AN EFFECT TO HANDLE THE INTER-LEAVING PSEUDO NOISE SEQUENCES

Bui Lai An[1], Nguyen Thuy Anh[2]

[1]Post and Telecommunication Institute of Technology, Hanoi
[2]Hanoi University of Technology,

ABTRACT

Instead of creating a inter-leaving non-linear pseudo noise (PN) sequence, we carry out a mixture component sub-sequences having 2^m-1 length form to make a larger sequence of various different levels (dimensions). For the mentioned sequence, scrambler mixer generated component PN sequence is considered as a linear finite state sequence machine (LFSSM) and the algorithm for mixing bit can be considered to be an effective treatment of inter-leaving non-linear PN sequences.

Keyword: inter-leaving, non-linear PN, signal randomization, multi-dimensional PN, nonlinear multi-level.

1. INTRODUCTION

In the consideration of a multi access interference (MAI) with a pseudo noise (PN) sequence by adopting the standard Gaussian approximation (SGA), improved Gaussian approximation (IGA), or improvedly simplified Gaussian approximation (ISGA) methods, the number of alteration status B is an important random variable as this variable is regarded to be a measure of the spread spectrum of signal and is directly related to autocorrelation functions [2]. Thus, B can be considered to represent the randomness of the sequence also to be a factor for optimization of transmission spectrum and for improvement of errors probability. B is the changed status number of the block bit at the same polarity. The sequence carried information bits can be either short or long periods consisting of unchanged polarity bit. This will lead to a disadvantage as the spectral characteristics of the transmitted signal depends upon the form of bits sequence to be transmitted, the spectrum of signal is quite sparsed on the frequency scale and spectral density is high in the low frequency range. To remove the same polarity bit blocks of too short or too long, an usual method is to adopt the bit scrambling algorithm.

2. SIGNAL MIXER

Inter-leaving PN code to be created by mixture component sub-sequences having 2^m-1 length form to make a larger sequence in variety of level is given by [1, 8] :

$$L = 2^n - 1 = \prod_{i=1}^{k} T_i L_{b_j} \text{, với } \prod_{2\le i}^{k} T_i L_{b_j} = 2^{m_j} - 1, \quad \forall i = \{2,3,...,k\} \tag{1}$$

To form non-linear characteristics for increasing the combination code one may carry out by either way as follows:

- Maintaining the order of inter-leaving but replace m sub-sequence components by m other sequences of the same length.

- Maintaining the order of inter-leaving but replace m sub-sequence components by a quasi-random distributed sequence of the same length.

- Using product sequence T_i of m sub-sequence components.

- Using product sequence T_i of m sub-sequences components from other sequences.

All of the above mentioned are nothing but the mixt of repeated binary sequences. Thus, the scrambler mixer generated component PN sequence can be considered as a linear finite state sequence machine (LFSSM). In the general, the output signal of the scrambler is a superposition of two components. The first one is the free response (signal and $Si = 0$) which is a PN sequence. The second component is the forced response to the generated by input signal. It is showed that on applying changes d to the linear scrambler [3], the input signal sequence and PN sequence are linearly independent and when PN sequence is long enough, then the output signal is balanced by $P(1)=P(0) = 1/2$. Since the inter-leaving PN sequence is a non-linear formed by the combination of inter-leaving sequence of m diffirent linear sequences, we can consider the signal processing on non-linear sequence as treatment with combination of m component sequence [5].

When the input signal is periodic with period M, then output signal of the mixer is also circle with period $L = L_{cm}(M,N)$, where N is the cycle of m sequences from free-response of the created mixer (free-response is defined as response of the mixer when the entire input sequence series of ‘0’). In addition, the spectrum of the binary sequence will be more flatter with much more spectral lines. In the general case, with respect yo a non-periodic input signal, the output sequence has two parts; transition and circulation. The length of transition part is given by $j + 1- m$, where j is the length of the input sequence, m is the length of the LFSR. The circulation part will have a period of $N = 2^m - 1$.

The mixer can be modeled as a linear sequence machine [4]. Thus, the output sequence can be divided into two independent components: the free response and forced response. Free-response is the initial state of the mixer decision, but forced response is input sequence of the mixer decision. Input-output characteristic of the mixer can be described simply through transfer function $H(d)$ in the spaced d in this expression:

$$Y(d) = X(d).H(d) \tag{2}$$

where $X(d)$ and $Y(d)$ are respectively the d-transform of the input sequence $x(n)$ and the output sequence $y(n)$. Transfer function of the de-mixer (inverse of d-transform) will be $1/H(d)$.

Properties of the concerned digital mixer are looked for the ability of preventing the blocked phenomenon, eliminating the consecutive assimilarity bit sequence, creating a large ELS sequences and extending the range distribution of '1' and '0'.

3. DISTRIBUTION OF MIXERS OUTPUT SEQUENCE

Suppose input bit sequence $\{I\}$ with cycle be s. After a suitable mixing, periodical output sequence $\{O\}$ is the smallest common multiple of s and $(2^m - 1)$. On the other hand, it may find that number of interchanging (switching) polarity of the TR in a cycle of the output sequence will almost follow a double inequality:

$$s(2^{m-1}-1) < TR < s.2^{m-1} \tag{3}$$

Maximum number of possible conversions for L = 2^m - 1 is (2^m-1).s, which occurs when the bit of sequence alternates its polarity. The above relation shows that the conversion actually occurs in output of the mixer $\{O\}$up to almost 1/2 of the possible conversion, independent of the input bit sequence. This can also be proved as follows.

Denote {O} for output sequence of digital mixer, $\{I\}$ for input sequence (forced response of mixer) and $\{U\}$ for sequence generated by LFSR (signal or free-response of the mixer). Probability of bit to be '0' and '1' at output sequence is $P_0(0)$ and $P_0(1)$ respectively. Probability of bit to be '0' and '1' at respective input sequence is $P_I(0)$ and $P_I(1)$. Probability of bit to be '0' and '1' at the sequence generated by LFSR is respectively $P_U(0)$ and $P_U(1)$. Since the mixer is a linear system, output sequence is:

$$\{O\} = \{I\} \oplus \{U\} \tag{4}$$

So, probability of bit to be '1' in the out sequence $\{O\}$ is:

$$P_0(1) = P_I(1).P_U(0) + P_I(0).P_U(1) \tag{5}$$

Sequence$\{U\}$generated by LFSR on satisfying balanced condition, ie, probability of bit '0' of the PRBS sequence generated by LFSR, and the probability of bit '1' satisfies:

$$P_U(1) \approx P_U(0) \approx \frac{1}{2} \tag{6}$$

So, one has

$$P_0(1) = P_I(1).\frac{1}{2} + P_I(0).\frac{1}{2} = \frac{1}{2}\left[P_I(1) + P_I(0)\right] \approx \frac{1}{2} \tag{7}$$

If input sequence $\{I\}$ and $\{U\}$sequence generated by LFSR are statistically independent, then the output sequence $\{O\}$ will be of the probability distribution:

$$P_0(1) \approx P_0(0) \approx \frac{1}{2} \tag{8}$$

Sequences of n-bit length unchanged output level may also happen to be, however with a small probability as that for the sequence $\{U\}$, ie $1/2^n$.

4. AUTOCORRELATION AND SPECTRAL PROPERTIES

Autocorrelation function of ouput sequence $\{O\}$ is defined as:

$$R(k) = \frac{A-D}{A+D} = \frac{A+D-2D}{A+D} = 1 - 2\frac{D}{A+D} = 1 - 2P_0(1) \approx 0 \tag{9}$$

where A is denoted for the number of similar bits (between original sequence and k bit shifted one, shifted by a period), D is for the number of different bits, between two sequences.

Output sequence of mixer $\{O\}$ will satisfy two of the randomness [8]:

$$P_0(1) \approx P_0(0) \approx \frac{1}{2}; \quad R(k) = 0 \tag{10}$$

It is shown in figure 1.a and 1.b that spectrum of output sequence is almost independent of information transmitted, with spectral lines closer each to the other and spectrum graph of the sequence is quite low, which is of close-characteristics with spectrum graph of a white noise.

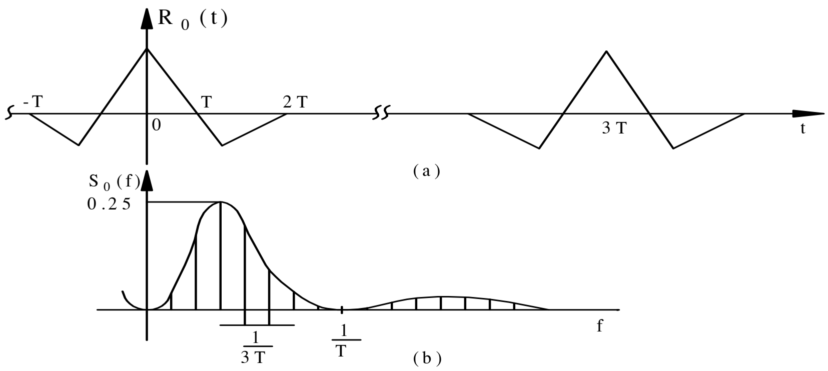

Figure 1a. Characteristics of NRZ bit periodical sequence 10110010

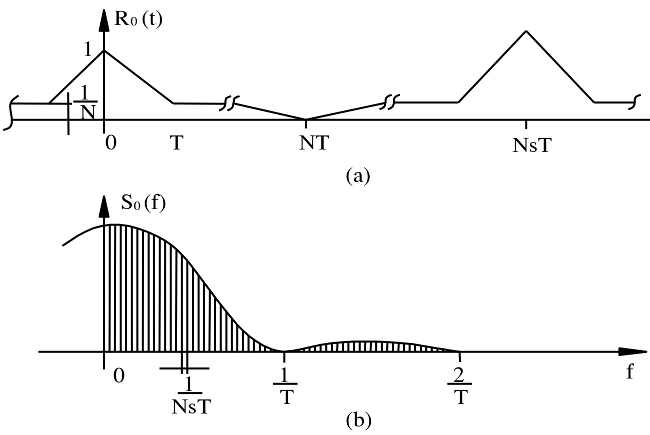

Figure 1b. Characteristics of the signal sequence after mixing

Spectral whitening of mixing are shown in the mentioned figures with input sequence bits $\{I\}$:... 10110010 ..., with repeating cycle $s = 8$ that distance between spectrum lines of sequence $\{I\}$ is $1/3T$ with the duration of a bit T, and that the spectrum of the signal distribution is clearly un-uniform one. Autocorrelation function and spectrum of mixed signal sequence $\{O\}$ are shown in the respective figure. It is seen that the distance between two spectral lines is reduced to $1/NsT$, with $N = 2^m - 1$. On the other hand, the peak of spectrum envelope reduced the rate *1/2N*. Thus, spectral distribution of the mixers output signal is more uniform and there exits no change almost in transmitted information content. For example, a pseudo-random sequence of maximum length with m = 12, one has N = 4095. Thus, by mixing this pseudo-random sequence, distance between spectral lines is reduced to 4095 folds and spectral envelope peak is less than 8190 times with respect to the value of input bits sequence.

Let examine the autocorrelation function of mixers output sequence in the general case. Denote input sequence by $\{I_n\} \in 0,1,\ 0 < n < \infty$, change (transform) d of this sequence by $I(d)$, generating polynomial of the mixer by $h(d)$ of degree m, and polynomial characterizing the initial state of mixer by $S(d)$ of degree less than m, [3, 5-7]. Output sequence is of the following form:

$$O(d) = \frac{I(d) + S(d)}{h(d)} = O_f(d) + O_a(d) \tag{11}$$

where, $O_f(d) = I(d)/h(d)$ and $O_a(d) = S(d)/h(d)$ in turn represent free and forced response of the mixer in the spaced *d*. When *I*(*d*) and *S*(*d*) are independent (independently chosen), then from the linear nature of the mixer, forced response and free response are independent each other. The inverse of change (transform) d of the output sequence o_n is obtained as:

$$D^{-1}\left[O_f(d) + O_a(d)\right] = o_n^f + o_n^a = o_n \tag{12}$$

ACF of output binary sequence is defined as:

$$R(k) = E\{a(o_n).a(o_{n+k})\} \tag{13}$$

where, $a(o_n) = 1$ when $o_n = 1$ and $a(o_n) = -1$ when $o_n = 0$. It is known that ACF is of random sequence being calculated as follows:

$$\begin{aligned} R(k) &= 1 - 2\left[P\left\{a(o_n) = -1,\;\; a(o_{n+k}) = 1\right\} + P\left\{a(o_n) = 1,\;\; a(o_{n+k}) = -1\right\}\right] \\ &= 1 - 2P\{a(o_n) \oplus a(o_{n+k}) = 1\} = 1 - 2P_1\{a(o_n) \oplus a(o_{n+k})\} \end{aligned} \tag{14}$$

with, $\oplus$ is denoted for the addition module 2, $P_1\{x_n\}$ is for probability to be '1' in the sequence. From expression (14), one has:

$$\begin{aligned} P\{a(o_n) \oplus a(o_{n+k})\} &= P\{(a^f(o_n) + a^f(o_{n+k}) + (a^a(o_n) + a^a(o_{n+k})) = 1\} \\ &= P\{x_n^f(k) + x_n^a(k) = 1\} = P_1\{x_n^f(k) + x_n^a(k)\} \end{aligned} \tag{15}$$

with, $\qquad x_n^f(k) = a^f(o_n) + a^f(o_{n+k});\; x_n^a(k) = a^a(o_n) + a^a(o_{n+k})$.
To evaluate (14) and (15), we will examine two cases as follows.

Case 1: When $k \neq pN$, with $N = 2^m - 1$ is the cycle of *m* sequence generated by the mixer in free response. In this case, $a^a(o_n)$ and $a^a(o_{n+k})$ are two *m* sequences dephasing each other. So, $x_n^a(k)$ is also an *m* sequence and hence, one gets:

$$P_1(x_n^a(k)) = P_0(x_n^a(k)) = -\frac{1}{2}, \text{ when } m \gg 1 \tag{16}$$

and

$$q_1 = P\{x_n^f(k) = 1\} = P_1\{x_n^f(k)\};\; q_0 = 1 - q_1 . \tag{17}$$

Since $x_n^f(k)$ and $x_n^a(k)$ are independent, so one has:

$$P_1\{x_n^f(k) + x_n^a(k)\} = P_1 q_0 + P_0 q_1 = \frac{1}{2} \tag{18}$$

Therefore

$$R(k) = 1 - 2P_1\{x_n^f(k) + x_n^a(k)\} = 0, \text{ when } k \neq pN \tag{19}$$

In other words, the input signal will be randomized into an effective independent of its statistical properties.

Case 2: When $k = pN$ (an integer number of cycles N). In this case, it is found that the result is much complicated due to the sequence (o_n) và $a^a(o_{n+pN})$ become synchronized phase and may cancel each other. As a result, mixer will not effect signal randomization. Therefore, in the ACF $R(k)$ can take a value different 0 when $k = pN$, but $\lim_{p\to\infty} R(pN) = 0$ can be surely calculated.

For multi-level inter-leaving non-linear codes, the period side of large sequence would be an integer number of sub-sequence lengths, which may reach to a larger length by scrambling as many folds as desired. To show effects of inter-leaving for randomization signals, simulations with the non-linear code level 2 are performed.

5. RESULTS OF MIXED SIGNAL SIMULATION

It can see autocorrelation function $R(k)$, $k = pN$ by performing process signal randomization from two mixers in series (each of a LFSR 7 triggers) and creating m sequence of 127 bits. Only different characteristic polynomial of LFSR are simulated illustrating in Table 1, in which, out of the 127 binary bit sequence, irregular shape input signal, only four special cases illustrated in figure 2 are considered for simulations only.

Table 1. Characteristic polynomials of the LFSR used in the simulation

M	$h(d)$
10000011	$1+d^6+d^7$
10010001	$1+d^3+d^7$
10101011	$1+d^2+d^4+d^6+d^7$
11000001	$1+d+d^7$
11010101	$1+d+d^3+d^5+d^7$
11110001	$1+d+d^2+d^3+d^7$
10001001	$1+d^4+d^7$
10011101	$1+d^3+d^4+d^5+d^7$

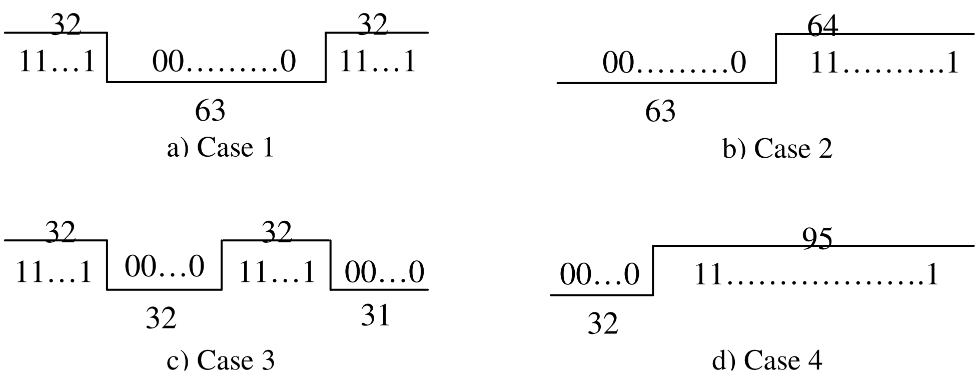

Figure 2. Four specific types of data

Input signal sequence is inserted to the first mixer for the first mixing signal, output signal of the first mixer is to the second mixer for the second mixing. Output signal of the second mixer is the transmitted random signals sequence. Some properties of output signal with different LFSR characteristic polynomials in the mentioned cases of input signals are summarized in Table 2.

Table 2. Input-output signal after mixing

m_1	m_2	N_1	N_0	N_1/N_0	M_1	M_0	TR
10000011	10000011	64	63	1.02	32	63	2
	10010001	60	67	0.89	4	9	66
	10101011	68	59	1.15	8	5	66
	11000001	48	79	0.6	8	8	55
	11010101	62	65	0.95	6	10	59
	11110001	58	69	0.84	7	10	61
	10001001	68	59	1.15	10	7	56
	10011101	64	63	1.02	5	10	56
10010001	10101011	72	55	1.31	6	4	66
	11000001	66	61	1.08	11	7	57
	11010101	62	65	0.95	9	6	63
	11110001	66	61	1.08	5	5	73
	10001001	74	53	1.39	6	4	68
	10011101	68	59	1.15	7	6	56
10101011	11000001	62	65	0.95	6	10	61
	11010101	72	55	1.31	9	4	65
	11110001	58	69	0.84	6	10	57
	10001001	64	63	1.02	8	6	64
	10011101	68	59	1.15	8	5	64
11000001	11010101	68	59	1.15	9	5	64
	11110001	80	47	1.7	8	6	58
	10001001	58	69	0.84	4	9	63
	10011101	66	61	1.08	4	6	71
11010101	11110001	68	59	1.15	8	5	56
	10001001	70	57	1.23	5	4	65
	10011101	54	73	0.74	4	7	61
11110001	10001001	62	65	0.95	7	14	51
	10011101	66	61	1.08	5	6	63
10001001	10011101	72	55	1.31	5	5	62

Where N_0 is symbols of bit '0' in the output signal sequence, N_1 is the number of bit '1' in the output signal sequence, N_1/N_0 is the ratio of the number bit '1' per the bit '0', M_0 is symbols of bit '0' maximum continuous (clusters '0' maximum), M_1 is symbols of bit '1' maximum continuous (cluster '1' maximum) and TR is symbol transition level of output signal sequence.

In the first case of Figure 2, input signal is a 127 bits sequence consisting of 64 bit '1', 63 bit '0', maximum 32 '1' continuous with twice signal level changes. The simulation input-output mixed signals (Table 2) shows that the signal after passing through two sets of mixer in series are improved significantly (closer with random signal characteristics) and that the number of change signal level transition increased significantly. This allows the recovery of synchronous signal at the receiver to be easier, limiting the loss of synchronization. Ratio between the number of bit '1' and bit '0' in the output signal sequence are relatively balanced, the probability of bit to be '1' and bit to be '0' becomes approximation equal each to other and autocorrelation function of the signal after mixing has a small value.

So, with two-step bit sequence input (step '1' with a 32 bit length and step '0' with a 63 bit length), through mixing, output signal has the number of steps to run larger and length of step to run much smaller (in most cases of mixed use different characteristic polynomials, length of steps to run always found smaller than 10). In some cases, by using the combination two characteristic polynomials in two mixers, the received signal has characteristics close to that of random signal.

Three cases have been taken with different LFSR characteristic polynomials $h_1(d)$ and $h_2(d)$ for examples. (i). With $h_1(d)=1+d^3+d^7$ and $h_2(d)=1+d+d^2+d^3+d^7$, after mixing signal becomes 66 bits '1', 61 bits '0', N_1/N_0 = 1.08, two steps to run with length 5 (one step run 5 bits '1' and other 5 bits '0'), remaining steps to run the length less than 5 and having 73 times the signal level changes. (ii). With $h_1(d)=1+d+d^7$ and $h_2(d)=1+d^3+d^4+d^5+d^7$, after mixing signal becomes 66 bits '1', 61 bits '0', N_1/N_0 = 1.08, a step to run of the length 6 (including 6 bits '0'), no steps to run length 5, four steps to run length 4 (two steps to run 4 bits '1', two steps to run 4 bits '0'), remaining steps to run length smaller 4, and having 71 signal level changes. (iii). With $h_1(d)=1+d+d^2+d^3+d^7$ and $h_2(d)=1+d^3+d^4+d^5+d^7$, signal obtained after mixing with 66 bits '1', 61 bits '0', N_1/N_0 = 1.08, a step to run with length six (including 6 bits '0' consecutive), two steps to run with length five (including 5 bits '1'), four steps to run with length four (2 steps to run 4 bits '1', 2 steps to run 4 bits '0'), remaining steps to run length less than 4, has 63 times signal level changes.

The above and simulation results for cases 2, 3, 4 (Figure 2) shows that with a larger input sequence length properties of mixers output signal will be closer with that of the random signal, N_1/N_0 will be more closer to 1. In a special case, where input signal sequence consists of many consecutive bits '1' and '0'), by suitable LFSR characteristic polynomials, after mixing one may obtain an output signal closer with random sequence in the sense that the number of '1' bits and that of '0' bits do not differ each other too much (difference between them is not more than one bit). Moreover, the length of steps to run is significantly reduced, the number of changing signal levels is large enough to ensure an easy recovery of timer signal at the receiver.

6. CONCLUSION AND DISCUSSION

The article focussed on analyzing the signal of the LFSR (mixer) by d variable desription method. Analysis content refers to the structure output sequence of a single mixer when the input sequence is linearly independent with initial state of the mixer. On the basics of the mixers output sequence, one can determine the initial state of the mixer leading to create various sequence with certain specific characteristics of probability distribution, autocorrelation functions as expected. It is found from the mixture nature of mixer generated by LFSR that non-linear multi-level inter-leaving sequence constructed by assembling *m* sub-sequence components to form sequence with larger structure has effective mixture bit similar to by carrying inter-leave sequence.

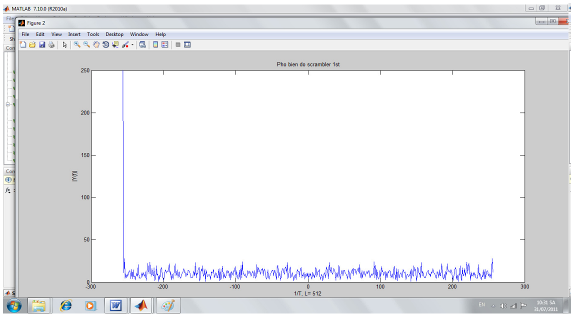

Figure 3a. Spectrum amplitude of the 1st mixer

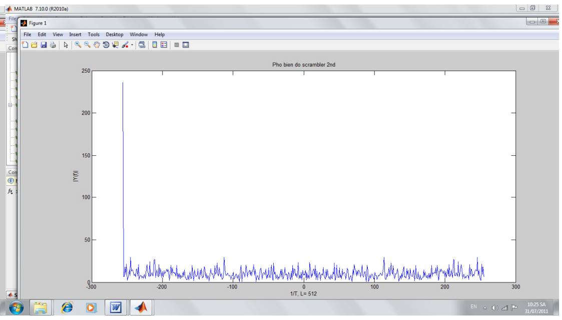

Figure 3b. Spectrum amplitude of the 2ndmixer

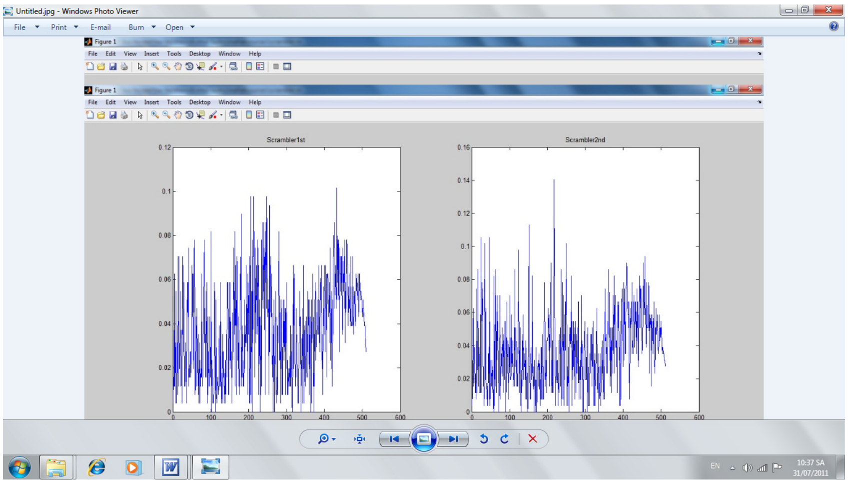

Figure 3c. Spectrum amplitude of input mixer 1st and output mixer 2nd

The simulation results for mixing bit of two linear sequences show that for a properly selected sequence pairs to mix, the output signal would be obtained having random '1' and '0' equilibrum sequence property with less number of steps to run, larger number of signal level changes. By simulation results shown in figures 3a, b, c with PN sequences of 511, 1023 bits that after mixing the selvedges of the "cloud spectrum" are lower and the 2nd inter-leaving level has increased random characteristics of the sequence.

The multi-degree inter-leaving non-linear PN sequences with inter-leaving (mixing) appropriate sub-sequences structure can be consider for “randomization” process to meet the need of spectrum spreading sequence. Sequence of multiple series mixers (multi-degree inter-leaving) and that of non-linear mixture (unchange inter-leaving order, replace components sub-sequence by *m* new same lenth sequences) are topics carried out for next research as their output sequences may have various advantages with respect to random properties, equivalent linear interval, set of sequence and distribution range '1' and '0'.

REFERENCE

1. Bui Lai An, Nguyen Xuan Quynh - On a general structure of nonlinear multi-dimensional PN code multi-level style inter-leaving, Journal of Science and Technology **47** (3) (2009) 9-17.
2. Lai Bui An, Nguyen Hoang Linh - Survey of interference multiple access spread spectrum PN sequence with non-linear inter-leaving, Journal of Professional Journal of the research, development and application of information technology **1** (1) (2010) 165-173.
3. L. C. Quynh, S. Prasad - A class of binary cipher sequences with best possible correlation funtion, IEE Proceeding Part F, **132** (1985) 560-570.
4. A. Gaug and H. Weinricter- Coding of m-seqences by digital data scramblers, NTZ **26** (1973) 234-236.
5. R. G. Gitlin, J. F. Hayer - Timming recovery and scramblers in data transmission, Bell Syst. Tech. Journal **54** (3) (1975) 589-593.
6. R. Mc Eliece - Finite Fields for computer scientis and Engineers, Kluwer Academi press, 2001.
7. R. Sh. Zigangirov - Theory of code division multiple access communication, John Wiley, Chapter 6, 2004.
8. X. D. Lin, K. H. Chang - Optimal PN sequences design forquasisynchro-nous CDMA communication systems, IEEE Trans. Comm **45** (1997) 221-226.

Liên hệ với tác giả:

Nguyễn Thuý Anh,

Trường Đại học Bách khoa Hà Nội

Email: *ngth.anh74@gmail.com*