International Journal of Engineering and Management Research
e-ISSN: 2250-0758 | p-ISSN: 2394-6962
https://ijemr.vandanapublications.com

Peer Reviewed & Refereed Journal
Volume-14, Issue-2 (April 2024)
https://doi.org/10.5281/zenodo.11201784

Collective Research Review on Chaotic Based Encryption Algorithms, Speech Encryption Algorithms and Cryptographic Requirements

Pushpalatha G S[1] and Dr. Ramesh S[2]
[1]Assistant Professor, Department of ECE, Dr. Ambedkar Institute of Technology, INDIA
[2]Professor, Department of ECE, Dr. Ambedkar Institute of Technology, INDIA

[1]Corresponding Author: pushpalatha13@gmail.com

Received: 27-03-2024 Revised: 13-04-2024 Accepted: 28-04-2024

ABSTRACT

Chaotic cryptography has been a recent development by researchers due to its interesting properties such as non-linear behavior, sensitivity to initial conditions, ergodicity, mixing, confusion and diffusion etc. This paper is a brief review of various standard encryption algorithms, cryptographic requirements for design of chaotic based cryptosystem and chaos-based speech encryption algorithms. This study also gives various statistical tests needs to be considered for conformity about suitable randomness of the binary sequences generated using either hardware or software means for cryptographic applications as key sequence.

Keywords— Chaotic Cryptography, Random Number Generation, Statistical Tests, Speech Encryption, Stream Cipher

I. INTRODUCTION

The advancements in internet technologies has made the wide use of multimedia data like image, audio, video in various applications such as entertainment, military, education, banking, communication, medical etc. Multimedia data is vulnerable to attack from various corners and hence it has to be protected to maintain confidentiality, integrity, and authenticity. This has led to the various research and developments in cryptography. Cryptography is the art of protecting data scientifically for secure communication [1][2].

Multimedia data is generally large in size and expensive. Traditional block encryption algorithms such as Data Encryption Standard (DES) [3], Advanced Encryption Standard (AES) [4], IDEA [5] and RSA [6] are found to be not ideal for multimedia applications in real time applications as they are generally slow to handle bulky data [7][8].

The stream cipher is more suitable for real time processing of large bulky multimedia such as speech, video, image etc. Chaos based functions can be used to generate key stream having desirable properties as required for cryptographic applications. They are of high interest due to their potential benefits such as high non-linearity and low cost [9][10].

II. REQUIREMENTS OF CHAOS BASED CRYPTOGRAPHY

Chaos functions are generally nonlinear dynamic systems. The main vital characteristics of chaotic functions are, non-linearity and high sensitivity to minutely changed initial conditions which can be exploited to obtain sequence of random bits which is required for good cipher system. In recent times chaotic theory based pseudorandom generators have been studied to explore the possibility to find application in cipher system. Thus chaotic functions are becoming a very important and reliable source of cryptography. The random behaviour of chaotic signals makes it more suitable for cryptographic applications. Some of the one-dimensional chaotic maps are discussed. These chaotic maps exhibit chaotic behaviour for the suitable range of system parameter 'r' and initial condition 'x_0'. One value of system parameter 'r' for which the systems behave chaotic is also mentioned for every system from (1) to (4).

- Logistic map

$$x_{n+1} = r x_n (1 - x_n), \quad r = 3.99 \tag{1}$$

Where, $x_n \in [0,1]$ and $r \in [0,4]$

- Tent map

$$x_{n+1} = \begin{cases} r\, x_n, & if\ x_n > 0.5 \\ r(1 - x_n), & if\ x_n \le 0.5 \end{cases}, \quad r = 1.97 \tag{2}$$

Where ,'r' is a positive real constant

- Sine map

$$x_{n+1} = r\sin(x_n), \quad r = 0.99 \tag{3}$$

Where , $x_0 \in [0,1]$ and $r \in [0,1]$

- Cubic map

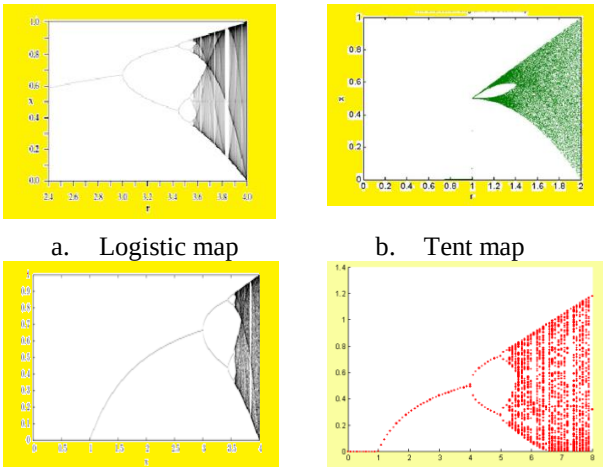
$$x_{n+1} = r x_n (1 - {x_n}^2), \quad r = 2.59 \tag{4}$$

Where , $x_n \in [0,1]$ and $r \in [0,4]$

Peer Reviewed & Refereed Journal
Volume-14, Issue-2 (April 2024)
https://doi.org/10.5281/zenodo.11201784

The bifurcation diagrams of the chaotic maps are as shown in Fig.1, where the chaotic behaviour can be observed for the specified range of initial values and 'r' as described from (1) to (4). These diagrams show the relationship between chaotic states and their corresponding control parameters.

These systems exhibit high sensitivity to a slight change in the seed parameters, such as initial conditions and control parameters. Hence, these chaotic maps are useful in generating pseudo random numbers. In most cases using chaotic function as stream generator for cryptographic applications, it is found that either the generation method is complex for implementation particularly it is difficult to analyze or sequences do not comply with standard requirements for such applications [11].



a. Logistic map b. Tent map

c. Sine map d. Cubic map

Figure 1: Bifurcation diagrams of Chaotic maps

To design a better crypto system, Gonzalo Alvarez and Shujun Li have suggested some of the rules to be considered during the implementation of chaos-based cryptosystems. They are listed as follows [12].

1. The implementation details of the chaotic systems should be provided.
2. Ease of implementation without compromising security, cost and speed.
3. Accurate definition of key and its range should be defined and it should be wide enough and exemption classes should be well defined to avoid non-chaotic regions and to make sure the avalanche effect is guaranteed.
4. Key should exhibit uniform distribution property such that, a minute information about the key should not give any clue to engineer on information on the plaintext (P).
5. The process of generating keys should be well defined.
6. Any minute change in Plain text or key should result in completely different cipher to thwart any statistical attacks.
7. It should be analysed for any weakness to avoid any type of attacks.
8. Random sequences generated using Pseudo-random bit generator for stream cipher should be tested for its randomness properties using standard statistical tests.

A new pseudo-random number generator using couple of chaotic systems suitable for digital cipher is described in [13]. Few examples of stream ciphers based on digital cross coupled random bit generator and their security, theoretical analyses is discussed. Authors claims its better cryptographic properties mainly suitable for stream ciphers-based systems [13]. Linear complexity property of a binary sequence is an important requirement for cryptographic applications and is achieved by matrix recurrence relation obtained over Z4 in the literature [14]. M. S. Baptista (1998) had proposed a one-dimensional chaotic cryptosystem, and its modifications and shows a very promising generator for its suitability for many applications along with cryptographic needs. In [15]. Shujun Lee et.al have analysed Baptista type generator and its variants for its cryptographic properties and its defects also proposes a method to enhance the security to thwart successfully security attacks [15].

III. SPEECH ENCRYPTION METHODS AND REQUIREMENTS

A. Special Requirements of Speech Encryption

Multimedia applications such as speech encryption have their own requirements due to their special characteristics such as large higher volumes, redundancy, interactive operations and requires such as real time quick responses.

Audio and speech signals are very important component of many multimedia applications. Encryption of audio data is more complex with high computation complexity compared to text and documented data as audio signals are lengthy and has negative values which can be lost after some transformations. Speech communication has been widely used in wireless communication scenario. Hence it is very important to have secured communication. Speech signals that carry very sensitive information need to be secured from unauthorized access [16].

Speech encryption algorithms must meet the tradeoff between real time processing and security. There is a need for designing an efficient, secure encryption algorithm for real time speech signal. Although speech

Peer Reviewed & Refereed Journal
Volume-14, Issue-2 (April 2024)
https://doi.org/10.5281/zenodo.11201784

signal is defined as a specific type of audio signal, its properties are different than conventional audio signal.

Wireless telephony industry provides speech and audio services such as video conferencing and news broadcasting, the security needs are enormous as the data is very high also vulnerable to attack. Real time fast secure stream cipher system could be the answer for the need of these types of applications.

The important requirements like high security, large key space, high sensitivity, demand for real time compliance and error minimizing capability, threats, attacks, high computational complexity and analysis are discussed in [16].

B. Speech Encryption Methods

Various speech encryption algorithms have been reported in the literatures some of the important schemes are discussed here.

Zhaopin Su, et.al. have developed selective encryption of G.729 speech [17]. In which two different schemes are proposed considering bit sensitivity. Two different techniques of encryption to achieve different level of security are proposed. These methods are suitable for low power and narrow bandwidth devices.

A speech encryption scheme is proposed in [18] in which scrambling technique to create confusion property for increasing security. Combination of AES and chaotic function are used. Authors claim that the scheme is resistant to linear and differential cryptanalysis and the scheme has obtained chaos behavior in signal diffusion and confusion parts.

Another speech encryption system is found in [19], in which the author has developed permutation and substitution of speech samples using secret keys in time and transform domains to achieve high security.

Large set of Kasami sequence for improved security in speech encryption system is proposed in [20]. The resultant sequence shows that it is very sensitive to the secret key with good diffusion and confusion properties. This method claim that it has achieved low residual intelligibility, very good audio quality and increased security.

Two partial-encryption techniques such as high protection scheme and low protection scheme are developed in a “Low complexity perception based partial encryption of speech signal” [21]. This work focuses to prevent many types of eavesdropping. Performance evaluation is carried out by signal inspection in time and frequency domains, objective distortion measures, and formal listening tests. This method provides high levels of speech content protection for low power, portable devices thus results in longer battery life.

In paper [22] Blind source separation (BSS) is a new scheme for speech encryption is presented and author claims that the proposed method has achieved increased security while retaining very good audio quality. A Standard Stream cipher-based algorithms A5 algorithm and its variants like enhanced A5/2 is used in providing voice privacy in the GSM cellular telephone protocol.

C. Chaotic Based Speech Encryption Methods

Speech encryption is a challenging task due to several reasons, including the nature of the speech signal, the need for real-time processing, and the requirements for maintaining quality and intelligibility of the speech signal. To design a secure and effective speech encryption system, there are several key design requirements that must be considered. Chaos cryptography meets the demands of real time processing of speech signal and hence makes it suitable for real time applications.

Some of chaotic speech encryption algorithms reported in the literatures are as shown in Table (1) with few observations such as proposed method, type of chaotic function and inference.

Table 1: Observations from chaotic based speech encryption methods

Reference	Proposed speech encryption	Chaotic function used	Inference
[23],[24] by E.Mosa et.al	A low complexity speech encryption system based on substitution and permutation	Baker map based high security speech encryption in both time and transform domains	Low complexity, high level of security, high speed
[25] by Long Jye Sheu	Speech encryption by fractional chaotic systems	Two channel using fractional Lorenz systems	Large key space and high level of security
[26] by Musheer Ahmad et.al	Mixed key stream generator for encryption of voice signal	High dimension al Chen and Lorenz Chaotic maps	high level of security and made suitable for real time voice encryption, good key distribution properties
[27] by P. Sathiyamurthy et.al	Fast Fourier Transform (FFT) and multiple chaotic map based speech communication	Logistic map and 3-D Lorenz map	Better security and good quality of reconstructed signal.

Peer Reviewed & Refereed Journal
Volume-14, Issue-2 (April 2024)
https://doi.org/10.5281/zenodo.11201784

D. Statistical tests

Random number sequences should possess the desirable statistical properties to use it as key sequence for cryptographic applications. Various testing schemes are available in the literature such as National Institute of Standards and Technology (NIST) [28], DIEHARD, Crypt-XS etc. NIST Test suite is a standard to determine the sequence as random enough for suitability for cryptographic applications. It includes 15 tests, which are developed to test the randomness of binary sequences generated by either hardware/software based cryptographic random/pseudorandom generators. The various statistical tests are listed as follows.

1. Frequency (Monobit) Test

In order to maintain number of 0's and 1's approximately same in the generated random sequence for uniform distribution of these symbols monobit test is necessary. Once this test pass then all other subsequence test may be performed

2. Frequency Test within a Block

This test is to check the occurrence of symbol 1's within the block of length M-bits. This test is necessary in order to check the occurrence of symbol 1's in the block of length M-bits is approximately half of M-bits as required for the assumed randomness.

3. Runs Test

The main purpose of this test is to find the repetition of similar bits pattern in a sequence.

The number of runs 0's and 1's of different lengths is as required for a random sequence.

4. Longest Run of Ones in a Block

This test is to check the longest length of occurrence of 1's within the block of M-bits. This test is necessary in order to check the length of occurrence of 1's in the block of M bits is uniform throughout the sequence as required for the assumed randomness.

5. Binary Matrix Rank Test

In this test the rank of disjoint submatrices entire sequence is determined and this is essential in order to find for linear dependency among given length substrings of the main sequence.

6. Discrete Fourier Transform (DFT) Test

The test is to determine the spectrum of the sequence in order to know the peaks in the DFT of the sequence. This test is necessary to detect periodicity of patterns that occur nearby other patterns.

7. Non-Overlapping Template Matching Test

This test is to find the number of repetitions of pre-defined target pattern. In this test occurrence of given non-periodic (aperiodic) patterns is determined to avoid repetitions of such patterns in the generated sequence. There should not more such aperiodic patterns in the sequence.

8. Overlapping Template Matching Test

This test is similar to test no.7 described above. In this case overlapping templates is considered instead of non-overlapping template.

9. Maurer's "Universal Statistical" Test

This test is necessary to find the compressibility of the sequence significantly without the loss of information.

If the sequence is not compressible the sequence can be considered to be random.

10. Linear Complexity Test

This test is to find the minimum order 'n' of the linear feedback shift register (LFSR) required to generate the sequence. Larger the linear complexity, likelihood of sequence appears to be random. The short LFSR indicates the sequence is non- random.

11. Serial Test

The focus of this test is to find frequency of overlapping *k*-bit patterns in the entire sequence. All possible such patterns are determined and it is checked for uniform distribution property. Also the number of such pattern is determined and checked for its frequency to that of random sequence.

12. Approximate Entropy Test

In this case the test is similar to the test 11. The objective of this test is to compare the two consecutive overlapping blocks and find the similarity between them (*k* and *k+1*) and compare it to the value expected of random sequence

13. Cumulative Sums (Cusum) Test

Cumsum test is made to find the algebraic sum of the value of mapped digits (-1, +1) corresponds to walk defined by the in the sequence. For any sequence to be random, the cumulative sum of random walk should approach zero.

14. Random Excursions Test

In this case (0 1) sequence is mapped to (-1, +1) the test is performed to determine the number of periods with exact π visits in a cumulative sum random walk, which is obtained from partial sums after the (0, 1) sequence is mapped to the two level (-1, +1) sequence. The purpose of this test is to find if the number of visits to a particular state within a cycle deviates from the expected result for a random sequence.

15. Random Excursions Variant Test

In a cumulative sum random walk the number of a particularly state visited is determined and its deviation from the expected number of visits to various states found in typical random sequence.

Upon validation of the randomness of the generator through all the statistical tests, the sequence would be considered it possesses good randomness properties suitable for cryptographic applications. The tested binary sequences are then referred to as

Peer Reviewed & Refereed Journal
Volume-14, Issue-2 (April 2024)
https://doi.org/10.5281/zenodo.11201784

cryptographically safe to be used as key and the corresponding generators are called Cryptographically Secure Pseudo Random Number Generator (CSPRNG).

The significance of the tests defined by the NIST for evaluating PRNGs lies in their role in assessing the quality and randomness properties of these generators.

A sample NIST results of G-SHA-1 binary sequence [28] is shown in Table (2).

Table 2: NIST results of G-SHA-1 binary sequence

Statistical Test	P-value	Status
Frequency	0.604458	Pass
Block Frequency (m = 128)	0.091517	Pass
Cusum-Forward	0.451231	Pass
Cusum-Reverse	0.550134	Pass
Runs	0.309757	Pass
Long Runs of Ones	0.657812	Pass
Rank	0.577829	Pass
Spectral DFT	0.163062	Pass
NonOverlapping Templates (m = 9, B = 000000001)	0.496601	Pass
Overlapping Templates (m = 9)	0.339426	Pass
Universal	0.411079	Pass
Approximate Entropy (m = 10)	0.982885	Pass
Random Excursions (x = +1)	0.000000	Pass
Random Excursions Variant (x = -1)	0.000000	Pass
Linear Complexity (M = 500)	0.309412	Pass
Serial (m = 16, 2 ∇Ψm)	0.760793	Pass

E. NIST Compliance Algorithms

Some of the NIST passed algorithms are briefly discussed here.

- A Pseudo Random Bit Generator (PRBG) based on chaotic Logistic map which uses two Logistic maps with two independent initial conditions which is Suitable for stream cipher design[29].
- A chaotic Logistic map based PRBG is designed using 3 chaotic Logistic maps suitable for stream cipher design is found in [30].In this case usage of multiple maps leads to complexity.
- Lorenz map based Pseudo Random Number Generator (PRNG) is obtained by combining Lorenz map with DCT permutation is suitable for Voice data encryption [31].
- A True Random Number Generator (TRNG) based on Galvanic skin response (GSR) which uses sensor to measure GSR signal which is suitable for stream cipher design as reported in [32].

These algorithms have shown the key generators proposed possess good randomness properties as required for the cryptographic applications.

IV. CONCLUSION

A brief survey on different encryption algorithms and chaos-based speech encryption algorithms is presented. Some of the important parameters such as confusion and diffusion properties of key, large key space, key sensitivity, good randomness properties of the key, a strong algorithm are the major contributions in achieving high level of security. The survey also summarized the cryptographic requirements for better design of a chaos-based cryptosystem for speech signal and Chaos based encryption algorithms. The study of various statistical tests for randomness testing of the binary sequences and the NIST compliance algorithms helps in understanding the various parameters needs to be taken care for designing a good hardware or software based random or pseudorandom generators for cryptographic applications.

REFERENCES

[1] Bruce Schneier. (1996). *Applied cryptography - Protocols, algorithms and source code in C*. (2nd ed.). New York: John Wiley and Sons.

[2] Alfred J Menezes, Paul C. Van Oorschot & Scott A. Vanstone. (1997). *Handbook of applied cryptography*. New York: CRC Press.

[3] FIPS PUB 46-3. (1999). *Federal information processing standards publication re affirmed*. U.S. Department of Commerce/National Institute of Standards and Technology.

[4] FIPS 197. (2001). *The advanced encryption standard (AES)*. Available at: http://csrc.nis"t.gov/publications/fips/fips197/fips-197.pdf.

[5] Xuejia Lai & James L. Massey. (1990). *A proposal for a new block encryption standard*. Springer-Verlag.

[6] Rivest R.L., Robshaw M.J.B., Sidney R. & Yin Y.L. (1998). The RC6 block cipher. Available at: http://people.csail.mit.edu/rivest/Rc6.pdf.

[7] Priyadarshini P, Prashant N, Narayan DG & Meena SM. (2016). A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science*, pp. 617-624. Available at: https://cyberleninka.org/article/n/593680.

[8] William Stallings. (2006). *"Cryptography and network security", principles and practice*. (5th ed.). Pearson Education Inc.

Peer Reviewed & Refereed Journal
Volume-14, Issue-2 (April 2024)
https://doi.org/10.5281/zenodo.11201784

[9] Rainer A. Rueppel. (1992). Stream ciphers in contemporary cryptology. *The Science of Information Integrity, IEEE Press, New York*.

[10] S Li, X Mou & Y Cai. (2001). Improving security of a chaotic encryption approach. *Physics Letters A 290*(3-4), 127-133.

[11] K. Chidananda murthy, Mahalinga V Mandi & R. Murali. (2018). Binary sequences in chaotic systems: A review. *IJAER*.

[12] Gonzalo Alvarez & Shujun Li. (2006). Some basic cryptographic requirements for chaos based cryptosystems. *International Journal of Bifurcation and Chaos, 16*(8), 2129-2151.

[13] Li Shujun, Mou Xuanqin & Cai Yuanlong. (2001). *Pseudo random bit generator based on couple chaotic systems and its applications in stream cipher cryptography, 2247, Springer-Verlag, Berlin* pp. 316-329.

[14] Ramesh S, K N Haribhat & R Murali. (2010). On linear complexity of binary sequences generated using matrix recurrence relation defined over Z_4. *IJDPS*.

[15] Shujun Li & Guanrong Chen , et.al. (2004). Baptista-type chaotic cryptosystems: Problems and countermeasures. *Physics Letters A, Elsevier Science, 332*(5-6), 368-375.

[16] Pushpalatha G S, Dr. Ramesh S & A Raganna (2019). Voice encryption with watermarking for secure speech communication. *JETIR*.

[17] Zhaopin Su, et.al. (2009). Selective encryption of G.729 speech using chaotic maps. *IEEE*.

[18] M. Ashtiyani, P. Moradi Birgani & S. S. Karimi Madahi. (2012). Speech signal encryption using chaotic symmetric cryptography. *Journal of Basic and Applied Scientific Research*.

[19] Saad Najim Al Saad & Eman Hato. (2014). A speech encryption based on chaotic maps. *International Journal of Computer Application.*

[20] Hemlata Kohad, Prof. V.R.Ingle & Dr.M.A.Gaikwad. (2012). Security level enhancement in speech encryption using kasami sequence. *IJERA*.

[21] Antonio servetti, et. Al. (2002). Perception based partial encryption of compressed speech. *IEEE, 10*(8).

[22] Qiu-Hua Lin, Fu-Liang Yin, Tie-Min Mei & Hualou Liang. (2006). Blind source separation based for speech encryption. *IEEE*.

[23] Mosa, Nagy.W. Messiha & O.Zahran. (2009). Chaotic encryption of speech signals in transform domains. *IEEE*.

[24] Mosa, Nagy.W. Messiha & O.Zahran. (2011). Chaotic encryption of speech signals. *Springer*.

[25] Long Jye Sheu. (2010). A speech encryption using fractional chaotic systems. *Springer*.

[26] Musheer Ahmad, Bashir Alam & Omar Farooq. (2012). Chaos based mixed keystream generation for voice data encryption. *IJCIS*.

[27] P. Sathiyamurthi & S. Ramakrishnan. (2020). Speech encryption algorithm using FFT and 3D-Lorenz–logistic chaotic map. *Multimedia Tools and Applications, 79*, 17817–17835.

[28] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray & San Vo. (2010). Statistical test suite for random and pseudo random number generators for cryptographic applications. *Special Publication 800-22 Revision 1a, NIST*.

[29] Vinod patidar, K K sud & N K Pareek. (2009). A PRBG based on chaotic Logistic map and its statistical testing. *Informatica*.

[30] Mickael Francois & David Defour. (2013). A pseudo random bit generator using three chaotic logistic maps. *LIRMM*.

[31] Sattar B Sadkhan & Rana Saad Mohammed. (2015). A proposed voice encryption based on Lorenz map with DCT permutation. *IJACT*.

[32] Carmen Camera, Honorio Martin, Pedro Peris-Lopez & Muawya Aldalaien. (2019). Design and analysis of a true random number generator based on GSR signals for body sensor networks. *Sensors*.