# Chaotic Neural Networks and Its Applications

Christian Gould, Tushar Jain

# Introduction

The Hopfield neural network [3] is a type of recurrent neural network that acts as an associative memory, that enables storage of patterns which can be retrieved using an iteration scheme starting from a user provided input pattern. The Hopfield network is also capable of producing strings of binary data given input, and a threshold function. This capability can drive the network to utilities in production of binary sequences for cryptography. First, a modified Hopfield Network, M-AdNN, that make it chaotic and capable of recalling patterns in the same way as the human have been reviewed. Then lastly, a modification to the Hopfield Neural network that makes it chaotic and capable of creating a high entropy encryption scheme is also reviewed.

# Methodology

In its basic form, the Hopfield network updates the input $y$ using the following rule,

$$\begin{aligned} y_i(t+1) &= \Theta\big(\sum_{j\neq i} w_{ij}y_j(t) + b_i\big) \\ \Theta(z) &= \begin{cases} +1, & z > 0. \\ -1, & z \leq 0. \end{cases} \end{aligned}$$

where $b_i$ denotes bias of the $i$'th neuron.

The Hopfield neural network minimizes the energy function defined as,

$$E = -\sum_{i,j<i} w_{ij}y_iy_j - \sum_i b_iy_i$$

The weights matrix that minimizes the energy function is,

$$w_{ij} = \frac{1}{p}\sum_{s=1}^{p} x_i^s x_j^s$$

where $x^s$ represents the pattern that is to be stored in the network, if interpreted as an associative memory, with $p$ being the number of patterns to be stored.

## Pattern Recognition

In order to emulate the brain's behavior of recalling patterns from stimuli, Adachi's Neural Network (AdNN) [5] was proposed. It was that shown that M-AdNN [1] is a truly chaotic neural network, which exhibits periodicity when the input pattern closely resembles one of the stored states. The M-AdNN prevents being attracted to a local minima of the energy function by remaining in a chaotic state when the input pattern does not resonate with any of the stored patterns.

The M-AdNN updates the input pattern $y$ using the rule,

$$\begin{aligned} y_i(t+1) &= f(\eta_i(t+1) + \xi_i(t+1)) \\ \eta_i(t+1) &= k_f \eta_N(t) + \sum_{j=1}^{N} w_{ij} y_j(t) \\ \xi_i(t+1) &= k_r \xi_N(t) - \alpha y_i(t) + a_i \end{aligned}$$

Here, $f$ is the logistic function, $f(u) = \frac{1}{1+e^{\frac{-u}{\varepsilon}}}$, where $\varepsilon$ is the parameter that controls the steepness. The logistic function plays the role of squashing the parameters between 0 and 1. $k_f$ and $k_r$ are constant parameters, that have the biological significance of decay with respect to feedback inputs and refractoriness. $a_i$ is a constant external input to the $i^{\text{th}}$ neuron, which is taken to be $a_i = y_i$, in order to make network more receptive to the input. It is shown that M-AdNN is chaotic using analysis of the lyapunov spectrum. The M-AdNN has the Jacobian matrix, starting at the initial point $A$, is of the form

$$J(A) = \begin{pmatrix} [J^1_{ij}] & [J^2_{ij}] \\ [J^3_{ij}] & [J^4_{ij}] \end{pmatrix}$$

$J^1_{ij}(t) = \frac{\partial \eta_i(t+1)}{\partial \eta_j(t)}, J^2_{ij}(t) = \frac{\partial \eta_i(t+1)}{\partial \xi_j(t)}, J^3_{ij}(t) = \frac{\partial \xi_i(t+1)}{\partial \eta_j(t)}, J^4_{ij}(t) = \frac{\partial \xi_i(t+1)}{\partial \xi_j(t)}$

The Lyapunov exponents of the system are given by the natural logarithm of the eigenvalues of the matrix $\Lambda_A := [J(A)J(A)^T]^{\frac{1}{2}}$, which are discovered to be $\frac{1}{2}ln(N) + ln(k_f)$ and $\frac{1}{2}ln(N) + ln(k_r)$, and the rest of the Lyapunov exponents being $-\infty$. Therefore, if either of the finite Lyapunov are positive, the system exhibits chaotic behavior. Although, it appears that $k_f$ and $k_r$ determine the behavior of the system, it is also discovered that $\alpha$ also plays an important role as a bifurcation parameter [8]. As a system capable of pattern recognition, it can determined weather the M-AdNN has converged to a periodic orbit by studying computing the distance of the output from each of the stored patterns. The periodicity was measured to be the number of steps between each step where the output was observed to be close to the same stored pattern. After a few transient steps, it was observed that the inputs resonated with only one of the stored pattern. Although possible that the output can resonate with another stored pattern, the authors argued that they did not observe such behavior in the 1000 iterations that they ran. If it were the case that there was another attractor, its periodicity would be orders of magnitude higher than the relatively lower periodicity observed for the trained pattern initially. In such case, the input pattern is classified as the stored pattern with lower periodicity.

## Cryptography

We begin by considering [7] which discusses the following discrete Hopfield neural network of two neurons with two delays and two decays.

$$\begin{cases} x_{n+1} = a_1 x_n + T_{12} g_2(y_{n-k_2}) \\ y_{n+1} = a_2 y_n + T_{21} g_1(x_{n-k_1}) \end{cases} \quad \forall n \geq \max(k1, k2) \tag{1}$$

The paper [6] shows that if the activation functions $(g_1, g_2)$ satisfy specific conditions. When the magnitudes of the connection coefficients $T_{12}, T_{21}$, are "large enough", the neural network exhibits chaotic behavior near that fixed point.

$$b = T_{12} g_2(0)' \cdot T_{21} g_1(0)' \tag{2}$$

The initial conditions of the network, $(a_1, a_2, g_1, g_2, T_{12}, T_{21}, N_0)$ is the key-space of the cryptography scheme. Where The values $a_1$, and $a_2$ are the

decays, and $N_0$ is the Transient Number iterations of the Neural network. Finally the parameter $b$ is the characteristic parameter of the system which determines our bifurcations. The paper gives us the following specific example:

$$\begin{cases} x_{n+1} = \frac{1}{4}x_n + \sin(y_n - 2) \\ y_{n+1} = \frac{3}{4}y_n + b\tanh(x_n - 1)) \end{cases} \quad \forall n \geq 2 \tag{3}$$

## Encryption Scheme

First, we normalize the node data $t_k$ between zero and one. Where the following applies to $t \in (t_0, t_k)$

$$\frac{t_k - d}{e - d} = 0.b_1b_2b_3\ldots$$

Note that the above is for the output of any of the two nodes, while the purpose as described by the paper is to switch between nodes. Using the following Series, and threshold function, we can represent any $b_i(t)$ as follows

$$b_i(t) = \sum_{r=1}^{2^i-1}(-1)^{r-1}\Theta_{(e-d)(r/2^i)+d}(t)$$

$$\Theta_\tau \begin{cases} 0, t < \tau \\ 1, t \geq \tau \end{cases}$$

Using the above, we take the following steps to complete the algorithm

1. Take the plaintext message and divide it into chunks of length 4 bytes.
2. Having iterated 38 times; take 32 bytes and produce a Integer $A_j$
3. Take the remaining 6 bytes and take 5 for an integer $D_j$ and 1 for determining the next trajectory (x or y)
4. Using the plain-text $P_j$ created earlier, we permute both $P_j$ and $A_j$ by $D_j$ giving $P'_j$ and $A'_j$. Then finally xor $P'_j$ and $A'_j$

## Security Analysis

### Statistical Attack ( periodic/"pattern" attack )

In the Paper the authors discuss the approximately random histogram distribution of correlation between cipher-text and plain-text. The flatness of the curve indicates the algorithm's strong resistance to statistical attack. Between adjacent pixel pairs it is shown, that the sequences are highly independent of one another.

### Differential Attack ( "difference from original" attack)

By comparing the gradients of pixels of the original image to their surrounding pixels in the ciphered image, it is shown that there was a more than 98% difference between the original pixel and the cipher pixels. Showing the System to be strong against differential attack.

### Security Key Analysis

The Hopfield network is considered to have highly sensitive keys with respect to it's initial condition. The authors also note, that a secure cryptosystem requires a large key space. Using the example (3) we note that the available combination of initial conditions and activation functions, can be considered infinitely large, and thereby increases the usability, and security of the key-space, and ultimately the cryptosystem.

# Conclusion

We have shown that modifications to the Hopfield Network that make it chaotic and capable of recalling patterns in similar ways as the human brain. We also showed modifications to the Hopfield Neural network that makes it chaotic, and capable of creating a high entropy encryption scheme. These two systems together are examples of the applications of Chaotic Hopfield Neural Networks. Further study that could include both areas of research might be that of a layered encryption scheme that encrypts an unrecognizable image, only recognizable through decryption then iteration via the M-AdNN. Further study might also include using a greater number of nodes in order to determine the recognition value at greater scale, or in the encryption case, attempting to encode sound and video at speed, using FPGA's or other

dedicated hardware as well as a analysis of its entropy when compared to a quantum brute force algorithm.

# References


1. Calitoiu, D., Oommen, B.J. & Nussbaum, D. Periodicity and stability issues of a chaotic pattern recognition neural network. Pattern Anal Applic 10, 175–188 (2007). https://doi.org/10.1007/s10044-007-0060-3

2. Darau, Mirela & Kaslik, Eva & Balint, Stefan. (2012). Cryptography using chaotic discrete-time delayed Hopfield neural networks. Mathematics in Engineering, Science and Aerospace MESA. 1.

3. Hopfield, J.J. Neural networks and physical systems with emergent collective computational abilities. Proc. Natl. Acad. Sci. USA 1982. 79, 2554–2558.

4. Freeman WJ (1992) Tutorial in neurobiology: from single neurons to brain chaos. Int J Bifurcat Chaos 2:451–482

5. Adachi M, Aihara K (1997) Associative dynamics in a cha- otic neural network. Neural Netw 10:83–98

6. Adachi M, Aihara K, et al. "Chaotic Dynamics of a Delayed Discrete-Time Hopfield Network of Two Nonidentical Neurons with no self-connections." Journal of Nonlinear Science, Springer-Verlag, 1 Jan. 1997, link.springer.com/article/10.1007/s00332-007-9015-5.

7. Darau, Mirela, et al. "Cryptography Using Chaotic Discrete-Time Delayed Hopfield Neural Networks." Journal | MESA, 25 Feb. 2012, nonlinearstudies.com/index.php/mesa/article/view/703.

8. Qin, Ke & Oommen, B.. (2008). Chaotic Pattern Recognition: The Spectrum of Properties of the Adachi Neural Network.