ESANN'2000 proceedings - European Symposium on Artificial Neural Networks
Bruges (Belgium), 26-28 April 2000, D-Facto public., ISBN 2-930307-00-5, pp. 147-152

Toward Encryption with Neural Network Analogy

Toru Ohira

Sony Computer Science Laboratories
3-14-13 Higashigotanda, Shinagawa, Tokyo, Japan 141-0022
e-mail: ohira@csl.sony.co.jp

Abstract. We propose here a new model of encryption of binary data taking advantage of the complexity of dynamics of a model motivated by a neural network with delays. In this scheme, the encryption process is a coupling dynamics with various time delays between different bits (or neurons) in the original data. It is observed that decoding of the encrypted data may be extremely difficult without a complete knowledge of the coupling manner with associated delays for all bits of the data.

1. Introduction

Decoding of information from biological neural networks and its spike dynamics is one of the central and most difficult issues in neural network research. Complexity from non-linearity and many–body interactions of neural networks dynamics makes this task a very challenging one to be explored. In this paper, however, we reverse the question: we actually take advantage of this complexity and propose a new model toward encryption motivated by neural network modelings. In particular, we take a hint from neural network models with delay (see e.g. Marcus & Westervelt,1989; Hertz et al., 1991). The encryption process is identified by a coupling dynamics with nonlinear threshold function and various time delays between different bits, or neurons, in the original data. The model here is designed not for the public key encryption such as RSA but for the secret key encryption. Though the purpose of this paper is more of a proposal of a new direction of neural network resaerch than a presentation of completed work, we show that the model produces a complex behavior which could be useful in an encryption scheme.

2. Model

Let us now describe the model in more detail. $\mathbf{S}(0)$ is the original data of N binary bits, whose ith element $s_i(0)$ takes a value $+1$ or -1. The dynamics for the encryption can be specified by a "key" which consists of the following three parts:

(1) a permutation $\mathbf{P}$ generated from $(1, 2, 3, .., N)$,
(2) a delay parameter vector $\boldsymbol{\tau}$ which consists of N positive integers,
(3) a number of iterations of the dynamics T.

Given the key $K = (\mathbf{P}, \boldsymbol{\tau}, T)$ and weight matrics $\mathbf{W}$ (which may be included in the key), the dynamics is defined as

$$s_i(t+1) = s_{p_i}(t - \tau_i) \times \theta(\sum_{j=1}^{N} W_{ij} s_j(t)), \tag{1}$$

where p_i and τ_i are ith element of $\mathbf{P}$ and $\boldsymbol{\tau}$, respectively. (If $t - \tau_i < 0$, we set $t - \tau_i = 0$.) θ is a step function such that

$$\begin{aligned} \theta(x) &= +1, \quad (x > 0) \\ &= -1, \quad (x \leq 0). \end{aligned} \tag{2}$$

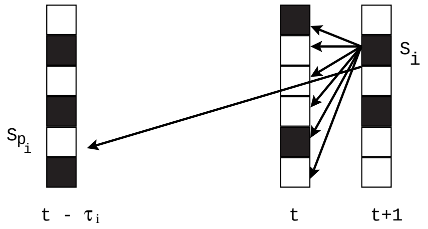


Figure 1: Sc hematic view of the model dynamics.

In Figure 1, this dynamics is sho wn schematically. The state of the ith element of $\mathbf{S}(t+1)$ is given b y the state of thep_ith element of $\mathbf{S}(t - \tau_i)$ and input from the state of all bits at time t. Thus this dynamics causes interaction between N bits of the data in both space and time. The encoded state $\mathbf{S}(T)$ is obtained by applying this operation of equation (1) iteratively T times starting from $\mathbf{S}(0)$.

3. Simulation Analysis

We inv estigate numerically the nature of the delayed dynamics from the perspectiv eof measuring the strength as an encryption scheme. (Hereafter, all w eigh tsW_{ij} are set to unity for simplicity.)

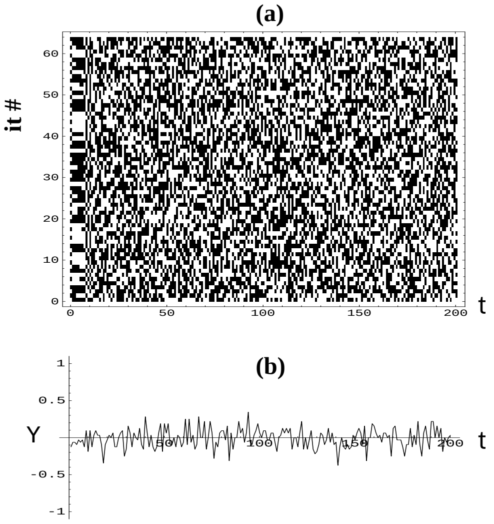
First, w e examinehow the state $\mathbf{S}(t)$ ev olv eswith time. In Figure 2(a) , we have shown an example of encoded states with different T using the same $\mathbf{P}$ and $\boldsymbol{\tau}$ for a case of $N = 64$. T obe more quantitativ e, w ecompute the

ESANN'2000 proceedings - European Symposium on Artificial Neural Networks
Bruges (Belgium), 26-28 April 2000, D-Facto public., ISBN 2-930307-00-5, pp. 147-152

following quantity as a measure of difference between two encoded states at different times t and t_f:

$$Y(t) = \frac{1}{N} \sum_{i=0}^{N} S_i(t) S_i(t_f) \tag{3}$$

A typical example is shown in Figure 2(b).



```
P =  {7,35,25,29,34,60,36,37,3,2
      42,43,63,38,64,4,52,40,13,4
      2,46,14,39,56,19,51,8,59,53
      6,57,5,33,26,61,27,32,21,10
      24,44,48,11,17,9,58,49,28,6
      5,1,18,45,12,41,30,20,16,23

τ =  {1,1,7,6,4,3,5,3,3,4,7,9,4,
      5,7,6,4,4,7,10,10,2,2,10,9,
      2,6,4,5,9,1,1,2,5,5,3,9,1,
      8,8,5,8,2,8,6,7,10,9,8,5,5,
      5,3,6,4,5,2,1,10,2,3,1,2,5}
```

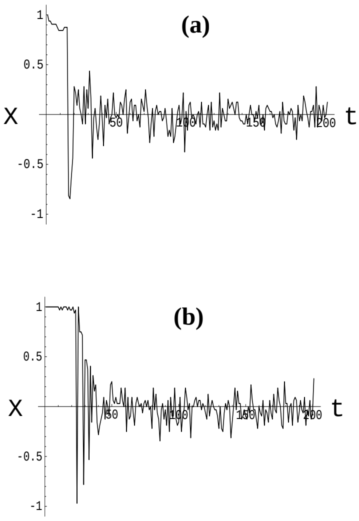
Figure 2: (a) Examples of encoding with the model dynamics from an initial state (odd bit $+1$; even bit -1) to $T = 200$ for $N = 64$ bits. The key is given as indicated. (b) Example of the correlation Y between encoded states at different time steps evaluated by equation (3). A case with $t_f = 200$ is plotted with the initial state and $\mathbf{P}$ and τ the same as in (a).

We note that the dynamics of our model has a property which generally gives us rather uncorrelated encoded states (i.e.,$Y \approx 0$) with different iteration times. This is a desirable property of the model as an encryption scheme: the same state can be encoded into uncorrelated states by changing T.

Next, we investigated the effect of a minor change of $\mathbf{P}$ and $\boldsymbol{\tau}$ on the model dynamics. Starting with the same initial condition, we evaluate how two states $\mathbf{S}(t)$ and $\mathbf{S}'(t)$ are encoded with slightly different $\mathbf{P}$ and $\mathbf{P}'$, respectively, by computing

$$X(t) = \frac{1}{N} \sum_{i=0}^{N} S'_i(t) S_i(t) \tag{4}$$

A representative result is shown in Figure 3(a). The same evaluation with $\boldsymbol{\tau}$ and $\boldsymbol{\tau}'$ is shown in Figure 3(b). These graphs indicate that if we take sufficiently large T, the same state can evolve into rather uncorrelated states with only a sligh t change of $\mathbf{P}$ and $\boldsymbol{\tau}$. This again is a favorable property in light of encryption. It makes iterativ e and gradual guessing of $\mathbf{P}$ and $\boldsymbol{\tau}$ in terms of their parts and elements very difficult: a nearly correct guess of the values of $\mathbf{P}$ and $\boldsymbol{\tau}$ does not help in decoding.



$$\begin{aligned}\mathbf{P'} = \{&7,35,25,29,34,60,\boxed{37,36},3,2\\&42,43,63,38,64,4,52,40,13,4\\&2,46,14,39,56,19,51,8,59,53\\&6,57,5,33,26,61,27,32,21,10\\&24,44,48,11,17,9,58,49,28,6\\&5,1,18,45,12,41,30,20,16,23\end{aligned}$$

$$\begin{aligned}\tau' = \{&1,1,7,6,4,3,5,3,3,4,7,9,4,\\&5,7,6,4,4,7,10,10,2,2,10,9,\\&2,6,4,5,9,1,\boxed{6},2,5,5,3,9,1,\\&8,8,5,8,2,8,6,7,10,9,8,5,5,\\&5,3,6,4,5,2,1,10,2,3,1,2,5\}\end{aligned}$$

Figure 3: Example of the correlation X ev aluated by equation (4) betw een t w o states encoded by slightly different (a) $\mathbf{P}$ and $\mathbf{P}'$, and (b) τ and τ'. The initial state and $\mathbf{P}$ and τ are the same as in Figure 2. The difference of $\mathbf{P}'$ from $\mathbf{P}$, and τ' from τ is indicated by the boxes.

Also, the model is designed such that a change of multiple bits in the initial state does not propagate to the encoded state as a simple superposition of change due to each changed bit. This is another desirable property for an encryption scheme. (This property is needed for robustness against certain types of cryptanalysis (or attac ks).) An example is shown in Figure 4 with $N = 8$. We have compared how the plaintext in the following evolves.

$$\begin{aligned}S &= (+1,-1,+1,-1,+1,-1,+1,-1)\\S^a &= (+1,-1,+1,-1,+1,-1,+1,+1)\\S^b &= (+1,-1,+1,+1,+1,-1,+1,-1)\\S^{ab} &= (+1,-1,+1,+1,+1,-1,+1,+1)\end{aligned}$$

The key is

$$\begin{aligned}\mathbf{P} &= (3,5,4,2,6,8,7,1)\\\tau &= (5,5,9,9,8,6,3,4)\end{aligned}$$

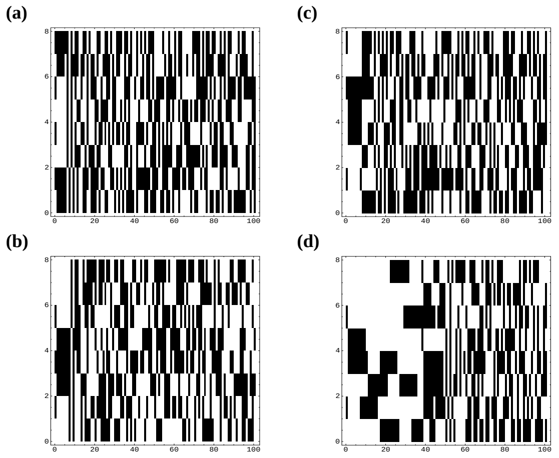


Figure 4: Encoding dynamics from slightly different initial conditions described in the text. The plaintexts are (a) S, (b) S^a, (c) S^b, (d) S^{ab}.

We observe that the evolution of S^{ab} cannot be decomposed simply to that of S^a and S^b when they are compared to the evolution of S. For example, with $T = 100$,

$$\begin{aligned} S(T) &= (-1,-1,-1,-1,-1,-1,+1,+1) \\ S^a(T) &= (+1,+1,-1,+1,-1,+1,+1,+1) \\ S^b(T) &= (+1,+1,+1,-1,-1,-1,-1,-1) \\ S^{ab}(T) &= (-1,+1,-1,-1,+1,-1,-1,+1) \end{aligned}$$

If an exhaustive search is applied to guess the key,we have a large space to search due to the factorial. Even if one knows N and τ_{max}, the largest element in $\boldsymbol{\tau}$, one is still required to search for the correct key from among $(N!)(\tau_{max})^N$ combinations and to guess T. DES (Data Encryption Standard), which has been commonly used until recently employs, 2^{56} bit keys (Menezes et al., 1996). We can obtain a similar order of search space with rather small values of N and τ_{max} due to factorial in N, for instance, $N \approx 11$ and $\tau_{max} \approx 10$.

4. Discussion

There are different methods possible for use of this model as a secure communication between two persons who share the key. One example is that the sender sends a series of encoded data in sequence for the interval between T and $T + \tau_{max}$ (or longer). The receiver can decode and recover the original data from this set of encoded data by applying a reverse dynamics with the key based on the following:

$$s_k(t) = s_u(t + \tau_u + 1) \times \theta(\sum_{j=1}^{N} W_{uj} s_j(t + \tau_u)), \ (p_u = k) \tag{5}$$

Or, in a situation where the data sent is a choice among multiple data sets known to the receiver, the receiver can run the encryption dynamics to all sets with the key for case matching.

Alternatively, one could possibly use this model as a one way function for a generation of a public key from a secrete key, for example. The model can be viewed as a special form of non-linear shift register also. Our preliminary numerical simulation with Kolmogorov-Smirnov test indicates that the associated dynamics could possess high degree of randomness.

The dynamical behavior of the model presented here is not analytically tractable as is often the case with delayed dynamical systems (e.g., Mackey & Glass, 1977; Cooke & Grossman, 1982; Ohira, 1997; Ohira & Sato, 1999). The model can be viewed as an extension of one previously proposed using delay (Ohira,1998) with the addition of nonlinearity used in neural network type models. The question of whether one could use this or related model toward encryption requires more thorough investigation from the point of view of information theory, evaluating such quantities like linear complexity, or order of correlation immunity. Neverthless, it is hoped that the model presented here will serve to call attention to the issue of encryption from the standpoint of neural network research.

References

1. Marcus, C. M. & Westervelt, R. M. (1989). Stability of Analog Neural Networks with Delay. *Physical Review A, 39*, 347–359.
2. Hertz, J. A., Krogh, A., & Palmer, R. G. (1991). *Introduction to the Theory of Neural Computation.* Redwood City: Addison–Wesley.
3. Menezes, A. J., van Oorschot, P., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography.* Boca Raton: CRC Press.
4. Mackey, M. C., & Glass, L. (1977). Oscillation and Chaos in Physiological Control Systems. *Science, 197*, 287–289.
5. Cooke, K.L., & Grossman, Z. (1982). Discrete delay, Distributed Delay and Stability Switches. *Journal of Mathematical Analysis and Applications, 86*, 592–627.
6. Ohira, T. (1997) Oscillatory Correlation of Delayed Random Walks, *Physical Review E, 55*, R1255–1258.
7. Ohira, T., & Sato, Y. (1999) Resonance with Noise and Delay, *Physical Review Letters, 82*, 2811–2813.
8. Ohira, T. (1998) Encryption with Delayed Dynamics, *Computer Physics Communications*, (To appear)