A Watermarking Method with a New SS technique

Kun Hua[1] and Liang Pu[2]

[1] Computer and Electronic Engineering Dept. University of Nebraska Lincoln,
1110 S 67th St. 68182, USA
[2] School of Energy and Power Engineering, Xi'an Jiaotong University
28 W Xianning Rd. Xi'an 710049 China
`khua@unlnotes.unl.edu`

Abstract. Among numerous techniques of information concealment, Spread spectrum watermarking (SSW) has proved to yield improved results when robustness against attack is at a premium. SSW hides information which is called watermark by spreading its spectrum and then adding them to a host image as a watermarked image. Spreading spectrum is done by a pseudo-noise (PN) sequence. But in standard SSW approaches, receiver must use a separate channel to achieve PN sequence used at the transmitter for detecting hidden information. The unique PN sequence must have a low cross correlation and thereby can be duplicated easily by hostile attackers. In this paper a novel approach based on the unconventional Random Encoding Spread Spectrum is proposed for recovering the spreading sequence of watermark signal without any information from the transmitter. It is contributed a higher secure feature by using of the time-varying random encoded spread spectrum.

Keywords: Data Mining, Spreading Spectrum Watermarking, Pseudo-noise.

1   Introduction

Nowadays, the digital watermarking technique is regarded as a promising means to address such problems as copyright protection, contention authentication, device control and signal multiplexing. The mostly important requirements for a digital watermarking system are the watermark transparency, robustness and security. Several kinds of digital watermarking techniques have been applied by industrial or academic approaches.

Spread spectrum technology is an important anti-interference technology in the watermarking. In traditional spread spectrum communications, short pseudo-noise (PN) codes are used broadly as spread spectrum sequences. For instance, m sequence and Gold sequence. PN codes have some noise-like characteristic. However it has certain periodicity and can be duplicated easily, which compromises the transmission security.

Recently, a lot of works have been done on hostile detecting by means of data mining [1]-[4]. Saeed raised a scheme based on Genetic Algorithm (GA) [5]. The approach is proposed for recovering PN sequence and detecting location with GA

optimization search, hence unauthorized users could detect hidden information from the watermarked signal. For example, by using of GA optimization search, a PN sequence with period of 63 chips and it's location can be detected by attackers in 70 seconds.

In order to improve the disadvantage of traditional spread spectrum, the theory of Random-Encoded Spread Spectrum (RESS) was presented in this paper, which avoids using the fixed spreading sequences. In this system, the spreading code is obtained from the transmission signal. To some extend, the dynamic variable spreading sequences assure the transmission security and low probability of detection (LPD) by attackers.

Comparing traditional spread spectrum, there are several advantages to exploit RESS into watermarking:

(1) RESS doesn't require a separate channel to transmit the spreading codes to the receiver. Watermarked signal is totally "white noise" to attackers.

(2) RESS can enhance watermarking transmission security by true random spreading sequence. Pseudo Noise sequence is just like random sequence.

(3) PN codes is fixed once they have been generated, so PN codes can be duplicated by unauthorized attackers. But in RESS, the spreading sequence is not only randomly generated and independent of the current symbol, but also dynamically changing form one symbol to the next. Also we can say it's time-varying random codes and is hard to be duplicated.

In this paper, we proposed a novel approach based on Random-Encoded Spread Spectrum for recovering PN sequence of watermark signal without any information from the transmitter. It is contributed a higher secure feature and LPD by using of the time-varying random encoded spread spectrum.

In section 2, we present the system model of the Random encoded spread spectrum system. The processing of RESS watermarking is described in section 3. The simulation parameters and results are presented in section 4. Conclusions of the paper are made in section 5.

2   Random Encoded Spread Spectrum

2.1   System Description

In the RESS system model, at the transmitter, delay registers are updated from N-tap delay of data where N is the code length. Delay registers generate the code chips that switch at N times the data rate for signal spreading. The random nature of the digital information source is assured by using data compression methods. The register contents at the transmitter and receiver should be identical initially. Differential coding (DC) is used in this system to avoid the error propagation among delay registers.

Our approach to improving the low probability of detection performance is to completely abandon the use of PN sequences. The random nature of the digital

information source is assured by applying appropriate data compression methods to remove any redundancy in the data stream, thereby maximizing its entropy. The binary data symbols can therefore be modeled as independent and identically distributed Bernoulli random variables. Symbol values of +1 and -1 occur equally likely with a probability of 1/2. As a result, the spreading sequence is not only randomly generated and independent of the current symbol, but also dynamically changing from one symbol to the next.

The random encoding operation at the transmitter is reversed at the receiver. The recovered data are fed back to the N-tap delay registers that provide an estimate of the transmitter's spreading codes required for signal de-spreading. Data recovery is by means of a correlation detector. As a result, random encoding makes unwanted detection of the data by an unintended receiver practically impossible. The security of the transmission can greatly be enhanced with this low probability of detection communication system.

3   Watermarking

3.1   Watermarking Embedding

Watermarking Embedding is performed in DCT domain. At first, we divide host image W into M non-overlapping 8×8 blocks[6]-[9],

$$W = \bigcup_{m=0}^{M-1} W_m(u,v), 1 \le u,v \le 8 \tag{1}$$

So there are M DCT coefficient $\tilde{W}(u,v)$ after DCT transformation for each block, and

$$\tilde{W} = \bigcup_{m=0}^{M-1} \tilde{W}_m(u,v) = \bigcup_{m=0}^{M-1} C_{DCT}[W_m(u,v)], 1 \le u,v \le 8 \tag{2}$$

Embed RESS watermarking data into 8 low frequency components of every 8×8 blocks of host image W, that is :

$$\tilde{W}_z = \bigcup_{m=0}^{M-1} \tilde{W}_{z_m}(u,v) = \bigcup_{m=0}^{M-1} C_{DCT}[W_m(u,v) + \alpha_m \bigcup_{i=8m}^{8m+7} Z_{s_i}] \tag{3}$$

The next step is to do IDCT to get the watermarked image W_Z,

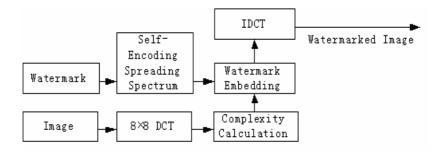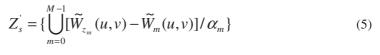$$W_Z = \bigcup_{m=0}^{M-1} C_{IDCT}^{-1}[W_m(u,v)] \tag{4}$$

Fig. 1. RESS Watermarking Embedding Structure

3.2 Watermarking Extracting

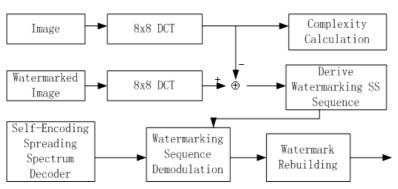To extract the watermark from the watermarked image, we first take 8×8 DCT and recover the watermark image by:

$$Z'_s = \{ \bigcup_{m=0}^{M-1} [\widetilde{W}_{z_m}(u,v) - \widetilde{W}_m(u,v)] / \alpha_m \} \tag{5}$$

Fig. 2. RESS Watermarking Extracting Structure

The last step will be RESS decoding part. After this step, recovered watermark image Z' is extracted and will be compared with the original watermark image Z.

4 Experimental Results

4.1 Watermarking Results

In our simulation experiments, the original host image is taken as a gray testing image and the testing watermarking image is a 2-values image. In water marked image, we choose PSNR as 50dB and Gaussian Noise variance as 0.01. Spreading factor N=128. Delay register length m=7.

Fig.3 is the original host image and Fig.4 is the testing watermarking 2-values image. Fig.5 is the watermarked image and Fig.6 is the recovered watermark.

Fig.3-Fig.6 show that the watermark image is totally invisible in watermarked figure and can be recovered desirably. We can conclude that RESS can not only achieve a similar performance as conventional PN sequence spreading spectrum do, but also acquires higher secure feature and simpler structure without the separate channel for spreading sequence.

Fig. 3. Original Figure

Fig. 4. Watermark image pattern

There was a shortage for regular spread spectrum watermarking algorithm: If the spreading sequence length is not long enough, the system can not achieve the ideal result. Thus, the original image must be very large which is hard to explore. But if we cut the image figure smaller, the spread spectrum sequence is also shorten, and the result is that the robustness of the whole system is influenced. But while Random-Encoded Spread Spectrum is introduced in this paper, any short sequence is still random.

What is more, we can now select much more spreading sequences than regular techniques[10]-[12]. This means for multi-users application in digital watermarking, more individual information can be sent in the same time without great interference comes from other information. This approach is still need to be proved by real experimental results.
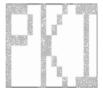
Fig. 5. Watermarked Figure

Fig. 6. Recovered Watermark

5　Conclusion

In this paper, a novel approach based on Random-Encoded Spread Spectrum is proposed for recovering spreading sequence of watermark signal without any information from the transmitter. It mainly contributed a higher secure feature by using of the time-varying random Random-encoded spread spectrum instead of the typical PN sequence. Random-Encoded Spread Spectrum can perform several advantages over PN sequences. The watermark detecting by the hostile unauthorized becomes almost impossible by developing the Random-Encoded Spread Spectrum Watermarking system. Such approach has been approved to be a better alternate data mining method which can be used in water marking technique easily. To some extend, the dynamic variable spreading sequences also assure the low probability of detection by attackers over the PN approach. Due to the random and dynamically changing, coded waveform, the techniques chart a completely different approach to spread spectrum techniques.

In multi-user application, we can select much more spreading sequences than regular PN techniques. This means for multi-users application in digital watermarking, more individual information can be sent in the same time without great interference comes from other information. Such approach is still need to be proved by real experimental results in the future.

References

1. Trivedi, S,Chandramouli, R.: Secret Key Estimation in Sequential Steganography, IEEE Transaction on signal processing, Volume 53, NO. 2, Feb. (2005)
2. Asghari, V. R. , Ardebilipour, M. : Spread Spectrum Code Estimation by Genetic Algorithm, International Journal of signal processing, VOL 1,Number 4, (2004).
3. Yen, K., Hanzo, L.: Genetic Algorithm Assisted Joint Multiuser Symbol Detection and Fading Channel Estimation for Synchronous CDMA Systems, IEEE Transaction on selected areas in communication, VOL. 19, NO. 6, JUNE (2001).
4. Asghari,V.R. , Ardebilipour ,M.: Spread Spectrum Code Estimation by Particle Swarm Algorithm, International Journal of Signal Processing, 2, No. 4, (2005) 268-272,
5. Sedghi, S. Mashhadi ,H. R, Khademi ,M. : Detecting Hidden Information from a Spread Spectrum Watermarked Signal by Genetic Algorithm 2006 IEEE Congress on Evolutionary Computation Sheraton Vancouver Wall Centre Hotel, Vancouver, BC, Canada July (2006) 16-21,
6. Gao,Q. Li, R. Wang, H. Dang, H, Liu, L.: Spread Spectrum Digital Watermarking Algorithm Using Gold Codes, Journal of xi'an jiaotong university, VOL 28, NO.2, Feb. (2004)
7. Marvel L M, Retter C T, Boncelet C GJ : Hiding information in images 1998 International Conference on Image Processing, Chicago , USA, (1998).
8. Ruanaidh J J K O, Csurka G :A Bayesian approach to spread spectrum watermark detection and secure copyright protection for digital image libraries IEEE Computer Society Conference on Computer Vison and Pattern Recognition, Fort Collins, USA, (1999).
9. Vassaux B, Bas P, Chassery J M. : A new CDMA technique for digital image watermarking, enhancing capacity of insertion and robustness 2001 International Corrence on Image Processing, Thessaloniki, Greece,(2001).
10. Peterson,R. L. Ziemer,R.E., Borth, D.E.: Introduction to Spread Spectrum Communications" Englewood Cliffs, NJ: Prentice Hall, (1995)
11. Dixon, R. C.: Spread Spectrum System New York, NY: John Wiley & sons, (1984)
12. Sarwate D. V., Pursley, M. B.: Crosscorrelation Properties of Pseudorandom and Related Sequences, Proceedings of IEEE, vol. 68, May (1980)593-619