GENERATION OF LARGE SET OF BINARY SEQUENCES DERIVED FROM CHAOTIC FUNCTIONS DEFINED OVER FINITE FIELD GF(2^8)WITH GOOD LINEAR COMPLEXITY AND PAIRWISE CROSS CORRELATION PROPERTIES

Mahalinga V. Mandi[1], Dr. K. N. Haribhat[2] and Dr. R. Murali[3]

[1]Research Scholar, Dr. MGR University, Chennai,
Assistant Professor, Department of Electronics & Communication Engineering,
Dr. Ambedkar Institute of Technology, Bangalore - 560 056, INDIA.
mvmandi@yahoo.com
[2]Dean Academic, Professor & Head, Department of Electronics & Communication Engineering, Nagarjuna College of Engineering & Technology, Bangalore - 562 110.
knhari.bhat@gmail.com
[3]Professor, Department of Mathematics, Dr. Ambedkar Institute of Technology, Bangalore - 560 056, INDIA.
dr_muralir@yahoo.co.in

ABSTRACT

Some of the techniques of deriving binary sequences from chaotic function is defined in the literature. In this paper a new algebraic structure for generation of sequences using chaotic functions defined over finite field GF(2^8) is proposed. The results indicate that for appropriate choice of bifurcation parameters and initial values both from GF(2^8), a periodic sequence of period (2^8 – 1) can be obtained. These sequences over GF(2^8) are transformed to binary using three techniques (i), (ii) and (iii)

i) expressing every element in GF(2^8)of the sequence as binary 8 tuple
ii) selecting a particular binary bit from each element of the sequence over GF(2^8)
iii) mapping every element in GF(2^8) to GF(2) using Trace function

The cross correlation and Linear Complexity properties of binary sequences so obtained are studied. It is found that they have good cross correlation values and large linear complexity and hence can be used as spreading sequences in CDMA applications.

KEYWORDS

Finite Field, Chaotic Map, Trace Function, Linear Complexity, Cross Correlation

1. INTRODUCTION

Chaotic signals are random like but they are produced by deterministic systems and can be reproduced. Chaotic sequences are easy to generate and store. Only few parameters and functions are needed for generating very long sequences. Chaotic systems are sensitive to initial conditions and thus even with a small difference in initial conditions will lead to the generation of very different signals from the same dynamical system [1] – [6]. In addition, an enormous number of different sequences can be generated simply by changing its initial condition. Also the natures of chaotic signals are deterministic, reproducible, uncorrelated and random like, which can be very helpful in enhancing the security of transmission in communication.

DOI : 10.5121/ijdps.2010.1107

In the past few decades, there has been a great deal of interest in the study of non-linear dynamical systems from which chaos developed. Chaos is of great interest in recent years in communication and more research are undergoing in either theory or practice [7] to [19]. One of the simplest and widely used chaos functions is Logistic map [20]. In recent years several methods to generate chaotic binary sequences using Threshold function [21] – [23] and Coupled Chaotic Systems [24] are proposed in the literature and are suitable for cryptographic applications.

In this paper we propose to generate chaotic binary sequences using chaotic logistic map equation defined over GF(2^8). The random sequence of finite field elements thus generated using chaotic map equation over GF(2^8) are transformed to binary using three different methods. The cross correlation properties and linear complexity properties of corresponding binary sequences are studied. The resulting binary sequences are divided into non-overlapping segments of 15 bits and found to have good pairwise cross correlation and linear complexity properties compared to Gold sequences of same length. The result is similar to binary sequences derived from chaotic sequences as reported in [25].

The work is organized as follows: In Sec-II a brief introduction to chaotic functions over finite fields is presented. In Sec-III, we present our proposed chaotic sequence generator defined over finite field GF(2^8). In Sec-IV, binary mapping expressing field elements as binary 8 tuple is presented. Sec-V deals with binary mapping choosing bits in location i (i=1 to 8) of each symbol in the sequence. In Sec-VI binary mapping using Trace function is presented. In Sec-VII, cross correlation and linear complexity properties of the binary sequences are defined. In Sec-VIII, properties of segments of chaotic binary sequences are investigated. Finally, Sec-IX contains concluding remarks.

2. INTRODUCTION TO CHAOTIC FUNCTIONS OVER FINITE FIELDS

Discrete time dynamical systems are defined by the state equation, $x_{k+1} = f(x_k)$, k = 0, 1, 2… where f maps the state x_k to the next state, $x_{k+1.}$ Starting with an initial condition x_0, repeated applications of the map f give rise to a sequence of points {x_k: k = 0, 1, 2……} called an orbit of the discrete-time system. The chaotic theory is built upon the discrete-time dynamical system defined by f. This section starts with the introduction to chaotic map equation defined over real numbers [20]. The concept is extended to chaotic map equation defined over finite field GF(2^8) in this paper. The proposed chaotic function over GF(2^8) is based on logistic map equation. We first consider logistic map equation over reals [20].

2.1. Logistic Map equation over reals

Consider $x_{k+1} = r\, x_k\, (1- x_k)$, defined over reals and $0 < x < 1$ (1)

where ‘r’ is called as the bifurcation parameter and $3.57 < r < 4$. For any initial value x_0 greater than 0 and less than 1, the sequences are found to be non periodic and non-converging. Even with two initial values differing by a very small value, the resulting sequences are highly uncorrelated [26] – [28]. A survey on generation of chaotic sequences is given in [29]. Techniques of generating sequences over Z_m and deriving binary sequences from them and study of their properties are discussed in [25], [30] and [31].

2.2. Finite Field GF(2^8)

Finite field GF(2^8) with addition multiplication modulo a primitive polynomial $x^8+x^6+x^5+x^4+1$ over GF(2) is considered. Let 'g' be a root of equation $x^8+x^6+x^5+x^4+1 = 0$. Then 'g' is a primitive or generating element whose powers g^2, g^3 ……g^{255} along with 'g' give all the nonzero elements in GF(2^8). Further every nonzero element of the form g^j for $j \geq 8$ can be expressed uniquely as a polynomial of degree less than or equal to 7 over GF(2). Every polynomial of degree 7 or less is of the form $b_7x^7 + b_6x^6 + \ldots.. b_1x + b_0$, where b_i Є (0, 1). Such polynomials can uniquely be represented in terms of its coefficients b_7 b_6 b_5 b_4 b_3 b_2 b_1b_0. Thus every nonzero element in GF(2^8) can be represented by g^j for some j, $1 \leq j \leq 255$ or by a corresponding binary 8 tuple. The '0' in GF(2^8) is denoted by 8 tuple of all zeros.

Proposed chaotic map equations over GF(2^8) are given by equation (2) and (3) and are based on logistic map [20].

$$x_{k+1} = r_1\, x_k\, (r_2 + x_k) \qquad (2)$$

where r_1, r_2 and x_k Є GF(2^8) and are some powers of 'g'. Here $x_0 \neq 0$.

$$x_{k+1} = r_1\, (r_2 + x_k) \qquad (3)$$

where r_1, r_2 and x_k Є GF(2^8) and are some powers of 'g'. In this case x_0 can be zero.

Equation (2) considered is the same logistic map equation (1) but the values of r_1, r_2 and x_k Є GF(2^8). Equation (3) is a variation of equation (2) and the values r_1, r_2 and x_k Є GF(2^8). The sequences generated will have elements from GF(2^8). Corresponding binary sequences are derived from sequences over GF(2^8). The computation over GF(2^8) is carried out using computer simulation.

Example 1: Using equation (2), for arbitrarily chosen values of r_1, r_2 and x_0, the random sequence of finite field elements are derived. For example, if $x_0 = g$, $r_1 = g^{23}$ and $r_2 = g^{24}$, then using equation (2) we get $x_1 = g^{107}$, $x_2 = g^{180}$, $x_3 = g^{214}$, $x_4 = g^{99}$.

Example 2: Similarly for arbitrarily chosen values of $x_0 = g$, $r_1 = g$ and $r_2 = g$, then using equation (3) we get $x_1 = 0$, $x_2 = g^2$, $x_3 = g^{233}$ and $x_4 = g^{61}$.

The r_1, r_2 and x_k can take the values 0, g, g^2, g^3… g^{255} and g is a primitive element in GF(2^8). By selecting proper initial values x_0 and bifurcation parameters r_1, r_2 in equation (2) and equation (3), sequences over GF(2^8) of maximum possible period can be generated.

The random sequence of finite field elements generated using chaotic map equations (2) and (3) over GF(2^8) as explained above are mapped to binary using the following methods.

1) Expressing field elements as binary 8 tuple.

2) Choosing bits in location i (where i = 1 to 8) of each symbol in the sequence.

3) Mapping into binary using Trace function, where every field element in GF(2^8) is mapped to 0 or 1 in GF(2) as discussed in section 6.

The binary transformations of finite field elements considered in example (1) based on equation (2) are listed in Table 1. The binary transformations of finite field elements considered in example (2) based on equation (3) are listed in Table 2.

Table 1. Binary mapping using equation (2)

Values of	Field element	Binary mapping technique using		
		Expressing elements as	Choosing bits in location i	Trace
x_0	g	00000010	0	0
x_1	g^{107}	01001110	0	0
x_2	g^{180}	11001011	1	0
x_3	g^{214}	01100010	0	0
x_4	g^{99}	11000110	1	1

Table 2. Binary mapping using equation (3)

Values of	Field element	Binary mapping technique using		
		Expressing elements as	Choosing bits in location i	Trace
x_0	g	00000010	0	0
x_1	0	00000000	0	0
x_2	g^2	00000100	0	0
x_3	g^{233}	00001100	0	1
x_4	g^{61}	00011100	0	0

3. CHAOTIC SEQUENCE GENERATOR OVER FINITE FIELD GF(2^8)

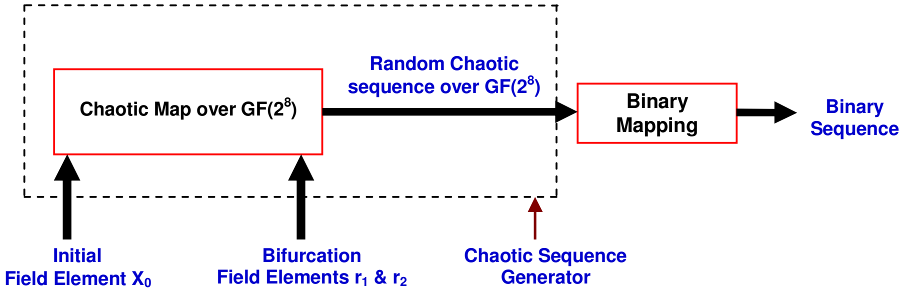

Chaotic Map over GF(2⁸)
Random Chaotic sequence over GF(2⁸)
Binary Mapping
Binary Sequence
Initial Field Element X₀
Bifurcation Field Elements r₁ & r₂
Chaotic Sequence Generator

Figure 1. Block diagram for chaotic sequence generator over GF(2^8)

The block diagram for chaotic sequence generator is as shown in the figure 1. The chaotic sequence generator shown in the block diagram generates random chaotic field elements defined over GF(2^8) for different initial values x_0 and the bifurcation parameters r_1 & r_2. For equations (2) and (3), the random chaotic sequence over GF(2^8) are mapped to binary using the three different techniques as discussed in Section 2.2. The generation of binary sequences from sequence over GF(2^8) is discussed next.

4. Expressing field elements as binary 8 tuple

For arbitrarily chosen values of x_0, r_1 and r_2, the maximum possible period of the sequence over GF(2^8) is determined by computer search and found to be 63 for equation (2) and 255 for equation (3). Each of the finite field elements are expressed as binary 8 tuple and concatenated to get binary sequence. Hence the period of the binary sequence is 63 x 8 = 504 bits using equation (2) and 255 x 8 = 2040 bits using equation (3). The binary sequence is then divided into 15 bit non-overlapping segments. The number of non-overlapping segments of length 15 bits using equation (2) is 33 and 136 for equation (3). Each of these segments is numbered as Segment 1, Segment 2 … and is shown in Fig 2.

$$BinarySequence = \underbrace{b_0, b_1, \ldots\ldots b_{14}}_{Segment\,1}, \underbrace{b_{15}, b_{16}, \ldots\ldots b_{29}}_{Segment\,2}, \ldots\ldots\ldots\ldots\ldots \underbrace{b_{1485}, \ldots\ldots b_{1499}}_{Segment\,100}$$

Figure 2. Non-overlapping segments of 15 bits.

5. Choosing Bits in location i (where i = 1 to 8) of each symbol in the sequence

In this method of binary mapping, choosing bits in location i (where i = 1 (MSB) to 8 (LSB)) of each symbol in the sequence, the period of the binary sequence is found to be 63 bits in case of Logistic map equation (2) and 255 bits in case of equation (3). To get the binary sequence we group the bits in location i (where i = 1 to 8) of each symbol in the sequence for each initial value x_0 and bifurcation parameters r_1 and r_2.

This binary sequence is divided into 15 bit non-overlapping segments. The number of 15 bit non-overlapping segments we get is 4 using equation (2) and 17 using equation (3). Each of these segments is numbered as Segment 1, Segment 2, … and is shown in Fig 3.

$$BinarySequence = \underbrace{b_0, b_1, \ldots\ldots b_{14}}_{Segment\,1}, \underbrace{b_{15}, b_{16}, \ldots\ldots b_{29}}_{Segment\,2}, \ldots\ldots\ldots\ldots\ldots \underbrace{b_{241}, \ldots\ldots b_{254}}_{Segment\,17}$$

Figure 3. Non-overlapping segments of 15 bits.

6. Mapping from GF(2^n) to GF(2) using Trace function

The trace function [32] Tr(g) of an element g, g Є GF(2^n), relative to GF(2) is defined by the equation, $Tr(g) = g + g^2 + \ldots. + g^{2^{n-1}}$

It is well known that the trace of an element of GF(2^n) relative to GF(2) is a binary number, either 0 or 1. The trace function is linear mapping over GF(2) from GF(2^n). The non zero elements of GF(2^n) form a cyclic group of order (2^n – 1) with generator g, where $g^{(2^n - 1)} = 1$.

$$\text{The trace of g over GF}(2^n)\text{ is defined as } Tr(g) = \sum_{i=0}^{n-1} g^{2^i}$$

For a primitive polynomial $p(x) = x^8+x^6+x^5+x^4+1$, the trace of g over GF(2^8) is given by,

$$Tr(g) = \sum_{i=0}^{8-1} g^{2^i} = g + g^2 + g^4 + \ldots\ldots\ldots\ldots + g^{128}$$

Table 3 gives some mapping using trace function for elements in GF(2^8).

Table 3. Some mapping using Trace function for elements in GF(2^8)

Trace	**Polynomial**	**Binary bit**
Tr(0)	0	0
Tr(g)	$g + g^2 + g^4 + \ldots.. .+ g^{128}$	0
Tr(g^2)	$g^2 + g^4 + g^8 + \ldots..+ g^{256}$	0
Tr(g^3)	$g^3 + g^6 + g^{12} + \ldots..+ g^{384}$	1
Tr(g^4)	$g^4 + g^8 + g^{16} + \ldots.+ g^{512}$	0
Tr(g^5)	$g^5 + g^{10} + g^{20} + \ldots.+ g^{640}$	1
Tr(g^{128})	$g^{128} = 1$	1

The sequence of elements from GF(2^8) generated using the chaotic maps as discussed in the previous section are expressed as symbols of 8 tuple. The 8 bit elements of GF(2^8) is mapped to GF(2) using Trace function to one bit binary (either 0 or 1) and concatenated.

Hence in case of binary mapping using Trace function, the maximum possible period of the binary sequence is same as that of sequence over GF(2^8). As mentioned earlier the period of sequence over GF(2^8) is determined by computer search and found to be 63 in case of Logistic map equation (2) and 255 in case of equation (3). This binary sequence is divided into 15 bit non-overlapping segments. The number of 15 bit non-overlapping segments we get is 4 for equation (2) and 17 for equation (3). Each of these segments is numbered as Segment 1, Segment 2 … and is shown in Fig 3.

The linear complexity of 15 bit sequences is computed using Berlekamp – Massey algorithm [36] and pairwise cross correlation values are computed using equation (4) given in next section. The number of sequences of length 15 bits having pairwise cross correlation values denoted by α, are determined for $\alpha \leq 0.35$, ≤ 0.5 and ≤ 0.6 for arbitrarily chosen initial value x_0, r_1 and r_2.

7. Cross Correlation (CCR) and Linear Complexity Properties

7.1. Cross Correlation (CCR) Property

Definition: The normalized cyclic hamming cross correlation function of two binary sequences x and y of length L symbols is defined [33] - [35] as

$$R_{x\,y}(\tau) = (n_\tau - d_\tau) / L, \; 0 \leq \tau \leq L\text{-}1. \qquad (4)$$

Where n_τ and d_τ are the number of locations at which symbols agree and disagree respectively between the two sequences x and y. τ is the number of locations by which one sequence say y is shifted with respect to the other sequence x.

7.2. Linear Complexity (LC) Property

Definition: Linear complexity (LC) of a binary sequence of finite length is the length of the shortest LFSR that generates the same sequence. Berlekamp – Massey algorithm is an efficient algorithm for determining the linear complexity or Linear Span of binary sequence of finite length [36]. Hence a necessary condition for the sequence generator to be secure is that it always produces an output sequence with very large linear complexity [37].

8. Properties of segments of chaotic binary sequences over GF(2^8)

The random finite field elements generated using chaotic map equations (2) and (3) over GF(2^8) are mapped to binary sequence as discussed in section 2.2. The initial values x_0, bifurcation parameters r_1 and r_2 are all from GF(2^8) and the total number of field elements are 256 for each x_0, r_1 and r_2. Hence the total number of possible input combinations is 256 x 256 x 256. Out of the 256^3 combinations, if equation (2) is used some of the sequences with $r_1 = 0$ and $x_0 = 0$ are trivial and similarly when equation (3) is used some sequences are trivial (when $r_1 = 0$ or simultaneously both r_2 and x_0 are zero). In what follows all the possible combinations are not used. To study the cross correlation and linear complexity properties of generated binary sequences, the initial values x_0 and bifurcation parameters r_1 and r_2 are limited to few values.

It is found by computer simulation that for arbitrarily chosen 9 initial values of x_0 as (g, g^2 ….g^9), 24 values of r_1 as (g, g^2 ….g^{24}) and 24 values of r_2 as (g, g^2….g^{24}), the maximum possible period is 63 over GF(2^8) using equation (2) and 255 over GF(2^8) using equation (3). This will lead to 9 x 24 x 24 = 5184 input combinations. For 5184 input combinations the period of sequence over GF(2^8) is found to be lessthan or equal to 63 using equation (2) and lessthan or equal to 255 using equation (3).

Out of the generated 5184 sequence of elements from GF(2^8) using equation (2) there are 18 sequences of period 63, 268 sequences of period 62, 182 sequences of period 31, 73 sequences of period 30, 202 sequences of period 28, 223 sequences of period 21, 827 sequences of period 15, 341 sequences of period 14, 558 sequences of period 12, 100 sequences of period 10, 587 sequences of period 7, 489 sequences of period 6, 136 sequences of period 5, 122 sequences of period 4, 309 sequences of period 3, 198 sequences of period 2 and 551 sequences of period 1.

Similarly using equation (3), there are 2579 sequences of period 255, 1494 sequences of period 85, 648 sequences of period 51, 216 sequences of period 17, 216 sequences of period 15 and 31 sequences of period 1. In this paper the cross correlation and linear complexity properties are investigated for generated sequences with maximum possible period using equation (2) and (3).

8.1. Expressing field elements as binary 8 tuple

From equation (2) it is seen that, if $r_1 = 0$ or $x_0 = 0$, the sequence is all zero sequence, which are avoided. For 5184 input combinations the period of sequence over GF(2^8) is found to be less than or equal to 63. Out of 5184 sequences we get 18 sequences of period 63 over GF(2^8) and each element is expressed as binary 8 tuple and concatenated. Hence the period is 63 x 8 = 504 bits. This results in 33 non-overlapping segments of length 15 bits. The 15 bit segments are numbered as Segment1, Segment2… Segment33 as explained in section 4. The pairwise CCR values of segment 1 with all other segments are computed using equation (4). If the maximum pairwise CCR value exceeds α, then those segments are discarded and if the maximum pairwise CCR value is ≤ α then those segments are selected. This is repeated for all other segments. The values of $x_{0,}$ r_1 and r_2 for the 18 sequences of period 63 is given in Table 4.

The results are obtained for 15 bit binary sequences with pairwise α ≤ 0.35, ≤ 0.5 and ≤ 0.6. The results obtained for different α are summarized in Table 4.

Details of Trial 1 are given. The linear complexity (LC) of the 4 binary sequences along with their segment number corresponding to trial number 1 in Table 4 with pairwise α ≤ 0.35 is given in Table 5.

Table 4. Number of sequences out of 33 sequences having pairwise α ≤ 0.35, ≤ 0.5 and ≤ 0.6 with primitive polynomial $x^8+x^6+x^5+x^4+1$.

Trial Number	**Initial Value x_0 chosen**	**r_1 chosen**	**r_2 chosen**	**Number of binary sequences having pairwise CCR value lessthan α**		
				α ≤ 0.35	**α ≤ 0.5**	**α ≤ 0.6**
1	g	g^{23}	g^{24}	4	8	19
2	g^2	g^{23}	g^{24}	4	10	21
3	g^3	g^{23}	g^{24}	3	10	21
4	g^4	g^{23}	g^{24}	4	10	25
5	g^5	g^{23}	g^{24}	2	5	22
6	g^6	g^{23}	g^{24}	3	9	22
7	g^7	g^{23}	g^{24}	3	10	21
8	g^8	g^{23}	g^{24}	3	9	20
9	g^9	g^{23}	g^{24}	4	6	21
10	g	g^{24}	g^{23}	4	8	20
11	g^2	g^{24}	g^{23}	2	9	22

12	g^3	g^{24}	g^{23}	4	6	19
13	g^4	g^{24}	g^{23}	2	8	20
14	g^5	g^{24}	g^{23}	3	8	19
15	g^6	g^{24}	g^{23}	4	9	18
16	g^7	g^{24}	g^{23}	3	9	22
17	g^8	g^{24}	g^{23}	3	7	18
18	g^9	g^{24}	g^{23}	3	10	20

Table 5. LC of 4 binary sequences having pairwise $\alpha \leq 0.35$ along with segment number

Segment Number	**Binary Sequence**	**Linear complexity**
9	110010010010110	9
10	000001101010101	8
30	001010010000101	7
33	000110101111110	8

Likewise sequences having pairwise $\alpha \leq 0.5$ are identified. The segment number of these 8 binary sequences and their linear complexity for trial number 1 in Table 4 is given in Table 6.

Table 6. LC of 8 binary sequences having pairwise $\alpha \leq 0.5$ along with segment number

Segment Number	**Binary Sequence**	**Linear complexity**
1	000000100100111	8
7	100000100010001	7
9	110010010010110	9
19	011101111010000	8
30	001010010000101	7
31	011011001011100	7
32	100001110011101	8
33	000110101111110	8

Likewise segment numbers of 19 sequences whose pairwise $\alpha \leq 0.6$, the corresponding binary sequence and computed linear complexity for trial number 1 in Table 4 are given in Table 7.

The 18 combinations which gave length L = 63 is listed in Table 4. From Table 5, Table 6 and Table 7, it is seen that the linear complexity of binary sequences of length 15 bits generated using Logistic map equation (2) over GF(2^8) varies between 7 and 9. The linear complexity of Gold sequence of length 15 is 8. Some of the segments of 15 bits have linear complexity 9, which is more than that of Gold sequence of same length.

There are 17 Gold sequences [38] and [39] of length 15 bits which have pairwise $\alpha \leq 0.6$. There are no Gold sequences of length 15 bits and pairwise $\alpha \leq 0.35$ or 0.5. However using the proposed scheme it is possible to obtain number of sequences which is greater than Gold sequences whose length is 15 bits.

Table 7. LC of 19 binary sequences having pairwise $\alpha \leq 0.6$ along with segment number

Segment Number	**Binary Sequence**	**Linear complexity**
4	100101111100000	8
7	100000100010001	7
12	011101001101011	8
14	100111101000110	9
15	011111010101000	7
16	011011011110000	8
18	001110101011011	7
19	011101111010000	8
20	111111001110110	7
21	111110010000010	7
22	011001000010110	7
24	111001010001010	7
25	101100010001011	7
27	100011100111101	8
28	000011101110010	8
30	001010010000101	7
31	011011001011100	7
32	100001110011101	8
33	000110101111110	8

It is observed that by modifying logistic map equation (2) into the form given in equation (3), the properties of the chaotic sequence over GF(2^8) is changed. Out of 5184 sequences for arbitrarily chosen values of x_0, r_1 and r_2 as discussed in section 8, we get 2579 sequences of period 255 over GF(2^8) and each element is expressed as binary 8 tuple and concatenated. Hence the period is 255 x 8 = 2040 bits. This results in 136 non-overlapping 15 bit segments as described in section 4. The first 16 sequences among 2579 sequences of period 255 are considered and the results are tabulated in Table 5. As explained earlier the pairwise CCR values are computed for 15 bit segments and if the maximum pairwise CCR value exceeds α, then those segments are discarded.

The results are obtained for 15 bit binary sequences with pairwise $\alpha \leq 0.35$, ≤ 0.5 and ≤ 0.6. The results obtained for different α are summarized in Table 8.

Details of Trail 1 are given below. The linear complexity (LC) of the two binary sequences along with their segment number corresponding to trial number 1 in Table 8 with pairwise $\alpha \leq 0.35$ is given in Table 9.

Table 8. Number of sequences out of 136 sequences having pairwise $\alpha \leq 0.35$, ≤ 0.5 and ≤ 0.6 with primitive polynomial $x^8+x^6+x^5+x^4+1$

Trial Number	**Initial Value x_0 chosen**	**r_1 chosen**	**r_2 chosen**	**Number of binary sequences having**		
				$\alpha \leq 0.35$	**$\alpha \leq 0.5$**	**$\alpha \leq 0.6$**
1	g	g	g	2	5	30
2	g^2	g	g	3	7	30
3	g^3	g	g	2	6	36
4	g^4	g	g	2	8	25
5	g^5	g	g	2	9	30
6	g^6	g	g	3	9	30

7	g^7	g	g	2	7	29
8	g^8	g	g	2	8	26
9	g^9	g	g	2	10	33
10	g	g^2	g	3	7	31
11	g^2	g^2	g	2	9	38
12	g^3	g^2	g	4	8	29
13	g^4	g^2	g	2	8	40
14	g^5	g^2	g	4	9	34
15	g^6	g^2	g	4	9	38
16	g^7	g^2	g	4	5	31

Table 9. LC of 2 binary sequences having pairwise $\alpha \leq 0.35$ along with segment number

Segment Number	**Binary Sequence**	**Linear complexity**
1	000000100000000	7
47	000110011110011	7

Likewise sequences having pairwise $\alpha \leq 0.5$ are identified. The segment number of these 5 binary sequences and their linear complexity for trial number 1 in Table 8 is given in Table 10.

Table 10. LC of 5 binary sequences having pairwise $\alpha \leq 0.5$ along with segment number

Segment Number	**Binary Sequence**	**Linear complexity**
1	000000100000000	7
14	111000100110110	10
16	001011001011001	6
82	010111000000001	9
107	111111101010000	7

Likewise segment numbers of 30 sequences whose pairwise $\alpha \leq 0.6$, the corresponding binary sequence and computed linear complexity for trial number 1 in Table 8 are given in Table 11. From Table 9, Table 10 and Table 11, it is seen that the linear complexity of binary sequences of length 15 bits generated using equation (3) varies between 6 and 11. As in the case of binary sequences of length 15 bits using equation (2), in this case also it is possible to obtain number of sequences which is greater than Gold sequences whose length is 15 bits. There are no Gold sequences of length 15 bits and pairwise $\alpha \leq 0.35$ or 0.5. A similar result in case of binary sequence obtained by transformation of chaotic sequence over reals is reported in [25].

Table 11. LC of 30 binary sequences having pairwise α ≤ 0.6 along with segment number

Segment Number	Binary Sequence	Linear complexity
8	001101101000011	8
10	111100110101110	8
14	111000100110110	10
28	000101001010011	10
38	011001010110100	8
50	001100001110001	8
51	101111100110000	8
53	001010010001010	9
54	101111010101000	8
58	110100111001110	8
64	001101000110000	8
70	110001100010111	9
71	111111100010110	8
73	111100011001011	8
84	000001101000110	8
87	101011001000110	6
89	011101011110111	11
90	010101001001001	7
93	111000101001010	7
96	001100001000101	8
104	010010000111101	7
107	111111101010000	7
112	101111111001011	8
113	111000111011001	7
117	111010001001011	8
119	100001101101110	10
123	110110101111010	8
131	110000101100010	8
134	011011101111011	7
135	001001111001111	8

8.2. Choosing Bits in location i (where i = 1 to 8) of each symbol in the sequence

Consider the logistic map given by equation (2). For 5184 input combinations we get only 18 sequences of period 63 over GF(2^8) as discussed in section 8 and when transformed to binary choosing bits in location i (i = 1 to 8) the period is 63. Hence there are 18 x 8 = 144 sequences of period 63. This results in only 4 non-overlapping segments of 15 bits. The first 2 combinations choosing bits in location i (i = 1 to 8) resulting in 2 x 8 = 16 sequences are tabulated in Table 12. As explained in section 8.1, the pairwise CCR values of 15 bit segments are computed and if the pairwise CCR value is ≤ α then those segments are selected.

The results are obtained for 15 bit sequences with pairwise α ≤ 0.35, ≤ 0.5 and ≤ 0.6 with the same $x^8+x^6+x^5+x^4+1$ as primitive polynomial defining GF(2^8) for equation (2) which gives maximum period of 63. The results obtained for different α for each bit selection are summarized in Table 12.

Table 12. Number of sequences out of 4 sequences having pairwise $\alpha \leq 0.35$, ≤ 0.5 and ≤ 0.6 with primitive polynomial $x^8+x^6+x^5+x^4+1$

Trial Number	**x_0 chosen**	**r_1 chosen**	**r_2 chosen**	**Bit Chosen**	**Number of binary sequences having**		
					$\alpha \leq 0.35$	**$\alpha \leq 0.5$**	**$\alpha \leq 0.6$**
1	g	g^{23}	g^{24}	1 (MSB)	2	3	4
2	g	g^{23}	g^{24}	2	3	3	4
3	g	g^{23}	g^{24}	3	2	3	4
4	g	g^{23}	g^{24}	4	3	4	4
5	g	g^{23}	g^{24}	5	3	4	4
6	g	g^{23}	g^{24}	6	3	4	4
7	g	g^{23}	g^{24}	7	3	4	4
8	g	g^{23}	g^{24}	8 (LSB)	3	4	4

Details of Trail 1 are given below. The linear complexity (LC) of the 2 binary sequences along with their segment number corresponding to trial number 1 in Table 12 with pairwise $\alpha \leq 0.35$ is given in Table 13.

Table 13. LC of 2 binary sequences having pairwise $\alpha \leq 0.35$ along with segment number

Segment Number	**Binary Sequence**	**Linear complexity**
3	100011101011111	6
4	101101000100001	6

Likewise sequences having pairwise $\alpha \leq 0.5$ are identified. The segment number of these 3 binary sequences and their linear complexity for trial number 1 in Table 12 is given in Table 14.

Table 14. LC of 3 binary sequences having pairwise $\alpha \leq 0.5$ along with segment number

Segment Number	**Binary Sequence**	**Linear complexity**
2	100000110111001	6
3	100011101011111	6
4	101101000100001	6

Likewise segment numbers of 4 sequences whose pairwise $\alpha \leq 0.6$, the corresponding binary sequence and computed linear complexity for trial number 1 in Table 12 are given in Table 15.

Table 15. LC of 4 binary sequences having pairwise $\alpha \leq 0.6$ along with segment number

Segment Number	**Binary Sequence**	**Linear complexity**
1	001010100100111	6
2	100000110111001	6
3	100011101011111	6
4	101101000100001	6

From Table 13, Table 14 and Table 15, it is seen that the linear complexity of binary sequences of length 15 bits generated using equation (2) is 6. However using the proposed scheme the number of 15 bit segments is limited to only 4. Also it is possible to generate few sequences of length 15 bits with pairwise $\alpha \leq 0.35$ or 0.5.

Next we consider equation (3). Out of 5184 sequences generated using equation (3) for arbitrarily chosen values of x_0, r_1 and r_2 as discussed in section 8, we get 2579 sequences of period 255 over $GF(2^8)$ and when transformed to binary choosing bits in location i (i = 1 to 8) results in 2579 x 8 = 20632 sequences. Each of this sequence can be divided into 17 non-overlapping segments of 15 bits as described in section 5. The first combination choosing bits in location i (i = 1 to 8) resulting in 1 x 8 = 8 sequences are tabulated in Table 16. As explained earlier, the pairwise CCR values of 15 bit segments are computed and if the pairwise CCR value exceeds α then those segments are discarded.

The results are obtained for 15 bit non-overlapping segments with pairwise α ≤ 0.35, ≤ 0.5 and ≤ 0.6 with the same ($x^8+x^6+x^5+x^4+1$) as primitive polynomial defining GF(2^8) using equation (3) which gives period of 255. The results obtained for different α for each bit selection are summarized in Table 16.

Table 16. Number of sequences out of 17 sequences having pairwise α ≤ 0.35, ≤ 0.5 and ≤ 0.6 with primitive polynomial $x^8+x^6+x^5+x^4+1$ with initial values $x_0 = g$ and $r_1 = g$ and $r_2 = 0$

Trial Number	**Bit Chosen**	**Number of binary sequences having pairwise CCR value lessthan α**		
	i	**α ≤ 0.35**	**α ≤ 0.5**	**α ≤ 0.6**
1	1 (MSB)	4	11	15
2	2	3	8	15
3	3	2	9	14
4	4	3	9	16
5	5	3	6	15
6	6	2	10	13
7	7	2	8	15
8	8 (LSB)	2	11	15

Details of Trail 1 are given below. The linear complexity (LC) of the four binary sequences along with their segment number corresponding to trial number 1 in Table 16 with pairwise α ≤ 0.35 is given in Table 17.

Table 17. LC of 4 binary sequences having pairwise α ≤ 0.35 along with segment number

Segment Number	**Binary Sequence**	**Linear complexity**
8	111001100011000	7
10	110100010100001	9
11	001000001111001	8
14	011011011001111	8

Likewise sequences having pairwise α ≤ 0.5 are identified. The segment number of these 11 binary sequences and their linear complexity for trial number 1 in Table 16 is given in Table 18. Likewise segment numbers of 15 sequences whose pairwise α ≤ 0.6, the corresponding binary sequence and computed linear complexity for trial number 1 in Table 16 are given in Table 19.

From Table 17, Table 18 and Table 19, it is seen that the linear complexity varies between 7 and 9, for binary sequences of length 15 bits generated using equation (3). Also it is possible to generate some sequences of length 15 bits with pairwise α ≤ 0.35 or 0.5.

Table 18. LC of 11 binary sequences having pairwise α ≤ 0.5 along with segment number

Segment Number	**Binary Sequence**	**Linear complexity**
1	000000011011110	8
2	101100000101010	8
4	101001100110100	8
7	010111011010010	7
8	111001100011000	7
9	011100100111101	7
10	110100010100001	9
11	001000001111001	8
13	101111101100010	8
16	011101111111010	8
17	011100001011110	8

Table 19. LC of 15 binary sequences having pairwise α ≤ 0.6 along with segment number

Segment Number	Binary Sequence	Linear complexity
1	000000011011110	8
2	101100000101010	8
3	100011111001110	9
4	101001100110100	8
6	001000110101011	8
7	010111011010010	7
8	111001100011000	7
9	011100100111101	7
10	110100010100001	9
11	001000001111001	8
13	101111101100010	8
14	011011011001111	9
15	110001011011100	8
16	011101111111010	8
17	011100001011110	8

8.3. Mapping in to binary using Trace function

Consider the logistic map given by equation (2). For 5184 input combinations we get only 18 sequences of period 63 over GF(2^8) as discussed in section 8 and when transformed to binary using trace function, the period is 63. This results in 4 non-overlapping segments of length 15 bits. The values of $x_{0,}$ r_1 and r_2 for the 18 sequences of period 63 is given in Table 20. The 15 bit segments are numbered as Segment1, Segment2, Segment3 and Segment4 as explained in section 5. The pairwise CCR values of segment 1 with all other segments are computed using equation (4). If the maximum pairwise CCR value exceeds α, then those segments are discarded and if the maximum pairwise CCR value is ≤ α then those segments are selected. This is repeated for remaining segments. The results are obtained for 15 bit binary sequences with pairwise α ≤ 0.35, ≤ 0.5 and ≤ 0.6 using equation (2) which gives maximum period of 63 bits. The results obtained for different α are summarized in Table 20.

Table 20. Number of sequences out of 4 sequences having pairwise α ≤ 0.35, ≤ 0.5 and ≤ 0.6 with primitive polynomial $x^8+x^6+x^5+x^4+1$

Trial Number	Initial Value x_0	r_1 chosen	r_2 chosen	Number of binary sequences		
				α ≤ 0.35	α ≤ 0.5	α ≤ 0.6
1	g	g^{23}	g^{24}	2	3	3
2	g^2	g^{23}	g^{24}	2	3	4
3	g^3	g^{23}	g^{24}	2	3	4
4	g^4	g^{23}	g^{24}	2	3	4
5	g^5	g^{23}	g^{24}	2	4	4
6	g^6	g^{23}	g^{24}	2	4	4
7	g^7	g^{23}	g^{24}	2	3	4
8	g^8	g^{23}	g^{24}	3	3	4
9	g^9	g^{23}	g^{24}	3	3	4
10	g	g^{24}	g^{23}	2	3	4
11	g^2	g^{24}	g^{23}	2	2	4
12	g^3	g^{24}	g^{23}	2	3	4
13	g^4	g^{24}	g^{23}	2	3	3

14	g^5	g^{24}	g^{23}	3	3	3
15	g^6	g^{24}	g^{23}	2	3	3
16	g^7	g^{24}	g^{23}	2	3	4
17	g^8	g^{24}	g^{23}	3	3	4
18	g^9	g^{24}	g^{23}	2	4	4

Details of Trail 1 are given below. The linear complexity (LC) of the 2 binary sequences along with their segment number corresponding to trial number 1 in Table 20 with pairwise $\alpha \le 0.35$ is given in Table 21.

Table 21. LC of 2 binary sequences having pairwise $\alpha \le 0.35$ along with segment number

Segment Number	**Binary Sequence**	**Linear complexity**
1	000011111011010	7
2	011110101100111	7

Likewise sequences having pairwise $\alpha \le 0.5$ are identified. The segment number of these 3 binary sequences and their linear complexity for trial number 1 in Table 21 is given in Table 22.

Table 22. LC of 3 binary sequences having pairwise $\alpha \le 0.5$ along with segment number

Segment Number	**Binary Sequence**	**Linear complexity**
1	000011111011010	7
3	011011010011101	7
4	111100011000110	7

Likewise segment numbers of 3 sequences whose pairwise $\alpha \le 0.6$, the corresponding binary sequence and computed linear complexity for trial number 1 in Table 20 are given in Table 23.

From Table 21, Table 22 and Table 23, it is seen that the linear complexity of binary sequences of length 15 bits generated using equation (2) is 7. However using the proposed scheme the number of sequences is limited to only 4 whose length is 15 bits.

Table 23. LC of 3 binary sequences having pairwise $\alpha \le 0.6$ along with segment number

Segment Number	**Binary Sequence**	**Linear complexity**
1	000011111011010	7
3	011011010011101	7
4	111100011000110	7

Next we consider equation (3). Out of 5184 sequences generated using equation (3) for arbitrarily chosen values of x_0, r_1 and r_2 as discussed in section 8, we get 2579 sequences of period 255 over $GF(2^8)$ and when transformed to binary using trace function results in 2579 x 1 = 2579 sequences. Each of this sequence can be divided in to 17 non-overlapping segments of 15 bits as described in section 6. The first 16 sequences among 2579 sequences of period 255 are considered and the results are tabulated in Table 24. As explained earlier, the pairwise CCR values of 15 bit segments are computed and if the pairwise CCR value is $\le \alpha$ then those segments are selected.

The results are obtained for 15 bit binary non-overlapping segments with pairwise $\alpha \le 0.35$, ≤ 0.5 and ≤ 0.6 using equation (3) which gives maximum period of 255 bits for arbitrarily chosen values of initial values x_0 and r_1 and r_2. The results obtained for different α using trace function are summarized in Table 24.

Table 24. Number of sequences out of 17 sequences having pairwise α ≤ 0.35, ≤ 0.5 and ≤ 0.6 with primitive polynomial $x^8+x^6+x^5+x^4+1$

Trial Number	**x_0 chosen**	**r_1 chosen**	**r_2 chosen**	**Number of binary sequences having**		
				α ≤ 0.35	**α ≤ 0.5**	**α ≤ 0.6**
1	g	g	g	2	6	12
2	g^2	g	g	3	7	11
3	g^3	g	g	4	6	14
4	g^4	g	g	2	6	14
5	g^5	g	g	3	7	14
6	g^6	g	g	3	5	14
7	g^7	g	g	5	7	13
8	g^8	g	g	2	6	10
9	g^9	g	g	3	6	14
10	g	g^2	g	3	6	11
11	g^2	g^2	g	4	7	12
12	g^3	g^2	g	3	6	13
13	g^4	g^2	g	3	7	11
14	g^5	g^2	g	3	8	14
15	g^6	g^2	g	4	9	13
16	g^7	g^2	g	2	6	12

Details of Trail 1 are given below. The linear complexity (LC) of the two binary sequences along with their segment number corresponding to trial number 1 in Table 24 with pairwise α ≤ 0.35 is given in Table 25.

Likewise sequences having pairwise α ≤ 0.5 are identified. The segment number of these 6 binary sequences and their linear complexity for trial number 1 in Table 24 is given in Table 26.

Table 25. LC of 2 binary sequences having pairwise α ≤ 0.35 along with segment number

Segment Number	**Binary Sequence**	**Linear complexity**
1	010010001010001	7
6	110001101111010	8

Table 26. LC of 6 binary sequences having pairwise α ≤ 0.5 along with segment number

Segment Number	**Binary Sequence**	**Linear complexity**
6	110001101111010	8
7	011101101100101	8
9	101111110111111	6
10	000100011101111	7
12	101010011111001	7
16	100000011100110	8

Likewise segment numbers of 12 sequences whose pairwise α ≤ 0.6, the corresponding binary sequence and computed linear complexity for trial number 1 in Table 24 are given in Table 27.

From Table 25, Table 26 and Table 27, it is seen that the linear complexity of binary sequences of length 15 bits generated using equation (3), varies between 6 and 9. There are no Gold sequences of length 15 bits and pairwise α ≤ 0.35 or 0.5. However using the proposed scheme it is possible to obtain some sequences having pairwise α ≤ 0.35 and 0.5 whose length is 15 bits.

Table 27. LC of 12 binary sequences having pairwise α ≤ 0.6 along with segment number

Segment Number	**Binary Sequence**	**Linear complexity**
3	011110010001100	8
4	111000001111101	9
6	110001101111010	8
7	011101101100101	6
9	101111110111111	6
10	000100011101111	7
12	101010011111001	7
13	000000001111111	9
14	001011011011100	9
15	000000100011111	7
16	100000011100110	8
17	010010001010001	8

The generated binary sequences are investigated for cross correlation and linear complexity properties for sequences of length 15 bits and found to have good cross correlation values.

9. CONCLUSIONS

In this paper, we have proposed a scheme for generation of binary sequences using logistic map equation defined over GF(2^8). Some segments of length 15 bits of the generated chaotic binary sequences are tested for cross correlation and linear complexity properties. The investigation is done for 15 bit binary sequences and compared with Gold sequences. From the results it is observed that there are segments of 15 bit with pairwise CCR value less than that of Gold sequences. There are 17 Gold sequences of length 15 bits that can be generated using two 4 stage Linear Feedback Shift Register (LFSR) and hence the linear complexity is 8. But the proposed sequences have linear complexity varying between 6 and 11. Some of the segments of 15 bits have linear complexity more than that of Gold sequences.

Gold sequences of length 15 have maximum pairwise CCR value of 0.6 [38] and [39]. Using the proposed model it is possible to generate few sequences with pairwise CCR value lessthan that of Gold sequences.

In general we can conclude that it is possible to generate binary sequences of length 15 bits using equations (2) and (3) with good cross correlation value compared to Gold sequences of the same length 15. Similar results for binary sequences derived from chaotic sequences over reals are reported in [25].

REFERENCES

[1] Wai M. Tam, F.C.M Lau and Chi K. Tse, "An Improved Multiple Access Scheme for Chaos-based Digital Communications using Adaptive Receivers", *IEEE ISCAS 2004*, pp. 605 – 608, 2004.

[2] K. Umeno and K. Kitayama, "Sreading Sequences using Periodic Orbits of Chaos for CDMA", *Electronics Letters*, Vol. 35, No. 7, pp. 545 – 546, April 1999.

[3] Sandoval-Morantes and D. Munoz-Rodrigues, "Chaotic Sequences for Multiple Access", *Electronics Letters*, Vol. 34, No. 3, pp. 235 – 237, Feb. 1998.

[4] Makot Itoh, "Spread Spectrum Communication via Chaos", *Int. J. Bifurcation and Chaos*, Vol. 9, No. 1, pp. 155 – 213, 1999.

[5] Jaffar M.H. Elmirghani and Robert A. Cryan, “Point-to-Point and Multi-User Communication based on Chaotic Sequences”, *IEEE*, pp. 582 – 584, 1995.

[6] Michail Sushchic, Lev S. Tsimring and Alexander R. Volkovskii, “Performance Analysis of Correlation-based Communication Schemes Utilizing Chaos”, *IEEE Trans. Circuits Syst. I*, Vol. 47, No. 12, pp. 1684 – 1691, Dec. 2000.

[7] Omar Farooq and Sekharjit Datta, “Signal-dependent Chaotic-state-modulated Digital Secure Communication”, *ETRI Journal*, Vol. 28, No. 2, pp. 250-252, April 2006.

[8] Ajeesh P. Kurian and Sadasivan Puthusserypady, “Secure Digital Communication using Chaotic Symbolic Dynamics”, *Turk J Elec Engin*, Vol. 14, No. 1, pp. 195-207, 2006.

[9] A.R.Volkovskii, L.h.Tsimring, N.F.Rulkov and I.Langmore, “Spread Spectrum Communication System with Chaotic Frequency Modulation”, *Chaos 15, American Inst. of physics*, pp. 033101-1-6, 2005.

[10] Alireza Mirzaee and Hassan Aghaeinia, “Design of a New Class of Spreading Sequence using Chaotic Dynamical Systems for Asynchronous DS-CDMA Applications”, IEEE, 2004.

[11] C Vladeanu, I.Banica and S.El Assaa, “Period Chaotic Spreading Sequences with Better Correlation Properties than Conventional Sequences-BER Performances Analysis”, IEEE, pp.649-652, 2003.

[12] Tohru Kohda, “Statistical Properties of Chaotic Sequences Generated by Jacobian Elliptic Chebyshev Rational Maps”, *IEEE-ISCAS 2004*, pp. 648-651, 2004.

[13] Daisaburou Yoshioka, Akio Tsuneda and Takahiro Inoue, “Search Algorithm of Maximal-Period Sequences based on One-Dimensional Maps with Finite Bits and its Application to DS-CDMA Systems”.

[14] S.J.Thiruvengadam, A.R.Karthikeyan, N.Muthuraja, V.K.Vinothkumar and V.Abhaikumar, “Performance Analysis of DS-CDMA System with Space-Time Multiuser Detection using a Class of Chaotic Spreading Sequences”, IEEE, 2003.

[15] Maide Bucolo, Riccardo Caponetto, Luigi Fortuna, Mattia Frasca, Alessandro Rizzo,“Does Chaos work Better than Noise”, *IEEE*, 2002.

[16] Zhang Xueyi, Jin Lu, Wang Kejun and Li Dianpu, “Logistic-Map Chaotic Spreading Spectrum Sequences under Linear Transformation”, *IEEE proceedings on Intelligent Control and Automation”*, pp. 2464-2467, Jul. 2000.

[17] Xingang Wang, Meng Zhan, Xiaofeng Gong, Choy Heng Lai, Ying-Cheng Lai, “Spread Spectrum Communication using Binary Spatiotemporal Chaotic Codes”, *Phys. Lett. A* 30-36, 2005.

[18] Yilmaz Akin and Sarp Ertiirk, “Chaotic Frequency Hopping for Code Division Multiple Access”, *IEEE,* pp. 716-719, 2004.

[19] Li Zan, Tie Yi, Jin Lijun, Chang Yilin and Cai Jueping, “Analysis of Multi-Access Performance Based on Non-Period Chaotic Frequency Hopping Sequences”, *Proc. International Conf. Computer Networks and Mobile Computing (ICCNMC’03)*, 2003.

[20] Ricardo Caponetto, Luigi Fortuna, Stefano Fazzino and Maria Gabriella Xibilia, “Chaotic Sequences to Improve the Performance of Evolutionary Algorithms”, *IEEE Trans. Evolutionary Computation,* Vol. 7, No. 3, pp. 289-304, June 2003.

[21] Ali Kanso, Nejib Smaoui, “Logistic Chaotic Maps for Binary Numbers Generations”, *Chaos, Solitons & Fractals (2007)*, *Elsevier*, pp. 1-12.

[22] Akeo Tsuneda, “On Autocorrelation Properties of Chaotic Binary Sequences Generated by One Dimensional Maps”, IEEE, 2000, pp. 2025-2030.

[23] Chong Fu, Zhi-liang Zhu, “An Improved Chaos-based Stream Cipher Algorithm”, *Third International Conference on Natural Computation (ICNC 2007), IEEE.*

[24] Li Shuzan, Mou Xuanqin, and Cai Yuanlong, "Pseudo-Random Bit Generator Based on Couple Chaotic Systems and its Applications in Stream-Cipher Cryptography", *Progress in Cryptology - INDOCRYPT 2001, LNCS*, Vol. 2247, pp. 316-329, Springer-Verlag, Berlin, 2001.

[25] Mahalinga V. Mandi , K.N. Haribhat , R. Murali, "Generation of Large Set of Binary Sequences Derived from Chaotic Functions with Large Linear Complexity and Good Cross Correlation Properties", *International Journal of Advanced Engineering Applications (IJAEA)*, June 2010, Vol. III, pp. 313 – 322, ISSN: 0975 – 7791 (Online), ISSN: 0975 – 7783 (Print).

[26] G.Heidari-Bateni and C.D.McGillem, "Chaotic Sequences for Spread Spectrum: An Alternative to PN-Sequences", *IEEE- ICWC'92*, 1992.

[27] G.Heidari-Bateni and C.D.McGillem, "A Chaotic Direct Sequence Spread Spectrum Communication Systems", *IEEE Trans.Commun.,* Vol.42, No.2/3/4, pp.1524-1527, Mar.1994.

[28] Wai M.Tam, Francis C.M.Lau and Chi K.Tse, "Performance Analysis of Multiple Access Chaotic-Sequence Spread-Spectrum Communication Systems using Parallel Interference Cancellation Receivers", *International Journal of Bifurcation and Chaos*, Vol.14, No.10, pp. 3633-3646, 2004.

[29] Mahalinga V. Mandi , K.N. Haribhat , R. Murali, "A Survey of Generation of Chaotic Sequences for Communication", *Proceedings of National Conference on Signal Processing and Communication(NCSPC-2006),* pp.59-60, July 7 - 8, 2006.

[30] Mahalinga V. Mandi , K.N. Haribhat , R. Murali, "Generation of Discrete Spreading Sequences using Chaotic Functions and their use in Spread Spectrum Communication", *Proc. Sonata International Conf. Computer, Communication and Controls,* pp.128 - 133, Nov 23 - 25, 2006.

[31] Mahalinga V. Mandi , K.N. Haribhat , R. Murali, "Chaotic Functions for Generating Binary Sequences and their Suitability In Multiple Access", *Proc. IEEE International Conference on Communication Technology 2006 (IEEE-ICCT 2006),* Vol. 1, pp.217 – 220, Nov 27 – 30, 2006.

[32] V.C. da Rocha Jr. and G. Markarian, "Simple Method to Find Trace of Arbitrary Element of a Finite Field", Electronic Letters, Mar. 2006, Vol. 2, No. 7.

[33] Robert Gold, "Optimal Binary Sequences for Spread Spectrum Multiplexing", *IEEE Trans. on Information Theory*, pp. 619 – 621, Oct. 1967.

[34] Nguyen Quang A, Laszlo Gyorfi and J.L. Massey, "Families of Sequences with Optimal Generalized Hamming Correlation Properties", *Proc. Int. Symp. on Information Theory,* IEEE, 1986.

[35] Guu-Chang Yang, Wing C. Kwang, "Prime Codes with Applications to CDMA Optical and Wireless Networks", Aptech House Inc., ISBN 1-58053-073-7, pp. 26 -27, 2002.

[36] J.L. Massey, "Shist Register Synthesis and BCH Decoding", *IEEE Trans. Information Theory*, Vol. IT-15, pp. 122-127, Jan. 1969.

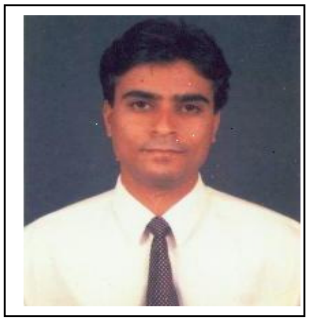
[37] J.L Massey, "Cryptography and System Theory", Proc. 24th Allerton Conf. on Commn., Control and Computing, Oct. 1-3, 1986.

[38] Robert Gold, "Maximal Recursive Sequences with 3-Valued Recursive Cross-Correlation Functions", *IEEE Trans. on Information Theory*, pp. 154 – 1556, Jan. 1968.

[39] John G. Proakis, "Digital communications", Mc. Graw Hill International Edition*,* 4th Edition, 2001.

Authors

Mahalinga V. Mandi received the B.E. Degree in Electronics and Communication Engineering from Mysore University, Karnataka, India in 1990 and M.Tech Degree in Industrial Electronics from Mysore Univeristy, Karnataka, India in 1998. He is currently working towards Ph.D Degree at Dr MGR University, Chennai, India. He is working as Faculty in the Department of Electronics & Communication Engineering, Dr Ambedkar Institute of Technology, Bangalore, India. His research areas include Digital Communication, Cryptography and Network Security.



Dr K N Haribhat received the B.E Degree with honors from Mysore University in 1966, M.Tech and Ph.D in Electronics & Communication Engineering from Indian Institute of Technology, Kanpur, in 1973 and 1986, respectively. He is currently working as Dean Academic and Head, Department of Electronics & Communication Engineering at Nagarjuna College of Engineering & Technology, Bangalore, India. He was with Karnataka Regional Engineering College, Suratkal, India (Currently known as NIT-K) for more than 30 years. His research areas include Analog Communication, Digital Communication and Cryptography. He has authored more than 25 papers in National/international Conferences and Journals. He has coauthored two books on communication.

Dr Murali R received the M.Sc Degree in Mathematics from Bangalore University, Karnataka, India in 1990 and Ph.D Degree in Mathematics from Bangalore University, India in 1999 and currently working as Professor in the Department of Mathematics, at Dr Ambedkar Institute of Technology, Bangalore, India. His research areas include Graph Theory-Hamiltonian graphs. He has authored more than 12 papers in National/International Journals.