

Sending Secret Messages with Synchronized Chaotic Systems

Kevin Phan

May 12, 2023

Abstract

This paper introduces an example of a synchronized chaotic system based on the Lorenz system. We will see how this can be applied to the field of communications as synchronized chaotic system can be used to send secret messages. Lastly, we see how resistant this method of encryption is to noise when transmitting the signal.

Contents

1	Introduction	3
2	Theory of Synchronized Chaotic Systems	3
3	Numerical Experiments	6
3.1	Algorithm Implementation	6
3.2	Testing Algorithm Against Noise	6
4	Conclusion	6
	References	7

1 Introduction

add introduction (do this last) [CO93]

2 Theory of Synchronized Chaotic Systems

A synchronized system is when two dynamical systems' trajectories are eventually identical as time $t \rightarrow \infty$. A definition of synchronization is given by He and Vaidya [HV92].

Definition 2.1. *Let $\dot{\mathbf{x}} = f(t, \mathbf{x})$ and $\dot{\mathbf{y}} = g(t, \mathbf{y})$ be two dynamical systems, where t is time and $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. Let $\mathbf{x}(t; t_0, \mathbf{x}_0)$ and $\mathbf{y}(t; t_0, \mathbf{y}_0)$ be solutions to the dynamical systems respectively. We say that the two dynamical systems synchronize if there exists a subset of \mathbb{R}^n , denoted $D(t_0)$, such that $\mathbf{x}_0, \mathbf{y}_0 \in D(t_0)$ implies*

$$\|\mathbf{x}(t; t_0, \mathbf{x}_0) - \mathbf{y}(t; t_0, \mathbf{y}_0)\| \rightarrow 0 \text{ as } t \rightarrow +\infty.$$

If the region of synchronization $D(t_0) = \mathbb{R}^n$, we say that the synchronization is global and otherwise, the synchronization is local.

Note synchronization does not depend on the initial conditions of the dynamical systems.

One example of a synchronized system is given by Cuomo and Oppenheim (1993) which was used in the application of communications and how to send secret messages:

$$\begin{aligned} \dot{x}_T &= \sigma(y_T - x_T), \\ \dot{y}_T &= rx_T - y_T - 20(x_T z_T), \\ \dot{z}_T &= 5x_T y_T - bz_T, \end{aligned} \tag{1}$$

which is the transmitter's dynamical system and

$$\begin{aligned} \dot{x}_R &= \sigma(y_R - x_R), \\ \dot{y}_R &= rx_T - y_R - 20(x_T z_R), \\ \dot{z}_R &= 5x_T y_R - bz_R, \end{aligned} \tag{2}$$

which is the receiver's dynamical system [CO93]. Notice that the only state variable of the transmitter's dynamical system that appears in the receiver's

dynamical system is x_T . This means that only information that the receiver need to know to reconstruct the trajectory is data about x_T .

Cuomo and Oppenheim proved that the system will synchronize using a Lyapunov function to show that the error asymptotically approaches the point $\mathbf{0} \in \mathbb{R}^3$ [CO93].

Theorem 2.1. *The pair of dynamical systems given by equations 1 and 2 are globally synchronized.*

Proof. Let $e_x = x_T - y_T$, $e_y = y_T - y_R$, and $e_z = z_T - z_R$. This gives us the dynamical system

$$\begin{aligned}\dot{e}_x &= \sigma(e_y - e_x), \\ \dot{e}_y &= -e_y - 20e_z x_T, \\ \dot{e}_z &= 5e_y x_t - be_z,\end{aligned}\tag{3}$$

which describes the error between each component of the trajectories given by transmitter and receiver's dynamical system. Let $\mathbf{e} = (e_x, e_y, e_z)^T$. To show synchronization, it is sufficient to show that for equation 3, the fixed point $\mathbf{0}$ is asymptotically stable. By inspection, a fixed point of equation 3 is $\mathbf{0}$.

To show that it is asymptotically stable, we will use a Lyapunov function. Let $V(\mathbf{e}) = \frac{1}{2}(\frac{1}{\sigma}e_x^2 + e_y^2 + 4e_z^2)$. By inspection, we see that $V(\mathbf{0}) = 0$ and $V(\mathbf{e}) > 0$ for all $\mathbf{e} \neq \mathbf{0}$. Taking the time derivative and substituting for e_x, e_y, e_z using equation 3, we get

$$\begin{aligned}\dot{V} &= \frac{1}{\sigma}e_x\dot{e}_x + e_y\dot{e}_y + 8\dot{e}_z \\ &= \frac{1}{\sigma}e_x(\sigma e_y - \sigma e_x) + e_y(-e_y - 20x_T e_z) + 4e_z(5x_T e_y - be_z) \\ &= -e_x^2 + e_x e_y - e_y^2 - 4be_z^2 \\ &= -\left(e_x - \frac{1}{2}e_y\right)^2 - \frac{3}{4}e_y^2 - 4be_z^2,\end{aligned}$$

where the last step is completing the square. Thus, for all $\mathbf{e} \neq \mathbf{0}$, $\dot{V} < 0$. As such, V is a Lyapunov function, so all trajectories of V flow toward the fixed point $\mathbf{0}$. This means that the error goes to 0 which prove that the pair of dynamical systems given by equations 1 and 2 are globally synchronized. \square

However, the definition of synchronization does not tell us how fast the pair of dynamical systems will synchronize. Fortunately, Cuomo, Oppenheim, and Strogatz (1993) proven that error converge exponentially by studying the error dynamics [COS93].¹

Theorem 2.2. *The error dynamics of equations 1 and 2 given by equation 3 converge to $\mathbf{0}$ exponentially. In other words, $e_x, e_y, e_z = O(e^{-t})$.*

Proof. Consider the function $V = \frac{1}{2}e_y^2 + 2e_z^2$. We wish to show that $\dot{V} \leq -kV$ where $k = \min\{2, 2b\}$. Taking the time derivative and substituting for e_y, e_z using equation 3, we get

$$\begin{aligned}\dot{V} &= e_y \dot{e}_y + 4e_z \dot{e}_z \\ &= e_y(-e_y - 20e_z x_T) + 4e_z(5e_y x_T - be_z) \\ &= -(e_y^2 + 4be_z^2).\end{aligned}$$

We see that $-(e_y^2 + 4be_z^2) \leq -k(\frac{1}{2}e_y^2 + 2e_z^2)$ where $k = \min\{2, 2b\}$.

Next, we establish that $e_2, e_3 = O(e^{-t})$. Integrating $\dot{V} = -kV$ with respect to t , we get $V(t) \leq V_0 e^{-kt}$ where V_0 is the initial condition of V . From this, we establish the inequalities

$$\frac{1}{2}e_y^2 \leq V(t) \leq V_0 e^{-kt}$$

and

$$2e_z^2 \leq V(t) \leq V_0 e^{-kt}.$$

Solving for e_y in the first inequality, we get

$$e_y \leq \sqrt{2V_0} e^{-\frac{kt}{2}}.$$

Simiarly, solving for e_z in the second inequality, we get

$$e_z \leq \sqrt{\frac{V_0}{2}} e^{-\frac{kt}{2}}.$$

This show that $e_y, e_z = O(e^{-t})$.

Lastly, we show that $e_1 = O(e^{-t})$. From equation 3, $\dot{e}_x = \sigma(e_y - e_x)$. This can be rewritten as $\dot{e}_1 + \sigma e_1 = \sigma e_2$. Since $e_y \leq \sqrt{2V_0} e^{-\frac{kt}{2}}$, we have

$$\dot{e}_1 + \sigma e_1 \leq \sqrt{2V_0} e^{-\frac{kt}{2}}.$$

¹This is also given as Exercise 9.1 in Strogatz's Nonlinear Dynamics and Chaos [Str19].

Multiplying by the integrating factor $e^{\sigma t}$, we get

$$(e_1 e^{\sigma t})' \leq \sqrt{2V_0} e^{(\sigma - \frac{k}{2})t}$$

Integrating and solving for e_1 , we get

$$e_1 \leq \frac{\sqrt{2V_0}}{\sigma - \frac{k}{2}} e^{-\frac{kt}{2}}$$

This established that $e_1 = O(e^{-t})$. Therefore, we proved that the error dynamics given by equation 3 converge to $\mathbf{0}$ exponentially. \square

give numerical example of synchronization and exponential convergence
(copy from presentation essentially)

3 Numerical Experiments

3.1 Algorithm Implementation

3.2 Testing Algorithm Against Noise

4 Conclusion

References

- [HV92] Rong He and P. G. Vaidya. “Analysis and synthesis of synchronous periodic and chaotic systems”. In: *Phys. Rev. A* (3) 46.12 (1992), pp. 7387–7392. ISSN: 1050-2947. DOI: 10.1103/PhysRevA.46.7387. URL: <https://doi.org/10.1103/PhysRevA.46.7387>.
- [COS93] K.M. Cuomo, A.V. Oppenheim, and S.H. Strogatz. “Synchronization of Lorenz-based chaotic circuits with applications to communications”. In: *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing* 40.10 (1993), pp. 626–633. DOI: 10.1109/82.246163.
- [CO93] Kevin M. Cuomo and Alan V. Oppenheim. “Circuit implementation of synchronized chaos with applications to communications”. In: *Phys. Rev. Lett.* 71 (1 July 1993), pp. 65–68. DOI: 10.1103/PhysRevLett.71.65. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.71.65>.
- [Str19] S. Strogatz. *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*. Chapman & Hall book. CRC Press, 2019. ISBN: 9780367092061.