Proceedings of the 5th WSEAS International Conference on Applications of Electrical Engineering, Prague, Czech Republic, March 12-14, 2006 (pp65-68)

A Study on the Copyright Protection using Watermarking Technique in Power Line Communication Network

Yang-Sun Lee Heau-Jo Kang Yoon-Ho Kim
Department of Computer Engineering
Mokwon University
Doan-dong 800, Seo-gu, Daejeon, 302-729
KOREA
http://www.mokwon.ac.kr

Abstract: - In this paper, we propose a device to track the location of illegal reproduction and monitor illegal reproduction by testing with digital watermark, in order to protect copyright of digital contents and prevent massive distribution through illegal reproduction.

Key-Words: - watermarking, copyright protection, Power Line Communication, track system

1 Introduction

The digital watermarking technique was proposed for the copyright protection of multimedia data. Here, the watermark must be inserted in voice or video signal. And, it must be by the uncopyrighter is not recognized. Also, it must be detected by only the copyrighter. The watermark is mark not visible with the technique in objective for a copyright protection in image or voice data. Namely, it talks a code or the pattern which is special is inserted in image or speech signal [1],[2].

But, it has many problems with only the fact that it inserts a water mark from digital data. Consequently, we propose the method for quickly prevent illegal reproduction with insertion of watermarking when detecting a watermark. And, we simulated proposed method using the DS-CDMA/BPSK system considered AWGN and impulsive noise in Power Line Communication (PLC) environment.

2 Watermarking detection and tracking system

2.1 Scenario

This study is to suggest a device to track the location of illegal reproduction and monitor illegal reproduction by testing with digital watermark, in order to protect copyright of digital contents and prevent massive distribution through illegal reproduction.

Figure 1 shows a scenario of watermark test and detection suggested by this paper, while figure 2 representing flow chart of the scenario. The device suggested is fitted to input and output equipments such as duplicator, scanner, and printer. Functions of the device are as in the following ;

(1) When illegal reproduction of the contents produced by a person or public agencies is being attempted via input and output equipment, it is possible to analyze the information of the contents put into the device suggested and detect watermark.
(2) If any correlation beyond a certain level is detected after comparing the detected watermark with the information of watermark stored in the device in question, it recognizes it as illegal reproduction and stop the operation of the input and output equipment.
(3) This device adds information on location to watermark data and transfer them to public agencies (investigation or monitoring agencies) through power line.
(4) The watermark data transferred serves to provide information the check and track the location of the sender for the public agency.

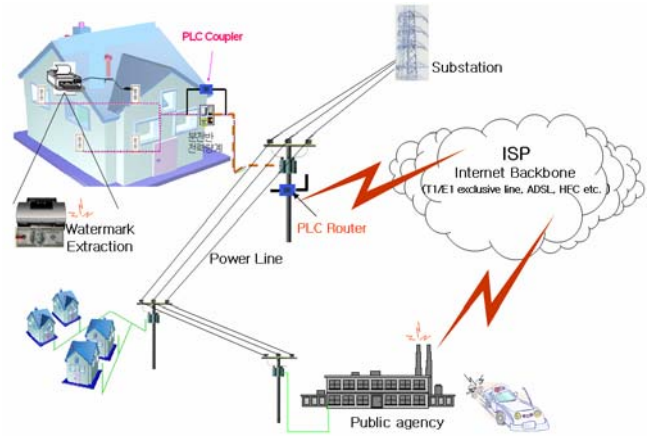

Fig. 1 Scenario of watermark detection and track.

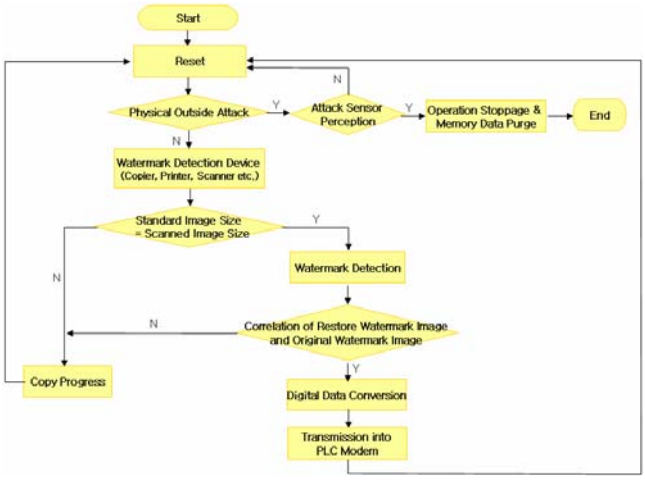

Fig. 2 Flowchart of proposed systems.

2.2 Watermarking algorithm

Figure 3 shows the process of inserting and detecting watermark image based on the Key value. A after performing a DCT (Discrete Cosine Transform) of image on the basis of 8X8 block and generating sequence through a specific Key value, you have to insert watermark to the intermediate frequency band, considering loss of data and frequency area, which is hard to be recognized by men [3].

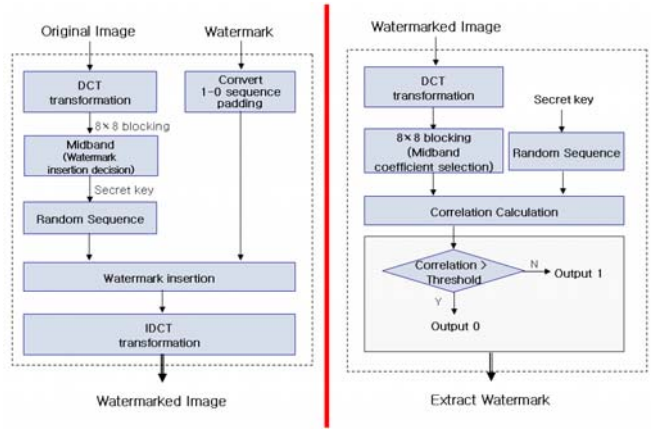

Fig. 3 Process of image insertion and extraction.

In addition, watermark image should be detected by generating sequence with secrete key in the same order as the insertion of watermark, measuring coefficient value and correlation of intermediate frequency area of the image with the inserted watermark and comparing threshold value of such coefficient value and correlation.

2.3 DS-CDMA/BPSK system

Direct Spread (DS), which is a method to modulate carrier frequency again into pseudo random noise code (PN code), has a lot of advantages including simple system configuration and easier modulation.

Figure 4 shows the interpretation model of DS-CDMA/BPSK simulated in this study.

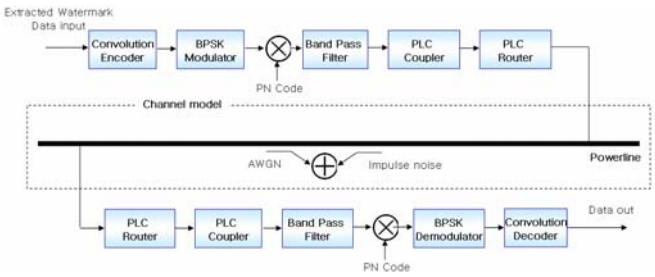

Fig. 4 System simulation model.

3 System simulation and review

Although judgment of quality of decoding image should be made by human beings, it is based on correlation of the original and detected image. Equation 1 is a correlation coefficient equation, which compares and processes correlation coefficient between the two images in the matrix (or vector) where A and B are identical [3].

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\sum_m \sum_n (A_{mn} - \bar{A})^2 \sum_m \sum_m (B_{mn} - \bar{B})^2}} \quad (1)$$

Where, A=original image,
B=decoding image,
$\bar{A}$ = the mean of the element of a matrix (A)
$\bar{B}$ = the mean of the element of a matrix (B)

Table 1 indicates correlation between the original watermark and the resulting watermark detected by inserting watermark according to key value.

Table 1. Correlation level according to variable threshold value.

Threshold	Correlation	Threshold	Correlation
0.1	0.6240	0.6	0.7386
0.2	0.7019	0.7	0.6863
0.3	0.7736	0.8	0.6085
0.4	0.7924	0.9	0.4659
0.5	0.7770		

According to table 1, correlation is the highest when the threshold value is 0.4. Therefore, in this paper, simulation of watermark detection judgment was based of the threshold value 0.4.

Table 2 shows watermark images detected at a threshold value 0.4. If correlation level between detected watermark and the original match each other to a certain degree, the system suggested in this study transfers the watermark images and address through power line, after modulating them using DS-CDMA/ BPSK system. Table 3 shows comparison of capability of watermark images according to the application of convolution encoding technique after transferring via power line.

Table 2. Result image in case of threshold value=0.4.

original image (512x512)	Original watermark (64x64)
	
Image inserted watermark (512x512)	**Extracted watermark image (64x64)**
	

Table 3. Comparison of watermark images according to the application of convolution encoding.

Before applying convolution			After applying convolution		
SNR	Image	correlation	SNR	Image	correlation
2		0.3094	2		0.6941
4		0.3990	4		0.8617
6		0.4498	6		0.9439
8		0.4796	8		0.9740
10		0.5071	10		0.9814
12		0.5292	12		0.9833

It indicates that when convolution is not applied, the capability is low down to the correlation level of 0.3990 at SNR=4dB, making the images damaged hard to recognize by the impulse intervention after

being transferred through power line. On the other hand, when convolution is applied, the capability is enhanced 2 times higher than before the application of convolution, showing correlation level 10.867 at SNR=4dB.

4 Conclusion

In this paper, we proposed ways to prevent illegal reproduction through quickly taking countermeasures at the time of detecting watermark as well as simply inserting watermark and conducted a simulation of system proposed by DS-CDMA/BPSK system in the PLC environment based on the consideration of AWGN and impulsive noise. Watermark detection and tracking device proposed in this study is considered suitable for illegal reproduction prevention system of image contents designed for special purposes.

References:

[1] A Z. Tirkel, R. G. Schyndel and C. F. Osborne, A digital watermark, *In Proc. Of IEEE ICIP'94*, Vol. 2, pp. 86-90, 1994.

[2] W. Bender, D. Gruhl, N. Morinoto and A. Lu, Techniques for data hiding, *IBM Systems Journal*, Vol. 35(3/4), pp. 313-336, 1996.

[3] Yu Zin Zang, Ting Chen, Juan Li, Embedding Watermarks into both DC and AC Components of DCT, *Proceeding of SPIE*, 2001.