

Lorenz System Image Encryption

Christian Ortiz

Nick Wade

16 Aug 2022

Presentation Outline

- State Goals
- Image Encryption Definition
- Lorenz System Review
- Image Encryption Method outline
- Results and observations
- Conclusion
- Scope for improvements
- References

Goals

- We will demonstrate how to accomplish an image encryption algorithm.
- Utilize the Lorenz equations.
- Show the utility of a subject learned in this class for a real-world application.

Image Encryption Definition

- We consider an image encryption algorithm to be any method of transforming the values of the pixels comprising an image in a way that produces a drastically different image and is only decipherable by the sender and receiver.[1-8]
 - Image deconstruction vs reconstruction.
 - Private, secure, and selectively accessible.

Why Use the Lorenz Equations?

- Ease of use for any image format
 - Size
 - Color
- Output based on input parameters
 - key generation
- Pseudo Random numbers
 - From Chaotic Behavior

Chaotic systems create Pseudo Random numbers

- Chaotic Waterwheel

$$\dot{a}_1 = \omega b_1 - K a_1$$

$$\dot{b}_1 = -\omega a_1 - K b_1 + q_1$$

$$\dot{\omega} = (-v\omega + \pi g r a_1)/I_{[7]}$$

- Lorenz equation

$$\dot{x} = \sigma(y - x)$$

$$\dot{y} = rx - y - xz$$

$$\dot{z} = xy - bz. \quad [7]$$

Lorenz Equation History

- Finite system of deterministic ordinary nonlinear differential equations representing forced dissipative hydrodynamic flow.[11]
- This derivation summary is from Lorenz's 1962 paper on Deterministic Nonperiodic Flow[11]:

Consider a system governed by:

$$\frac{dX_i}{dt} = F_i(X_1, \dots, X_M), \quad i = 1, \dots, M \dots \dots \dots (1)$$

All points possess a unique solution:

$$X_i = f_i(X_{1_0}, \dots, X_{M_0}, t), \quad i = 1, \dots, M \dots \dots \dots (2)$$

And satisfy the condition:

$$f_i(X_{1_0}, \dots, X_{M_0}, t_0) = X_{i0}, \quad i = 1, \dots, M \dots \dots \dots (3)$$

Unique trajectory through each point of the system.

This forced dissipative system can be generalized by

$$\frac{dX_i}{dt} = \sum_{j,k} a_{ijk} X_j X_k - \sum_j b_{ij} X_j + c_i \dots \dots \dots (4)$$

Lorenz allows several terms be constants, mandated by:

$$Q = \frac{1}{2} \sum_i X_i^2, \dots \dots \dots (5)$$

where e_1, \dots, e_M are roots of the equation, then:

$$\sum_j (b_{ij} + b_{ji}) e_j = c_i \dots \dots \dots (6)$$

Combining (6), (5), and (4) give:

$$\frac{dQ}{dt} = \sum_{i,j} b_{ij} e_i e_j - \sum_{i,j} b_{ij} (X_i - e_i)(X_j - e_j) \dots \dots (7)$$

Lorenz Derivation continued

To solve (1) numerically,

Lorenz chooses initial time and time increment:

$$X_{i,n} = X_i(t_0 + n\Delta t) \dots \dots \dots (8)$$

And he uses auxiliary approximations:

$$X_{i(n+1)} = X_{i,n} + F_i(P_n)\Delta t \dots \dots \dots (9)$$

$$X_{i(n+2)} = X_{i,(n+1)} + F_i(P_{(n+1)})\Delta t \dots \dots \dots (10)$$

And uses the double-approximation procedure:

$$X_{i,n+1} = X_{i,n} + \frac{1}{2} [F_i(P_n) + F_i(P_{(n+1)})]\Delta t \dots \dots \dots (13)$$

And rewrites it using (9) and (10):

$$X_{i,n+1} = \frac{1}{2} (X_{i,n} + X_{i(n+2)}) \dots \dots \dots (14)$$

This equation is successively evaluated to accomplish Lorenz's computations.

In the special case where all motion is parallel to the x-z plane, and there is no variation in the y-axis direction,

Lorenz rewrites his governing equations as:

$$\frac{\partial}{\partial t} \nabla^2 \Psi = - \frac{\partial(\Psi, \nabla^2 \Psi)}{\partial(x,z)} + \nu \nabla^4 \Psi + g\alpha \frac{\partial \theta}{\partial x} \dots \dots \dots (17)$$

$$\frac{\partial}{\partial t} \theta = - \frac{\partial(\Psi, \theta)}{\partial(x,z)} + \frac{\Delta T}{H} \frac{\partial \Psi}{\partial x} + \kappa \nabla^2 \theta \dots \dots \dots (18)$$

Where Ψ is a "stream function" for two dimensional Motion, θ is a temperature difference, and the constants g, α, ν , and κ denote gravity, thermal expansion, viscosity, And thermal conductivity.

Lorenz Derivation continued

Lorenz then used Rayleigh's equation for the fields of motion:

$$\Psi = \Psi_0 \sin(\pi a H^{-1} x) \sin(\pi H^{-1} z) \dots \dots \dots (19)$$

$$\theta = \theta_0 \cos(\pi a H^{-1} x) \sin(\pi H^{-1} z) \dots \dots \dots (20)$$

and he notes that these equations require the Rayleigh number:

$$R_a = g \alpha H^3 \Delta T \nu^{-1} \kappa^{-1} \dots \dots \dots (21)$$

To exceed a critical value:

$$R_c = \pi^4 a^{-2} (1 + a^2)^3 \dots \dots \dots (22)$$

Lorenz builds on the work of Saltzman, who expanded Ψ and θ

In a double Fourier series in x and z , substituted them into (17)

And (18), swapped products of trigonometric functions for sums,

Reduced the infinite system for a finite system by omitting sets

And only using a specified finite set of functions of t .

Lorenz then truncated the series to include three terms:

$$a(1 + a^2)^{-1} \kappa^{-1} \Psi = X \sqrt{2} \sin(\pi a H^{-1} x) \sin(\pi H^{-1} z) \dots \dots \dots (23)$$

$$\pi R_c^{-1} R_a \Delta T^{-1} \theta = Y \sqrt{2} \cos(\pi a H^{-1} x) \sin(\pi H^{-1} z) - Z \sin(2\pi H^{-1} z) \dots \dots \dots (24)$$

The Lorenz Equations

Finally, substitutes (23) and (24) into (17) and (18) and omits the trig terms to get:

$$\begin{aligned}\dot{X} &= -\sigma X + \sigma Y \\ \dot{Y} &= -XZ + rX - Y \\ \dot{Z} &= XY - bZ\end{aligned}$$

Where dimensionless time is used: $\tau = \pi^2 H^{-2} (1 + a^2) \kappa t$

The Prandtl number is: $r = R_c^{-1} R_a$

And $b = 4(1 + a^2)^{-1}$

- x is proportional to the intensity of the convective motion[15]
- y is proportional to the temperature difference between the ascending and descending currents.[15]
 - similar signs of x and y denoting that warm fluid is rising, and cold fluid is descending. [15]
- The variable z is proportional to the distortion of the vertical temperature profile from linearity. [15]
 - A positive value indicating that the strongest gradients occur near the boundaries.[15]

Uses for Lorenz Equations

- Demonstrate unpredictability of weather patterns[7]
- Physics, biology, complex networks, economics[1]
- Generators, chemical reactions, brushless DC motors, forward osmosis, lasers, electrical circuits and passive heat exchange[4]
- Cryptography and encryption[1-8]

Chaotic Behavior

- Aperiodic long-term behavior in a deterministic system that exhibits sensitive dependence on initial conditions.[7]
 - trajectories which do not settle down
 - Sensitive dependence on initial conditions
 - Deterministic
 - Essential for decryption

When Does Chaotic Behavior Occur?

- Just after the Hopf Bifurcation.
- Where does the Bifurcation Occur?
- When $r = r_H = \frac{\sigma(\sigma + b + 3)}{\sigma - b - 1}$
 - From problem 9.2.1 the characteristic equation for the fixed points C+ and C-:
 - $\lambda^3 + \lambda^2(\sigma + b + 1) + \lambda b(\sigma + r) + 2b\sigma(r - 1) = 0$
 - Hopf Bifurcation occurs when λ crosses imaginary axis.
 - r is the Rayleigh number or bifurcation parameter.

Now, letting $\lambda = i\omega$, I get:

$$\diamond (i\omega)^3 + (i\omega)^2(\sigma + b + 1) + (i\omega)b(\sigma + r) + 2b\sigma(r - 1) = 0$$

$$\diamond -i\omega^3 - \omega^2(\sigma + b + 1) + i\omega b(\sigma + r) + 2b\sigma(r - 1) = 0$$

Grouping the real and imaginary parts gives:

❖ Real:

$$\blacksquare \omega^2(\sigma + b + 1) = 2b\sigma(r - 1)$$

$$\triangleright \omega^2 = \frac{2b\sigma(r-1)}{\sigma+b+1}$$

❖ Imaginary:

$$\blacksquare i\omega^3 = i\omega b(\sigma + r)$$

$$\triangleright \omega^2 = b\sigma + br$$

➤ Using the equation from the real part:

$$\bullet \frac{2b\sigma(r-1)}{\sigma+b+1} = b(\sigma + r)$$

• Solving for r :

$$\circ 2b\sigma r - 2b\sigma = (\sigma + b + 1)(b\sigma + br)$$

$$\circ 2b\sigma r - 2b\sigma = (b\sigma^2 + b^2\sigma + b\sigma) + (\sigma br + b^2r + br)$$

$$\circ 2b\sigma r - (\sigma br + b^2r + br) = (b\sigma^2 + b^2\sigma + b\sigma) + 2b\sigma$$

$$\circ \sigma br - b^2r - br = b\sigma^2 + b^2\sigma + 3b\sigma$$

$$\bullet br(\sigma - b - 1) = b\sigma(\sigma + b + 3)$$

$$\circ r = r_H = \frac{\sigma(\sigma+b+3)}{(\sigma-b-1)}$$

Exercise 9.2.2- bounded behavior

9.2.2 (An ellipsoidal trapping region for the Lorenz equations) Show that there is a certain ellipsoidal region E of the form $rx^2 + \sigma y^2 + \sigma(z - 2r)^2 \leq C$ such that all trajectories of the Lorenz equations eventually enter E and stay in there forever.

$$\text{Let } C = rx^2 + \sigma y^2 + \sigma(z - 2r)^2$$

$$\text{Then } \dot{C} = 2rx\dot{x} + 2\sigma y\dot{y} + 2\sigma(z - 2r)\dot{z}$$

$$\dot{C} = 2rx\sigma(y - x) + 2\sigma y(rx - y - xz) + 2\sigma(z - 2r)(xy - bz)$$

$$\dot{C} = -2\sigma(rx^2 + y^2 + bz^2 - 2brz) = -2\sigma(rx^2 + y^2 + b(z - r)^2 - br^2).$$

$$\text{Now, if } rx^2 + y^2 + b(z - r)^2 - br^2 > 0$$

then $\dot{C} < 0$ and C decreases along all trajectories.

C decreases along trajectories outside the ellipsoid $rx^2 + y^2 + b(z - r)^2 \leq br^2$

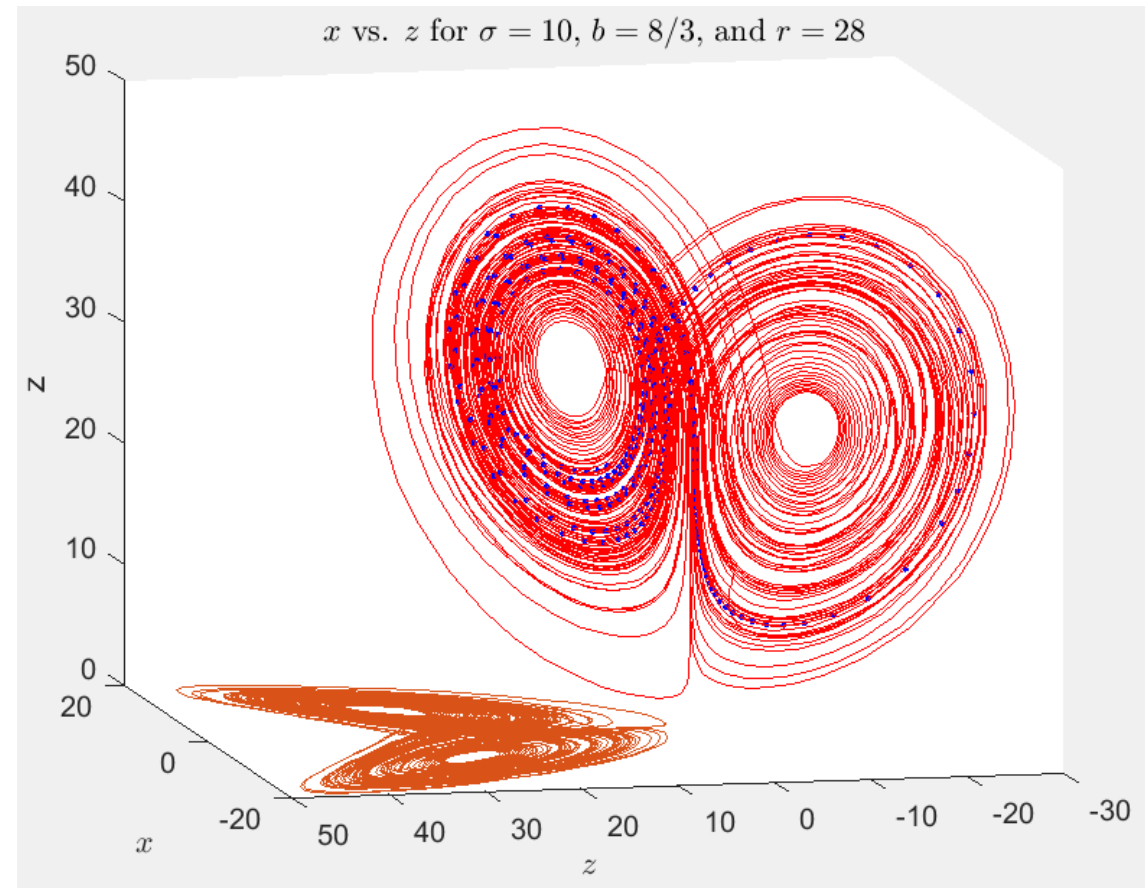
$$\text{Choosing } C > br^2$$

Then C decreases for trajectories on the ellipsoid $rx^2 + y^2 + b(z - r)^2 = C$

Therefore, the trapping region for the Lorenz system is $E: rx^2 + \sigma y^2 + \sigma(z - 2r)^2 \leq C$

Behavior of the Lorenz system for $r > r_H$

- Bounded movement between unstable limit cycles and "distant attractor"
 - "An amazingly complicated invariant set." [7]
 - "Trajectories are confined to a bounded set of zero volume... they manage to move on this set forever without intersecting themselves or others" [7]



Behavior as "r" varies

- $r=13.926$
 - homoclinic bifurcation
 - unstable limit cycles
- $r=24.06$
 - infinite wander time
 - strange attractor.
- $r=24.74$
 - subcritical Hopf bifurcation

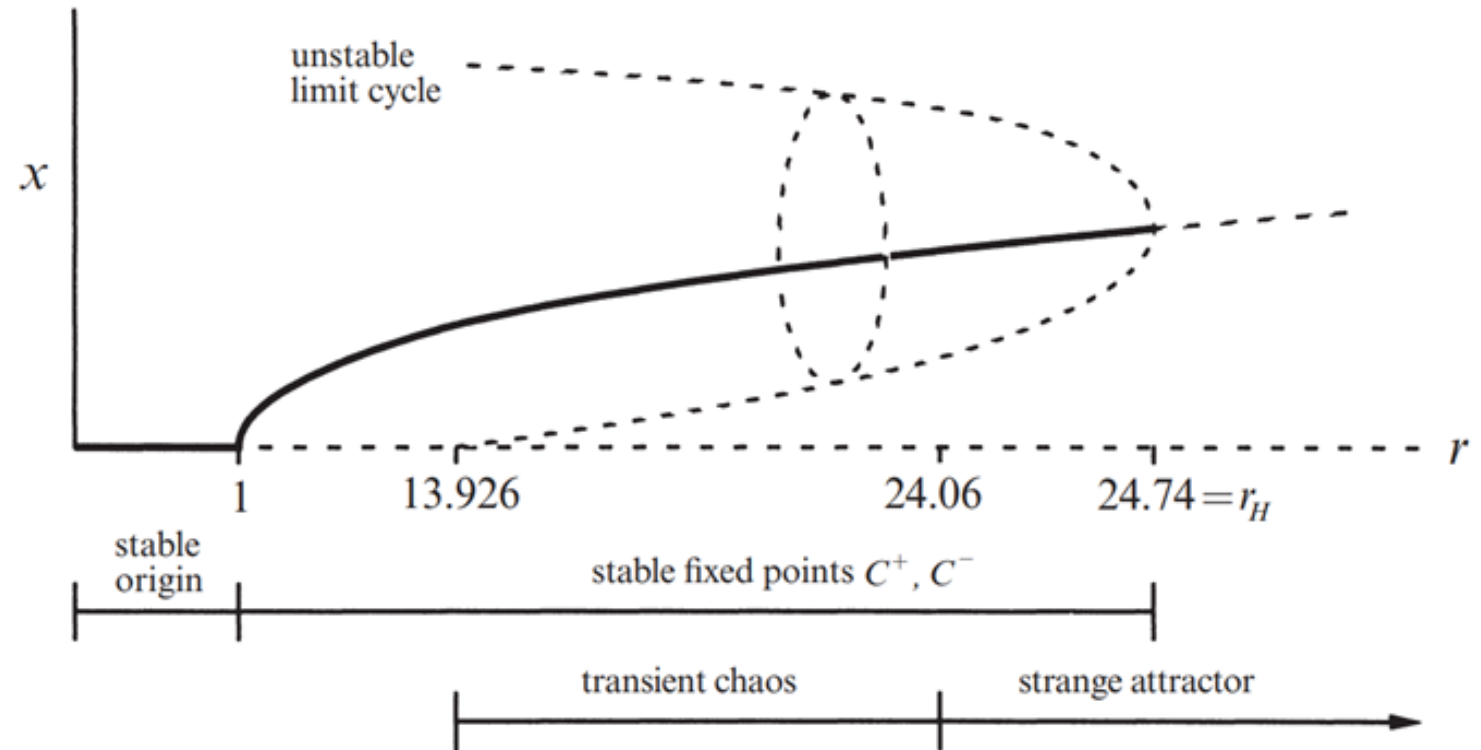
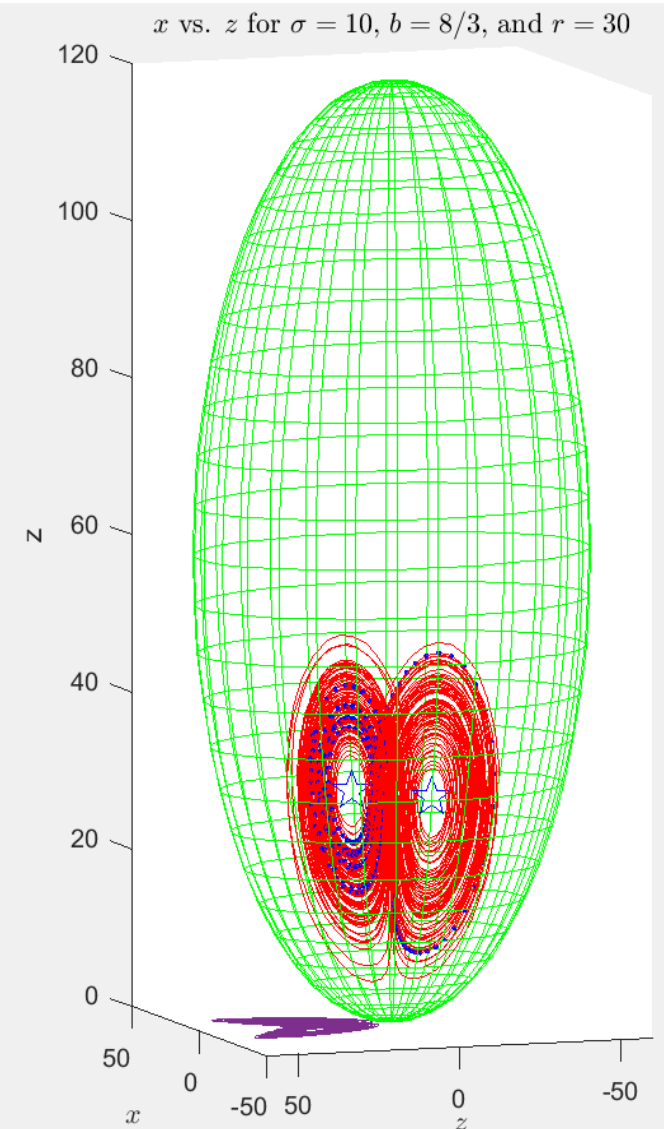
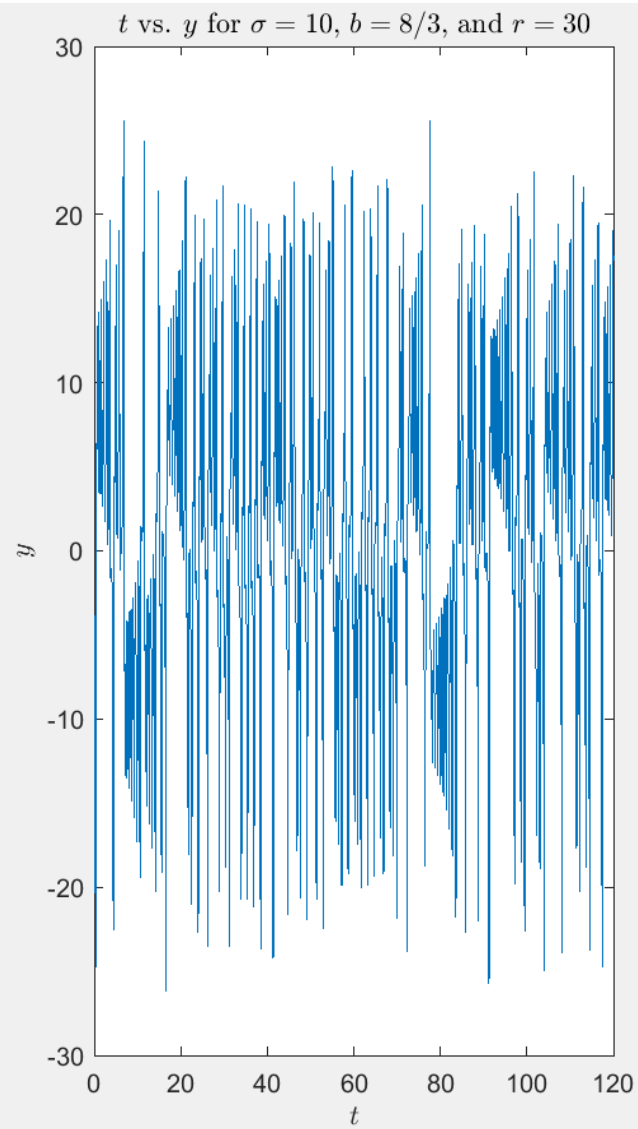
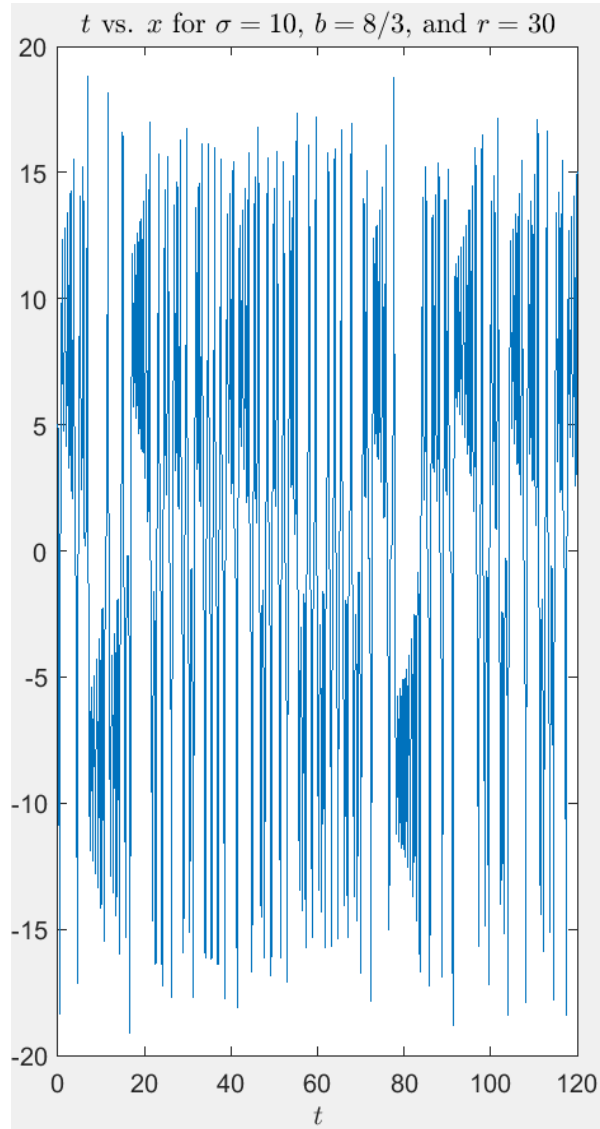
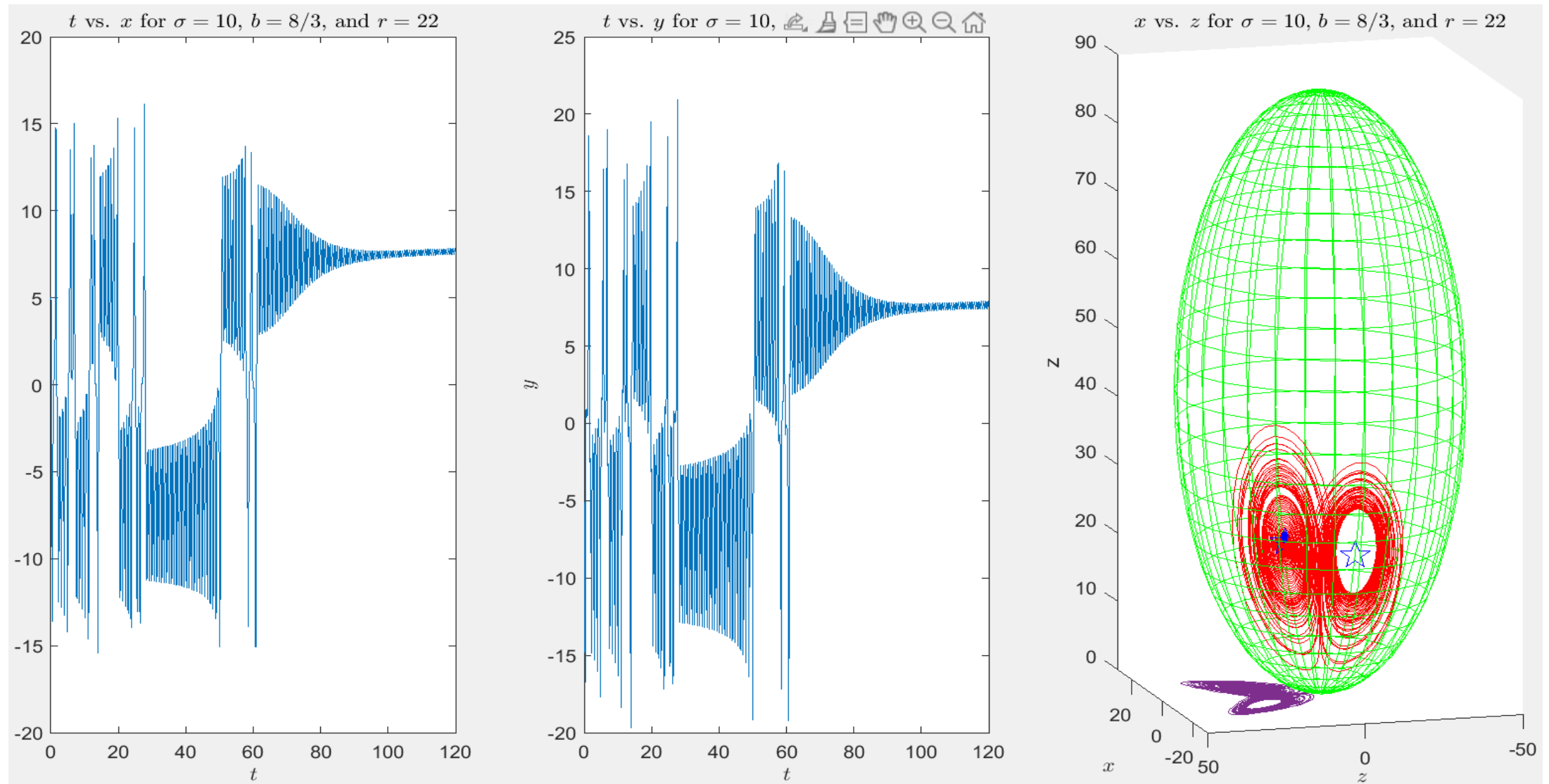


Figure 9.5.1

Our Parameters: $r=30$, $\sigma=10$, $b=8/3$

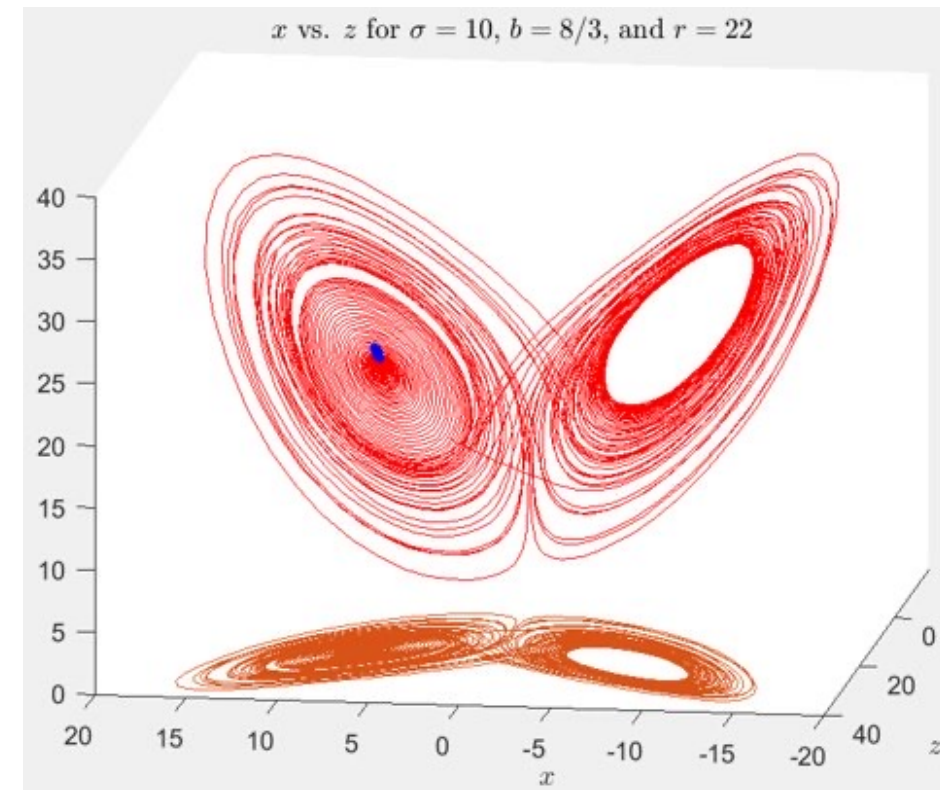


Our parameters: $r=22$, $\sigma=10$, $b=8/3$



Transient Chaos

- "Transient chaos shows that a deterministic system can be unpredictable, even if its final states are very simple. In particular, you don't need strange attractors to generate effectively random behavior." [7] (Strogatz 340)



Summary of Desirable Lorenz System Characteristics

- Ease of use.
 - Receiver has access to Lorenz system and key.
 - Easy to transform pixel values based on generated pseudorandom numbers.
- Output based on input parameters
 - Facilitates key generation from parameters and initial conditions.
- Pseudo Random numbers
 - From Chaotic Behavior
 - Prevents "hacking" via Fourier decomposition and other statistical methods.

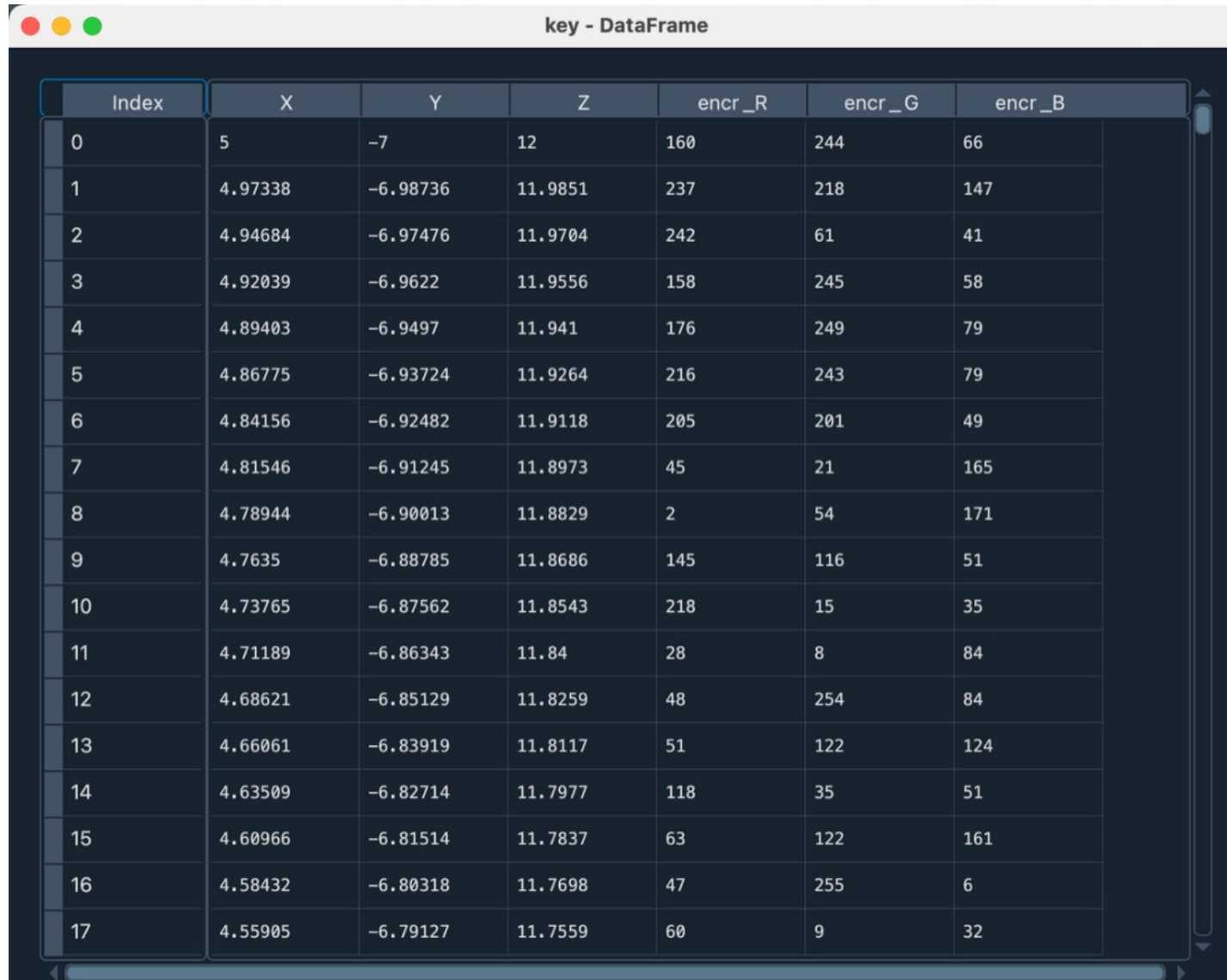
Encryption Methods

- Separate functions were created for the encryption and decryption of the image but utilize same principle.
- Both methods rely on Lorenz equations.
 - Solve for x/y/z trajectories based on initial x, y, z and system parameters.
 - From these, create a set of pseudorandom numbers [12]
 - Correlate pseudorandom numbers with pixel RGB values using XOR op

Encryption algorithm steps:

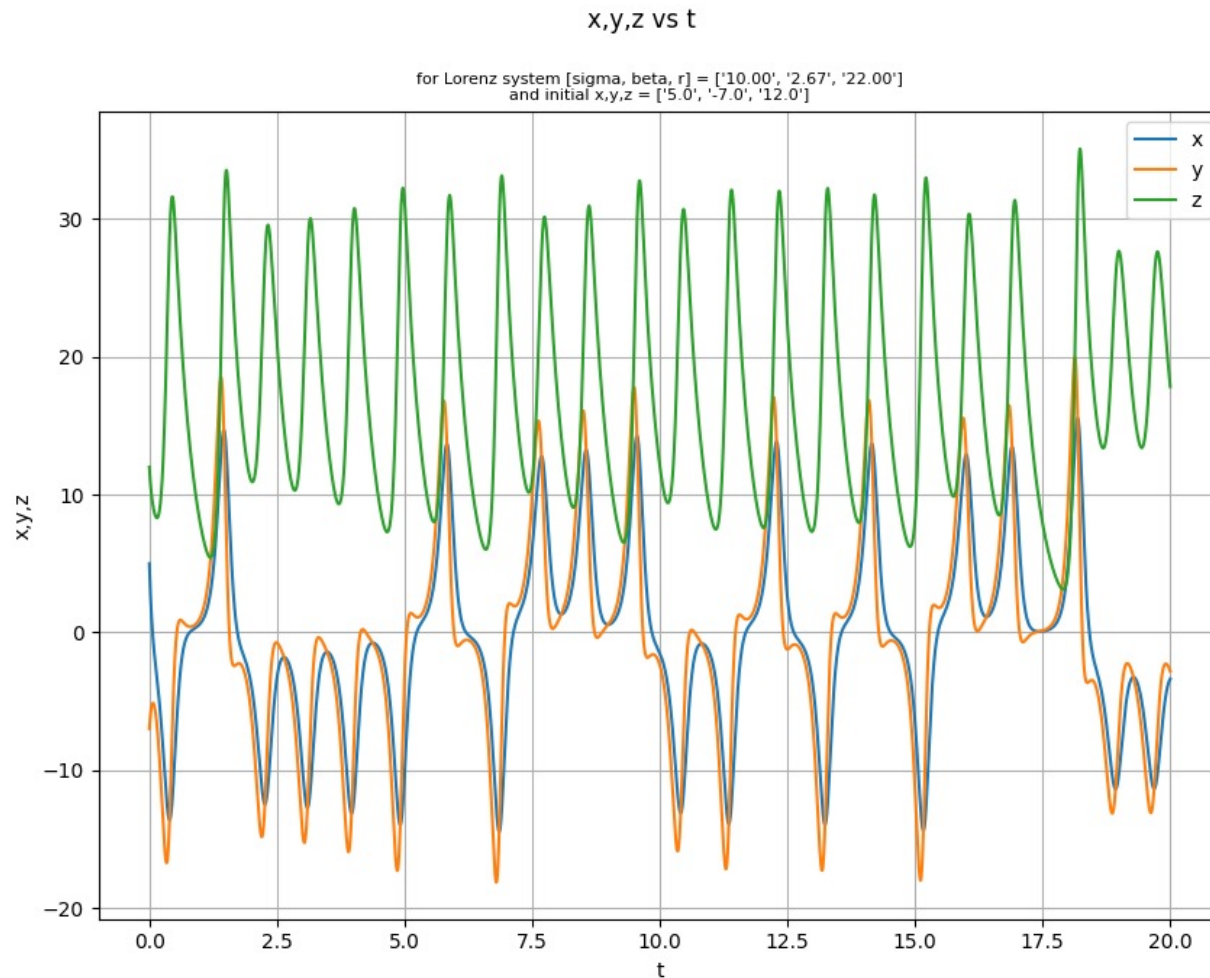
- Given initial conditions x_0, y_0, z_0 , Lorenz parameters σ, r, b , and an $N \times M$ image to encrypt.
 1. Produce PRNs at least $N \times M$ datapoints of $x/y/z$ over the desired t -space. [12]
 - a. Create x, y, z values from Lorenz equations w/ initial conditions and parameters over desired t -space.
 - b. Multiply each x, y , and z value by 10^{13} and convert to IEEE754 floating point.
 - c. The last 8 bits to step 1b is the PRN. This is achieved using $\text{step1b} \bmod 256$. Result is stored as $[X_c, Y_c, Z_c]$
 2. Pixel $[R, G, B]$ XOR Step 1 result $[X_c, Y_c, Z_c]$
 3. Resplice image pixels together. The order in which this is achieved is user preference.
- Note: In testing, " t -space" was 0 to 20 in $300 \times 300 = 90,000$ steps. However, further simplification can be utilized by setting the end time to the absolute value of the product of the Lorenz parameters ($|\sigma * r * b|$) and the number of steps to the number of pixels ($N \times M$)
- Note 2: Decryption is the same algorithm, just applied against the encrypted image

Generated random numbers

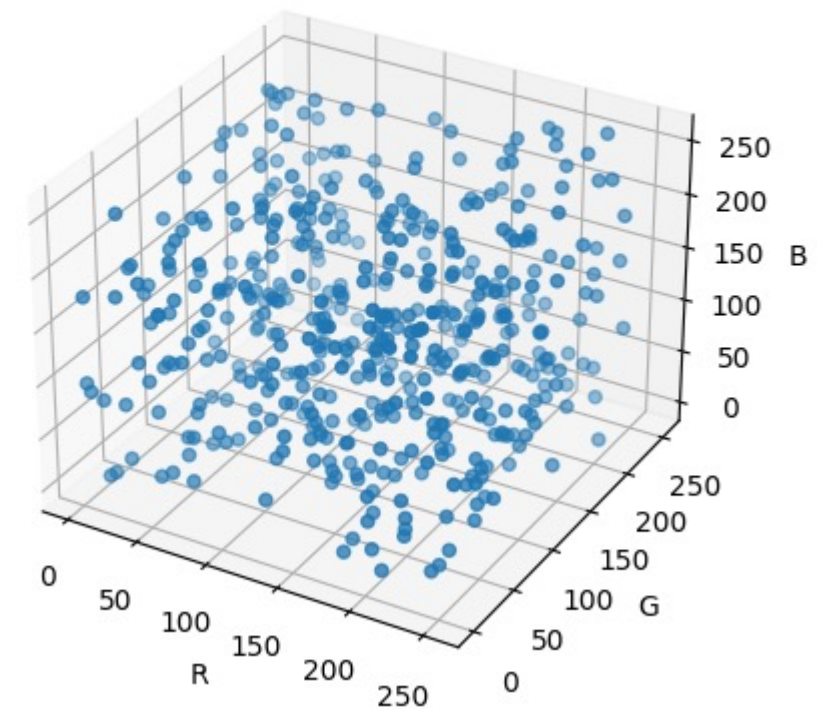


Index	X	Y	Z	encr_R	encr_G	encr_B
0	5	-7	12	160	244	66
1	4.97338	-6.98736	11.9851	237	218	147
2	4.94684	-6.97476	11.9704	242	61	41
3	4.92039	-6.9622	11.9556	158	245	58
4	4.89403	-6.9497	11.941	176	249	79
5	4.86775	-6.93724	11.9264	216	243	79
6	4.84156	-6.92482	11.9118	205	201	49
7	4.81546	-6.91245	11.8973	45	21	165
8	4.78944	-6.90013	11.8829	2	54	171
9	4.7635	-6.88785	11.8686	145	116	51
10	4.73765	-6.87562	11.8543	218	15	35
11	4.71189	-6.86343	11.84	28	8	84
12	4.68621	-6.85129	11.8259	48	254	84
13	4.66061	-6.83919	11.8117	51	122	124
14	4.63509	-6.82714	11.7977	118	35	51
15	4.60966	-6.81514	11.7837	63	122	161
16	4.58432	-6.80318	11.7698	47	255	6
17	4.55905	-6.79127	11.7559	60	9	32

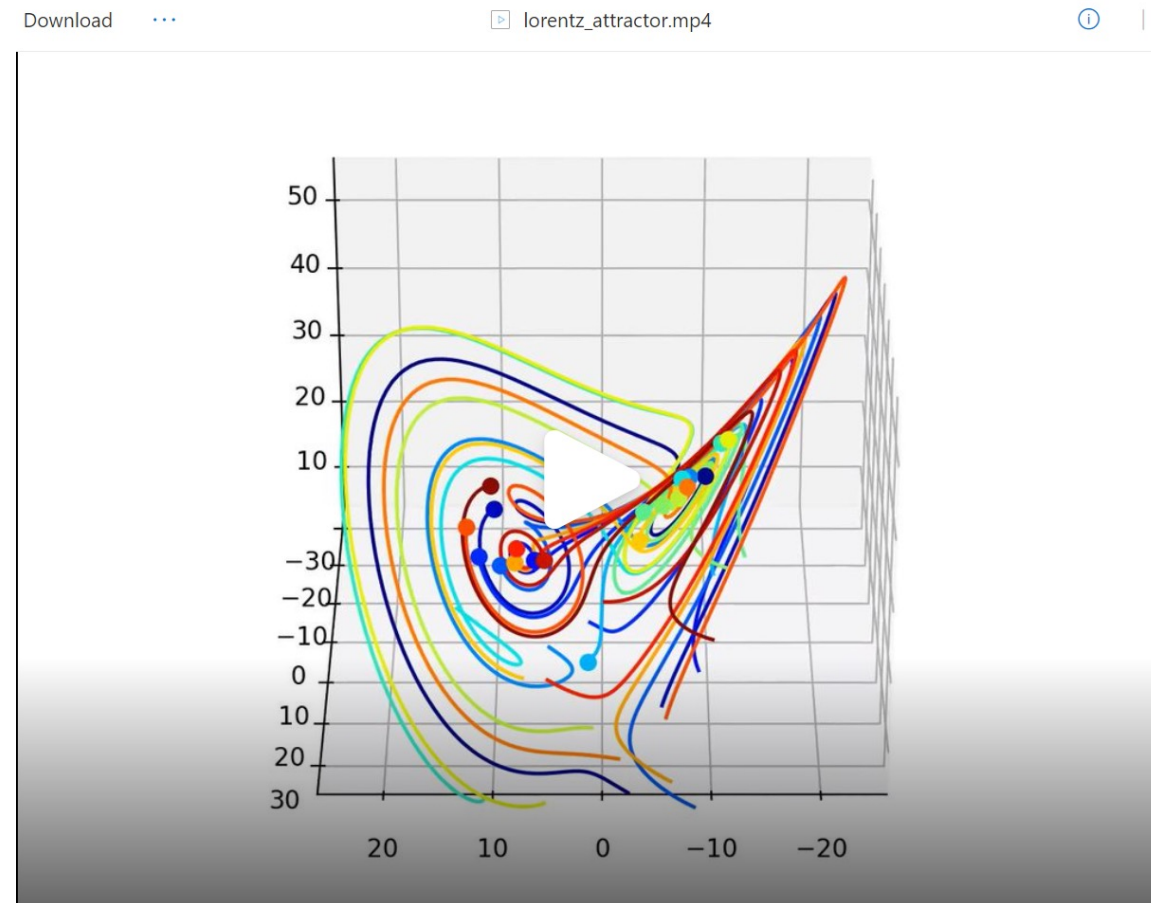
Results: step 1 Pseudorandom Number Generation



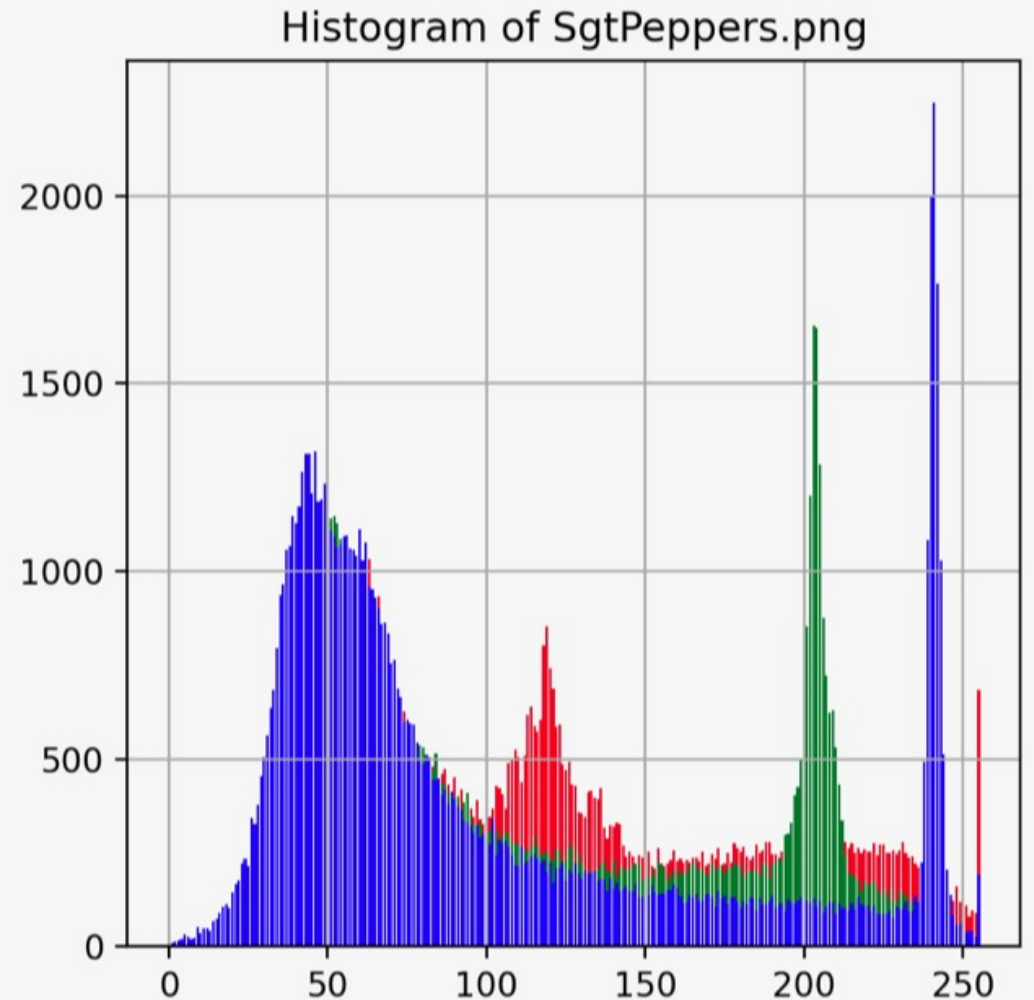
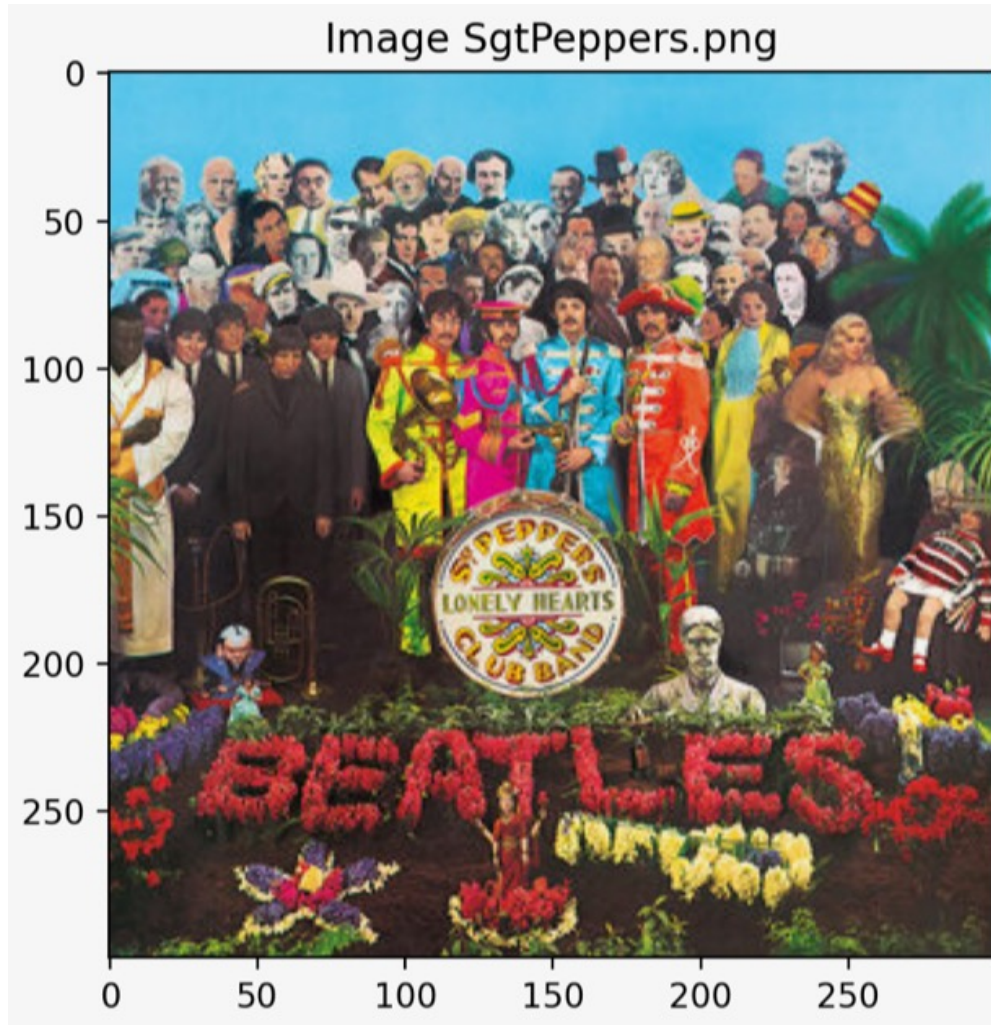
Pseudorandom numbers generated from Lorenz system



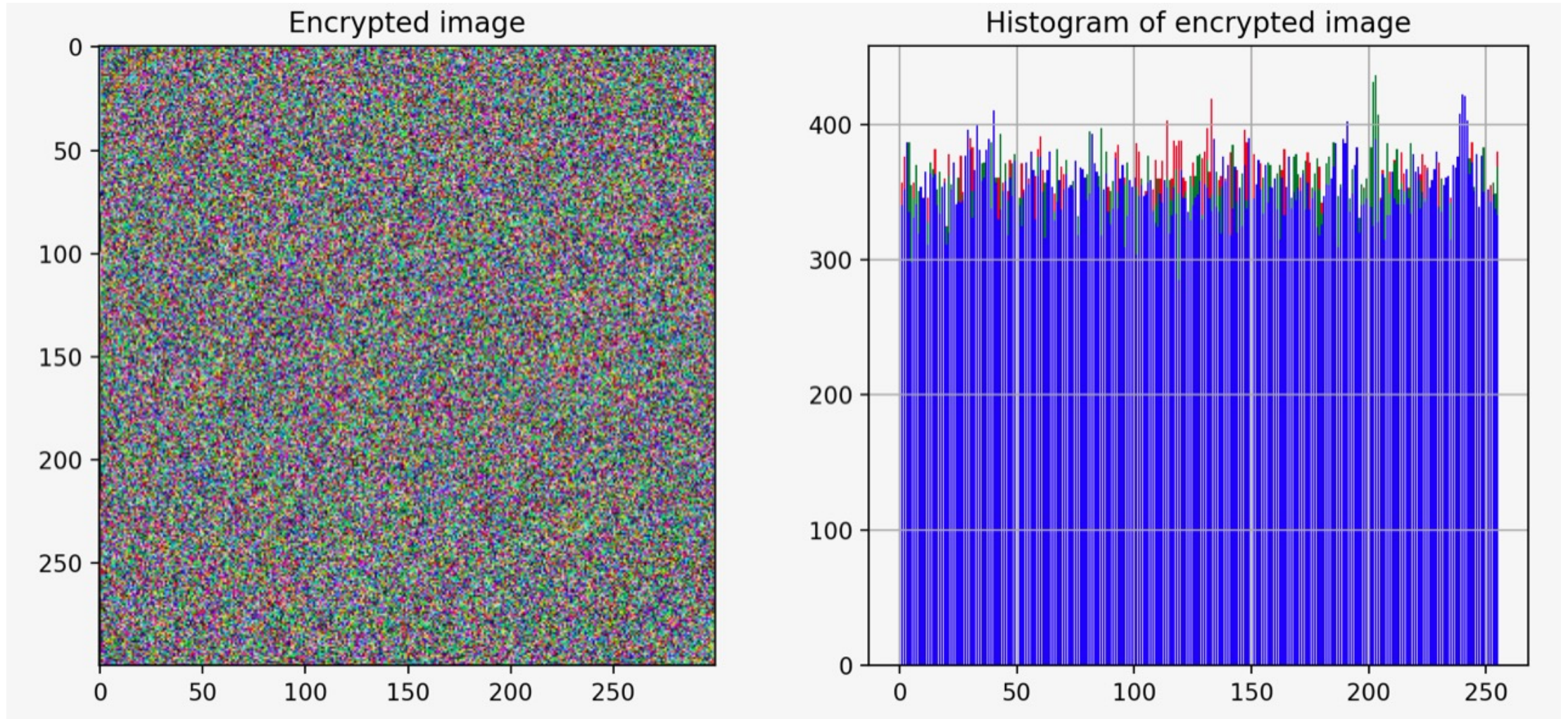
Lorenz Attractor Video



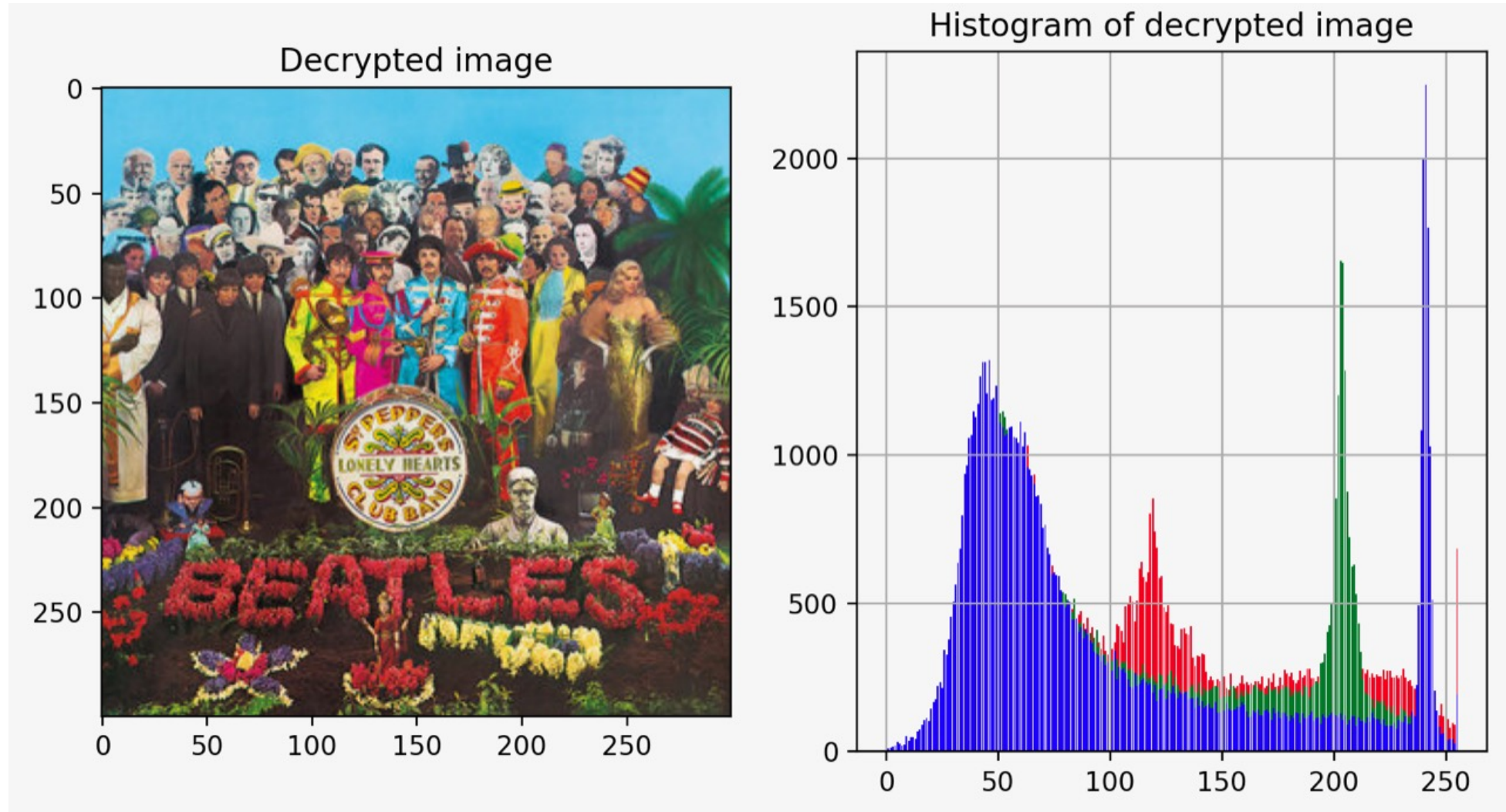
Results: Original Image



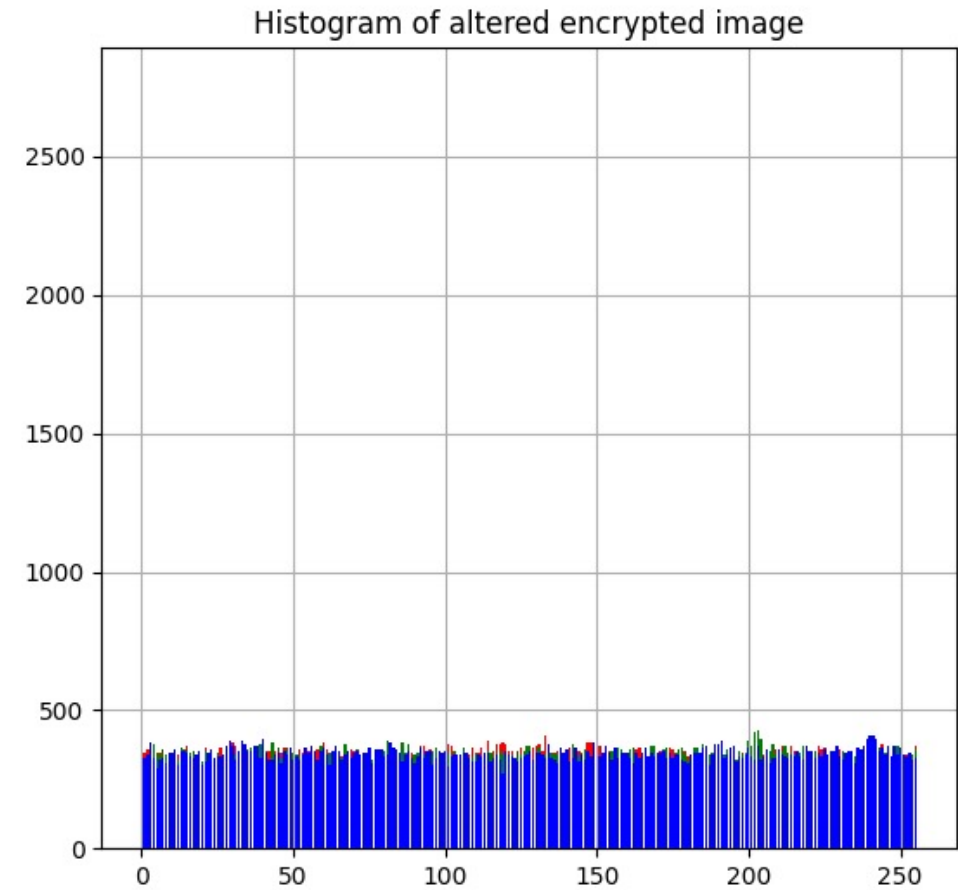
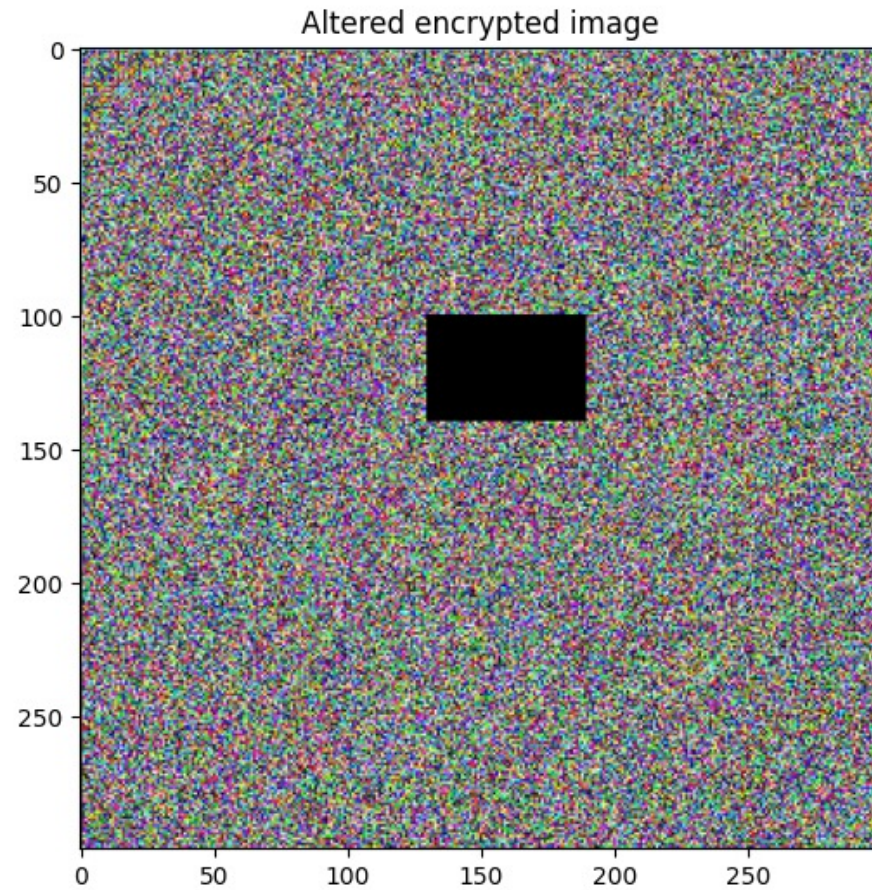
Results: Encrypted Image



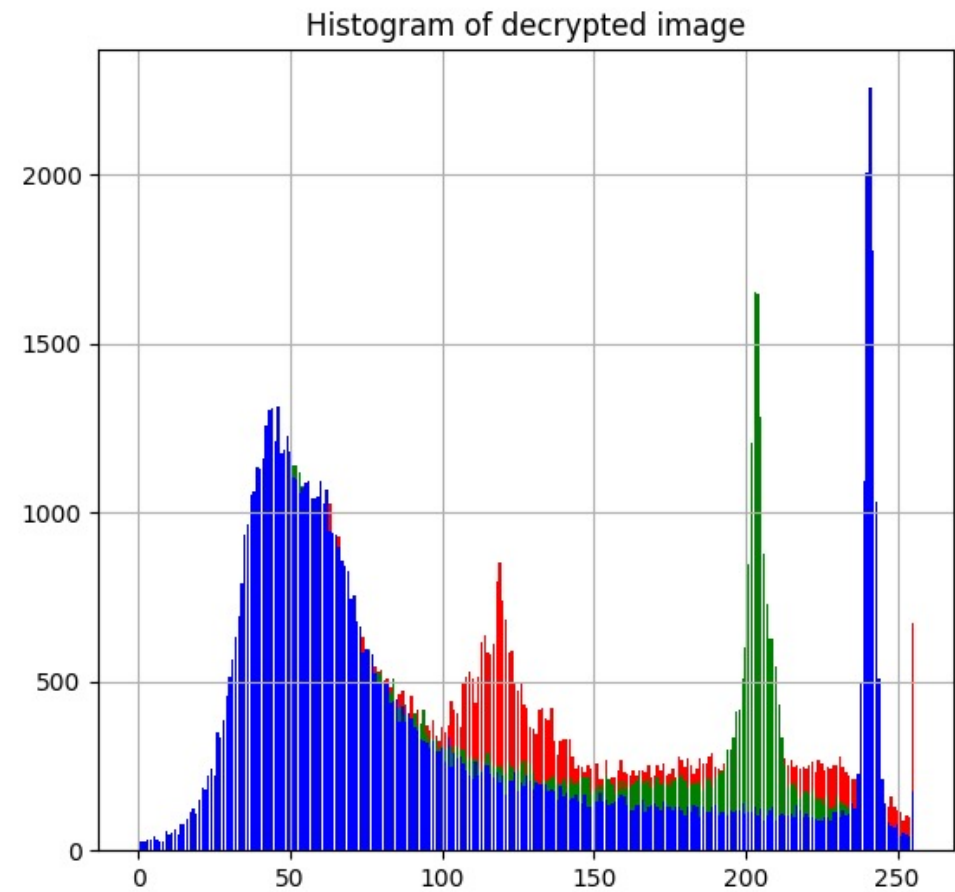
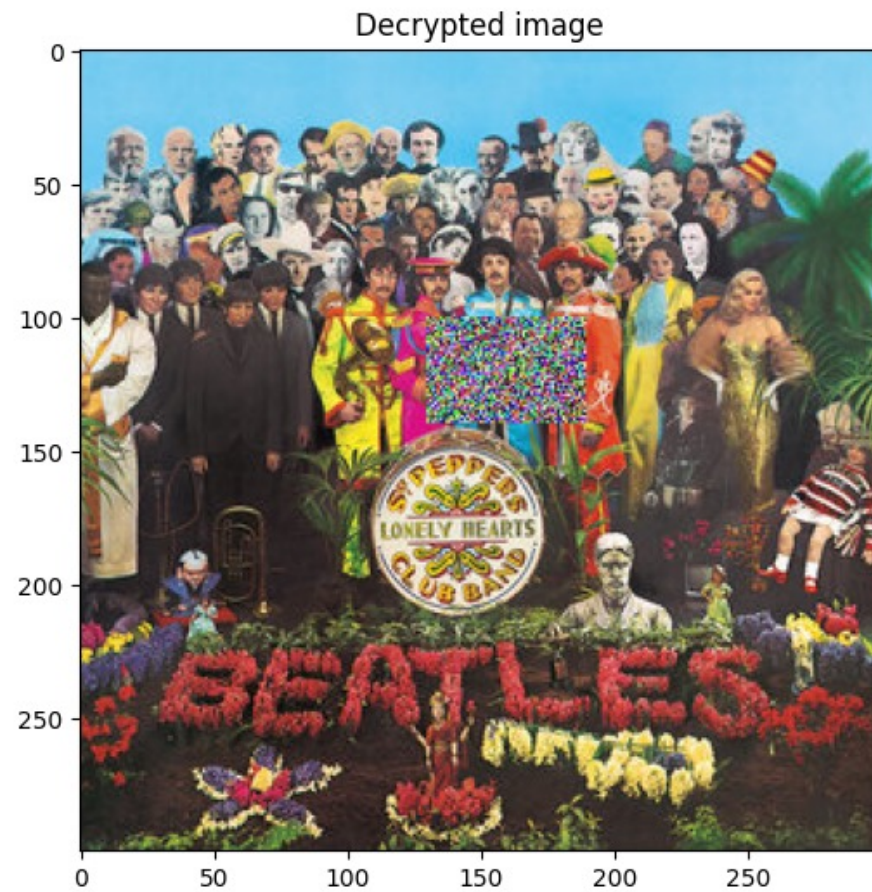
Results: Decrypted Image



Results: Added noise



Results: Added noise



Results: Time Analysis

on a 2.3 GHz i5 processor Macbook Pro with 8 GB of memory

Function	Description	Elapsed Time (sec)
Load Lorenz Trajectories (N=300*300)	Solve Lorenz system w/ specific initial conditions and parameters and calculate cipher values (PRNs)	15.678
Read Image	Read saved .png file into numpy arrays (encrypted & decrypted)	0.713
Encrypt Image	Encrypt image based on PRNs and pixel RGB	13.845
Decrypt Image	Decrypt image based on PRNs and pixel RGB	14.021

300x300 Image test

Function	Elapsed Time (sec)	Increase from 300x300 image processing time*
Load Lorenz Trajectories (N=1920*1080)	310.218	+1978.7%
Read Image	2.681	+376.0%
Encrypt Image	284.824	+2057.2%
Decrypt Image	291.122	+2076.3%
Total	888.845	+2008.4%

1920x1080 Image test

*image has x20 more pixels

Conclusion

- We find the Lorenz equations to be an effective tool for accomplishing Image Encryption.
 - Pseudorandom numbers can be injected into a simple encryption algorithm to encrypt image data sufficiently albeit slowly.
- The concise equations afford lower code complexity while the disorganized algorithm is likely to blame for most efficiency bottlenecks.
- Lorenz Equations provide sufficient chaotic behavior to employ adequate encryption techniques

Scope for improvements

- Higher levels of security are accomplished by adding layers of encryption.
- To improve this project, the key could be encrypted. [6][8]
 - Asymmetric encryption
 - End-to-end encryption
 - Public and private key
- Several papers have suggested using some form of "improved Lorenz system"[1][2][3][4]
 - Pixel permutation of rows and columns
 - Varying parameters

References

1. Zou, C., Zhang, Q., Wei, X., & Liu, C. (2020). Image encryption based on improved Lorenz system. *IEEE Access*, 8, 75728-75740.
 - <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9072440>
2. Kaur, M., & Kumar, V. J. E. L. (2018). Efficient image encryption method based on improved Lorenz chaotic system. *Electronics Letters*, 54(9), 562-564.
 - <https://ietresearch.onlinelibrary.wiley.com/doi/epdf/10.1049/el.2017.4426>
3. Huang, L., Shi, D., & Gao, J. (2016). The design and its application in secure communication and image encryption of a new Lorenz-like system with varying parameter. *Mathematical Problems in Engineering*, 2016.
 - <https://downloads.hindawi.com/journals/mpe/2016/8973583.pdf>
4. Arshad, U., Batool, S. I., & Amin, M. (2019). A novel image encryption scheme based on Walsh compressed quantum spinning chaotic Lorenz system. *International Journal of Theoretical Physics*, 58(10), 3565-3588.

References cont.

5. Peng, X., & Zeng, Y. (2020). Image encryption application in a system for compounding self-excited and hidden attractors. *Chaos, Solitons & Fractals*, 139, 110044.

- <https://www.sciencedirect.com/science/article/pii/S0960077920304410>

6. Narasimhan Aarthie and Rengarajan Amirtharajan, 2014. Image Encryption: An Information Security Perceptive. *Journal of Artificial Intelligence*, 7: 123-135.

- <https://scialert.net/fulltext/?doi=jai.2014.123.135>

7. Strogatz, S. H. (2018). *Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering*. CRC press.

References cont.

8. Pandya, D., Ram, K., Thakkar, S., Madhekar, T., & Thakare, B. (2015). Brief History of Encryption. *International Journal of Computer Applications*, 131(9), 28-31.
 - <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.741.6752&rep=rep1&type=pdf>
9. Lyon, R. F. (2006, February). A brief history of 'pixel'. In *Digital Photography II* (Vol. 6069, p. 606901). SPIE.
 - <http://www.dicklyon.com/tech/Photography/Pixel-SPIE06-Lyon.pdf>
10. Smith, A. R. (1995). A Pixel Is Not A Little Square, A Pixel Is Not A Little Square, A Pixel Is Not A Little Square!. *Microsoft Computer Graphics, Technical Memo*, 6.
 - http://alvyray.com/Memos/CG/Microsoft/6_pixel.pdf

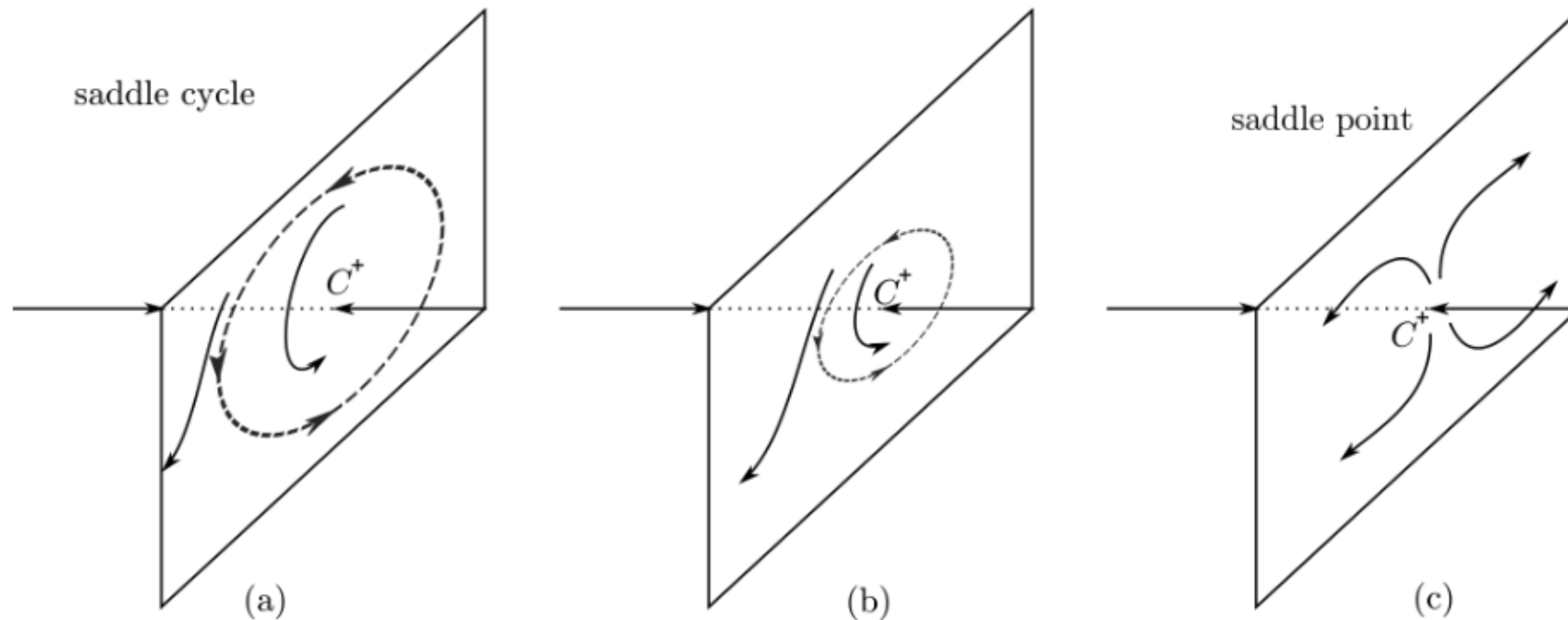
References cont.

11. Lorenz, E. (1962). Deterministic Nonperiodic Flow. *Journal of Atmospheric Sciences*. Volume 20 Issue 2, pages 130-141.
12. Lynnyk, V., et al (2015). Pseudo random number generator based on the generalized Lorenz chaotic system, 4th IFAC Conference on Analysis and Control of Chaotic Systems CHAOS 2015. Volume 48, Issue 18, pages 257-261.
13. McGuinness, P. (2022, January 26). *The Beatles album covers explained*. uDiscover Music. Retrieved August 14, 2022, from
 - <https://www.udiscovermusic.com/stories/the-beatles-album-covers-explained/>
15. Marsden, J. E., & McCracken, M. (2012). *The Hopf bifurcation and its applications* (Vol. 19). Springer Science & Business Media.

Additional slides:

Lecture 10, Hopf Bifurcation

The figure below shows exactly how the Hopf bifurcation occurs as r increases.



Be aware that the “planes” drawn, are really surfaces that will later evolve into the “wings of the Lorenz butterfly”. In part (c) of the figure, C^+ becomes a saddle point. This brings up an interesting question: where do the trajectories go? It turns out that they enter and remain inside an ellipsoid.

Lecture 10: Attractor Definition:

Definition 9.3.1. An **attractor**, A , is a closed set with the following properties:

- (a) A is invariant,
- (b) A attracts an open set of initial conditions, i.e. there is an open set U , with $A \subset U$ and $\mathbf{x}(0) \in U$ such that for any $\mathbf{y} \in A$, $\|\mathbf{x}(t) - \mathbf{y}\| \rightarrow 0$ as $t \rightarrow \infty$.
- (c) A is minimal, i.e. no subset of A can satisfy the previous two items.

The last item in the definition above can also be given as:

Transitivity: Given any points $\mathbf{y}_1, \mathbf{y}_2 \in A$ and any open neighborhoods U_j about \mathbf{y}_j in U , there is a solution curve that begins in U_1 and later passes through U_2 .

This condition is included to guarantee that we are looking at a single attractor rather than a collection of dynamically different attractors.

- $\sigma = K^{(-1)} \cdot \nu$ is the Prandtl number, where K is the coefficient of thermal expansion and ν is the viscosity;
- r , the Rayleigh number, is the bifurcation parameter.

always unstable. A simple computer program determines the regions of stability and instability in the b - σ plane. See Figure 4B.1

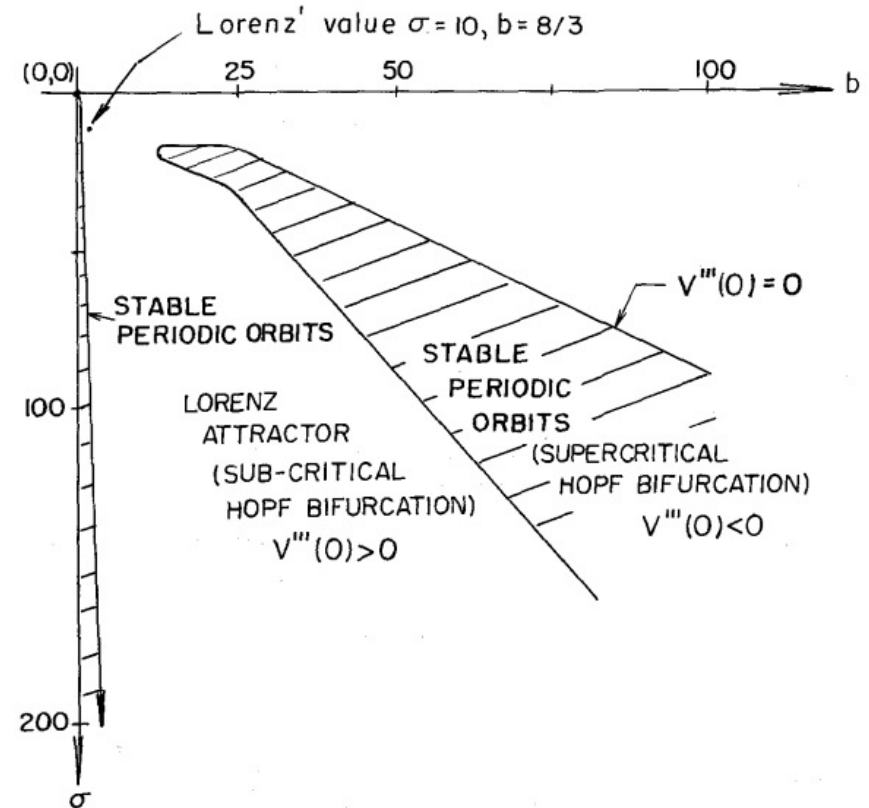


Figure 4B.1