A Review Paper on ASCII Coded Cryptography for Artificial Neural Networking

Shreekalpa Sarkar[1] Srijeet Chatterjee[2]
[1,2]Department of Computer Engineering
[1,2]Netaji Subhash Engineering College India

Abstract— Cryptography is the method of altering data or information into unreadable for unauthorized persons. In cryptography method encrypted information transferred from sender to receiver in a manner that restricts from unlawful third person. There are many cryptography procedures available which based on number theory. The cryptography based on number system has some disadvantages such as large computational power, complexity and time consumption. Artificial neural network based cryptography is used to secure the data at high efficiency. The Artificial neural network have many distinctiveness such as learning, generation, less data requirement, fast computation, ease of implementation and software and hardware availability. It is important for many applications.

Key words: Artificial Neural Networking, ASCII Coded Cryptography

I. INTRODUCTION

Cryptography provides the information security for some functional applications for example in encryption, message digests and digital signature. A neural network is a device which is designed for modeling the way in which the brain performs a fussy task. Cryptography is defined as the exchange of data into mix code. Cryptography is also used in many applications such as computer passwords, ATM cards and electronic commerce.

Cryptography has two types of encryption data:

A. Symmetrical Encryption

In symmetrical encryption the same key is used for encryption and decryption process and it defines secret-keys, shared keys and private keys.

B. Asymmetric Encryption

In asymmetric cryptography uses different keys for encryption and decryption process. It has pair of keys one for encryption and one for decryption process

II. BIOLOGICAL MODEL

The human nervous system can be broken down into three stages that may be represented as follows:

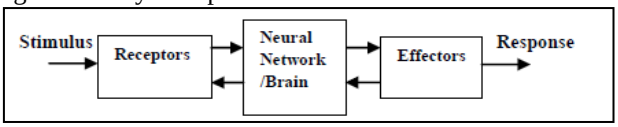

Fig. 1: Block Diagram of a Human Nervous System.

The receptors collect information from the stimulus. The effectors generate interactions with the activate muscles. The flow of information is represented by arrows. There is a hierarchy of interlink levels of organization: Molecules and Ions Synapses, Neuronal microcircuits, Dendritic trees Neurons, Local circuits, Interregional circuits, Central nervous system.

A. Artificial Neural Network

Artificial Neural Network is a system for processing and modeling information which reproduce the learning capability of biological systems in understanding and its activities.

ANN is used for a specific application, such as pattern recognition or data classification, through a learning process. Learning in biological systems involves adjustments to the synapses between nerve cells. ANNS have developed as generalizations of mathematical models of human process of acquiring knowledge and understanding through thought, experience, and the senses.

An Artificial Neural Network is a network of many very simple processors as units, each possibly having a small amount of local memory. The units are linked by unidirectional communication channels which hold numeric data. The units work only on their local data and on the inputs they obtain by means of the connections. The design drive is what distinguishes neural networks from other numerical techniques. A neural network is a processing device, either an algorithm, or actual hardware, whose design was motivated by the design and working of human brains and components.

There are many different types of Neural Networks, each of which has different strengths particular to their applications. The abilities of different networks can be related to their structure, dynamics and learning methods.

B. Cryptography using Artificial Neural Network

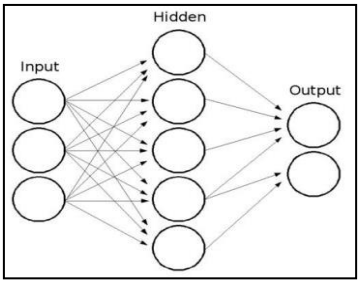

Fig. 2: The block diagram of trained ANN model.

The block diagram of the proposed ANN model is given in Figure 2. As shown in the figure, three initial conditions and time variable were applied to the inputs and three chaotic dynamics ˆx, ˆy and ˆz were obtained from the outputs of the ANN. For the training and test phases of the ANN, approximately 1800 input-output data pairs which belong to 24 different initial condition sets were obtained from Equation (4). A quarter of those 1800 data pairs were sorted to use in the test phase and the rest of data were used in the training phase.

Cryptography is the most important field of computer security providing secure services. It is the process of transferring private data through open network communication. Earlier cryptography was considered the domain of military and governments only. Everywhere the

All rights reserved by www.ijsrd.com

use computers and the advent of internet has made it an integral part of our daily lives. Today cryptography is at the heart of many secure applications such as online banking, online shopping, online government services such personal income taxes, cellular phones, and wireless LANS (Local Area Networks) etc.

III. Requirement of Cryptography

Cryptography is generally used in practice to provide four services: privacy, authentication, data integrity and non-repudiation. The goal of privacy is to ensure that communication between two parties remain secret. This often means that the contents of communication are secret; however in certain situations the of fact communication took place and must be a secret as well. Encryption is generally used to provide privacy in modern communication. Authentication of one or both parties during a communication is required to ensure that information is exchanged with the legitimate party. Passwords are common examples of one-way authentication in which users authenticate themselves to gain access to system.

IV. ASCII code

ASCII stands for American Standard Code for Information Interchange. Computers can only understand numbers, so an ASCII code is the numerical representation of a character such as 'a' or '@' or an action of some sort. ASCII was developed a long time ago and now the non-printing characters are rarely used for their original purpose. Below is the ASCII character table and this includes descriptions of the first 32 non-printing characters. ASCII was actually designed for use with teletypes and so the descriptions are somewhat obscure. If someone says they want your CV however in ASCII format, all this means is they want 'plain' text with no formatting such as tabs, bold or underscoring - the raw format that any computer can understand. This is usually so they can easily import the file into their own applications without issues. Notepad.exe creates ASCII text, or in MS Word you can save a file as 'text only.

V. Advantages

1) The advantages to this system are that it appears to be exceedingly difficult to break without knowledge of the methodology behind it.
2) It is tolerant to noise. Most messages cannot be altered by even one bit in a standard encryption scheme.
3) The system based on neural networks allows the encoded message to fluctuate and still be accurate.
4) Neural networks are ideal in recognizing diseases using scans since there is no need to provide a specific algorithm on how to identify the disease.
5) ANNs are used experimentally to implement electronic noses. Electronic noses have several potential applications in telemedicine. Telemedicine is the practice of medicine over long distances via a communication link.
6) There is a marketing application which has been integrated with a neural network system. The Airline Marketing Tactician (AMT) is a computer system made of various intelligent technologies including expert systems.

VI. Our proposed model

Parameter values of both ANNs in our experimental study are the following:

- Each input layer consists of 7 nodes, which represents the 7- bit blocks;
- Each hidden layer consists of 7 nodes;
- Each output layer consists of 7 nodes, used to define the decrypted output message;
- Fully connected networks;
- a sigmoid activate function; The Error function history SENDING AND RECEIVING MESSAGES In this model, a 7-bit plain text is entered (N = 7) and a 7-bit cipher text is the output (2N). Imagine that we want to send the following message:
- HELLO→"1001000100010110011001001100100111 1"
- WORLD→"1010111100111110100101001100100010 0"
- HELLOWORLD→"1001000100010110011001001100 1001111101011110011111010010100110010001000"

VII. Training data

A General n-state Sequential Machine will be required as described in the last chapter. As an example, the serial adder should be used in this machine.

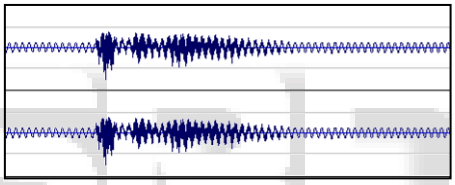

Fig. 5: The plotted graph of the error function after the learning process

The data from the state table of the Serial Adder needs to be entered into the program. The current state represents any previous carry that might be present whereas the next state represents the output carry. Thus, this sequential machine consists of 2 input, 1 output and 2 states. After the training data has been entered into the program, the back-propagation algorithm, to minimize the error function, executes.

ASCII BINARY ALPHABET

A	1000001	N	1001110
B	1000010	O	1001111
C	1000011	P	1010000
D	1000100	Q	1010001
E	1000101	R	1010010
F	1000110	S	1010011
G	1000111	T	1010100
H	1001000	U	1010101
I	1001001	V	1010110
J	1001010	W	1010111
K	1001011	X	1010111
L	1001100	Y	1011001
M	1001101	Z	1011010

Fig. 6: ASCII binary alphabet

References

[1] William Stallings, "Cryptography and Network Security: Principles and Practices", second edition.
[2] Aloha Sinha, Kehar Singh, "A Technique for Image Encryption using Digital Signature", Optics Communications, Vol.2 No.8 (2203), 229-234.

All rights reserved by www.ijsrd.com

[3] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, R. Tourki, "A Modified AES Based Algorithm for Image Encryption", World Academy of Science, Engineering and Technology 27 2007.
[4] K.Deergha Rao, Ch. Gangadhar, "Modified Chaotic Key-Based Algorithm for Image Encryption and its VLSI Realization", IEEE, 15th International. Conference on Digital Signal Processing (DSP), 2007.
[5] Saroj Kumar Panigrahy, Bibhudendra Acharya, Debasish Jen, "Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm", 1st International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008.
[6] http://www.asciitable.com/

All rights reserved by *www.ijsrd.com*