International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 4, July- August 2017 ISSN 2278-6856

Generation of Non Binary Non Word Oriented Pseudorandom Sequence from Discrete Equally Spread Periodic Samples Viewed Orthogonally as an Envelope, Study of its Characteristics, Testing and Application for Stream Cipher System

Sudeepa K B[1] , Ganesh Aithal [2]

[1] Research Scholar, Department of Computer Science and Engg., NMAM Institute of Technology , Nitte-574114, India

[2] Mangalore Institute of Technology and Engineering, Moodabidri, Mangalore , Karnataka, India.

[3]Monash University, Department of Management, McMahons Road, Frankston 3199, Austria

Abstract

Due to the wide spread of Internet technologies, past decades have witnessed enormous transmission of the multimedia content over the Internet. This multimedia content needs to be transmitted over insecure wireless channel and indented only to be transmitted to its legal owner, which generates the need for the protection of this multimedia data. Multimedia security and issues related to it, has therefore attracted many researchers to it. Cryptography is necessary to protect the confidential information transmitting over the network. The strength of the stream cipher is not only depending upon its encryption / decryption algorithm, it also depends upon the randomness properties of the key sequence such as length, uniformity, independence etc. In this work a finite set of uncoupled objects of same shape and dimension may be used display sine/cosine wave which alternatively looks like travelling waves, standing waves, and random disorder patterns. These random disorder patterns are used to generate non binary random numbers and these numbers are used as key in stream cipher system.. This is having greater advantages like one time padding / to achieve perfect security in cryptographic application. The same non binary key sequence generated is applied for the cryptographic application and the security parameters of the result obtained from cryptographic application are also evaluated to observe the strength of security level.

Keywords: Stream Cipher System, Pseudo Random Number Generator, Residue Number System,

1. INTRODUCTION

Data can hacked during transmission of data through network channel and hence it is very essential to be transmitted in a secure manner. Cryptography, watermarking and stegnography are the major techniques to ensure security of the data. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The main goal of cryptography is data privacy (confidentiality), data authenticity (it came from where it claims) and data integrity (it has not been modified in any way) in the digital world. Based on type of key will be used for encryption/decryption cryptography systems are categorized as symmetric key-system and asymmetric key system [1].

In symmetric crypto system same key will be shared for both encryption and decryption operation. But in case asymmetric crypto system , a pair of private and public key is used for encryption/decryption operation on message so that it arrives securely. Symmetric cryptography is split into block ciphers and stream ciphers which are easy to distinguish. A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (key stream) to produce cipher text. Symmetric key system such as DES [2][3], AES[4][5] and RC4[6] that use same key for encryption and decryption. In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of the key stream to give a digit of the cipher text stream. Stream ciphers are often used for their speed and simplicity of implementation in hardware.

A stream cipher submitted by P. Ekdahl and T. Johansson[7] has a secret shared key of 128 or 256 bits and IV value of 128 bits. This stream cipher uses an LFSR of length 16 on GF (232) and a non-linear finite state machine. D. H. Lehrer [8] introduced a method to produce pseudo random sequence where previously generated number (X_{n+1}) is used for the generation of next number X_n by equation

$$(aX_n + c)\ mod\ m. \quad (1)$$

Where multiplier *a,* modulus *m* and *c* the increment. Eichenauer and Lehn [9] in 1986 introduced an alternative method for the generation , which is inverse congruential method, where new pseudo random numbers is are obtained by

$$X_{n+1} = (X_n^{-1} + c) \, mod \, p \qquad (2)$$

Here inverse is defined by $X^{-1}X \equiv 1 \, mod \, p$, p is prime number, X_n $\varepsilon\{0, 1\ldots p\text{-}1, \infty\}$.

The simple one-dimensional chaotic Logistic and Cubic maps are integrated to generate the real-valued chaotic sequences, which on pre-processing and quantization give a PN sequence that has noise-like characteristics [10].

A nonlinear functions are also used with Chaotic sequence to generate pseudo random sequence and which is used for Digital Image Encryption [11]. Based on summation of numbers from Z_M, chosen as multiples of number from previous iteration and Mapped again to Z_M pseudo random numbers are generated for the application of cryptography [12]. Logistic map equation are used to generate the key sequence and applied for the cryptographic applications.[13]. Maximum length pseudorandom number sequence generated for RNS based stream cipher systems [14].

This work proposes generator consist of set of equally spaced discrete oscillating samples of decreasing period. These samples oscillates, with a periodically increasing order, the envelop of which generates wave form, observed from orthogonal plain. This wave form has a frequency which increases in order with respect to time.

The displacement of these samples is considered as individual points. These individual points at a particular frequency of the envelop wave will be random in nature. These patterns considered for the as non binary non word oriented pseudo random sequence with number of sample as length of the sequence. The overall design of this model is discussed in the next section. The result of the generated PRN is discussed in the result and analysis section numbered 3. Section 4 deals with the application and its result analysis for cryptographic strength. are discussed in 5 .

2. GENERATION OF NON BINARY NON WORD ORIENTED PSEUDO RANDOM SEQUENCE FROM DISCRETE EQUALLY SPREAD PERIODIC SAMPLES VIEWED ORTHOGONALLY AS AN ENVELOPE.

As it is seen in case of feedback shift register the generation of pseudorandom number, the length of the sequence is fixed when the numbers of registers are fixed. To extend the length of the sequence it is necessary to increase the number of registers. A thought has been provoked in this paper, is it possible to vary the generation function dynamically so that the sequence length increases. The answer for this question is yes, it is possible to get discrete samples of variable frequency trigonometric functions with a fixed timing, at a particular instant of time it behaves as a random pattern of sampling. By increasing the number of samples it is possible to get the higher length of the sequence.

The generator consists of set of equally spaced discrete oscillating samples of decreasing / increasing in period. When these object, starts oscillating from a single line of points, it looks like a wave form of discrete samples with increasing in frequency, from orthogonal plane. Figure number 2, 3, 4, 5, 6, 7, 8, 9 and 10 shows how it looks like as the time increases. These patterns of samples can be described by the continuous mathematical function *y[x, t]* , where y_i is the displacement at position *x* and time *t* of a particular sample o_i where *i=.1, 2, . . . n*

$$y_i[x,t]=A\cos[t*1/p] \qquad (1)$$

Where *t* is time, *A* is amplitude of the envelop and p_i is period of i^{th} sample o_i .
The period p_i of an sample o_i is defined as the number of oscillation per time, where Γ is the total time period of the envelop wave form (starts oscillating from a single line of points, till it come back to the same point), it is described by

$$p_i = \Gamma / (N + k_i) \qquad (2)$$

where k_i the increase in period of with respect to its previous sample o_i*-1.* The equation (2) says that the period of the sample is inversely proportional to the number of oscillations of the sample. As the number of oscillation per cycle *Γ* increases the distance of the sampling the waveform decreases. At time *t = 0* the phase shift between adjacent sample is zero as shown in figure 1. At time *t = Γ/2* every sample is exactly out of phase with nearest neighbors, so the phase shift between adjacent sample is π *radian,* as shown in the figure 5. At time *t = Γ* the objects will be back in starting position so the phase shift between the adjacent sample is 2π *radian,* that is same as at time t = 0 as shown in figure 1 and 9.

As an Example, let us consider 40 samples of varying period placed at equal distance between adjacent objects in decreasing order. The period of the objects are tuned such that the pattern repeats at time 30 units of time i.e Γ=30. When we simulate the scenario using equation (1) with amplitude 7,*k*=1 and *N=3,*the result exhibited at time *t=0,t=1, t=7, t=11 and t=15 i.e* at some particular point between *t=0 to* Γ/2 *is* shown in the figure [1-5] and result exhibited at time *t*= Γ/2 to Γ is shown in the figure[5-9]. Comparing the result from time *t=0 to* Γ/2 and Γ/2 to 0 shows that the displacement at *t=0 and t*= Γ are same and the pattern from *t=0 to* Γ/2 repeats at *t* = Γ/2 to Γ in reverse order. At some particular point of time period between *t=0 and t*= Γ, the displacement pattern of objects will be random and it satisfies randomness properties .

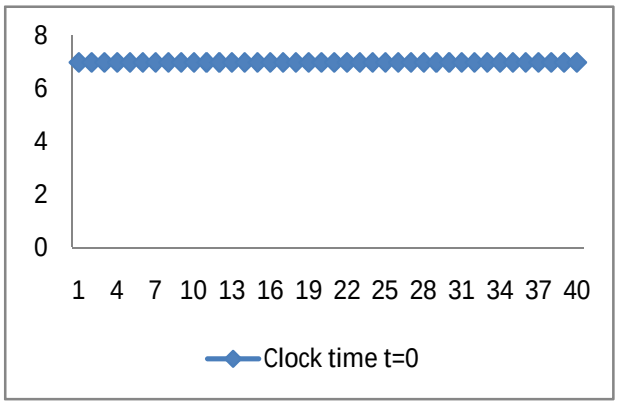

Figure. 1. Displacement of object at time t=0

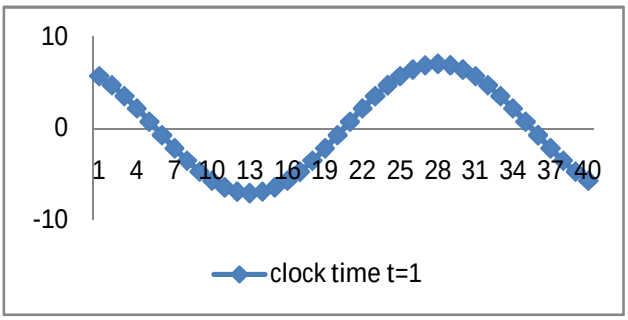

Figure. 2 Displacement of object at time t=1

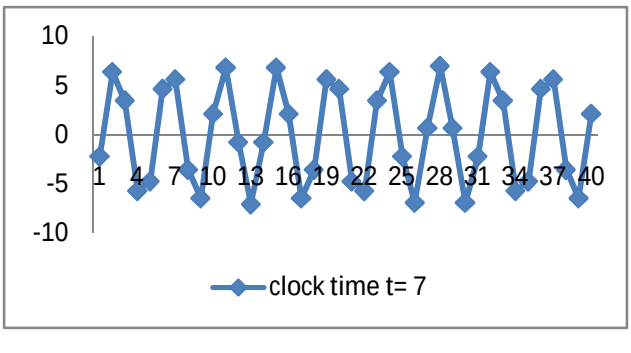

Figure 3. Displacement of object at time t=7

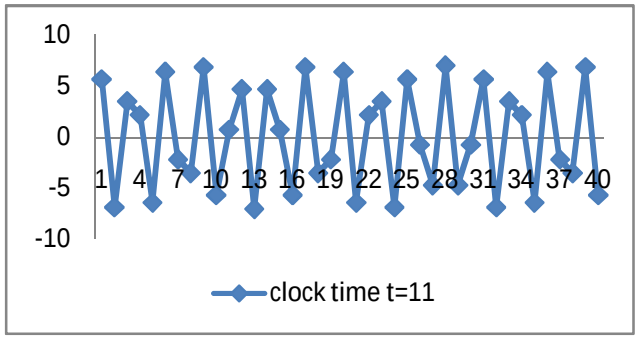

Figure 4. Displacement of object at time t=11

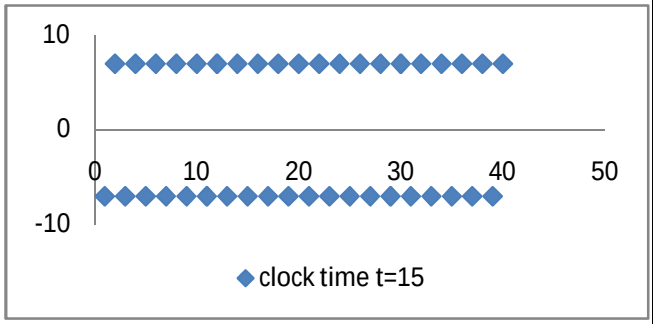

Figure.5. Displacement of object at time t=15

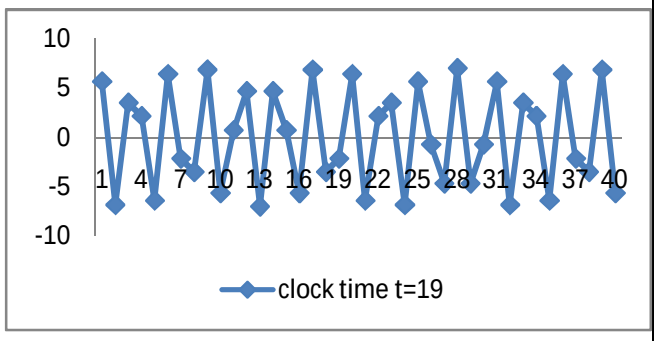

Figure.6. Displacement of object at time t=19

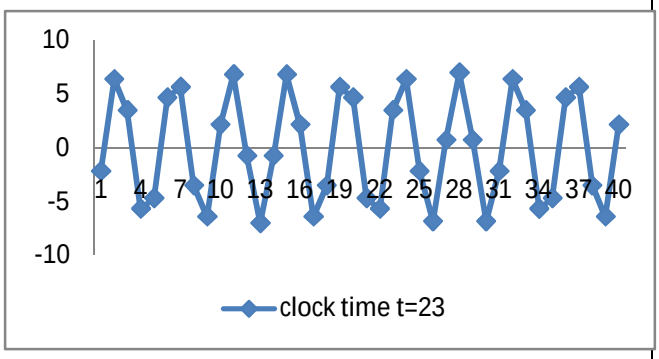

Figure.7 Displacement of object at time =23

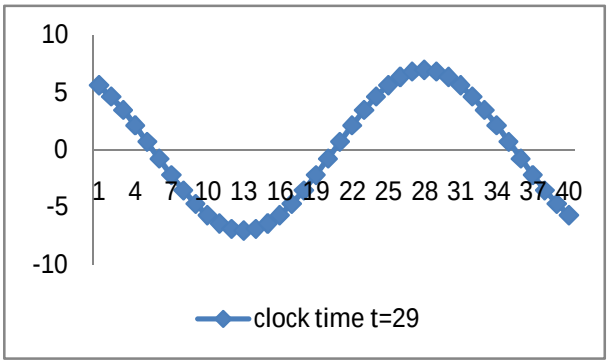

Figure. 8 Displacement of object at time t=29

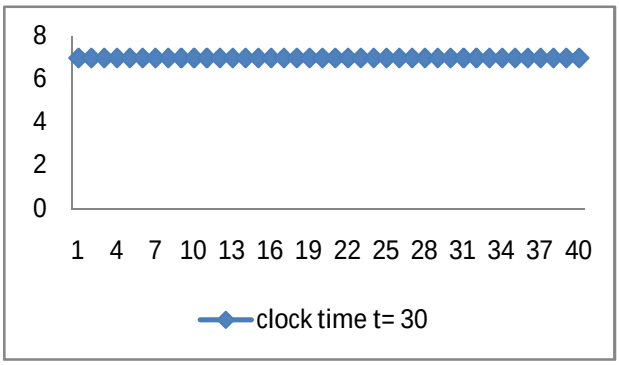

Figure.9. Displacement of object at time t=30

3.RESULTS AND ANALYSIS OF PSEUDO RANDOM SEQUENCE

The effectiveness of Pseudo Random Number Sequence could be analyzed based on the the statistical test result. The result of generator produces pseudo random sequence over the range [0,14] and [0, 16] and the result of statistical test conducted are discussed in this section.

3.1 Generation of non binary Pseudo Random sequence over the range [0,14] .

Let us consider a sequence of pseudorandom numbers of finite set are required for the stream cipher system. Considering 30 objects, the time of cycle Γ is 30s, the number of oscillation is longest object is 5 and the next longest 6 and so on. With these initial condition will generate the pseudo random sequence over the range [0,14] given by equation (2). Considering amplitude *A=7*, it returns the displacement of objects over the space -7 to 7 . The columns of the table represents clock time and each row shows indiudual objects displacement at corresponding clock time. First row shows the displacement of first object at different clock time, second row shows displacement of second object at different clock time and so on. Due to aliasing affect the displacement of object repeats in reverse order. Therefore only clock time form 0 to Γ/2 is considered in table. To generate the pseudo random number sequence, displacement is mapping to integer over the range is required. In this example we considered the space -7 to 7 and possible integers are over the range from integer 0 to 14. Therefore the amplitude space is divided into 15 divisions of ranges from -7 to 7. At each clock time the displacement of the object is determined and corresponding integer is generated based on division to which the displacement belongs. The displacement position belongs to -7 to-6.07 is mapped to integer 0, -6.07 to -5.14 is mapped to integer 1, -5.14 to -4.21 is mapped to integer 2, -4.21 to-3.28 is mapped to integer 3 , -3.28 to -2.35 is mapped to integer 4, -2.35 to -1.42 is mapped to integer 5, -1.42 to -0.49 is mapped to integer 6, -0.49 to 0.44 is mapped to integer 7, 0.44 to 1.37 is mapped to integer 8, 1.37 to 2.3 is mapped to integer 9, 2.3 to 3.23 is mapped to integer 10, 3.23 to 4.16 is mapped to integer 11, 4.16 to 5.09 is mapped to integer 12, 5.09 to 6.02 is mapped to integer and 13 and 6.02 to 7 is mapped to integer 14.

The displacements of oscillating object with respect to amplitude about x- axis at different clocks time *t =0, t =1, t =7, t =11, t =15, t =19, t =23, t =29* and *t =30*,are shown in table 1. These variations of displacement are due to variation in number oscillation of same dimension object. This variation leads to generation of pseudo random number sequence. The generated number at each and corresponding indiudual clock time given in table 2.Each column represents number sequence with respect to corresponding clock time.

Among these number sequences few satisfies pseudo randomness properties and these pseudo random sequences are considered as key sequence for cryptographic application. The key sequence at clock time 7 and 11 is shown in figure (10) which satisfies randomness properties.

In similar way using equation (1) pseudo random sequences are generated over the range [0,16] and these sequences are used for the cryptographic applications.

Table. 1: Displacement of objects at different clock time.

Object Position	Clock t	0	1	7	11	15	19	23	29	30
1	Displacement over amplitude 7	7.0	5.6	-2.1	5.6	-7.0	5.6	-2.1	5.6	7.0
2		7.0	4.6	6.3	-6.8	7.0	-6.8	6.3	4.6	7.0
3		7.0	3.4	3.4	3.5	-7.0	3.5	3.4	3.4	7.0
4		7.0	2.1	-5.6	2.1	7.0	2.1	-5.6	2.1	7.0
5		7.0	0.7	-4.6	-6.3	-7.0	-6.3	-4.6	0.7	7.0
6		7.0	-0.7	4.6	6.3	7.0	6.3	4.6	-0.7	7.0
7		7.0	-2.1	5.6	-2.1	-7.0	-2.1	5.6	-2.1	7.0
8		7.0	-3.5	-3.5	-3.4	7.0	-3.4	-3.5	-3.5	7.0
9		7.0	-4.6	-6.3	6.8	-7.0	6.8	-6.3	-4.6	7.0
10		7.0	-5.6	2.1	-5.6	7.0	-5.6	2.1	-5.6	7.0
11		7.0	-6.3	6.8	0.7	-7.0	0.7	6.8	-6.3	7.0
12		7.0	-6.8	-0.7	4.6	7.0	4.6	-0.7	-6.8	7.0
13		7.0	-7.0	-7.0	-7.0	-7.0	-7.0	-7.0	-7.0	7.0
14		7.0	-6.8	-0.7	4.6	7.0	4.6	-0.7	-6.8	7.0
15		7.0	-6.3	6.8	0.7	-7.0	0.7	6.8	-6.3	7.0
16		7.0	-5.6	2.1	-5.6	7.0	-5.6	2.1	-5.6	7.0
17		7.0	-4.6	-6.3	6.8	-7.0	6.8	-6.3	-4.6	7.0
18		7.0	-3.9	-3.4	-3.5	7.0	-3.5	-3.4	-3.9	7.0
19		7.0	-2.1	5.6	-2.1	-7.0	-2.1	5.6	-2.1	7.0
20		7.0	-0.7	4.6	6.3	7.0	6.3	4.6	-0.7	7.0
21		7.0	0.7	-4.6	-6.3	-7.0	-6.3	-4.6	0.7	7.0
22		7.0	2.1	-5.6	2.1	7.0	2.1	-5.6	2.1	7.0
23		7.0	3.4	3.4	3.5	-7.0	3.5	3.4	3.4	7.0
24		7.0	4.6	6.3	-6.8	7.0	-6.8	6.3	4.6	7.0
25		7.0	5.6	-2.1	5.6	-7.0	5.6	-2.1	5.6	7.0
26		7.0	6.3	-6.8	-0.7	7.0	-0.7	-6.8	6.3	7.0
27		7.0	6.8	0.7	-4.6	-7.0	-4.6	0.7	6.8	7.0
28		7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0
29		7.0	6.8	0.7	-4.6	-7.0	-4.6	0.7	6.8	7.0
30		7.0	6.3	-6.8	-0.7	7.0	-0.7	-6.8	6.3	7.0

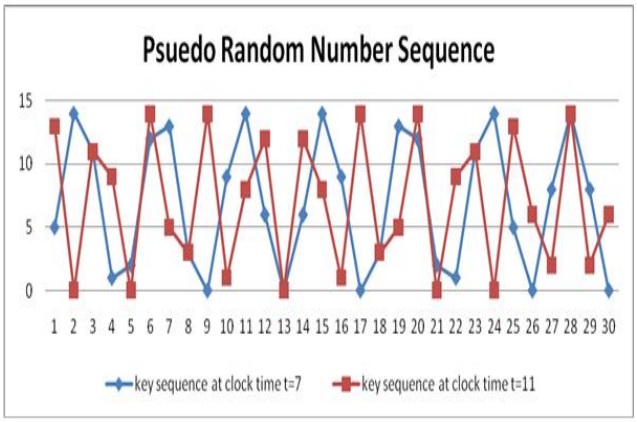

Figure 10. Graph of pseudo random key sequence at clock time 7 and 11.

Table 2: Generated integer by mapping displacement corresponding to table 1

Object Position	Clock t	0	1	7	11	15	19	23	29	30
1	Displacement over amplitude -7 to 7	14	13	5	13	0	13	5	13	14
2		14	12	14	0	14	0	14	12	14
3		14	11	11	11	0	11	11	11	14
4		14	9	1	9	14	9	1	9	14
5		14	8	2	0	0	0	2	8	14
6		14	6	12	14	14	14	12	6	14
7		14	5	13	5	0	5	13	5	14
8		14	3	3	3	14	3	3	3	14
9		14	2	0	14	0	14	0	2	14
10		14	1	9	1	14	1	9	1	14
11		14	0	14	8	0	8	14	0	14
12		14	0	6	12	14	12	6	0	14
13		14	0	0	0	0	0	0	0	14
14		14	0	6	12	14	12	6	0	14
15		14	0	14	8	0	8	14	0	14
16		14	1	9	1	14	1	9	1	14
17		14	2	0	14	0	14	0	2	14
18		14	3	3	3	14	3	3	3	14
19		14	5	13	5	0	5	13	5	14
20		14	6	12	14	14	14	12	6	14
21		14	8	2	0	0	0	2	8	14
22		14	9	1	9	14	9	1	9	14
23		14	11	11	11	0	11	11	11	14
24		14	12	14	0	14	0	14	12	14
25		14	13	5	13	0	13	5	13	14
26		14	14	0	6	14	6	0	14	14
27		14	14	8	2	0	2	8	14	14
28		14	14	14	14	14	14	14	14	14
29		14	14	8	2	0	2	8	14	14
30		14	14	0	6	14	6	0	14	14

3.2 Statistical test Result

Chi square test for uniformity, autocorrelation rest for independence and run test are conducted for the sequence generated from equation (2) over the range [0,14] . The sequence shown in table 2 at clock time 7 and clock time 11 are tested and corresponding statistic values are compared with critical values of chi-square test, autocorrelation and run test at significance level 0.05. Since statistic values of number sequences at clock time 7 and clock time 11 are less than critical value as shown in table 3,these sequences satisfies randomness properties. If statistic values of autocorrelation and run test lies between -1.96 to 1.96 at significance level 0.05, then the sequence considered satisfies randomness. The table 4 shows the statistic result at clock 7 and clock 11 for autocorrelation, run up and down and run above and below the mean test. It shows that number sequence at clock time 7 and clock time 11 satisfies randomness properties.

Table 3. Comparison of Statistic value for chi square test

Clock time *t* of Sequence	Statistic value	Critical Value	Accept/Reject
7	22.0	23.7	Accept
11	21.6	23.7	Accept

Table 4. Statistic value for autocorrelation test, run up and down test and run above and below test.

Clock time of Sequence	Statistic value of Autocorrelation	Statistic value of Run up and down	Statistic value of Run above and below	Accept /Reject
7	0.22	1.66	0.16	Accept
11	0.97	0.63	1.73	Accept

4. APPLICATION OF HYBRID MODEL IN IMAGE ENCRYPTION AND ITS RESULT ANALYSIS

Generated key key sequences over the range [0,14] and [0,16] are applied in image encryption based on RNS stram cipher system[16].A composte integer *m* can be represented as a product of *k* realative prime numbers . Therefore by using RNS , a large a large integer which is less than *m* can be decomposed into *k* components. There in this application each pixel is devided into two components of modular 15 and modular 17. The encryption opratioon of stream cipher is performed based on eaquation (3) and decryption opeartion is performed based on equation (4) where c_{ij} *is* jth cipher component of ith pixel, p_{ij} is jth plain text component of ith pixel, X_{ji} ith key of jth key generator ang g_j jth generotor modular component.

a. Additive encryption algorithm

$$Cipher\ data\ element\ \{c_{ij}\}=[\{p_{ij}\}+\{X_{ji}\}]mod g_j \qquad (3)$$

Where $i= 1,2,3….n$ and $j=1,2,3,……k$.

b. Additive decryption algorithm

$$Plain\ text\ \{p_{ij}\} =[\{c_{ij}\}-\{X_{ji}\}]mod\ g_j \qquad (4)$$

where $i = 1,2,3….n$ and $j=0,1,2,3,……k$

The input image for the encryption operation and the result of encryption i. e the cipher image is shown in figure (11) and figure (12) respectively.

Figure 11. Original Image

Figure 12. Encrypted Image

4.1 Histogram of number of occurrences

The distribution of pixel values in cipher image is observed by comparing the histogram of pixel occurrence in of original image and cipher text (encrypted image).Figure 13 shows the histogram of original image and figure 14 shows the histogram of cipher image. It clearly shows the uniform distribution of pixels in cipher image. This observation clarifies that the image encryption proposed has higher the security against the attacks.

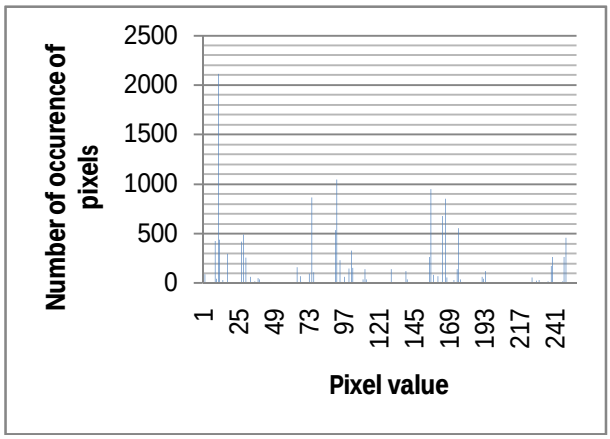

Figure 13. Histogram of original image

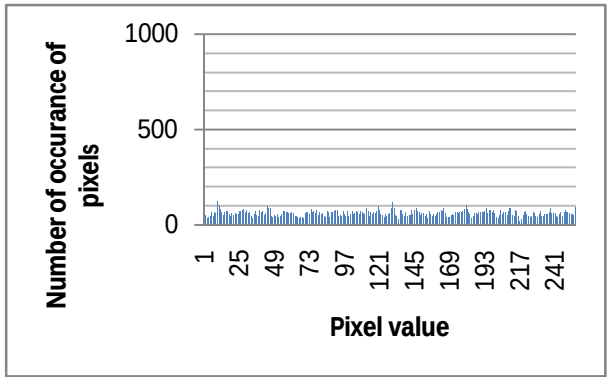

Figure 14. Histogram of cipher image

4. CONCLUSION

Non Binary Non Word Oriented pseudorandom sequence of pseudo random sequences are generated from of discrete periodic samples of equally spread objects viewed orthogonally as an envelope of samples. These sequences are tested for statistical test at each clock time and it is observed that the sequence satisfies pseudo randomness properties such as test for uniformity and test for independence. The generated pseudo random key sequences are applied as key sequence for RNS based stream cipher system. The strength of cipher system is analyzed based on the histogram comparison of original image and cipher image. It shows that the cipher image pixels are uniformly distributed and hence there is no information about the actual data. Therefore the system has got immunity to the attack.

References

[1]. W. Stallings, Cryptography and Network Security-Principles and Practice, 3rd ed. Pearson Education.
[2]. Barker, W. Introduction to the Analysis of the Data Encryption Standard (DES). Laguna Hills, CA: Aegean Park Press, 1991 .
[3] , H. “Cryptography and Computer Privacy.” Scientific American, May 1973.
[4]. Daemen, J., and Rijmen, V. “Rijndael : The advanced Encryption Standard.” Dr. Dobb’s Journal, March 2001 .
[5]. Daemen, J., and Rijmen, V. The Design of Rijndael: The Wide Trail Strategy Explained. New York: Springer-Verlag.
[6]. Robshaw, M. Block Ciphers. RSA Laboratories Technical Report TR-601, August 1995. http://www.rsasecurity.com/rsalabs.
[7]. PatrikEkdahl and Thomas Johansson,(2001) “SNOW-a new stream cipher”, In Proceedings of First NESSIE Workshop, Heverlee, Belgique
[8]. D. H. Lehmer, “Mathematical Method in Large-scale Computing Unit”, Proceeding of the second symposium on Large-scale Digital. Computing Machinery, Harvard University Press, Cambridge, Massachusetts, pp. 141-146, 1951.
[9]. Donald D Knuth “Art of Computer Programming Semi numerical Algorithm” Vol 2 Third Edition Pearson Education Inc. Publication. 2006.
[10]. Musheer Ahmad , Omar Farooq “Chaos Based PN Sequence Generator for Cryptographic Applications “, International Conference on Multimedia, Signal Processing and Communication Technologies, 2011.
[11]. H. Ogras, M. Turk. “Digital Image Encryption Scheme using Chaotic Sequences with a Nonlinear Function” World Academy of Science, Engineering and Technology, 2012.
[12]. Ankur, Divyanjali , “A New Approach to Pseudorandom Number Generation”, Fourth International Conference on Advanced Computing & Communication Technologies, 2014,IEEE.
[13]. Shruthi KM, Sheela S, Sathyanarayana SV. Image encryption scheme with key sequences based on chaotic functions. In international conference on contemporary computing and informatics 2014 (pp. 823-7). IEEE.
[14]. Sudeepa K B, Ganesh aithal. “Generation of maximum length non-binary key sequence and itsapplication for stream cipher based on residue number system”, journal of computational science, Volume-21,2016(379-386), Elsevier.
[15]. James. A. Flaten ,Kevin . A. Perando. “Pendulum wave: A lesson in aliasing”, American Journal of Physics, 2001.
[16]. Aithal, Ganesh, KN Hari Bhat, and U. Sripathi. "Implementation of Stream Cipher System based on representation of integers in residue number system." Advance Computing Conference (IACC), 2010 IEEE 2nd International. IEEE, 2010.

AUTHOR

Sudeepa K B working as associate professor for the department of computer science, NMAMIT, Nitte. I completed my bachelor of engineering with first class in 2002 from Visvesvaraya Technological University, Belgaum, Karnataka, India. I have completed my Master of engineering (First class with Distinction) from Bangalore University, Karnataka, India in 2009. In year 2012 I have registered for my PhD at Visvesvaraya Technological University under the guidance of Dr. Ganesh Aithal. I am having total 12 years of teaching experience and have published papers in 3 international conferences and published 1 journal paper.

Dr. Ganesh Aithal currently working as Research dean at Mangalore Institute of Technology and Engineering, Moodbidri, Mangalore. He has completed his bachelor of engineering from Manipal Institute of Technology, Mangalore University. He has completed is PhD from NITK, Surathkal, Karnataka, India in the year 2010.He has published papers in IEEE transaction, and other international journals.