Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN: 2581 - 611X)

VOLUME:8, ISSUE:1, FEBRUARY 2025, PAPER NUMBER:78

Speech and audio encryption using multiple chaotic maps

Nithish kumar M
Dept of Electronics and Communication Engineering
Bannari Amman Institute of Technology
Sathyamangalam, India
nithishkumar.ec21@bitsathy.ac.in

Praveen kumar S
Dept of Electronics and Communication Engineering
Bannari Amman Institute of Technology
Sathyamangalam, India
praveenkumar.ec21@bitsathy.ac.in

Nityathanush T
Dept of Electronics and Communication Engineering
Bannari Amman Institute of Technology
Sathyamangalam, India
nityathanush.ec21@bitsathy.ac.in

Abstract

There are various ways of social communication including writing (WhatsApp, Messenger, Facebook, Twitter, Skype, etc), calling (mobile phone)and voice recording (record your voice and then send it to the other party), but there are ways to eavesdropping the calls and voice messages, One way to solve this problem is via cryptographic approach. Chaos cryptography build on top of nonlinear dynamics chaotic system has gained some footstep in data security. It provides an alternative to conventional cryptography built on top of mathematical structures. This research focuses on the protection of speech recording by encrypting it with multiple encryption algorithms, including chaotic maps (Logistic Map and Sine Maps).

Keywords — Speech encryption, Chaotic map, Fourier transform, Logistic map, Tent map

I. INTRODUCTION

The Information security can be regarded as the prevention of unauthorized access and the protection of valuable assets [1]. Various approaches derived from disciplines such as mathematics, computer science, and engineering have been introduced to enhance security. These mechanisms focus on protecting different layers, including network security (firewalls, intrusion prevention systems, intrusion detection systems) [2, 3], system security (biometrics, passwords) [4], and the security of the information itself through techniques such as steganography and cryptography [5-7]. Cryptography, particularly encryption algorithms, forms the cornerstone of secure communications [8]. The primary subjects of encryption typically include text, images, video, and speech.

Mathematically based encryption algorithms are generally classified into symmetric and asymmetric systems [6, 8]. Encrypting audio recordings, especially speech, is vital to preventing unauthorized access and protecting sensitive information from potential misuse. Numerous cryptographic algorithms have been developed for securing voice recordings. In this paper, we utilize multiple chaotic maps to encrypt audio and speech data. Chaotic maps, due to their inherent sensitivity to initial conditions and unpredictability, provide a robust framework for encryption.

However, several challenges arise when handling speech data, including environmental factors such as noise, delay, and data loss. Additionally, certain medical conditions, like Parkinson's Disease (PD), can impact speech quality. PD, a common neurodegenerative disorder, affects the central nervous system, leading to symptoms such as tremors and speech difficulties. When a sender records speech via a microphone or speaker using speech-to-text applications (e.g., Windows Speech Recognition or Android's Speech Texter), it becomes essential to encrypt the speech data before transmission to ensure confidentiality.

In this work, we employ multiple chaotic maps, including the Logistic Map and Tent Map, for encrypting and decrypting speech and audio data. These maps, known for their chaotic properties, enhance the security of the encryption process. The proposed system allows the sender to encrypt voice data before transmission and ensures that the recipient can securely decrypt the message. The structure of the speech encryption/decryption system is designed to handle real-world speech data, addressing common challenges such as noise and signal degradation while ensuring secure communication.

II. CHAOTIC MAPS

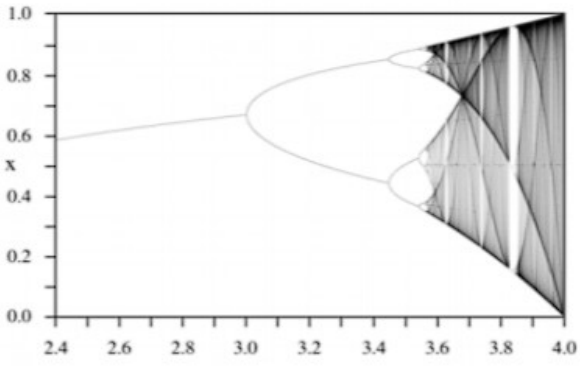
A chaotic-based cryptosystem is an encryption system characterized by nonlinear, deterministic, and dynamic chaotic functions [9-12]. These functions are highly sensitive to initial conditions and input values, making them ideal for encryption due to their unpredictability and complexity. In this paper, we utilize multiple chaotic maps, specifically the Logistic Map, Tent Map, and Henon Map, for encrypting speech and audio data. The sensitivity of these chaotic maps to initial conditions ensures that even minor changes in the input result in significantly different outputs, enhancing the security of the encryption process. The following sections provide a summarized overview of the three chaotic maps used in our approach: Logistic Map, Tent Map, and Henon Map.

A. Logistic map

The Logistic Map is a commonly used chaotic system that operates as a non-linear map, making it ideal for cryptographic applications. It is defined by the following conditions:

- Xn takes values from the interval [0,1]
- r is a control parameter, with r□[0,4]
- The initial value is x0=0.3

The system exhibits different behaviors depending on the value of r, known as the bifurcation parameter. As r approaches 4, the system becomes increasingly chaotic, which enhances the security of the encryption process. This sensitivity to initial conditions and control parameters makes the Logistic Map an effective component in the multiple chaotic maps used for speech and audio encryption in this paper.



B. Tent map

The Tent Map is a discrete chaotic system governed by a piecewise linear equation. The map is defined as:

- Xn □ [0,1], and
- A control parameter r □ [0,2].

The Tent Map exhibits chaotic behavior as r approaches 2. It is simple yet effective, offering strong encryption capabilities with relatively low computational complexity, making it suitable for secure speech and audio encryption.

C. Henon map

The Henon Map is another discrete chaotic system, described by the following equations:

- Xn+1=1−aXn2+Yn,
- Yn+1=bXn, where a and b are constants, typically set to a=1.4 and b=0.3, and Xn,Yn□R.

The Henon Map is more complex than the Tent Map, offering richer chaotic behavior and greater unpredictability, which enhances security. When the parameters are set appropriately, the Henon Map demonstrates high sensitivity to initial conditions, a characteristic that is crucial for secure encryption. These properties make both the Tent Map and Henon Map well-suited for use in chaotic encryption schemes.

III. LITERATURE REVIEW

This section describes various chaotic algorithms designed for voice and audio encryption. In [14, 15], an algorithm was developed for encrypting audio files using a shuffling procedure, where different shuffle bits were chosen, and substitutions were altered. The statistical analysis, based on PSNR (Peak Signal-to-Noise Ratio), indicated that the algorithm is resistant to statistical attacks, except when applied to low-quality audio files. Another study [16] introduced an encryption algorithm based on a chaotic map combined with the Blowfish algorithm, offering a fast and efficient encryption process that is difficult to break. In [17], a speech encryption algorithm was proposed using three-dimensional chaotic maps. The algorithm comprises

three primary components: key generation, sample substitution, and sample permutation. Substitution is performed in two steps with cipher feedback. The Lorenz and Rossler chaotic systems were employed for generating key streams used in the substitution and permutation processes, increasing the confusion and diffusion of speech samples. Research in [18] proposed a novel algorithm for speech encryption by dividing the speech signal into overlapping blocks and shuffling these blocks in the time domain. A second permutation was applied to the coefficients of each block, obtained via wavelet transforms, using a chaotic key generated from the Henon map. This approach, designed for real-time environments, provided strong encryption by partially encoding the shuffled speech signal within a transformed domain. In [19], a new algorithm for speech encryption was introduced, involving two steps. It utilized three chaotic maps—Henon, Logistic, and Ikeda—combined with noise and a bio-chaotic stream cipher to encrypt the speech signal for secure storage in databases. The encryption process employed a biometric key and bio-chaotic functions to enhance security. This algorithm proved to be fast, secure, and efficient. Another study [20] proposed a hybrid speech encryption algorithm combining DES-RSA and a genetic algorithm. The classification of audio files was performed using neural networks (NN) and support vector machines (SVM), with performance evaluated using MSE (Mean Square Error) and PSNR to validate the effectiveness of the proposed approach. The algorithm demonstrated a high level of security for speech cryptography, offering protection at multiple levels.

IV. PROPOSED SYSTEM

The proposed encryption system for speech and audio can be summarized as follows:

-- Input speech signal:

The audio or speech signal is fed into the encryption system.

-- First processing step:

-- Apply a Fast Fourier Transform (FFT) to convert the time-domain speech signal into its frequency components for better manipulation and transformation.

-- Second processing step:

-- Generate a chaotic sequence using the Logistic Map. This sequence acts as the key for initiating the encryption process.

-- Begin the confusion process by shuffling the speech signal using the chaotic sequence to obscure the original information.

-- Third processing step:

-- Generate a diffusion key using the Tent Map or Henon Map. This step ensures the spreading of small changes across the entire signal to maximize security.

-- Fourth processing step:

-- Perform an XOR operation between the output of the second step (confusion process) and the diffusion key from the third step. This step completes the encryption by combining the chaotic maps for both confusion and diffusion, ensuring robust encryption of the speech signal.

A. Input Speech Signal

The process begins with an audio or speech signal. This signal is typically captured through a microphone or other input devices, and it exists in the time domain as a series of discrete values. The signal is represented as a digital sequence of samples, where each sample corresponds to the amplitude of the sound wave at a given point in time.

B. Fast Fourier Transform[FFT]

The Fast Fourier Transform (FFT) is used to convert the time-domain audio signal into its frequency-domain representation. This step is important for breaking down complex audio signals into their constituent frequencies, which can then be manipulated more effectively.

C. Confusion with Logistic Map

```
import numpy as np

def logistic_map(x, r, n):
    seq = np.zeros(n)
    seq[0] = x
    for i in range(1, n):
        seq[i] = r * seq[i-1] * (1 - seq[i-1])
```

```
    return seq
```

D. Diffusion using Henon Map

```
def henon_map(x0, y0, a, b, n):
    x = np.zeros(n)
    y = np.zeros(n)
    x[0] = x0
    y[0] = y0
    for i in range(1, n):
        x[i] = 1 - a * (x[i-1] ** 2) + y[i-1]
        y[i] = b * x[i-1]
    return x
```

EXPERIMENTAL SETUP

1. Tools and Environment

The encryption and decryption of speech signals using multiple chaotic maps were carried out using the following tools and programming environment:

Programming Language: Python 3.10

Python was chosen for its extensive scientific libraries, ease of use, and robust handling of mathematical functions. The chaotic maps and encryption algorithms were implemented using the following libraries:

-- Numpy: Used for generating chaotic sequences and performing matrix operations.

-- Scipy: Utilized for signal processing, especially Fourier transforms, and to handle speech signals.

-- Matplotlib: For plotting graphs and visualizing the results.

Soundfile (or wave): For handling audio files during reading and writing of speech signals.

Hardware Setup:

CPU: Intel Core i7 processor with 8 cores at 2.8 GHz.

RAM: 16 GB of memory.

Operating System: Windows 10 64-bit.

Software Libraries:

Librosa: For handling and manipulating audio files (specifically speech files), providing functions to load, play, and visualize audio signals.

Soundfile or Wave: Used to read and write .wav files.

2. Datasets

The experiments were carried out on multiple datasets of speech signals. The speech signals were obtained from publicly available datasets as well as custom-recorded audio files.

Speech Dataset:

LJ Speech Dataset: A publicly available speech dataset with clean speech audio recordings, mostly used for text-to-speech systems. The dataset was chosen for its diversity of voice recordings and audio formats.

Custom Speech Samples: Several custom speech samples were recorded in .wav format to test the algorithm under different conditions, including noisy and clean environments.

Audio Format:

The audio files used in the experiments were 16-bit PCM .wav files with sampling rates ranging from 16 kHz to 44.1 kHz, and different durations (between 5 and 20 seconds).

3. Encryption and Decryption Process

The encryption and decryption processes were implemented using Python. The encryption involves converting the speech signal into the frequency domain using Fast Fourier Transform (FFT), applying chaotic maps for confusion and diffusion, and XOR operations for encryption.

Steps in the Process:

Input Speech Signal: The speech signal was read from a .wav file and preprocessed using Fast Fourier Transform (FFT) to convert it into the frequency domain.

Chaotic Map for Confusion: A chaotic sequence was generated using the Logistic Map, with an initial condition (x_0) and a control parameter (r). This sequence was used to shuffle the frequency components of the speech signal.

Chaotic Map for Diffusion: Another chaotic sequence was generated using either the Tent Map or Henon Map. This diffusion sequence was applied after confusion to further randomize the signal.

XOR Operations for Encryption: An XOR operation was applied between the speech signal and the confusion and diffusion sequences to complete the encryption process.

Decryption Process: The reverse XOR operations were applied in the decryption phase, followed by the inverse FFT to recover the original speech signal.

Implementation Workflow:

Encryption:

The encryption process starts with converting the speech signal into the frequency domain using FFT.

Chaotic sequences are generated using Logistic, Tent, and Henon maps.

XOR operations are applied between the chaotic sequences and the speech signal.

Decryption:

The decryption process reverses the XOR operations, regenerates the same chaotic sequences, and applies the inverse FFT to retrieve the original signal.

4. Challenges and Constraints

Noise: Some speech samples were recorded in noisy environments, leading to challenges during decryption, where small errors introduced distortions.

Real-Time Processing: Ensuring real-time encryption and decryption required optimizing the algorithm for performance.

Chaotic Map Parameters: The initial conditions and control parameters of chaotic maps required careful selection to ensure both security and the correct decryption.

5. Evaluation Metrics

Encryption/Decryption Time: The time taken to encrypt and decrypt the speech signals was measured to evaluate performance.

Security Analysis: Entropy and key sensitivity analysis were performed to assess the robustness of the encryption algorithm.

Signal-to-Noise Ratio (SNR): The SNR of the decrypted speech signals was calculated to evaluate the quality of the decrypted signal.

Perceptual Quality: Subjective listening tests were performed to assess the intelligibility and perceptual quality of the decrypted audio.

REFERENCES

[1]H. H. Carr, C. A. Snyder, "Data Communications & Network Security," McGraw-Hill,2006.

[2]A. Shamim, et al., "Layered Defense in Depth Model for IT Organizations," 2nd International Conference on Innovations in Engineering and Technology (ICCET'2014), pp. 21-24.

[3]S. Juma, Z. Muda, M. A. Mohamed, W. Yassin, "Machine Learning Techniques for Intrusion Detection System: A Review,"Journal of Theoretical & Applied Information Technology,vol. 72, no. 3, pp. 422-429, 2015.

[4]N. A. Mahadi, M. A. Mohamed, A. I. Mohamad,M. Makhtar, M. F. A. Kadir, M. Mamat, "A survey of machine learning techniques for behavioral-based biometric user authentication," Recent Advances in Cryptography and Network Security, IntechOpen,2018.

[5]S. Pund-Dange, "Steganography: A Survey," In: Bokhari M., Agrawal N., Saini D. (eds) Cyber Security. Advances in Intelligent Systems and Computing,2018.

[6]O. G. Abood, S. K. Guirguis, "A Survey on Cryptography Algorithms," International Journal of Scientific and Research Publications,vol. 8, no. 7, pp. 495-516, 2018.

[7]M. A. Mohamed, "A Survey on Elliptic Curve Cryptography," Applied Mathematical Sciences,vol. 8, no. 154, pp. 7665-7691, 2014.

[8]R. Sivakumar, B. Balakumar, and V. A. Pandeeswaran, "A Study of Encryption Algorithms (DES, 3DES and AES) for Information Security,"International Research Journal of Engineering and Technology,vol. 5, no. 4, pp. 4133-4137, 2013.

[9]S. Vaidyanathan, et al., "A new chaotic jerk system with three nonlinearities and synchronization via adaptive backstepping control,"International Journal of Engineering & Technology,vol. 7, no. 3, pp. 1936-1943, 2018

[10]Aceng Sambas, et al., "A new hyperchaotic hyperjerk system with three nonlinear terms, its synchronization and circuit simulation,"International Journal of Engineering & Technology,vol. 7, no. 3, pp. 1585-1592, 2018.

[11]E. Hato, "Lorenz and Rossler Chaotic System for Speech Signal Encryption," International Journal of Computer Applications,vol. 128, no. 11, pp. 25-33, 2015.

[12]W. Sayed, A. G. Radwan, and H. A. H. Fahmy, "Design of a Generalized Bidirectional Tent Map Suitable for Encryption Applications," 11th International Computer Engineering Conference (ICENCO),pp. 207-211, 2015.[13]Y. Liu, L. Chen, "A Survey of Chaos Theory," Chaos in Attitude Dynamics of Spacecraft, 2013.

[14]A. A. Tamimi, A. M. Abdalla, "An Audio Shuffle-Encryption Algorithm," Proceedings of the World Congress on Engineeringand Computer Science,WCECS 2014, vol. 1,San Francisco, USA,22-24 October, 2014.

[15]M. Farouk, O. Faragallah, O. Elshakankiry, A. Elmhalaway, "Comparison of Audio Speech Cryptosystem Using2-D Chaotic Map Algorithms," Mathematics and Computer Science,vol. 1, no. 4, pp. 66–81, 2016.

[16]M A. Nasser, I. Q. Abduljaleel, "Speech Encryption UsingChaotic Map and Blowfish Algorithms," Journal of Basrah Researches (Sciences),vol. 39, no. 2, pp. 68–76, 2013.

[17]S. Vishwakarma, S. Qureshi, "Secure Transmission of Video using (2, 2) Visual Cryptography Scheme and Share Encryption using Logistic Chaos Method," International Journal of Scientific Research in Computer Science, Engineering and Information Technology,vol. 3, no. 1, pp. 1502–1514, 2018.

[18]H. Oğraş, M. Türk, "A Secure Chaos-based Image Cryptosystem with an Improved Sine Key Generator," American Journal of Signal Processing,vol. 6, no. 3, pp. 67–76, 2016.

[19]A. Belazi. A. A. A. El-latif, "A simple yet efficient S-box method based chaotic sine map," Opt. -Int. J. Light Electron Opt.,vol. 130, pp. 1438-1444, 2016.

[20]Y. Alemami, L. Almazaydeh, "Pathological Voice Signal Analysis Using Machine Learning Based Approaches," Computer and Information Science, vol. 11, no. 1, pp. 8–13, 2018.

[21]Y. Saleem, M. Amjad, M. H. Rahman, F. Hayat, T. Izhar, M. Saleem, "Speech Encryption Implementation of 'One Time Pad Algorithm' In Matlab," Pakistan Journal of Science,vol. 65, no. 1, pp. 114-118, 2013.

[22]P. Sun, N. AlJeri and A. Boukerche, "A Fast Vehicular Traffic Flow Prediction Scheme Based on Fourier and Wavelet Analysis," IEEE Global Communications Conference (GLOBECOM),pp. 1-6, 2018.

[23]F. Mansouri et al.,"A Fast EEG Forecasting Algorithm for Phase-Locked Transcranial ElectricalStimulation ofthe Human Brain," Frontiers in neuroscience,vol. 11, 2017.

[24]R. Lafta, et al. “A Fast Fourier Transform-Coupled Machine Learning-Based Ensemble Model for Disease Risk Prediction Using a Real-Life Dataset,” In: Kim J., Shim K., Cao L., Lee JG., Lin X., Moon YS. (eds) Advances in Knowledge Discovery and Data Mining. PAKDD 2017. Lecture Notes in Computer Science,vol. 10234. 2017.

[25]P. Sathiyamurthi, S. Ramakrishnan, “Speech encryption using chaotic shift keying for secured speech communication,” J.Audio Speech Music Proc.,2017