a secret message was spread with the assigned chip-rate. The spread sequence was modulated by a pseudo-random noise sequence. The modulated signal was then scaled with a factor α before being added to the original image pixel-by-pixel. Due to the noisy nature of pseudo-random noise sequence, the embedded watermark was difficult to be detected, located, and manipulated.

3. Background

Since the proposed watermarking applies the spread spectrum techniques, which consist of Direct Sequence Spread Spectrum (DS-SS) technique and Frequency Hopping Spread Spectrum (FH-SS) technique, the principle of DS-SS technique will be first given. Then, the concept of FH-SS technique will be briefly described.

3.1 Direct Sequence Spread Spectrum Technique

In the DS-SS communications [7], a low level wideband signal can be easily hidden within the same spectrum as a high power signal, which each signal appears to be noise to the other. The core component of these spread spectrum systems is a Pseudo Random Noise Sequence (PRNS). For these direct sequence spread spectrum systems, the original baseband bit stream is multiplied by the PRNS to produce a new bit stream. Only those receivers equipped with correct PRNS can decode the original message. At the receiver, the low level wideband signal will be accompanied by noise. By using a suitable detector/demodulator with the correct PRNS, this signal can be squeezed back into the original narrow baseband. As the noise is completely random and uncorrelated, the desired signal can easily be extracted.

3.2 Frequency Hopping Spread Spectrum Technique

The FH-SS technique involves a periodic change of transmission frequency [8]. A frequency hopping signal may be regarded as a sequence of modulated data bursts with time-varying, pseudo-random carrier frequencies. The set of possible carrier frequencies is called the hopset. Hopping occurs over a frequency band that includes a number of channels. Each channel is defined as a spectral region with a central frequency in the hopset. The bandwidth is large enough to include most of the power in a narrow band modulation burst, having the corresponding carrier frequency. Data is therefore sent by hopping the transmitter carrier to seemingly random channels which are known only to the desired receiver. On each channel, small bursts of data are sent using conventional narrowband modulation before the transmitter hops again.

4. The Proposed Scheme

As already mentioned, the DS-SS technique is used in the watermark generating process to provide robustness to the embedded signal, while the FH-SS technique is used in the locations determining process to determine the embedding positions in the original image. This section will describe the detail of the watermarking scheme which consists of watermark generating, locations determining, watermark embedding and extracting, respectively.

4.1 Watermark Generating

First, a sequence of information bits, consisting of −1 and 1, is spread by multiplying with a large factor, called chip-rate *Cr*, to obtain the spread information sequence. The size of this sequence is equal to the value of chip-rate multiplied by number of information bits [9]. The spread sequence is then modulated with a binary pseudo-noise sequence to yield the modulated spread sequence, and is finally amplified with a locally adjustable amplitude factor to obtain the watermark signal. The block diagram of watermark generating process is illustrated in Fig. 1, part A.

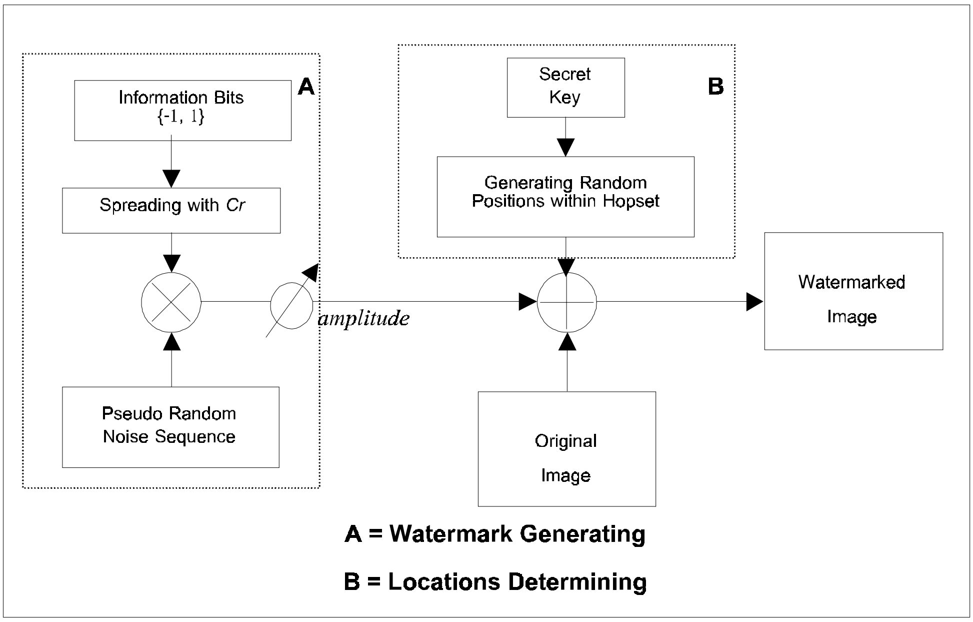


Fig. 1 Block diagram of the watermarking scheme

4.2 Locations Determining

In this step, each bit of the watermark signal will be embedded into some assigned locations (or pixels), which is randomly determined by a key-based FH-SS technique, within the image frame, instead of whole frame [10]. Therefore, each watermark bit will only be dispersed over its corresponding locations within some parts of the image. The block diagram of location determining process is illustrated in Fig. 1, part B.

For example, considering an original image with the size of 256x256 pixels, all available pixels in the image is equal to 65536, and is considered as a hopset. If 10% of image frame is required to embed the watermark, 6554 locations within the hopset will be pseudo-randomly determined, with no repeated locations, and used to carry the watermark signal. According to the figure, those selected locations are used to perform the watermark embedding process.

4.3 Watermark Embedding

In this step, each watermark bit is merely embedded into the assigned pixels by using additive operation. The output will be the watermarked pixels. Note that the image will contain both unmarked and marked pixels. This ratio is up to the applications and user's satisfaction. Furthermore, in the proposed scheme, only some selected bits, e.g. 4, 5, 6-bit, within the selected pixels will be used to carry the watermark signal. Note that in the ordinary watermarking scheme, 8-bit within a pixel, which represents the number ranging between 0-255, is used to carry one bit of watermark signal, while in the propose scheme, only some bits with in a pixel, e.g. 5-bit which represents the number ranging between 0-31, is used in stead.

4.4 Watermark Extracting

To recover the embedded information, it is necessary to precisely determine the hopping locations, where the watermark signal is added. The watermarked pixels is firstly correlated with the same pseudo-noise sequence used in the watermark generating process. Correlation here is demodulation followed by summation over the width of the chip-rate. Finally, the sign of the correlation sum determines the embedded information bit [9].

5. Experimental Design and Evaluation Method

The original image used in the experiments consisted of various 8-bit standard images with the size of 256x256 pixels such as *Airplane*, *Lena*, *Boat*, *Barbara* etc. MATLAB program was used as a tool to simulate the watermarking scheme by embedding the watermark signal into some random parts within the image frame. It was also used to measure the scheme's performance against various types of attack such as brightness/contrast enhancement, lowpass/highpass/median filtering, JPEG compression standard, additive Gaussian/uniform distributed noise.

Since PSNR (Peak Signal to Noise Ratio) is the standard metric for evaluating the differences between two versions of image, in this paper, it is used to assess the quality of the watermarked images, compared to the original one's. In the image-processing field, the PSNR is defined below

$$\mathrm{PSNR} = 20\log_{10}\left(\frac{\mathrm{b}}{\mathrm{RMSE}}\right) \tag{1}$$

when b is the maximum value of the luminance signal, in case of gray scale, b is equal to 255. The RMSE is Root Mean Square Error, and equal to $\sqrt{\mathrm{MSE}}$. The variable in the square root is Mean Square Error (MSE), which is an estimation of the population variance in the analysis of variance, and is defined as follows :

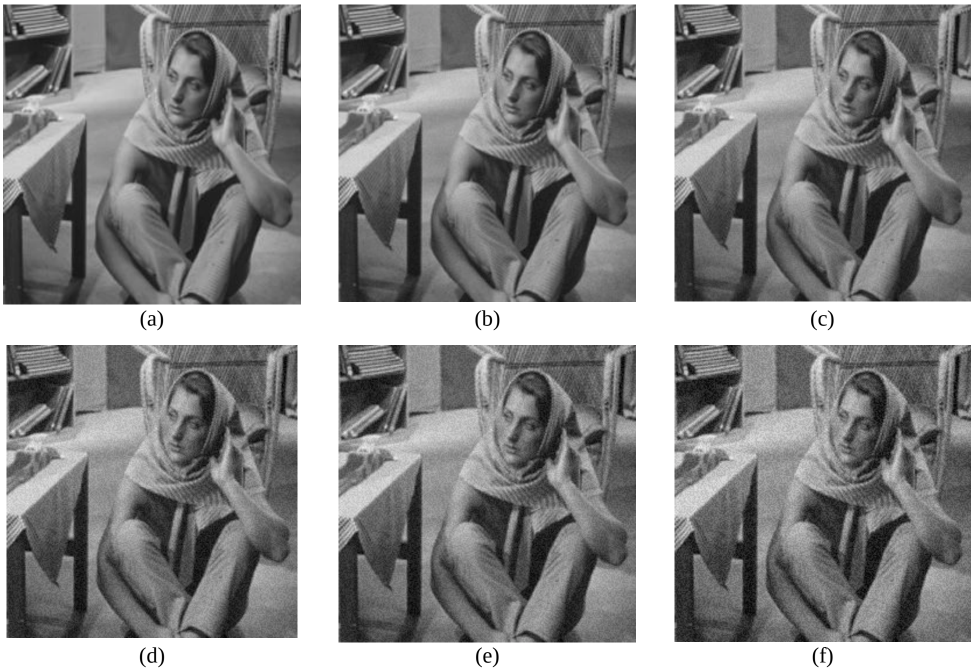
$$\mathrm{MSE} = \frac{1}{\mathrm{N}} \times \left(\mathrm{SUM}_{\mathrm{ij}} \left| \mathrm{Org}_{\mathrm{ij}} - \mathrm{Wmk}_{\mathrm{ij}} \right|^{2} \right) \qquad (2)$$

where N is total number of pixels within an image, $\mathrm{Org}_{\mathrm{ij}}$ and $\mathrm{Wmk}_{\mathrm{ij}}$ are the value of pixel (i, j) in the original and watermarked images, respectively.

Since the PSNR is used to indicate how much the watermarked image is differed from the original image, it can be said that the lower the value of PSNR, the more different the two images are. In other words, the quality of the watermarked image is much deteriorated if its PSNR is low. On the other hand, if the value of PSNR is high, it implies that the quality of the watermarked image is as close as that of the original one.

6. Experimental Results

The experiment was first performed by embedding the watermark signal into the original image *'Barbara'*, with the aim of determining a proper value of amplitude factor, α. Fig. 2 shows a number of resultant outcome of the original and watermarked images at various amplitude factors.



(a) (b) (c)

(d) (e) (f)

Fig. 2 Comparison of the watermarked images at various amplitude factors

(a) original image

(b) watermarked image with α = 1

(c) watermarked image with α = 3

(d) watermarked image with α = 5

(e) watermarked image with α = 7

(f) watermarked image with α = 10

From Fig. 2, it is obvious that the higher the amplitude factor, the higher the degradation of image. The plot of PSNR value at each amplitude factor resulted from Fig. 2 is also shown in Fig. 3.

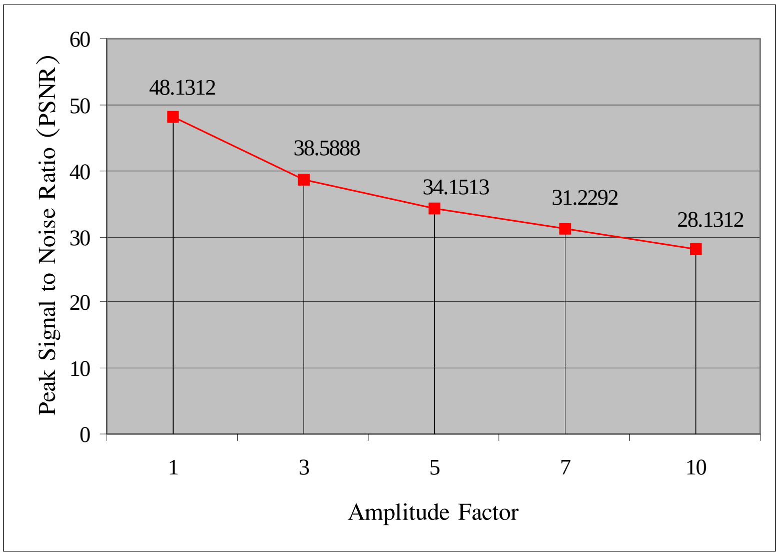


Fig. 3 The plot of PSNR values at various amplitude factors

After the proper amplitude factor was selected, i.e. $\alpha = 3$, the experiments were carried on by embedding the watermark signal into parts of the original image at different levels ranging from 10%, 20%, ... 100%. The experimental results are shown in Fig. 4.

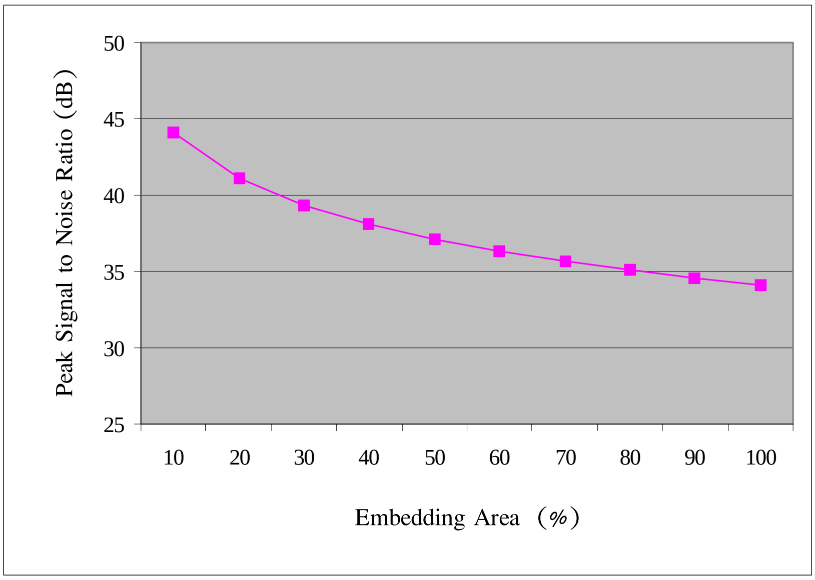


Fig. 4 Average PSNR value at various level (%) of embedding area within an image

Furthermore, when the embedding area was reduced, the resulting outcome effected directly to the processing time used in the watermark embedding process. Fig. 5 shows the plot of processing time needed at different values of embedding.

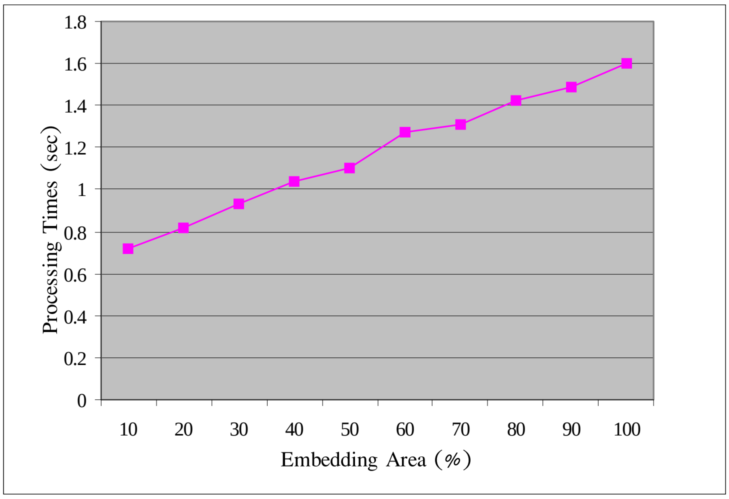


Fig. 5 Average processing time VS. Embedding area

When the image area used to embed the watermark signal was decreased, it apparently reduced the amount of information rate in the embedded signal. Therefore, the technique of reducing the block size used to carry the watermark signal was applied. In other words, only some selected bits within the selected pixels were used to carry the watermark signal. It was concluded in [11] that the smaller the block size, the smaller value the chip-rate required to recover the information bits correctly.

Since a smaller value of chip-rate was used, the amount of information bits to be embedded into the image frame would be increased. Table 1 shows the smallest value of chip-rate required to correctly recover the embedded bits at various block sizes.

Table 1 The smallest value of chip-rate required at various block sizes

	Chip-rate c_r required to correctly recover the embedded bits					
Original Image	Block Size 3	Block Size 4	Block Size 5	Block Size 6	Block Size 7	Block size 8
Airplane	20	65	235	320	1890	4000
Tiffany	20	75	220	620	2300	3950
Splash	22	55	168	580	2000	3150
Boats	20	95	270	480	1200	2950
Barbara	18	68	245	560	1300	2450
Logo	45	220	720	2500	6000	10000

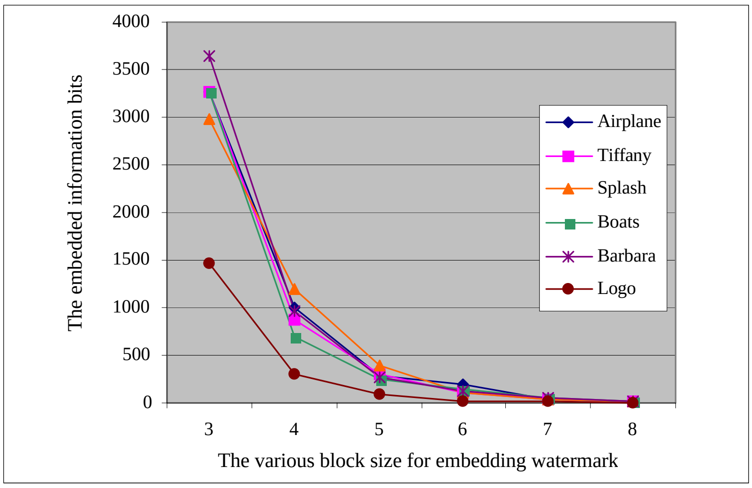


Fig. 6 The plot of embeddable information bits at various block size

When the information rate was kept constant while the block size used to carry the watermark signal was changed, the improved value of PSNR would be obtained, and the results were shown in Fig. 7.

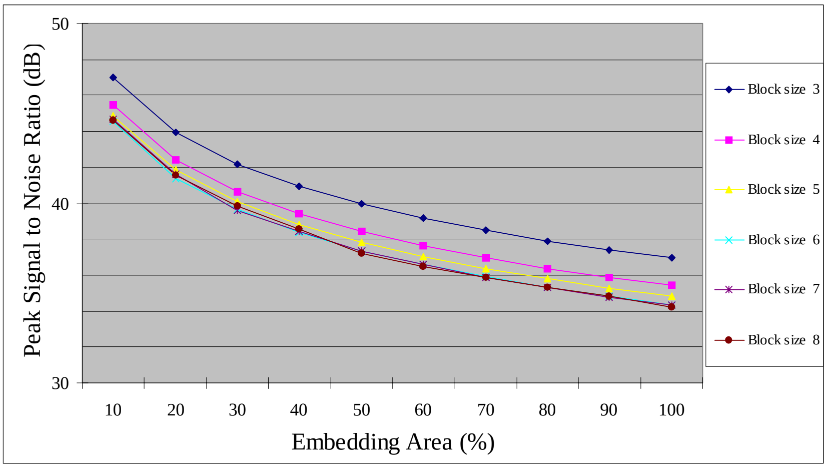


Fig. 7 The plot of value of PSNR at various percentages when block size was changed

To evaluate the robustness of the proposed watermarking scheme. Various types of attack, which is admiringly used in image-processing field, were applied to the watermarked images. These types of attack were as follow: Brightness enhancement at 33%, Contrast enhancement at 42%, Lowpass filtering with radius of 0.24 pixel, Highpass filtering with radius of 7 pixel, Median filtering with radius of 1 pixel, JPEG compression standard at 90% quality, additive Gaussian distributed noise at 80%, additive Uniform distributed noise with variance 0.001. Note that, at the specific value given above, the watermarking scheme could robust against all of those attacks without any error in the extracting process. However, other higher values or higher levels of attacks resulted in occurrence of errors in the extracted watermark bits.

7. Discussions

From the experimental results, it can be obviously seen that the quality of the watermarked image was significantly improved since the watermark signal was embedded into some parts of the image frame only. Moreover, the scheme provided the same level of robustness against common attacks since the attackers need to modify all pixels of the watermarked image in order to destroy the embedded signal, provided the attackers have no ways to determine such locations used in the watermark embedding process. In other words, it can be said that the proposed scheme provided the same security level as the existing scheme, where the watermark signal was embedded into the whole image frame. Furthermore, this scheme gave less time-consuming used in the computational process. One advantage of using the FH-SS technique that can be undoubtedly claimed is that the embedded signal is robust to some potential attacks, especially to the collusion attack, since attempting to determine the watermark's location from different copies will not be possible.

Since the information rate was decreased, after reducing the embedding area within the image, it can be compensated by using some selected bits within the selected pixels to carry the watermark signal. To clearly see the advantage of our technique, the following example is given. Let an image's resolution be 256x256 pixels, which can carry the watermark bits up to 65536 bits/frame. Using the ordinary watermarking scheme, which uses block size of 8 to embed the watermark bits, the chip-rate must be at least 10000 in order to be able to correctly recover the embedded bits, according to Table 1, and the information up to 6.5 bits are then allowed to be embedded within such image frame. In contrary, by using our scheme with 50% embedding area at the block size of 5, the same image can carry the information up to 32768 bits/frame. However, since the block size of 5 is used, the smaller value of chip-rate at 720 is required, and therefore the information rate will be increased to 45.5 bits/frame, which is 7 times higher.

8. Conclusions

In this paper we have presented the watermarking scheme based on the spread spectrum techniques. The scheme used the FH-SS technique to locate the watermark embedding positions, while the DS-SS technique was used to generate the watermark signal. The proposed scheme improved the quality of watermarked image, while provided the same level of security, compared to the existing schemes. Although decreasing the embedding area caused the information rate to fall off, we could compensate this incident by adding the watermark signal into some selected bits within a pixel. The experimental results have shown that the total information rate was significantly improved, due to a smaller value of chip rate required to correctly recover the embedded signal.

9. Acknowledgements

The authors would like to thank the National Electronics and Computer Technology Center (NECTEC) for financial support throughout this work (Funding Code: NT-B-06-4C-20-319).

10. References

1. Shaw, S., 2000, "Overview of Watermarks, Fingerprints, and Digital Signatures," http://www.jtap.ac.uk/reports/htm/jtap-034.html.

2. Rakocevic, I., Reljin, B., and Reljin, I., 1999, "A Method for Providing Digital Image Authenticity," Telecommunications in Modern Satellite, Cable and Broadcasting Services, *The 4th International Conference*, Vol. 1, pp. 173-176.

3. Cox, I. J., Kiliant, J., Leighton T., and Shamoon, T., 1997, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transaction on Image Processing*, Vol. 6, December, pp. 1673-1687.

4. Ng, K. S., Cheng, L. M., Cheng, L. L., and Wong, M. K., 1999, "Adaptive Watermarking by Using Pixel Position Shifting Technique," *IEEE Transaction on Consumer Electronics*, Vol. 45, No. 4, November, pp. 1057-1064.

5. Hsu, C. T. and Wu, J. L., 1998, "Multiresolution Watermarking for Digital Images," *IEEE Transaction on Circuits and Systems II : Analog and Digital Signal Processing*, Vol. 45, No. 8, August, pp. 1097-1101.

6. George, M., Chouinard, J. Y., and Georganas, N., 1999, "Digital Watermarking of Images and Video using Direct Sequence Spread Spectrum Techniques," *Proceedings of the 1999 IEEE Canadian Conference on Electrical and Computer Engineering Skhaw Conference Center*, Edmonton, Alberta, May 9-12, Canada, pp. 116-121.

7. Pickholtz, R., Schilling, D., and Millstein, L., 1982, "Theory of Spread Spectrum Communications a Tutorial," *IEEE Transaction on Communication*, Vol. COMM-30, pp. 855-884.

8. Rappaport, T. S., 1996, Wireless Communications Principle and Practice, New Jersey, Prentice Hall, pp. 276-280.

9. Hartung, F. and Girod, B., 1998, "Watermarking of Uncompressed and Compressed Video," *Signal Processing (Special issue on Watermarking)*, Vol. 66, No. 3, May, pp. 283-301.

10. Jirakulsawad, P. and Amornraksa, T., 2001, “Watermark Embedding using Frequency Hopping Technique,” *Proceedings of the 39th Kasetsart University Annual Conference*, February 5-7, Bangkok, Thailand, pp. 185-192.

11. Amornraksa, T., 2000, “Transmitting Extra Information Bit using Direct Sequence Spread Spectrum,” *Proceedings of the 3rd International Symposium on Wireless Personal Multimedia Communications*, Thailand, November 12-15, pp. 76-80.