

An Inaudible Pseudonoise Sequence Generation for Digital Audio Watermarking

Jongweon Kim*, Youngseok Lee**

- *Dept. of Copyright Protection, Sangmyung University, 7, Hongji-dong, Jongno-gu, Seoul, Korea

**Dept. of Electronic Eng., Chungwoon University, San 29, Hongsung-gun, Chungnam, Korea

jwkim@smu.ac.kr, yslee@chungwoon.ac.kr

Abstract— Digital watermarking is a technique that embeds imperceptible and statistically undetectable information into digital data. Most digital audio watermarking schemes have used pseudonoise (PN) sequence as a secret key. PN sequence embedded in an audio signal for watermarking reduces audio quality while it plays a vital role in security. In this paper, a PN sequence generation to improve imperceptibility in perceptual region of the human auditory system for audio watermarking purpose. The basic idea of this work was a modification of a PN sequence according to the frequency analysis of adjacent binary digits that have different signs in a PN sequence. The canonical signed digit code (CSDC) was also used to modify a general PN sequence and the pair-matching function between general and its modified PN sequence is proposed for PN sequence modification. Additionally, statistical properties of new PN sequence was evaluated and discussed by an auto-correlation and a cross-correlation analysis.

Keywords—Pseudonoise sequence, Audio watermarking, Canonical signed digit coding, Security, Pair-matching

I. INTRODUCTION

In recently, due to the development of network technologies and the widespread use of personal computers as multimedia system, people have easy access to vast amounts of copyrighted digital data. While this data, which includes text, digital audio, image and video, offers various advantages, they can be reproduced without loss of quality, shared by multiple users, distributed over networks, and managed for long periods of time without any damage. However, unauthorized copying and distribution of digital data are serious threats to the rights of content owners in content industry [1].

Digital Watermarking has been proposed as a potential solution to this problem. Digital watermarking is a technique that embeds imperceptible and statistically undetectable information into digital data (e.g. video, images and audio signals). This embedded pseudonoise (PN) sequence or image

as secret key contains certain information uniquely related to the owner or distributor [1]. Compared to digital video and image watermarking, audio watermarking studies are restricted for several reasons. First, the human auditory system (HAS) is extremely more sensitive than human visual system (HVS).

The HAS is sensitive to a dynamic range of amplitudes from one billion to one, and of frequencies from one thousand to one. Even a small amount of embedded noise can be detected by the naked human ear. Secondly, audio clips are rather short compared with video clips in terms of time and file size. Thus, the amount of hidden information in audio clips is relatively large compared with the image or video. Consequently, this information tends to degrade the audio quality. There is always a conflict between inaudibility and robustness in current audio watermarking methods. Finding a satisfactory balance between these two aspects becomes an important index by which to evaluate digital audio watermarking techniques.

To improve the imperceptibility of audio watermarking, previous approaches had focused on the development of a psychoacoustic model of the HAS. One of the representative popular approach is that a modified watermark is embedded into psychoacoustic imperceptible region of the HAS by using temporal or frequency masking effect based on the psychoacoustic model of the HAS [2, 3]. However, it has an extremely high computational complexity in masking process and also cannot be adopted by some watermarking algorithms as spread spectrum-based algorithms [1, 4].

An alternative approach is more intuitive and simple compared with the first approach. It was embedded for an imperceptible PN sequence as a watermark into a perceptible region of HAS. But unfortunately a general PN sequence used for audio watermarking cannot apply to this approach because of its white noise-like spectral characteristics which has spectral components over all frequency band, furthermore few researcher have addressed the imperceptible PN sequence.

In this work, a PN sequence generation to improve

imperceptibility in perceptual region of the HAS, was investigated for audio watermarking purpose. Especially the auditory frequency range from 20Hz (0.20Bark) to 5 KHz (14.51Bark) is known to the perceptually significant region (PSR) that is extremely sensitive in the basilar membrane, the organ of HAS. Therefore a watermark embedding in the PSR causes quality degradation of an audio signal and then feeling of repulsion by listener [5, 6].

The basic idea of this work was a modification of a PN sequence according to the frequency analysis of adjacent binary digits that have different signs in a PN sequence. The canonical signed digit code (CSDC) [7, 8] was also used to modify a general PN sequence and the pair-matching function between general and its modified PN sequence is proposed for PN sequence modification. Additionally, statistical properties of new PN sequence was evaluated and discussed by an auto-correlation and a cross-correlation analysis. The rest of this paper is organized as follows. The new generation method of random sequence with imperceptibility was proposed in Section II. Simulation experiments were conducted in Section III to validate analysis. Section IV concluded the paper.

II. NEW GENERATION METHOD OF PN SEQUENCE

In this section, we proposed a novel PN sequence with the low frequency magnitude at the PSR in the HAS. The proposed PN sequence was characterized by not allowing nonzero digit between adjacent digits. Over all procedure for generating the proposed PN sequence showed in Figure 1.

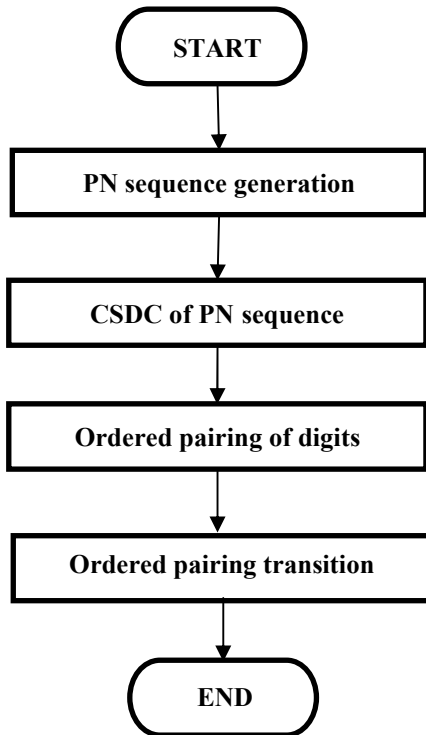


Figure 1. Procedure of the proposed PN sequence generation

A single digit vector D of E is a sparse recoding of binary vector E using digits from the set $\{\bar{1}, 0, 1\}$ where $\bar{1}$ denotes -1 . The recoding is canonical if D contains no adjacent nonzero digit

The first step in generation of the proposed PN sequence was starting from generating the typical PN sequence with secret key, and then it was coded by canonical signed digit coding (CSDC). In binary digit vector analysis, CSDC is known to optimum representation to minimize nonzero digit of binary sequence.

Thus, a canonical signed digit vector of E is the form $D = (D_{n-1}, D_{n-2}, \dots, D_0)$, $D_i \in \{1, 0, \bar{1}\}$. In order to CSD-code, it can be shown that the canonical signed digit vector for E is unique if the binary expansion of E is viewed as padded with an initial zero. This canonical signed digit vector can be constructed by the canonical recording algorithm of Reitwiesner [9]. Because that the CSD-coded PN sequence did not allow nonzero elements between adjacent digits, the set P , elements of which are the ordered pairs of the CSD-coded PN sequence was defined as in(1).

$$P \equiv \{(0,0), (1,0), (0,1), (\bar{1}, 0), (0, \bar{1})\} \quad (1)$$

And we also defined a set Q in (2). The elements of set Q were characterized by having different signed ordered pair.

$$Q \equiv \{(1, \bar{1}), (\bar{1}, 1)\} \quad (2)$$

The correspondence between the set P and the set Q was shown in Fig. 2.

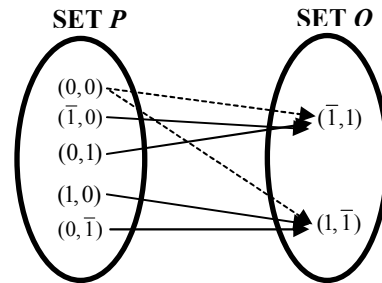


Figure 2. Correspondence between the set P and the set Q

The ordered pair $(0,0)$ in the set P has two correspondences in the set Q ; if the ordered pair immediately before $(0,0)$ in the set P is $(1, \bar{1})$, then $(0,0)$ in the set P transits to $(\bar{1}, 1)$ in the set Q and if it is $(\bar{1}, 1)$ then $(0,0)$ transits to $(1, \bar{1})$. Two dashed-lines in Figure 2 denote the transition of $(0,0)$ in the set P to the set Q . In the time domain, the proposed PN sequence with a delay n_0 and period N was represented in (3).

$$r_{new}(n) = \sum_{i=0}^{N-1} r_i (\delta(n - n_0 - i) - \delta(n - n_0 - i - 1)) \quad (3)$$

In the frequency domain, the frequency components of the proposed PN sequence differed from those of the original PN sequence while the proposed PN sequence kept its randomness in the time domain. The frequency domain representation of (3) was represented in (4).

$$R_{new}(\omega) = \sum_{i=0}^{N-1} r_i(e^{-j\omega(n_0+i)} - e^{-j\omega(n_0+i+1)}) \quad (4)$$

We can observe that $(e^{-j\omega(n_0+i)} - e^{-j\omega(n_0+i+1)})$ is very small value when frequency ω is small in (4). This observation implies the frequency components of our PN sequence slowly changed in low frequency band. We can extend the correspondence of the set P and the set Q to n -digit ordered pair to m -digit ordered pair. For example 2-digit ordered pairs in (1) was extended to 4-digit ordered pair as in Table 1.

TABLE 1. Correspondence of 2- to 4- digit in the set P and the set Q

Set P	Set Q
(0,0)	$\bar{Q}(t-1)$
(1,0)	($\bar{1}$, 1, $\bar{1}$, 1)
(0,1)	(1, $\bar{1}$, $\bar{1}$, 1)
($\bar{1}$, 0)	(1, $\bar{1}$, 1, $\bar{1}$)
(0, $\bar{1}$)	($\bar{1}$, 1, 1, $\bar{1}$)

In Table 1, $Q(t-1)$ means that the ordered pair in the set Q is changed 1 to $\bar{1}$ and $\bar{1}$ to 1 by the correspondence of immediately before (0,0) in the set P . We could observe that the element in Set Q still satisfies the results in (3) and (4).

Satisfying in (3) and (4), a correspondence of 3- to 8- digit also was constructed as in Table 2.

TABLE 2. Correspondence of 3 to 8- digit in the set P and the set Q

Set P	Set Q
(0,0,0)	$\bar{Q}(t-1)$
(0,1,0)	($\bar{1}$, 1, 1, $\bar{1}$, 1, $\bar{1}$, 1, 1)
(1,0,0)	($\bar{1}$, 1, 1, $\bar{1}$, 1, $\bar{1}$, 1, 1)
(1,0,1)	($\bar{1}$, 1, 1, $\bar{1}$, $\bar{1}$, 1, $\bar{1}$, 1)
(0, $\bar{1}$, 0)	($\bar{1}$, 1, 1, $\bar{1}$, $\bar{1}$, 1, 1, $\bar{1}$)
($\bar{1}$, 0, 0)	($\bar{1}$, 1, $\bar{1}$, 1, 1, $\bar{1}$, $\bar{1}$, 1)
($\bar{1}$, 0, $\bar{1}$)	($\bar{1}$, 1, $\bar{1}$, 1, 1, $\bar{1}$, 1, $\bar{1}$)
($\bar{1}$, 0, 1)	($\bar{1}$, 1, $\bar{1}$, 1, $\bar{1}$, 1, $\bar{1}$, 1)
(1,0, $\bar{1}$)	($\bar{1}$, 1, $\bar{1}$, 1, $\bar{1}$, 1, 1, $\bar{1}$)

As a result, we could induce the new PN sequence with improved imperceptibility.

III.SIMULATION RESULTS

In simulation experiment, we analyzed 100 PN sequences generated by the proposed method described in Section III. Each PN sequence was generated based on typical PN

sequences generated by different secret keys and composed with 256 samples. The our simulation processes included the generation process of the typical PN sequence with secret key, the result of CSDC in the process for generating new PN sequence. Auto and cross correlation analysis and frequency magnitude spectrum analysis were carried out to analyze properties of the proposed PN sequence in time and frequency domain

Figure 3 shows an example of typical PN sequence that is satisfied with the Golomb's randomness postulates [9]. In the generation process of the typical PN sequence, a random seed as secret key is applied for security

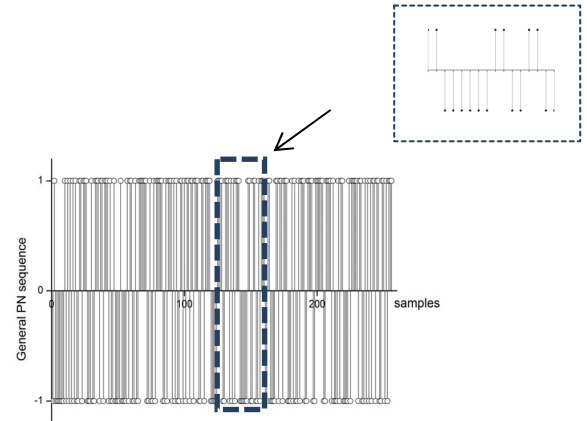


Figure 3. An example of typical PN sequence that satisfies with Golomb's randomness postulates

A sequence in the dashed box shows 16 samples from 140 sample point to 155 sample point in the generated typical PN sequence. We can observe consecutive samples of 1 or -1 in samples of dashed box.

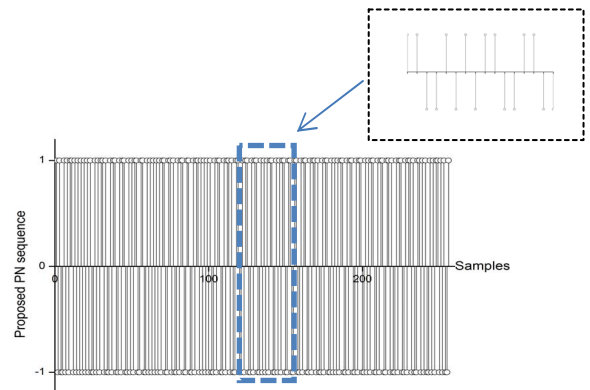
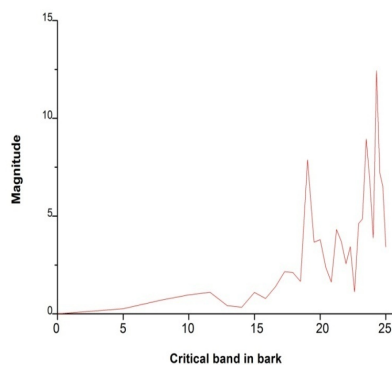


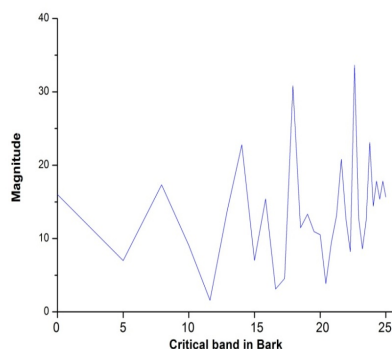
Figure 4. The example of the proposed PN sequence

In the sequence, consecutive sequences of 1 or -1 lead to the high and fluctuating magnitude spectrum in frequency domain and then an unwanted noise occurs in audible frequency band including the PSR. Figure 4 shows an example of new PN sequence generated from Figure 3. A sequence in the dashed box shows 16 samples of the same sample positions of Figure 3 in the new PN sequence. We can observe that the ordered pairs of new PN sequence are always (1,-1) or (-1, 1). This property of new PN sequence causes slow change of frequency spectrum in low frequency band as described in (4) and leads to convergence to approximate zero in difference of frequency spectrum of adjacent samples. Therefore the proposed new PN sequence has little affect the PSR in HAS.

Figure 5 shows frequency magnitude spectrums of PN sequences in Figure 3 and Figure 4. In Bark scaled horizontal axis, 0-15Bark covers the PSR in HAS. The frequency magnitude spectrum of the proposed PN sequence is approximate zero and little fluctuation while that of the typical PN sequence is high and heavy fluctuation. This observation implies that the audience can little hear and feel the influence of noise caused by PN sequence inserted as watermark.



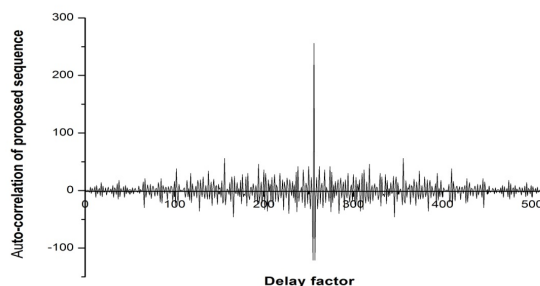
(a)



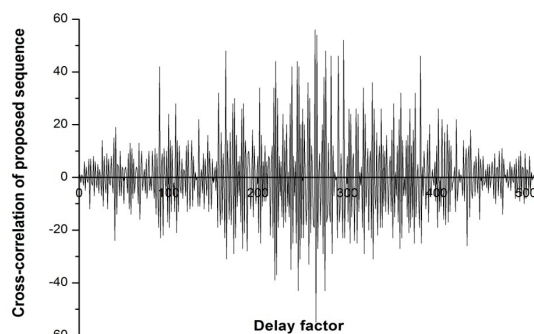
(b)

Figure 5. Frequency magnitude spectrum of (a) Proposed PN sequence (b) Typical PN sequence

The PN sequences used as watermark have high auto-correlation and low cross-correlation property for security and this property plays an important role in correlation based detection process of a watermarking scheme.



(a) Auto-correlation of proposed sequence



(b) Cross-correlation of proposed sequence

Figure 6. Auto- and cross- correlation examples of the proposed PN sequence

Figure 6(a) shows the autocorrelation example of the proposed PN sequence randomly selected from 100 sequences. The maximum value of autocorrelation is the strength of sequence when delay factor is zero. This means that the autocorrelation of the proposed sequence is strong as much as that of the typical PN sequence. Figure 6(b) shows the cross correlation example of the proposed PN sequences randomly selected from 100 sequences. We can observe that that the cross correlation values of the proposed sequences are uncorrelated as the property of a typical PN sequence.

IV. CONCLUSIONS

In this paper we proposed the generation method of PN sequence that is imperceptible in the PSR of HAS. The PN sequence generated by the proposed method was analyzed in frequency domain analysis, and correlation analysis and simulation results are compared with those of the typical PN sequence that satisfies the Golomb's randomness postulates.

In frequency domain analysis the frequency magnitude spectrum of the proposed PN sequence showed the explicit

small value and low fluctuation in PSR of HVS. This implies that the proposed PN sequence is much imperceptible in comparison of the typical PN sequence. This property is significant in the view point of imperceptibility of audio watermarking. The imperceptibility of watermark in the PSR of HAS improves the quality of watermarked audio signal in audio watermarking scheme.

In time domain analysis we could observe that the proposed PN sequence had same or much strong autocorrelation and same or less cross correlation from simulation results. And also the proposed PN sequence is much applicable than the typical PN sequence for audio watermarking in comparison of maximum cross-correlation in sample number change and the percentage ratio of maximum cross-correlation values and sample number. We expect to apply for audio watermarking with high imperceptibility in the PSR of HAS.

ACKNOWLEDGMENT

This research project was supported by Ministry of Culture, Sports and Tourism (MCST) and from Korea Copyright Commission in 2011.

REFERENCES

- [1] I.J. Cox, M.L. Miller, J.M.G. Linnartz, T. Kalker, "A Review of Watermarking Principles and Practices" in *Digital Signal Processing for Multimedia Systems*, K.K. Parhi, T. Nishitani, eds., New York, New York, Marcel Dekker, Inc., 1999, pp 461-482
- [2] David J. M. Robinson, and Malcolm O. J. Hawksford, "Psychoacoustic Models and Non-Linear Human Hearing," *AES 109th Convention, Los Angeles*, Sept. 22-25, 2000, pp.1-14.
- [3] N. Cvejic, T. Seppänen, "Improving audio watermarking scheme using psychoacoustic watermark filtering," *Proceedings of the First IEEE International Symposium on Signal Processing and IT*, Cairo, Egypt, 2001, pp. 163-168.
- [4] M. Swanson, B. Zhu, A. Tewfik, and L. Boney, "Robust Audio Watermarking Using Perceptual Masking," *Signal Processing*, vol. 66, no. 3, May 1998, pp. 337-355.
- [5] M. Bosi, R. E. Goldberg, *Introduction to audio coding and standards*, Kluwer Academic Publishers, Boston, 2003.
- [6] L.D. Chen and G. Gong, *Communication System Security*, CRC Press, 2011.
- [7] I. Koren, *Computer Arithmetic, Principles, Architectures and Design*, Wiley, New York, 1979.
- [8] O. L. MacSorley, "High-speed arithmetic in binary computers," *Proc. IRE*, vol. 49, pp. 67-91, 1961.
- [9] G. W. Reitwiesner, "Binary arithmetic," *Adv. Comput.*, vol. 1, pp. 231-308, 1960.