Chaos: An Introduction to Dynamical Systems

Alligood provides an excellent course in the study of such dynamical systems. She successfully explains chaotic phenomena in nature using Linear Algebra, Differential Equations and Numeric Analysis. The book defines chaos as a field of study while introducing the idea of chaotic maps. These maps are recursive in nature, and are highly sensitive to initial conditions. Each iteration is mapped to a new phase-space for which the rate of separation of points in the sequence is directly related to the system's Lyapunov Exponents. There is one exponent for each degree of freedom the chosen system has. The scalar value of the exponent determines how the basis stretch ($LE > 1$) or shrink ($LE < 1$). Sequences created by such maps, though deterministic, can be unstable. These unstable sequences are known as chaotic orbits. This instability is statistically indistinguishable in nature to randomness, making them ideal candidates for providinging repeatable pseudo-random arrays.

A Review on Applications of Chaotic Maps in Pseudo-Random Number Generators and Encryption

In 2019 Naik and Singh gave a detailed review of Chaotic Neural Networks applications for encryption. The key aspect, as in many of the papers in this section is the creation of a viable generator. One way chaotic maps are used to generate a sequence of length **N**, which is equal to the byte-length of the plaintext file. These values are then converted to binary and one byte are taken from each value, often the first byte after the decimal point. This sequence is then reshaped to match the dimensions of the file being encrypted. The resulting matrices are then XORed with the original file masking the data. If we preform this action a second time, we will revert to the original data. This is extremely useful for the decryption process.

This paper also goes through another chaotic tool, diffusion, the act of swapping indices. The Arnold Cat Map (ACM)~[**?**] provides an efficient way to diffuse desired file prior to encrypting, but is most often used for image encryption only. After several iterations of this map on a matrix the original data is unrecognizable. It should be noted that orbits of ACM are finite, therefore if the map is iterated to the length of the orbit, all diffusion will be undone.

The largest takeaway of this paper is the review of an audio encryption model using sequences from the Henon and Tent maps. Said sequences are XORed to create a secret key. This secret key is then XORed with the audio file to encrypt. Their correlation coefficient between the plain and ciphered files were as low as 0.0014 with entropy was as high as 7.9995.

Comparison of Cryptography by Chaotic Neural Network and by AES

This 2019 paper by Skovajsová~ gives a step by step explanation of how AES encryption works and compares it to a prebuilt CNN@. Both algorithms were tested on five random images of each of the following sizes: 512b, 1024b, 2048b,

3KB, 30KB and 3MB@. For both ciphering and deciphering, the CNN significantly outperformed the AES model in terms of speed. The ciphertext created by both models were identical in size to the plaintext file, showing no degradation of information. It was noted that the CNN used here was a Hopfield network that 1D chaotic maps for its neural weights. 1D maps are much faster for generation, but only require a single initial value. If this initial condition is found by a bad actor, the algorithm will be broken. To counteract this, we will be building multiple layer networks of varying dimensionality, each requiring unique sets initial conditions.