International Journal of Modern Science and Technology *Vol. 1, No. 7, October 2016. Page 230-235.*
http://www.ijmst.co/ ***ISSN: 2456-0235.***

Mini-Review

An Artificial Neural Network based Cryptosystem

R. Preethi, A. R. Rishivarman

Department of Mathematics, Theivanai Ammal College for women (Autonomous),
Villupuram 605 401. Tamilnadu, India.

*Corresponding author's e-mail: rishivarmanar@gmail.com

Abstract

Cryptography is the ability of changing information into obvious unintelligibility in a way allowing a secret method of un-mangling. The vital idea of cryptography is the capability to send information between participants in a way that prevents others from reading it. Much cryptography methods are available which are based on number theory but it has the disadvantage of requirement a large computational power, complexity and time consumption. To overcome these drawbacks, artificial neural networks (ANN's) have been applied to solve many problems. The ANN's have many characteristics such as learning, generalization, less data requirement, fast computation, ease of implementation, and software and hardware availability, which make it very attractive for many applications. The present paper provides a state-of-the-art review on the use of artificial neural networks in cryptography.

Keywords: Artificial neural network; Cryptography; Decryption; Encryption; Key generation.

Introduction

There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography. Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication There are, in general, three types of cryptographic schemes typically used to accomplish the goals secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into ciphertext, which will in turn (usually) be decrypted into usable plaintext [1].

Recently many investigations have been carried out by various researchers in Cryptography using Neural Networks. As such, few literatures are discussed below [2]. Zurada has discussed artificial neural network with respect to different learning methods and network properties. Supervised and unsupervised learning has been elaborated in detail with the help of network architecture. The usage of parameters for training is illustrated. The minimization of error functions in multilayer feed forward networks has been explained using the back propagation algorithm [3]. Koshy has emphasized on the problem solving techniques and their applications. With the help of Fermat's Little Theorem, we may find the least residues. Different cryptosystems and their algorithms illustrate the encryption-decryption methods. Depending on the key usage, the cryptosystem has been subdivided and explained in detail [4].

Kanter and Kinzel presented the theory of neural networks and cryptography based on a new method by the synchronisation of neural

Received: 17.10.2016; Received after Revision: 25.10.2016; Accepted: 25.10.2016; Published: 26.10.2016
©International Journal of Modern Science and Technology. All rights reserved.

networks for the secure transmission of secret messages. The encryption based on synchronisation of neural networks by mutual learning has been used which involves construction of two neural networks, where the synaptic weights are synchronised by the exchange and learning of mutual outputs for the given inputs. The network of one may be trained by the output of the other. In case, the outputs do not comply with each other, the weights are adjusted and updated using the Hebbian learning rule. The synchronisation of those two networks occurs in a definite time which tends to decrease with the increasing size of inputs. The author focuses on accelerating the synchronisation process from hundred of time steps to the least possible value and maintaining the security of the network at the same time [5].

Laskari studied the performance of artificial neural networks on problems related to cryptography based on different types of cryptosystems which are computationally intractable. They have illustrated various methods to address such problems using artificial neural networks and obtain better solutions. The efficiency of a cryptosystem may be judged by its computational intractability. This paper deals with the study of three problems, namely, discrete logarithmic problem, Diffie-Hellman key exchange protocol problem and factorisation problem. The artificial neural networks have been used to train a feed forward network for the plain and ciphered text using backpropagation technique. It aims to assign proper weights to the network in order to minimise the difference between the actual and desired output. The normalised data is fed to the network and then its performance is evaluated. The percentage of trained data and its near measure is evaluated [6].

Meletiou has discussed RSA cryptography and its susceptibility to various attacks. The author has used the artificial neural network for the computation of the euler totient function in the determination of deciphering key and hence, RSA cryptography may be easily forged. The multilayer feed forward network is used for training the data set with backpropagation of errors. Learning rate of network may not be ideal but is asymptotically approachable. The network performance is measured by using the complete and near measure of errors. Also the result has been verified for prime numbers ranging from high to low values [6].

Types of cryptographic algorithms

There are several ways of classifying cryptographic algorithms. Here they will be categorized based on the number of keys that are employed for encryption and decryption [7]. The three types of algorithms are shown in Fig. 1.

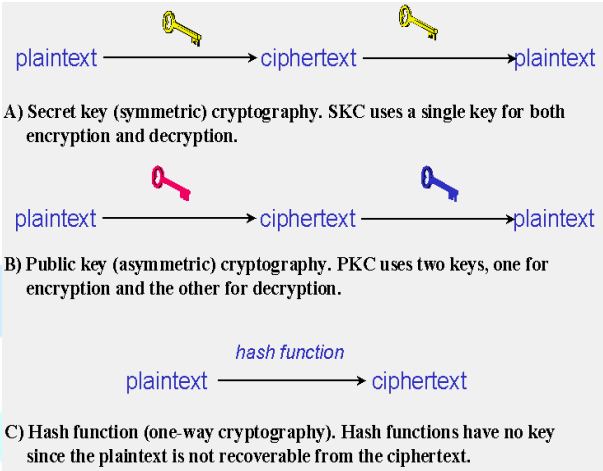

Fig. 1. Types of cryptographic algorithms

Secret key cryptography

With secret key cryptography, a single key is used for both encryption and decryption. As shown in the figure1, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key (or rules) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

Public key cryptography

Public-key cryptography has been said to be the most significant new development in cryptography in the last 300-400 years. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key. In PKC, one of the keys is designated the public key and may be advertised as widely as the owner wants. The other key is designated the private key and is never revealed to another party. It is straight forward to send messages under this scheme.

©International Journal of Modern Science and Technology. All rights reserved.

Hash functions

Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense, use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.

Artificial neural network

Artificial neural networks are parallel adaptive networks consisting of simple nonlinear computing elements called neurons which are intended to abstract and model some of the functionality of the human nervous system in an attempt to partially capture some of its computational strengths. Neural networks are non-linear statistical data modeling tools. The development of ANN's comes from simulating intelligent tasks which are performed by human brain. They are most widely used by soft computing techniques that have the capability to capture and model complex input/output relationships of any system.

The advantages of ANNs are the ability to generalize results obtained from known situations to unforeseen situations, the fast response time in operational phase, the high degree of structural parallelism, reliability and efficiency. If a set of input-output data pairs which belongs to a problem is available, ANNs can learn and exhibit good performance. For these reasons, application of ANNs has emerged as a promising area of research, since their adaptive behaviors have the potential of conveniently modeling strongly nonlinear characteristics [8].

Network Architectures

There are three fundamental different classes of network architectures [9].

Single-layer feed forward Networks

In a layered neural network the neurons are organized in the form of layers. In the simplest form of a layered network, we have an input layer of source nodes that projects onto an output layer of neurons, but not vice versa. This network is strictly a feed forward type. In single-layer network, there is only one input and one output layer as in Fig. 2. Input layer is not counted as a layer since no mathematical calculations take place at this layer.

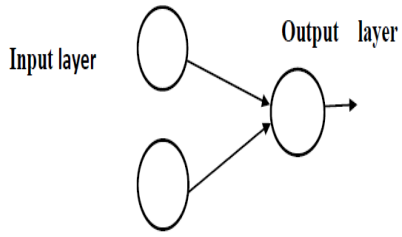

Fig. 2. Single–layer feed forward networks

Multilayer feed forward Networks

The second class of a feed forward neural network distinguishes itself by the presence of one or more hidden layers. The function of hidden neuron is to intervene between the external input and the network output in some useful manner. By adding more hidden layers, the network is enabled to extract higher order statistics. The input signal is applied to the neurons in the second layer. The output signal of second layer is used as inputs to the third layer as in Fig. 3, and so on for the rest of the network.

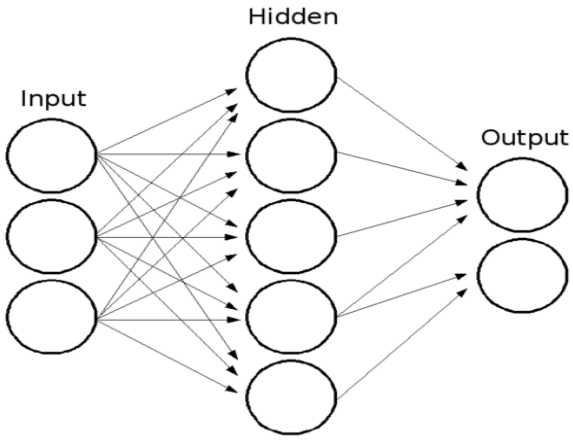

Fig. 3. Multilayer feedforward network

Recurrent networks

A recurrent neural network has at least one feedback loop. A recurrent network may consist of a single layer of neurons with each neuron feeding its output signal back to the inputs of all the other neurons as in Fig. 4. Self-feedback refers to a situation where the output of a neuron is fed back into its own input. The presence of feedback loops has a profound impact on the

©International Journal of Modern Science and Technology. All rights reserved.

learning capability of the network and on its performance

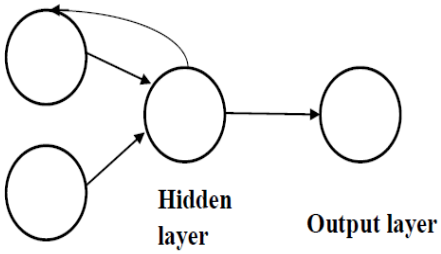

Fig. 4. Recurrent network

Neural cryptography

It is a branch of cryptography dedicated to analyzing the application of stochastic algorithms, especially neural network algorithms, for use in encryption and cryptanalysis. Neural Networks are well known for their ability to selectively explore the solution space of a given problem. This feature finds a natural niche of application in the field of cryptanalysis.

At the same time, Neural Networks offer a new approach to attack ciphering algorithms based on the principle that any function could be reproduced by a neural network, which is a powerful proven computational tool that can be used to find the inverse-function of any cryptographic algorithm. The ideas of mutual learning, self learning, and stochastic behavior of neural networks and similar algorithms can be used for different aspects of cryptography, like public-key cryptography, solving the key distribution problem using neural network mutual synchronization, hashing or generation of pseudo-random numbers [10].

Block diagram of process of a behavior of neural networks

This model presents an attempt to design an encryption system based on artificial neural networks of the backpropagation type as in Fig 5. The proposed ANN has been tested for various numbers of plain text. The simulation results in Table1 have shown very good results [11]. The neural network works reliably and absolutely no errors are found in the outputs. During encryption; the neural network also works reliably during the decryption process, which is the reverse of Encryption process.

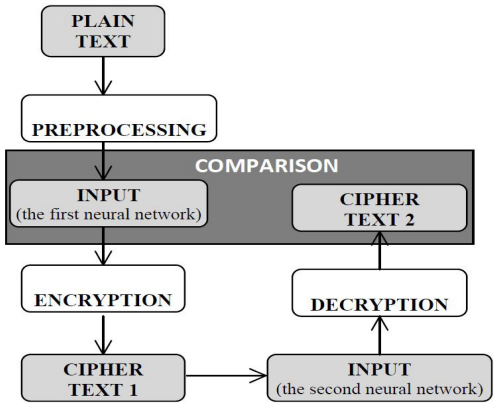

Fig. 5. Tested process behavior of neural networks

Thus the neural net application represents a way of the next development in good cryptography. The limitations of this type of system are few, but potentially significant. This is effectively a secret-key system, with the key being the weights and architecture of the network. With the weights and the architecture, breaking the encryption becomes trivial. However, both the weights and the architecture are needed for encryption and decryption. Knowing only one or the other is not enough to break it [12].

Advantages

The advantages of this system are that it appears to be exceedingly difficult to break without knowledge of the methodology behind it, In addition, it is tolerant to noise. Most messages cannot be altered by even one bit in a standard encryption scheme. The system based on neural networks allows the encoded message to fluctuate and still be accurate [13].

Conclusion

In the present paper, we illustrated some recent researches on the application of Artificial Neural Network in the field of cryptography. The designed ANN-based cryptosystem is a good idea of building very complicated cryptosystem, where the crypto analyst or the cracker not just need the topology of the ANN and the key to crack the system, but also need to know the number of adaptive iterations and the final weights for the encryption and decryption systems. Applying higher numbers of plain-text/cipher-text to the ANN-based cryptosystem so as to make the error rate as minimum as possible. The common attacks in cryptography such as known plain text attack, Brute Force Attack, Differential Attack may not be so easy in

©International Journal of Modern Science and Technology. All rights reserved.

case of data encryption using Neural Networks. Lastly, according to the survey of this work, the trend for the years to come regarding the use of ANN's for cryptography tasks will be focused mainly on Tree Parity Machines (TPM), Chaotic Neural Networks (CNN) and Layer Recurrent Neural Network (LRNN).

Table1. The simulation results

THE PLAIN TEXT			THE CIPHER TEXT
Char	ASCII Code (DEC)	The Chain of bits	The chain of bits
0	48	110000	111111
1	49	110001	110010
2	50	110010	101100
3	51	110011	111010
4	52	110100	101010
5	53	110101	100011
6	54	110110	111000
7	55	110111	000111
8	56	111000	010101
9	57	111001	110011
Punct.	32	100000	101111
Others	0	000000	011101
A	97	000001	000010
B	98	000010	100110
C	99	000011	001011
D	100	000100	011010
E	101	000101	100000
F	102	000110	001110
G	103	000111	100101
H	104	001000	010010
I	105	001001	001000
J	106	001010	011110
K	107	001011	001001
L	108	001100	010110
M	109	001101	011000
N	110	001110	011100
O	111	001111	101000
P	112	010000	001010
Q	113	010001	010011
R	114	010010	010111
S	115	010011	100111
T	116	010100	001111
U	117	010101	010100
V	118	010110	001100
W	119	010111	100100
X	120	011000	011011
Y	121	011001	010001
Z	122	011010	001101

Acknowledgement

The authors are thankful to referees for their valuable comments and suggestions for improving this paper.

Conflict of interest

Authors declare there are no conflicts of interest.

References

[1] Stallings W. Cryptography and Network Security: Principles and Practice (5th Edition). Prentice Hall, 2010.

[2] Volna E, Kotyrba M, Kocian V, Janosek M. Cryptograpy based on neural network. Journal of Engineering Science and Technology 2 (2014) 37-48.

[3] Jacek M, Zurada. Introduction to artificial neural systems. West Publishing Company, St. Paul, 1992.

[4] Ghosh A, Nath A. Cryptography algorithms using artificial neural network. International Journal of Advance Research in Computer science and Management studies 2 (2014) 375-381.

[5] Kinzel W, Kanter I. Neural Cryptography. International Journal of Soft Computing 4 (2003) 147-153.

[6] Laskari EC, Meletiou GC, Tasoulis DK, Vrahatis MN. Performance of ANN related to cryptography, Elsevier, 2005.

[7] Komal T, Ashutosh R, Roshan R. Encryption and decryption using artificial neural network. International Advanced Research Journal in Science, Engineering and Technology 2 (2015) 45-64.

[8] Fausett LV. Fundamentals of artificial Neural Networks. Prentice-Hall, Inc, Englewood Cliffs, New Jersey, 1994.

[9] Chakraborty RC. Fundamentals of Neural Networks. Lecture Notes, 2010. Available at http://www.myreaders.info/assets/applets/08_Neural_Networks.pdf

[10] Klein E, Mislovaty R, Kanter I, Ruttor A, Kinzel W. Synchronization of neural networks by mutual learning and its application to cryptography. International Journal of Network Security 7 (2004) 56-72.

[11] Adel A. Zoghabi, Amr H. Yassin, Hany H. Hussien. Cryptography based on neural networks. International Journal of Emerging Technology and Advanced Engineering 3 (2013) 47-69.

©International Journal of Modern Science and Technology. All rights reserved.

[12] Pointcheval D. Neural networks and their cryptographic applications, in Proc. of the IEEE Symposium on Foundations of Computer Science, 1993. pp. 586-597.

[13] Jha GK. Artificial neural networks and its applications. I.A.R.I, New Delhi, 1993.

[14] Wasnik TP, Patil V, Patinge S. Cryptography as an instrument to network security. International Journal of Application or Innovation in Engineering and Management 2 (2013) 72-80.

[15] Godhavari T, Alainelu NR, Soundararajan R. Cryptography using neural network, IEEE 2005. pp. 258-261.

*****

©International Journal of Modern Science and Technology. All rights reserved.