Data Security using Genetic Algorithm and Artificial Neural Network

Mr. Mohana, K. V. K. Venugopal, Sathvik H. N.

Abstract – By making use of Genetic Algorithm, Optimization problems can be solved and the best fit individual can be selected out of a given population. Artificial Neural Networks, a part of Artificial Intelligence, are used to simulate Human Intelligence on a machine. Cryptography is the science and art of encrypting data so that only the intended receiver can decrypt and retrieve the original data. This paper makes use of both Genetic Algorithm and Artificial Neural Networks for encryption and decryption of digital data. Genetic Algorithm is firstly used to generate two random numbers, both of which are later used as initial parameters for the Neural Network. The weights and bias of the Neural Network are created using the initial parameters by a specific procedure as decided by the user. The receiver who knows the initial parameters can decrypt and retrieve the original data, but the one without those parameters cannot retrieve the original data. This ensures optimal security of data over an open channel.

Index terms – Artificial Intelligence, Artificial Neural Network, Chaotic Neural Network, Decryption, Encryption, Genetic Algorithm,Security.

------------------------*-------------------------

1 INTRODUCTION

The ability to build a secure channel is one of the most challenging fields of research in modern communication. Since the secure channel has many applications, in particular for mobile phone, satellite and internet-based communications, there is a need for fast, effective and secure transmission protocols. Nowadays, information security has become an important aspect in every organization. The people have to be assured that the information is to be read by only the sender and the receiver. There comes the role of Cryptography, which ensures the secure transmissions of data.

Cryptography is the exchange of confidential information among the users without leakage of information to a third person. Cryptology was as significant as weapons during the World War II and the Cold War. There were lots of studies to develop robust crypto-systems and to use them in communications. These studies have continued up to now. In spite of all such studies and implementations, this field has some loop holes or drawbacks. Howsoever there is topmost security, sometimes it happens that the data is leaked or stolen or manipulated by wrong hands. Such things can be of major concerns sometimes, especially of national importance or personal importance. To deal with such conflicts in cryptography, researchers have made use of artificial intelligence, a field which uses the concept of self-learning and adaptation by machine itself, i.e. and intelligent or smart machine which can change its behaviour as per the demand of the situation.

Artificial Intelligence (AI) is a branch of computer science that emphasis on developing intelligent machines and software using applied logic. It claims the simulation of intelligence of humans by a machine by employing reasoning, learning, communication and manipulation. AI is found to have intense applications in various fields such as medical diagnosis, stock trading, robot control, law and remote sensing. One of the important and our field in AI is Artificial Neural Networks (ANN). An Artificial Neural Network (ANN) is a mathematical model consisting of an interconnected group of artificial neurons motivated by the working of brain. The brain learns from experience and adaptation to environment. Also, inter neuron connection strengths, called weights, are used to store the acquired knowledge. ANN is a nonlinear parallel adaptive system that is used to model variegated relationships between inputs and outputs. The output of a unit is decided by I/O characteristics while the overall working of ANN is determined by its structure and the training algorithm.

Advantages of ANN include adaptive interaction between elements, self-organization, real time operation, parallel computation, and Fault Tolerance. ANN helps in handling complex problems and are used in robotics, pattern recognition, medicine, manufacturing, optimization, signal processing, system modelling & identification, control of power-generation systems.

ANN also suffers from optimization problems, like getting the best values for weights. One of such algorithm used for solving optimization problems is Genetic Algorithm (GA). The main idea behind Genetic Algorithms (GAs) is to replicate the randomness of the nature where population of individuals adapts to its surroundings through natural selection process and behaviour of natural system. GAs produce a population in such a way that the trait which is dominant, that is has higher fitness value is replicated more likewise rest is rejected based on threshold which is then evolved by the iterative application of a set of stochastic operators like mutation, crossover, and selection. Highest rank signifies the better fitness.

We use both GA and ANN in cryptography to make the encryption more secure and almost non-vulnerable to any intruder from breaking into it. For that, we first make use of GA to create random numbers which will be serving as confidential parameters for initiating the chaotic ANN which will convert the input data bits into a cipher form and the original data can only be recovered if the receiver has the information of both the initiating parameters.

2 LITERATURE SURVEY

Many Research papers dealing with applications of Neural Networks and Genetic Algorithm in cryptography have been studied and analysed to get an idea of the previous attempts made in this field. It was found that the use of ANN along with GA has not as yet been explored. It is essential for a key to possess randomness for key strength and security and thus making the code hard to break.

One of the papers presents Public key cryptography using artificial Neural Networks and Genetic Algorithm [1] in which Random Numbers are generated with high randomness using genetic algorithm. Other paper presents cryptography using neural networks [2] in which the mutual learning of two neural networks has been used for encryption. Other paper present An Empirical investigation of using ANN based N-state sequential machine and chaotic neural networks [3].

Other thesis presents Genetic algorithms in Cryptography [4] in which the use of genetic algorithms in field of cryptography is presented. Other paper presents The Theory of Neural Networks and Cryptography [5] which also deals with n-state sequential machine and chaotic neural network. A textbook Artificial intelligence, A modern approach by J. Russell and Peter Norvig [6] has been referred to study some basics of Artificial Intelligence. [7] also presents some typical applications of Artificial Neural Networks in the Field of Security. [8] presents Cryptography using N-state Sequential Machine as well as Chaotic Neural Network. [9] presents Chaotic Neural Generator which is used in Cryptography.

3 RANDOM NUMBER GENERATION USING GENETIC ALGORITHM

Genetic Algorithm begins with an initial population generation. Next the fitness of each individual is calculated according to a given fitness or objective function. Based on this fitness, the next generation is selected. Now two parents are selected at random from the next generation individuals and reproduction is performed. For this, cross-over is done by randomly making a cut point and converging the bits accordingly. After crossover, mutation is performed which involves the flipping of any randomly selected bit in the individual, or by using any specific mutation function. Again a new population is generated which serves as the initial population for the next generation. This process continues until the GA reaches the fittest value, or it is stopped by a user defined criteria. This may be the bounds of number of generations or the fitness values. After stopping the process, GA displays the final result of the fittest individual and its fitness.

4 ALGORITHM FOR CHAOTIC NEURAL NETWORK

Artificial Neural Networks (ANN) claims the simulation of intelligence of human by a machine by employing reasoning, learning, communication and manipulation. We have used the Chaotic Neural Network (CNN) for encryption and decryption of data, which is different from other neural networks in the sense that the weights and biases of such a neural network are always chaotic, i.e. extremely random and disordered so that any outsider or third parties cannot break in and steal the data due to strong encryption. The chaotic parameters for chaotic neural network is provided by GA. GA generate a random number in every execution which is almost unpredictable. We can generate both the initial weight as well as the bias using GA and feed it to the neural network. This CNN will now process the parameters according to its algorithm and generate encrypted keys for the given input data.

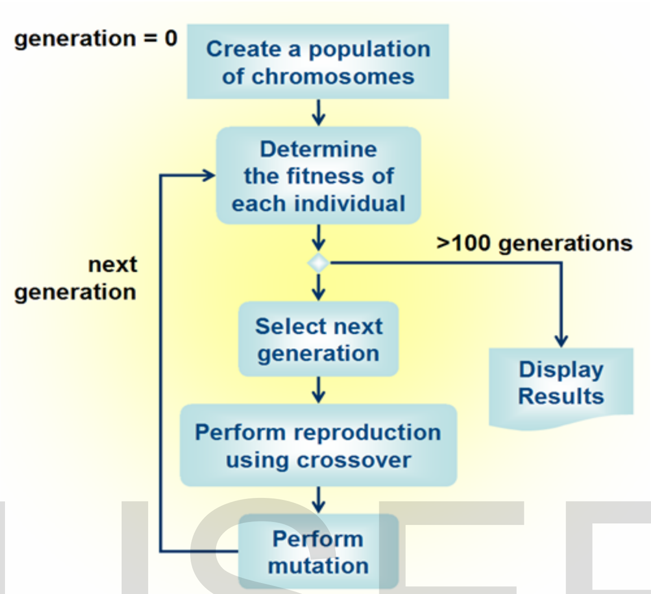

generation = 0
Create a population of chromosomes
Determine the fitness of each individual
>100 generations
next generation
Select next generation
Display Results
Perform reproduction using crossover
Perform mutation

Fig. 1. Genetic Algorithm Flowchart

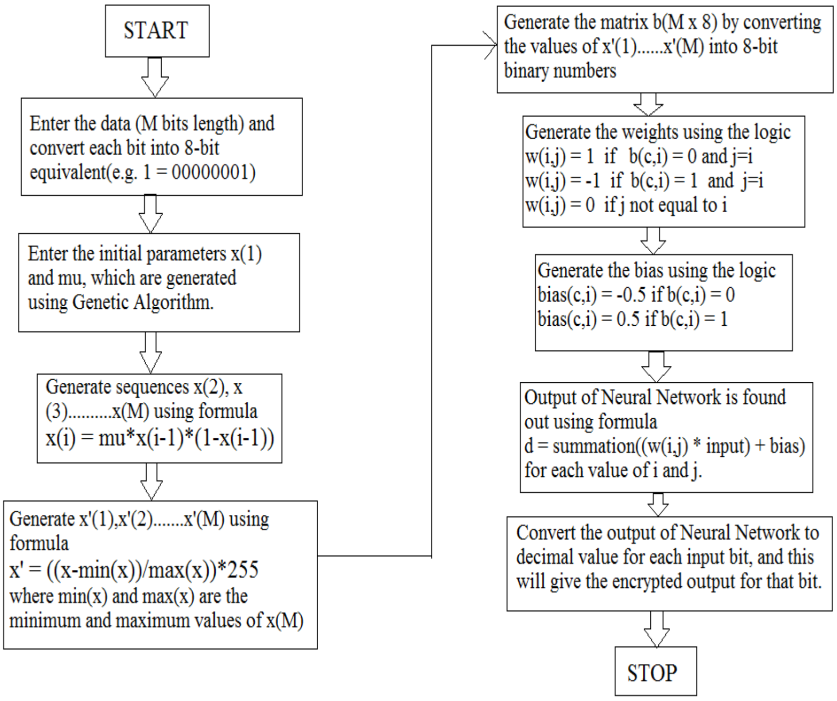
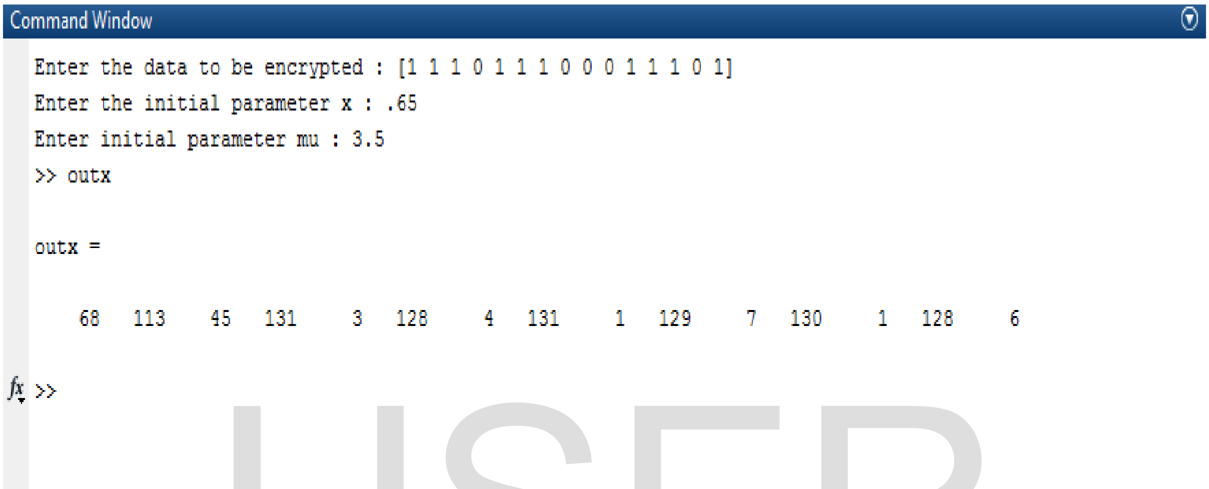

START
Enter the data (M bits length) and convert each bit into 8-bit equivalent(e.g. 1 = 00000001)
Enter the initial parameters x(1) and mu, which are generated using Genetic Algorithm.
Generate sequences x(2), x (3)..........x(M) using formula x(i) = mu*x(i-1)*(1-x(i-1))
Generate x'(1),x'(2).......x'(M) using formula x' = ((x-min(x))/max(x))*255 where min(x) and max(x) are the minimum and maximum values of x(M)
Generate the matrix b(M x 8) by converting the values of x'(1)......x'(M) into 8-bit binary numbers
Generate the weights using the logic w(i,j) = 1 if b(c,i) = 0 and j=i w(i,j) = -1 if b(c,i) = 1 and j=i w(i,j) = 0 if j not equal to i
Generate the bias using the logic bias(c,i) = -0.5 if b(c,i) = 0 bias(c,i) = 0.5 if b(c,i) = 1
Output of Neural Network is found out using formula d = summation((w(i,j) * input) + bias) for each value of i and j.
Convert the output of Neural Network to decimal value for each input bit, and this will give the encrypted output for that bit.
STOP

Fig. 2. Chaotic Neural Network Coding Logic

5 Results And Analysis

We have obtained the encryption of digital data in MATLAB, as mentioned in snapshot below. And the same CNN is used to obtain the decrypted data, provided that the weight and bias is same as that provided in the encryption stage. We have used the values x (0) = 0.65 and μ = 3.5 for initialization and have achieved encryption of digital data successfully. For the decrypted data to be same as the original data, the values of initial parameters must be same. This concept is illustrated in the tables which show that different values of initial parameters will lead to different output, i.e. different from the original data.



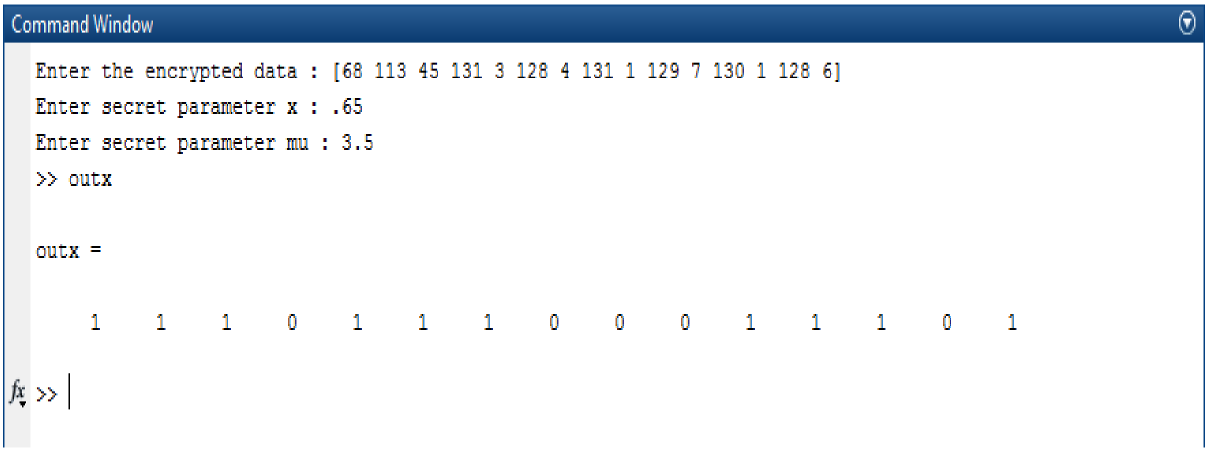
```
Enter the data to be encrypted : [1 1 1 0 1 1 1 0 0 0 1 1 1 0 1]
Enter the initial parameter x : .65
Enter initial parameter mu : 3.5
>> outx

outx =

    68   113    45   131     3   128     4   131     1   129     7   130     1   128     6

fx >>
```

Fig. 3. MATLAB Command Window for Encryption using CNN



```
Enter the encrypted data : [68 113 45 131 3 128 4 131 1 129 7 130 1 128 6]
Enter secret parameter x : .65
Enter secret parameter mu : 3.5
>> outx

outx =

     1     1     1     0     1     1     1     0     0     0     1     1     1     0     1

fx >>
```

Fig. 4. MATLAB Command Window for Decryption using CNN

TABLE 1
DIFFERENT INPUT DATA AND CORRESPONDING ENCRYPTED DATA

Original data	Value of x(1)	Value of µ	Encrypted data
[1 0 1 1 0 1 1 0 1 1 0]	0.6500	3.5000	[69 111 42 131 1 129 5 130 1 129 5]
[1 0 1 0 1 1 0 0 0 1 1]	0.6500	3.5000	[69 111 42 130 0 129 4 130 0 129 4]
[0 1 1 0 0 1 1 0 1]	0.6500	3.5000	[68 110 42 130 1 129 5 130 1]
[1 1 1 1 0 0 1 0 0 1]	0.6500	3.5000	[69 110 42 131 1 128 5 130 0 129]
[1 1 0 1 1 0 0 0 0 1 1]	0.6500	3.5000	[69 110 43 131 0 128 4 130 0 129 4]

TABLE 2
DECRYPTED DATA OBTAINED FROM DIFFERENT INITIAL PARAMETERS

Encrypted data	Different values of x(1)	Different values of µ	Decrypted data
[69 111 42 131 1 129 5 130 1 129 5]	0.5500	4.5000	[186 144 213 124 254 126 250 125 254 126 5]
[69 111 42 131 1 129 5 130 1 129 5]	0.8500	7.8000	[186 144 213 124 254 126 250 125 254 126 5]
[69 111 42 131 1 129 5 130 1 129 5]	0.7500	5.5000	[186 144 213 124 254 126 250 125 254 126 5]
[69 111 42 131 1 129 5 130 1 129 5]	0.2900	5.4500	[186 144 213 124 254 126 250 125 254 126 5]
[69 111 42 131 1 129 5 130 1 129 5]	0.6500	3.5000	[1 0 1 1 0 1 1 0 1 1 0]

6 CONCLUSION

We have Generated Random numbers x(1) and µ using Genetic Algorithm toolbox in MATLAB. The random numbers are generated between the bounds 0 and 1 for x(1) and 1 and 5 for µ. These two random numbers are given as initial parameters to the Chaotic Neural Network (CNN). CNN generates the weights and bias using a specified logic or formula which are required to process the input bits. After processing, the Neural Network generates a unique key as its output for each individual input bit given as input. In this way we have encrypted the original data into a form which can be reconstructed only using the two initial parameters x(1) and µ.In receiver side, after receiving the encrypted data now we need to decrypt it to achieve the original data. For this purpose we again need the same encryption keys which were used as initial parameters for encryption, i.e. x(1) and µ. The algorithm for decryption is same as the encryption, the only difference being the input data. Now we give the encrypted data as input to the same CNN and get the original data as the output.

7 ACKNOWLEDGMENT

The authors thank and gratefully acknowledge the support of Mr. Mohana(RVCE, Bangalore), Dr. K. Sreelakhsmi(RVCE, Bangalore), Dr. H. V. Kumaraswamy(RVCE, Bangalore) and Dr. B. S. Satyanarayana(RVCE, Bangalore).

8 REFERENCES

[1] Smita Jhajharia, Swati Mishra, Siddharth Bali. : “Public Key Cryptograpy Using Neural Networks and Genetic Algorithms”, IEEE Trans. 978-1-4799-0192-0/13/©2013 IEEE

[2] T. Godhavari, N. R. Alainelu and R. Soundararajan "Cryptography using neural network”, IEEE INDICON 2005 Conf., Chennai, India, pp. 258-261, 11-13 Dec. 2005.

[3] https://globaljournals.org/GJCST_Volume12/3-An-Empirical-Investigation-of Using-ANN.pdf

[4] B. Delman, “Genetic algorithms in cryptography”, M.S. thesis, Rochester Institute of Technology, Rochester, New York, July 2004.

[5] I. Kanter, W. Kinzel. : “The Theory of Neural Networks and Cryptography”, Quantum Computers and Computing, V. 5, No.1, 2005

[6] Stuart J. Russell, Peter Norvig, “Artificial Intelligence – A Modern Approach”, Prentice Hall 2005

[7] Navita Agarwal, Prachi Agarwal : “Use of Artificial Neural Networks in the field of Security”, Vol. 3, No.1, Jan. 2013, pp. 42-44 ISSN 2230-7621 © MIT Publications

[8] Nitin Shukla, Abhinav Tiwari : “An Empirical Investigation of Using ANN Based N-State Sequential Machine and Chaotic Neural Network in the Field of Cryptography”, Global Journal of Computer Science and TechnologyNeural & Artificial Intelligence Volume 12 Issue 10 Version 1.0 Year 2012, Online ISSN: 0975-4172 & Print ISSN: 0975-4350

[9] Ilker DALKIRAN, Kenan DANIS¸MAN “Artificial neural network based chaotic generator for cryptology”, Turk J Elec Eng & Comp Sci, Vol.18, No.2, 2010, c_ T¨UB˙ITAK doi:10.3906/elk-0907-140.