Symmetry-Based Chaotic Communication System

Ananya Nawale* and Simran Sinha†
Department of Physics
Indian Institute of Technology Bombay

In the realm of modern communication systems, the pursuit of heightened security and efficient data transmission techniques is unceasing. One area that has garnered significant attention is Chaos-based communications, which draw upon the intricate principles of chaos theory and nonlinear dynamics. These systems offer a tantalizing promise of concealed transmission, robust security, and the ability to harness native broadband signals for data exchange. While the theoretical groundwork for Chaos-based communications is well-established, its practical implementation faces challenges, such as demanding hardware, complex signal processing algorithms, and a dearth of efficient chaotic signal modulation techniques. Our primary objective is to explicitly showcase the viability of covert data transmission using a chaotic transmitter and receiver, both seamlessly integrated within a general-purpose microcontroller unit.

I. INTRODUCTION

One of the great achievements of the chaos theory is the application in secure communications. Chaotic signals depend very sensitively on initial conditions, have unpredictable features and noise like wideband spread spectrum. So, it can be used in various communication applications because of their features of masking and immunizing information against noise. The chaos communication fundamentally depends on the synchronization of two chaotic systems under suitable conditions if one of the systems is driven by the other.

Literature supports the possibility of practical communication using chaotic signals. In particular, the understanding of nonlinear circuits have shown that chaotic oscillators can synchronize. This surprising observation appears to contradict the very essence of chaos: complex, unpredictable dynamics of a deterministic system characterized most commonly as extreme sensitivity to initial conditions. However, if certain requirements are met, then a chaotic circuit (called the driving system) can be designed to drive a similar system (the receiving circuit or subsystem) and obtain a correlated response.

As reported in the literature [1], [2], synchronization of chaotic systems suggests the possibility for communication using chaotic waveforms as carriers, perhaps with application to secure communication. The obvious approach uses a chaotic oscillator as the transmitter and a synchronous chaotic system for the receiver, and several designs have been suggested that fit within this construct. One approach employed to achieve secure communications uses a chaotic signal to mask the sensitive information signal. In this approach, a synchronous chaotic system is used in the receiver to identify the chaotic part of the signal, which then is subtracted to reveal the information signal.

In this work we use a simple electronic system to develop a scheme for chaos secure communication with two coupled Chua circuits. First, we analyze separately each oscillator to study their dynamic behavior when a parameter of control is changed, and then we investigate the synchronization effect in the coupled circuits. Bifurcations of the output voltage are constructed using a resistance as a control parameter. While using two channels, we may send an information signal via one of the channels and recover the signal via another channel. We will show that this scheme can improve synchronization in a system with coexisting attractors. Finally secure communications with chaos is demonstrated experimentally using the novel communication scheme.

II. GENERAL THEORY

A. Chaos and Synchronisation

Chaos refers to the behavior exhibited by specific deterministic physical systems, arising from the extreme sensitivity of the system's dynamic evolution to minute changes in the initial conditions, commonly referred to by SDIC (Sensitive Dependence to Initial Conditions).

Classical chaotic motion is characterized by the existence of positive Lyapunov exponents or positive Kolmogoroff-Sinai entropy. The definition of these quantities is based on the properties of classical trajectories in phase space. They indicate that trajectories will diverge exponentially as the system evolves. This divergence implies that the path of any given point in phase space cannot be replicated by retracing through the future states of the system.

Synchronization on the other hand encapsulates the concept of strong correlations existing between coupled systems. At its most fundamental and intuitive core, synchronization denotes the inclination for coupled systems

* 21d170004@iitb.ac.in
† 210260051@iitb.ac.in

to exhibit identical or near identical dynamic behaviors.

Interaction between similar self-excited oscillators can result in mutual synchronization. One of the classical problems of nonlinear dynamics theory is how this synchronization is affected by how the oscillators are coupled. Usually, understanding this phenomenon is done by modelling the partial differential equations.

1. The Chua Circuit

The Chua circuit, a straightforward and simple nonlinear electronic circuit design, possesses the capacity to display typical chaos theory behavior. These circuits can be effectively and accurately modeled mathematically, earning them recognition as a "paradigm of chaotic systems". Even a single Chua's circuit exhibits complicated bifurcations. Hence, we have opted to employ synchronous control of Chua circuits for the project.

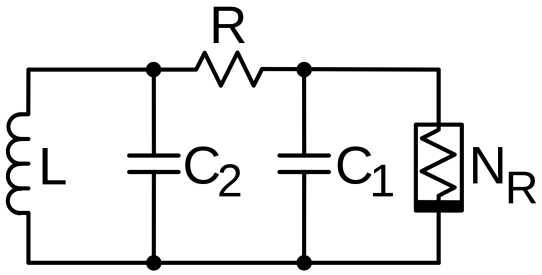


Fig1: The Chua's circuit. The component N_R, called a Chua's diode, which is a nonlinear negative resistance.

$$C_1 \frac{dV_{C_1}}{dt} = \frac{V_{C_2} - V_{C_1}}{R} - f(V_{C_1})$$

$$C_2 \frac{dV_{C_2}}{dt} = \frac{V_{C_1} - V_{C_2}}{R} + i_L$$

$$L \frac{di_L}{dt} = -V_{C2}$$

Here, i_L represents the inductor current, V_{C_1} and V_{C_2} denote the voltages across capacitors C_1 and C_2 respectively. The equations describe the circuit dynamics, where $\frac{dV_{C_1}}{dt}$ and $\frac{dV_{C_2}}{dt}$ represent the rates of change of V_{C_1} and V_{C_2} with respect to time. Additionally, L is the inductance, and $\frac{di_L}{dt}$ represents the rate of change of inductor current.

And the characteristic function $f(V_C)$ is defined as:

$$f(V_C) = G_a V_C + 0.5(G_a - G_b)(|V_C + E| - |V_C - E|)$$

Here, G_a, G_b, and E are as defined in the figure.

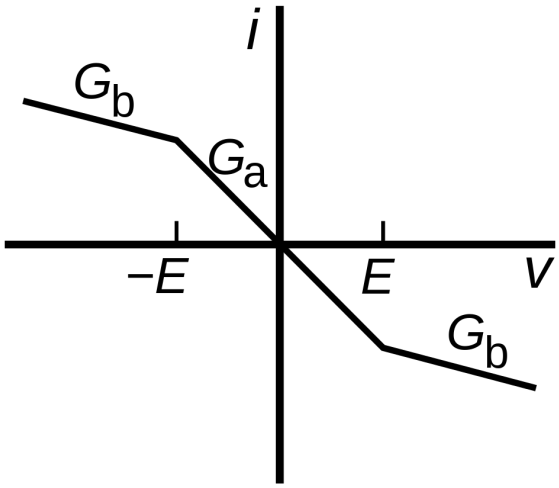


Fig2: The current–voltage characteristic of the Chua diode N_R

2. Attractors and The Double Scroll

Eric Weisstein [3] defines attractors as a set of states represented by points in the phase space, invariant under the dynamics, towards which neighboring states in a given basin of attraction asymptotically approach in the course of dynamic evolution.

Strange attractors distinguish themselves from other phase-space attractors by virtue of the uncertainty regarding the precise location of the system on the attractor. The system's trajectory on the attractor exhibits a notable characteristic: two points that are in close proximity at a given moment can become arbitrarily distant at subsequent times. The sole constraint is that the system's state must persist on the attractor. Furthermore, strange attractors possess a distinctive quality in that they never exhibit self-closure—the system's motion never repeats, indicating a non-periodic behavior. The erratic motion observed on these strange attractors encapsulates what is defined as chaotic behavior.

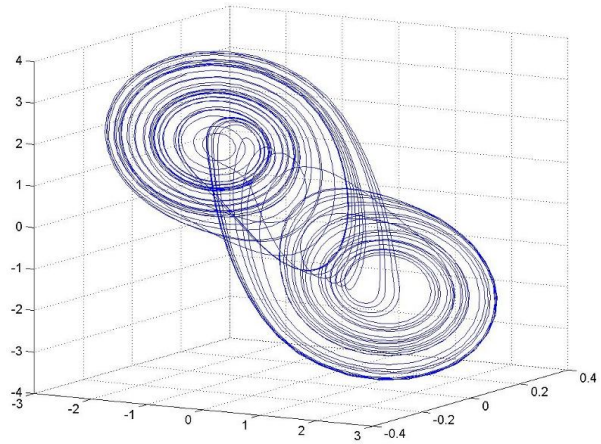


Fig3: The Double Scroll Attractor

A common example of a strange attractor is the Double-scroll attractor, recognized as a foundational element in contemporary chaos theory. This attractor, occasionally referred to as Chua's attractor, manifests as a peculiar trajectory in the phase space and is commonly observed in the dynamics of physical electronic chaotic circuits, notably Chua's circuit.

Within the scope of the project, Chua's circuit functions as the mechanism instigating chaos, and at its core lies the Double-scroll attractor, playing a central role in shaping the chaotic dynamics.

3. Synchronization of the Chua Circuit

Synchronization of chaotic oscillators constitutes a fundamental phenomenon within nonlinear dynamics, encompassing various types that have been both theoretically described and experimentally observed. These include complete synchronization (CS), lag synchronization (LS), generalized synchronization (GS), and phase synchronization (PS).

Complete synchronization (CS) entails the coinciding states of coupled oscillators, expressed as $x_1(t) \approx x_2(t)$. In this scenario, the disparity between the state vectors of the coupled systems converges to zero as $t \to \infty$. CS manifests when interacting systems are identical. If there is a slight mismatch in the parameters of coupled chaotic oscillators, the state vectors remain close ($|x_1(t) - x_2(t)| \approx 0$) but deviate from perfect coincidence.

A pair of resistively coupled Chua's circuits, which are identical in nature, can manifest the phenomenon of multi-stability. This term refers to the simultaneous coexistence of multiple distinct periodic and chaotic attractors within phase space [4]. Although there are several proposed methods of coupling two Chua circuits, such as using inductors or memristor, complete synchronization can only be obtained in the resistor coupling scheme and thus that is what we have employed.

B. Cryptography

Cryptography provides for secure communication in the presence of malicious third-parties—known as adversaries. Encryption uses an algorithm and a key to transform an input (i.e., plaintext) into an encrypted output (i.e., ciphertext). A given algorithm will always transform the same plaintext into the same ciphertext if the same key is used. Algorithms are considered secure if an attacker cannot determine any properties of the plaintext or key, given the ciphertext. An attacker should not be able to determine anything about a key given a large number of plaintext/ciphertext combinations which used the key.

1. Symmetric and Asymmetric Cryptography

With symmetric cryptography, the same key is used for both encryption and decryption. A sender and a recipient must already have a shared key that is known to both. Key distribution is a tricky problem and was the impetus for developing asymmetric cryptography.

With asymmetric crypto, two different keys are used for encryption and decryption. Every user in an asymmetric cryptosystem has both a public key and a private key. The private key is kept secret at all times, but the public key may be freely distributed.

Data encrypted with a public key may only be decrypted with the corresponding private key. So, sending a message to John requires encrypting that message with John's public key. Only John can decrypt the message, as only John has his private key. Any data encrypted with a private key can only be decrypted with the corresponding public key. Similarly, Jane could digitally sign a message with her private key, and anyone with Jane's public key could decrypt the signed message and verify that it was in fact Jane who sent it.

Symmetric is generally very fast and ideal for encrypting large amounts of data (e.g., an entire disk partition or database). Asymmetric is much slower and can only encrypt pieces of data that are smaller than the key size (typically 2048 bits or smaller). Thus, asymmetric crypto is generally used to encrypt symmetric encryption keys which are then used to encrypt much larger blocks of data. For digital signatures, asymmetric crypto is generally used to encrypt the hashes of messages rather than entire messages.

A cryptosystem provides for managing cryptographic keys including generation, exchange, storage, use, revocation, and replacement of the keys.

2. Problems solved by Cryptography

A secure system should provide several assurances such as confidentiality, integrity, and availability of data as well as authenticity and non-repudiation. When used correctly, crypto helps to provide these assurances. Cryptography can ensure the confidentiality and integrity of both data in transit as well as data at rest. It can also authenticate senders and recipients to one another and protect against repudiation.

Software systems often have multiple endpoints, typically multiple clients, and one or more back-end servers. These client/server communications take place over networks that cannot be trusted. Communication occurs over open, public networks such as the Internet, or private networks which may be compromised by external attackers or malicious insiders.

It can protect communications that traverse untrusted networks. There are two main types of attacks that an adversary may attempt to carry out on a network. Passive attacks involve an attacker simply listening on a net-

work segment and attempting to read sensitive information as it travels. Passive attacks may be online (in which an attacker reads traffic in real-time) or offline (in which an attacker simply captures traffic in real-time and views it later—perhaps after spending some time decrypting it). Active attacks involve an attacker impersonating a client or server, intercepting communications in transit, and viewing and/or modifying the contents before passing them on to their intended destination (or dropping them entirely).

The confidentiality and integrity protections offered by cryptographic protocols such as SSL/TLS can protect communications from malicious eavesdropping and tampering. Authenticity protections provide assurance that users are actually communicating with the systems as intended. For example, are you sending your online banking password to your bank or someone else?

It can also be used to protect data at rest. Data on a removable disk or in a database can be encrypted to prevent disclosure of sensitive data should the physical media be lost or stolen. In addition, it can also provide integrity protection of data at rest to detect malicious tampering.

III. METHODS

The fundamental concept here involves incorporating the message or information signal, denoted as $i(t)$ or $m(t)$, into a chaotic signal, represented by $x(t)$, resulting in the creation of a new signal, $s(t) = i(t) + x(t)$. The underlying assumption is that the amplitude of $x(t)$ significantly surpasses that of $i(t)$. This technique is termed "masking information". Given that chaotic signals exhibit noise-like characteristics and span a broad range of frequencies, deciphering the embedded message becomes challenging. The retrieval of the message relies on synchronization.

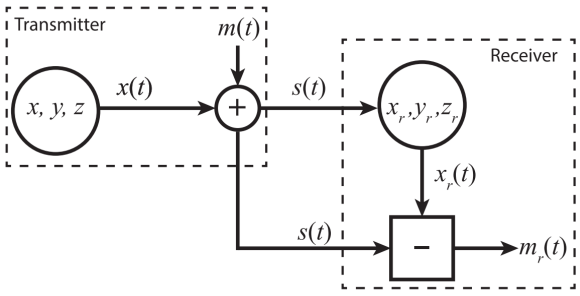


Fig4: Illustration of message masking scheme is depticted. The transmitter generates a chaotic signal $x(t)$ and adds the message $m(t)$ to it, resulting in the combined signal $s(t) = x(t) + m(t)$. This composite signal is sent to the receiver, where both systems synchronize. By discarding the synchronized signal x_r from s, the restored message $m_r \sim m$ is obtained.

The crucial aspect lies in carefully selecting transmitter and receiver systems to achieve synchronization. Additionally, both systems are presumed to be identical, implying that the receiver possesses knowledge of the transmitter's parameters. The retrieval of the message becomes feasible when these parameters are known, with the parameters essentially serving as an encryption key.

In our implementation, we use the "Chaotic Masking approach", where the transmitter contains a chaotic oscillator, that is the Chua circuit, that modulates an information signal. The receiver consists of a synchronous identical Chua circuit for recovering the information signal.

A. Privacy Considerations in Chaotic Communication

The matter of privacy naturally emerges in discussions about chaotic communication and serves as a significant driver for research in this field. Claude Shannon, in his seminal paper "Communication Theory of Secrecy Systems", delineated three crucial aspects of secret communication systems: concealment, privacy, and encryption. These aspects are applicable to systems employing chaotic waveforms for communication and can be understood within that context.

Concealment in chaotic communication arises from the irregular and aperiodic nature of the chaotic carrier or masking waveform. This characteristic makes it nonobvious to an eavesdropper that an encoded message is being transmitted. Privacy in chaotic communication systems stems from the requirement that an eavesdropper must possess the correct hardware and parameter settings to decode and recover the message. In traditional encryption methods, a key is employed to modify the symbols conveying information, and both the transmitter and receiver share this key for information recovery. In a chaotic communication system, a transmitter generating a time-evolving chaotic waveform serves as a "dynamical key" to transform information symbols. Recovery of information necessitates a receiver with an identical dynamical key, where its configuration and parameter settings match those of the transmitter.

It's worth noting that the use of a chaotic carrier for dynamic encoding doesn't exclude the possibility of employing traditional digital encryption schemes. Dynamical encoding with a chaotic waveform can thus be viewed as an additional layer of encryption.

B. Chaotic Communication System Architecture

The choice of hardware often determines the key properties of the designed system. We implemented the testbench for a one-way chaotic master/slave type communication system using two 8-bit microcontroller units, namely Arduino UNO. In the proposed architecture, the transmitting controller generates the chaotic signal using the master system and sends the signal into the com-

munication channel. The receiver controller acquires a signal from the communication channel, synchronizing it with the chaos generator based on a slave discrete system. To transmit and receive a chaotic signal, we used built-in digital-to-analog and analog-to-digital converter modules. In addition, the I^2C bus was used for communicating the controllers with each other. This allowed us to change the generation parameters in two controllers simultaneously during the experiments. A digital display was added to indicate the current parameter values, and a keyboard was added for input purposes. The toggle control allows for switching the experimental set between the modes of changing parameters and generating a signal. One of the important parts of the research was the investigation of how the noise in the channel affects chaotic communication systems with various types of modulation. We implemented the mixing of white noise to the channel as a simple sum of signals generated by the transmitter and the special noise generator. A summing operation was implemented using a circuit based on two inverting analog adders. One should note that the circuit power is bipolar and equals ±9 V. By changing the noise level in the noise generator, one can achieve the desired signal-to-noise (SNR) level in the communication channel to investigate the considered modulation types under different noise conditions.

1. *Hardwares Used*

- **Arduino UNO:** Arduino UNO, built around the ATmega328P microcontroller, features 14 digital input/output pins (6 usable as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, USB connection, power jack, ICSP header, and a reset button. This is the cornerstone of our transmitter and reciever system.

- **Keypad:** A 4×4 matrix keyboard serves as the input interface for the transmission signal.

- **16×2 LCD display:** Two 16×2 LCD displays were employed to visually present both the transmitted and received messages, serving as output interfaces on both the transmitter and receiver ends.

- I^2C **LCD:** I^2C, or Inter-Integrated Communication, is a serial interface facilitating interaction between devices using a multi-master/multi-slave approach. Utilizing two lines, SCL and SDA, for transmission and reception, I^2C devices are uniquely identified through individual addresses. In the case of I^2C LCD, this communication interface streamlines data transfer, necessitating only two lines (SDA and SCL), thereby reducing circuit complexity.

- **TL082 IC:** The amplifiers are versatile, applicable in various contexts like high-speed integrators, fast D/A converters, and circuits requiring low input offset voltage, bias current, high impedance, slew rate, and wide bandwidth. They also exhibit low noise and offset voltage drift. TL082 operational amplifiers serve as the central components in the circuit's non-linear part.

C. Hardware Implementation of Chua Circuit

It is crucial to approach the construction of the Chua circuit with careful consideration, as its chaotic nature renders it highly sensitive to minute variations that can lead to significant effects or even failure of the entire circuit. Factors such as loose connections or uneven voltages can have a profound impact on the circuit's output.

The construction of Chua's circuit on a breadboard demands careful attention, and even a slight disturbance can result in loose connections, leading to unpredictable changes in the circuit's output. Additionally, it is important to note that the output quality from a breadboard is generally inferior to that of a soldered circuit board.

An essential component of Chua's circuit, the Chua's diode, must be constructed, as it is not commercially manufactured. Various methods exist for creating a Chua's diode, essentially a form of nonlinear resistor.

Furthermore, the inductor in Chua's circuit can be effectively replaced and simulated with an additional circuit known as a gyrator, composed of basic components. For a comprehensive understanding of how this is achieved, refer to [5].

Utilizing this inductor simulator allows the construction of a fully realized circuit using only resistors, capacitors, and op-amps. These standard circuit components are typically found in most laboratories making this circuit easily reproducible.

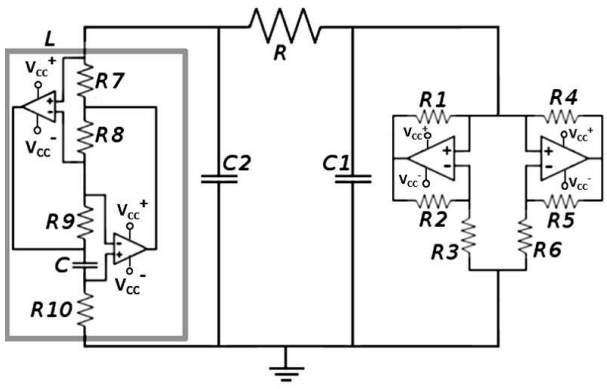


Fig5: A fully realised Chua Circuit composed of capacitors, Op-amps, and Resistors.

The values of the components are as follows:
$R_1, R_2 = 220\Omega$
$R_3 = 2.2k\Omega$
$R_4, R_5 = 22k\Omega$
$R_6 = 3.3k\Omega$

$R_7 = 100\Omega$

$R_8, R_9 = 10k\Omega$

$C = 100nF$

$C_1 = 10nF$

$C_2 = 100nF$

R and R_{10} are adjustable through a potentiometer.

In the examination of Chua's circuit, three critical signals necessitate measurement: X, Y, and Z. Specifically, X denotes the voltage across capacitor C_1, Y represents the voltage across capacitor C_2, and Z signifies the current flowing through the inductor. These measurements ($X(t)$, $Y(t)$, $Z(t)$) provide us a comprehensive understanding of the circuit's behavior and dynamics over time t.

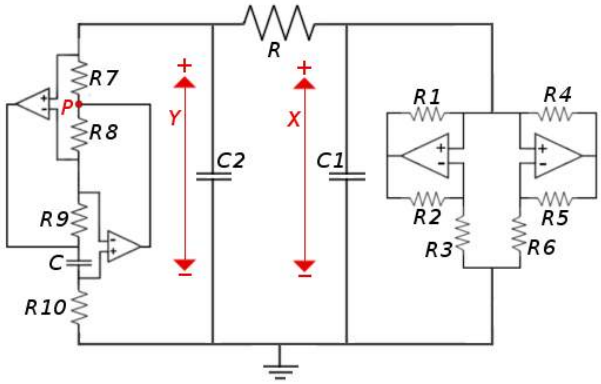


Fig6: Labeled signals in the realized chua circuit

L in Fig.(5) represents the inductance value of the gyrator, which we are using in place of an actual inductor. Calculating this value can be done as follows: $L = (R_7 R_9 R_{10} C)/R_8$. This gyrator simulates an ideal inductor. Since we are using a gyrator to simulate the inductor, all we need to do is measure the voltage at point P [Fig. (6)], since we can determine the state vectors from just that. The actual current through our simulated inductor can be calculated by: $Z = (V_P - Y)/R_7$. That gives some sinusoidal waveforms like in Fig.(20), (21), (22) when hooked up to the oscilloscope.

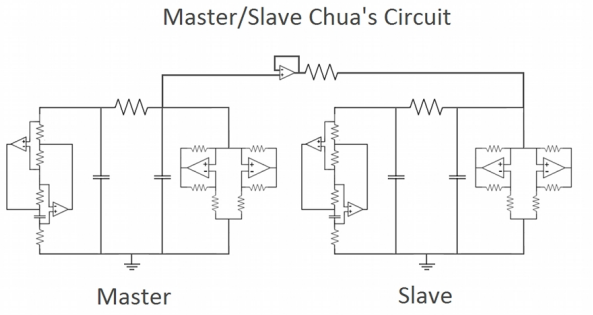


Fig7: Master/Slave coupling

IV. EXPERIMENTAL IMPLEMENTATION

A. Chua Circuit

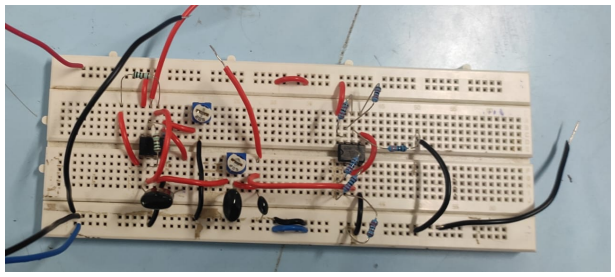
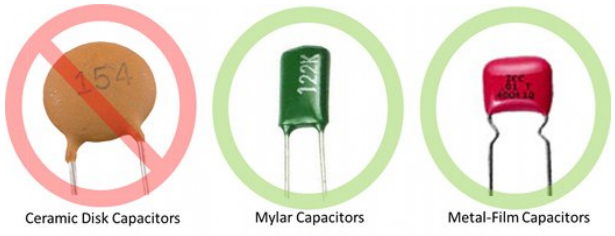


Fig8: Chua's Circuit

The figure showcases physical realization of the Chua circuit. A notable drawback of the setup is the inability to choose initial conditions manually. The initialization occurs upon turning on the voltage supply for the operational amplifiers. However, this becomes inconsequential when synchronization is employed.



The common, round, ceramic capacitors are avoided, instead mylar or metal-film capacitors is preferred. They work much better and will make the output much sharper.

B. Circuit for Chaotic Communication System

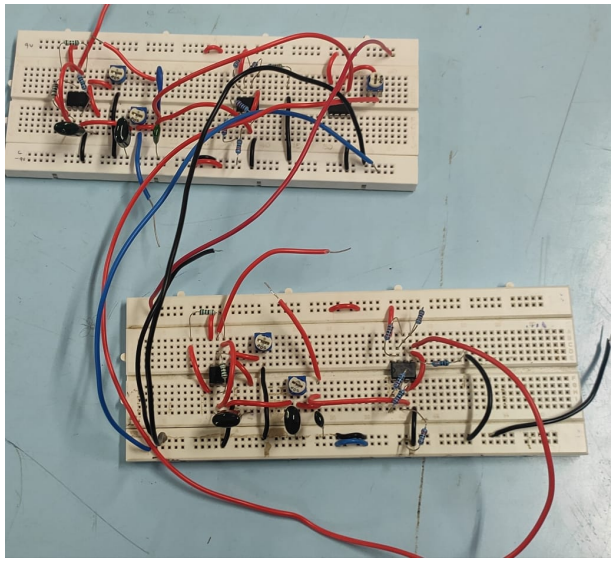


Fig9: Experimental realization of the Master/Slave (Unidirectional) synchronization of Chua's Circuit.

To achieve fundamental synchronization between two circuits, an intermediate coupling circuit, is necessary. In the Master/Slave approach, the singular Master Chua operates independently, unaffected by the Slave circuit or coupling mechanism. The Slave Chua circuits synchronize with the Master's signal using the coupling circuitry, while the Master Chua remains impervious to their influence.

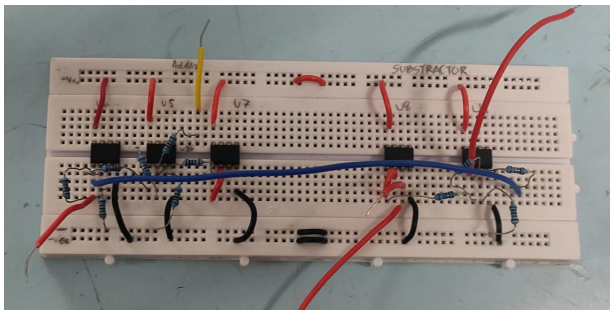


Fig10: Experimental realization of the Adder and Substractor circuits

The adder and subtractor circuits employ TL072 Op amps, with the adder integrated into the transmitter system and the subtractor part of the receiver system.

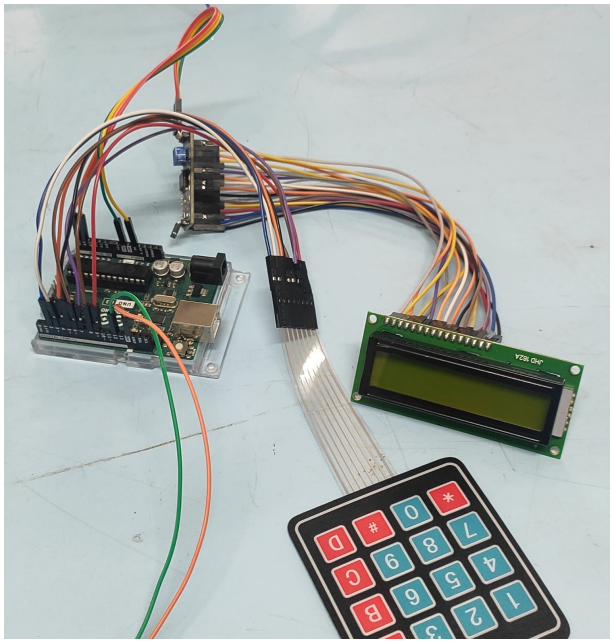


Fig11: Transmitter Circuit

The transmitter circuit integrates key components: a 4×4 keypad for user input, a 16×2 I^2C LCD screen for visual feedback, the master Chua circuit, and an Arduino Uno forming a cohesive system.

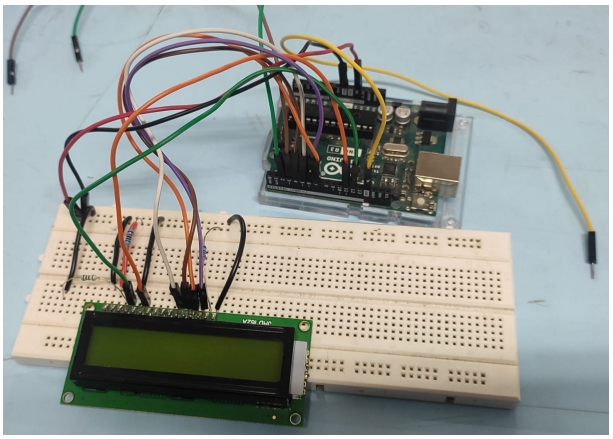


Fig12: Receiver Circuit

The receiver system replicates the transmitter setup, incorporating a 16×2 LCD screen, the slave Chua circuit, and an Arduino Uno. Distinct codes have been uploaded into the Arduino here, distinguishing the receiver's role in signal reception.

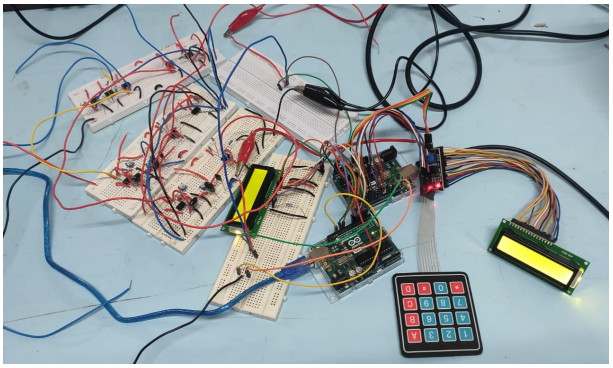


Fig13: Chaotic Communication System test bench

V. RESULTS

A. Chua circuit on Oscilloscope

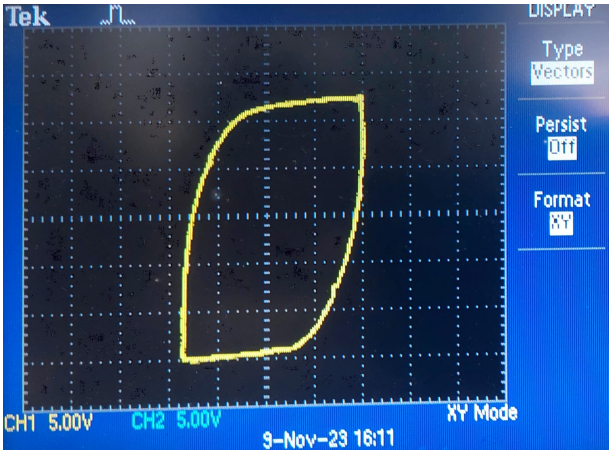


Fig14(a): Plot before tuning of chua circuit

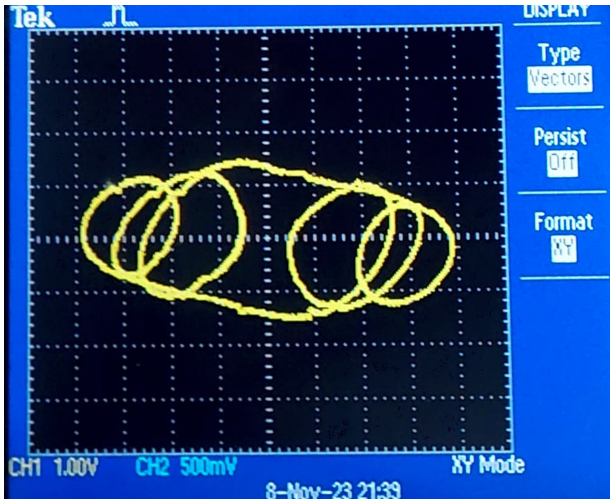


Fig14(b): Plot before tuning of chua circuit

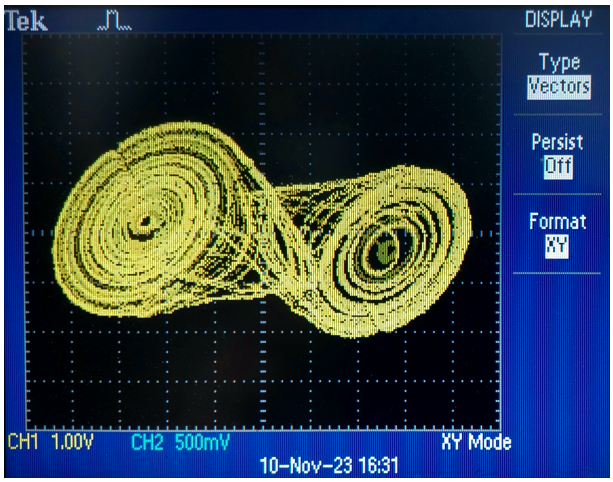


Fig15: Double scroll of Master chua circuit from an analog scope after tuning

This is the classic chaotic double-scroll attractor also known as Chua's attractor, obtained on plotting X vs Y, X vs Z and Y vs Z to see the scroll from different 2D perspectives.

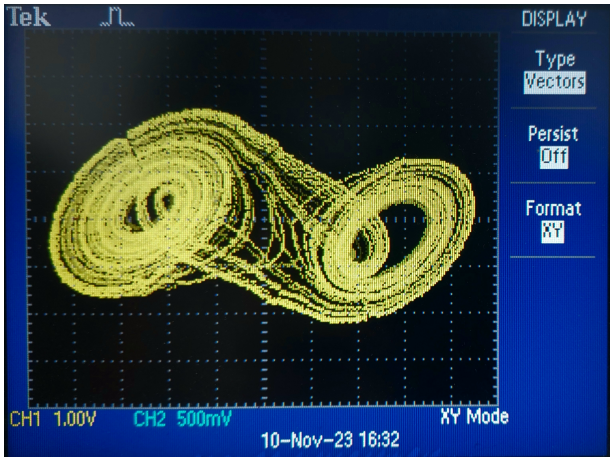


Fig16: Double scroll of Slave chua circuit

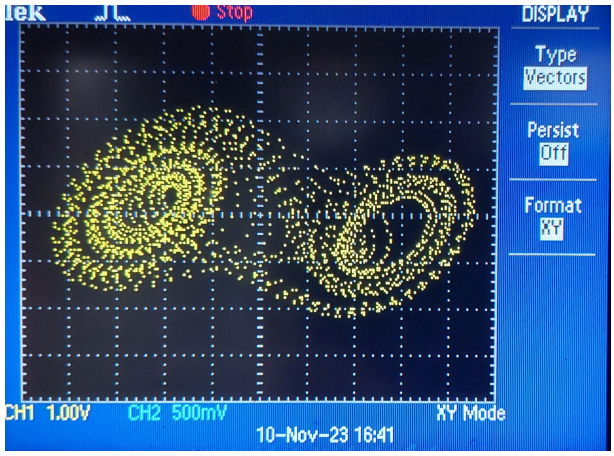


Fig17: Double scroll of Master chua circuit from a digital scope

B. Chaotic Communication System on oscilloscope

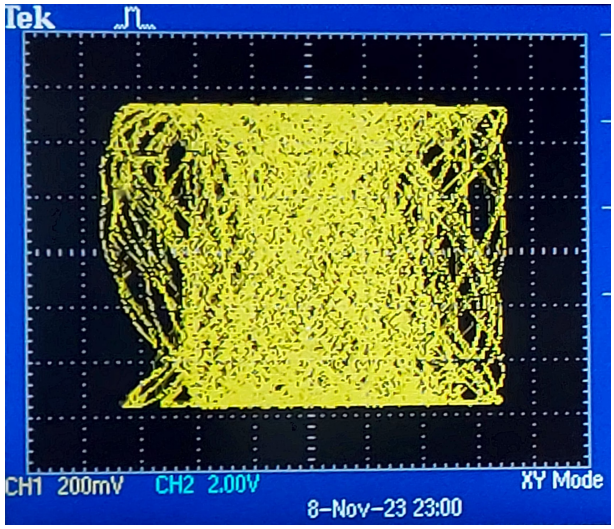


Fig18: The phase portrait of unsynchronized case

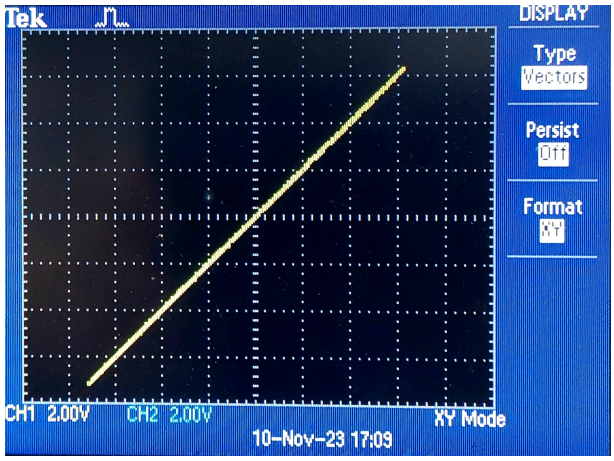


Fig19: X-Xr Synchronization.

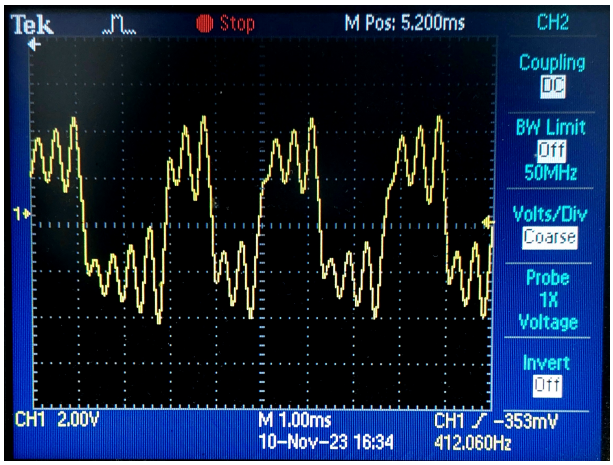


Fig20: Voltage across capacitor C_1 (X) after synchronization

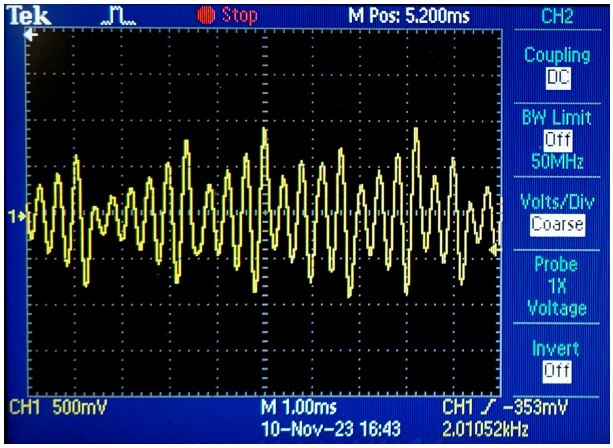


Fig21: Voltage across capacitor C_2 (Y) after synchronization

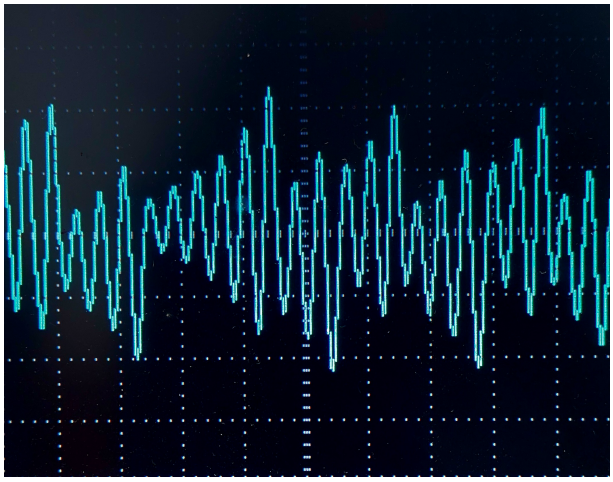


Fig22: Voltage at point P (Z) after synchronization

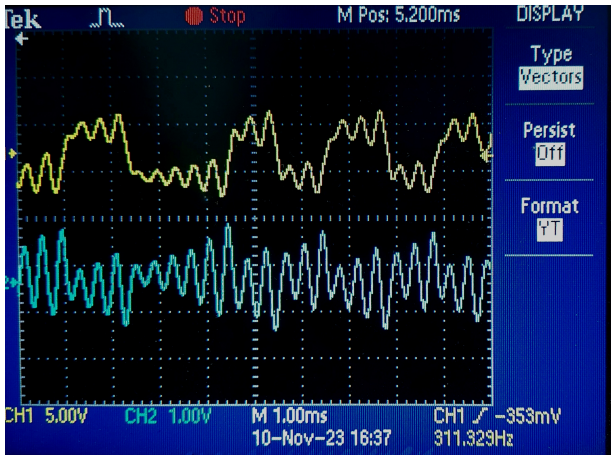


Fig23: Voltage across capacitor C_1(yellow) and at point P(blue) after synchronization

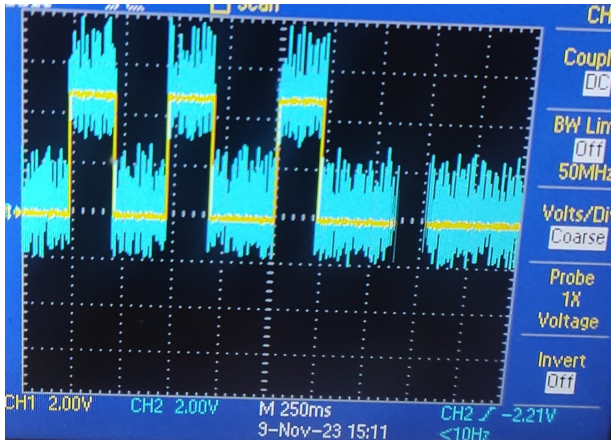


Fig24: Masked and response system chaotic signals after synchronization

VI. DISCUSSIONS

In the proposed approach, the designated threshold for the recovery of the information signal at the receiver system is approximately 200mV. Signals falling below this established threshold are lost as noise and are consequently irretrievable. Furthermore, as the signal intended for modulation is discrete, the inherent discreteness persists even post the introduction of noise. This implies that the information signal remains incompletely masked. To enhance the masking process, the integration of zero-order-hold (ZOH) blocks can be employed, to convert the discrete-time signal into a piecewise continuous-time signal, with each sample being held for one second. Subsequently, applying a low-pass-filter (LPF). In the retrieval process at the receiver, a dynamic filter is employed for signal recovery. This nonlinear filter may offer improved performance for practical chaotic communication systems.

VII. CONCLUSION

Developing physical prototypes of chaos-based communication systems is of great importance for better understanding the physics of chaotic signals transmission, their noise resistivity, and attenuation features. The project focuses on the chaotic oscillator circuit and the identical synchronization of the Chua's attractor and its applications in signal masking communications. Chua's chaotic circuit system is studied in detail by varying mostly the control parameter R (potentiometer). The system has rich chaotic dynamics behaviors. We have demonstrated that chaos can be synchronized and applied to secure communications.

ACKNOWLEDGMENTS

We extend our heartfelt appreciation to our course instructor, Prof. Pramod Kumar, for providing us with the opportunity to work on this project and guiding us throughout the process. Additionally, we acknowledge the dedicated support from the lab staff, whose continuous contributions have greatly facilitated our work. We would also like to thank the teaching assistants of the course for their assistance in various aspects of the project. Their prompt response and willingness to help made the project progress smoother.

CODE REPOSITORY

The codes developed for the project can be found here.

[1] L. M. Pecora and T. L. Carroll, Physical review letters **64**, 821 (1990).
[2] L. M. Pecora and T. L. Carroll, Physical review A **44**, 2374 (1991).
[3] E. W. Weisstein, "Attractor," From MathWorld–A Wolfram Web Resource.
[4] P. C. Matthews, R. E. Mirollo, and S. H. Strogatz, Physica D: Nonlinear Phenomena **52**, 293 (1991).
[5] V. Siderskiy, "The antoniou inductance-simulation circuit derivation," From: www.chuacircuits.com.