Cryptography Using Artificial Intelligence

Arpita Gupta[1], Poonam Tiwari[2] Deepak Nagaria[3]
1,2. M.Tech Scholar 3. Professor
Department of Electronics & Communication
Bundelkhand Institute of Engineering & Technology,
Jhansi, India.

Abstract

Cryptography is the secret code science of writing. Not only does it protect information from theft, it can also be used to authenticate users. Public keys are available in the feed-forward learning algorithm, depending on the number theory where the information or input travels in one direction and has the barrier that requires enormous computing energy, complexity and time consumption during the feed-forward learning generation of key. A neural network with a combination of feed forward & back propagation algorithm (BPA) can be used to overcome all these disadvantages, which decreases the mistake.

The various criteria that the user uses to scramble the information so that hackers get more crisis to hack the information, thus offering greater safety. The simulated result demonstrates better results from the combinations of the two algorithms and thus uses lesser weights and neurons.

KEYWORDS: Artificial intelligence, neural network, encryption and decryption.

I. Introduction

Cryptography was the combination of two words called "crypto" means hidden and "spelling" means writing. The hiding method of information safety emails is acknowledged as "cryptography." [19] The earlier Roman technique of cryptography, was popularly referred to as CAESAR SHIFT CIPHER depends on changing the letters of message information by AN in agreement variety (three was a typical choice), the addressee of this message information then modify the letters back by identical variety and procure the first message data [20]. With the advancement during this field, government organizations, military units, and a few company homes started adopting the applications of cryptography [20]. All of them used this technique to save lots of their secrets from others. Now, the arrival of computers and also the web has bought effective cryptography inside the reach of folk.

Modern cryptography is that the cornerstone of personal computer (PC) and communication security [21]. Its basic relies on numerous ideas of arithmetic theory like variety theory, process complexness theory, and applied mathematics [1]. It relies on the formula for committal to writing the knowledge. Secrecy is made by a secret key that is employed because the seed for the algorithms. It needs parties inquisitive about secure communication to possess the key solely. Cryptology's, the revise of a cryptosystem are often divided into 2 branches:

- Cryptography
- Cryptanalysis

CRYPTOGRAPHY: Cryptography is the technique of constructing a cryptosystem that's able of giving info security. Its concern with the particular secure of digital knowledge .

Cryptography concern with the look of cryptosystems, whereas crypt analytics studies the breaking of cryptosystems. The first goal of exploitation cryptography is to produce the four elementary info security services [20].

Confidentiality: It's a Military Intelligence (MI) Section 5 that keeps the knowledge from AN unauthorized person. It's generally mentioned as secrecy and privacy [15].

Data Integrity: It's a MI that deals with characteristic any alteration to the info. This service confirms may or may not the information is unbroken or not since it absolutely was last created, transmitted or keep by a certified user [15].

Authentication: It gives the identification of originators. It tells the recipient that the received information has been sent solely by associate known and verified sender [15].

Non-Repudiation: It's a MI that ensures that associate entity will refuse the possession of a previous commitment or an action. It's a property that the majority fascinating in things wherever there are possibilities of a dispute over the exchange of information [15].

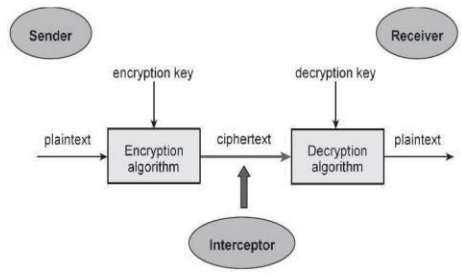

Figure.1. Basic Block of Cryptography

This figure shows a sender / transmitter who wants to send some data to a receiver so that the data cannot be detected by any interceptor in the communication channel. The purpose of this cryptographic system is to know the plain text at the end of the process only by the sender and the receiver.

II. Literature Review

Diflie & Hellmann, found a way which is based on numerical theories to create a secret key through a public channel accessible to any attacker, et al [1] .Toru Ohira, acknowledged the encryption method through a dynamic coupling function with a threshold non-linear and different time delays between dissimilar bits, or neuron, in the original data, et al [2]. Amera I.'s thesis developed a Jewish network through a primary qualitative weight that had a huge dimension to the cryptography process, et al [3]. Furthermore, the neural network has interesting properties such as high non-linearity, parameter sensitivity and learning ability, so they have been widely used as an alternative option for protecting information such as data encryption, authentication and detection. data. of intruders, etc. [4]. Consequently, several cryptographic algorithms based on chaotic nerves are proposed, et al [5-8]. In this article, an algorithm for a hash function in one way depends upon a neural network that feeds two layers together with a chaotic linear map by parts. The analysis shows that the hash function is in a way with high sensitivity and key against birthday attacks, et al [9]. In this article, the neural network uses a cryptographic algorithm down along with shorthand. Filter bank secret writing is employed to write the wave secret separate, the transformation (DWT) is employed to cover the encrypted message, et al [10]. During this work different types of interchangeable and uneven cryptography are studied. Algorithmic program has been planned for RSA to implement public key cryptography by using two public keys and a few mathematical relationships. It is used for the system that desires high security with traditional speed, et al [11]. During this paper, the experimental result shows that the planned serial full adder provides higher results with power and time delay. The convergence of the planned estimate supported the neural network is better because of learning and training, et al [12].

III. Architecture of Standard BPN

A neural multilayer network with a layer of concealed units (Z units) as shown in Figure 2. There may also be bias between output units (Y units) and concealed units. Wok denotes the bias in an excessively typical output unit Y_k; voj is marked as the bias in a typical concealed unit Z_j. These polarization terms act as weights within the connections of the units output [1].

Only the information flow direction is shown for the operation progress phase. Throughout the backward propagation part of learning, the signals are sent in the reverse track [10]. The algorithm in the subsequently part is presented for a hidden layer, which is suitable for a large number of applications.

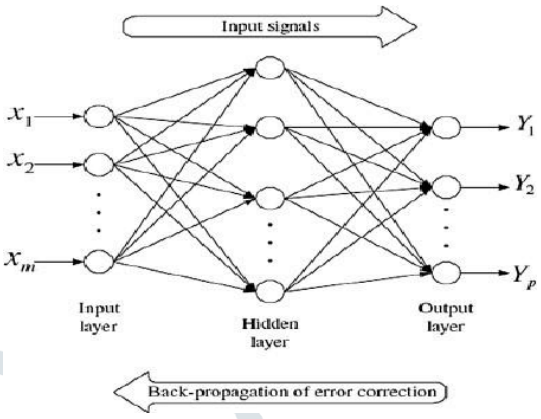

Figure 2: BPN with one hidden layer

IV. Proposed Method

Several studies have already studied with totally different machine learning methodologies, specifically neural networks and their applications in cryptography; however it's a rare technique to use the sequential state machine supported on the artificial neural network and on the chaotic neural network within the field of cryptography.

(a) Sequential Machine

A sequential machine output depends on the state of the machine and also the input equipped to the sequential machine. Therefore, Michel I Jordan Network was designed as a result of the output is taken into account as input [6]. This sort of input is used as a state.

The multilayer network was designed with the help of Michel I Jordan Network.

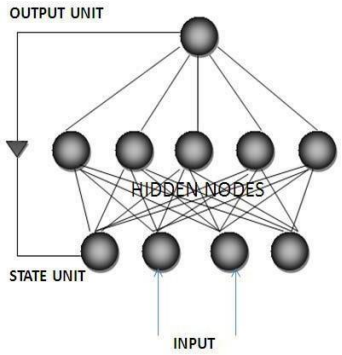

Figure 3: Michel I Jordan Network.

There are three levels in this network: an input level, a hidden level, and an output level [6]. The input level sizes depend on the amount of inputs and also the amount of

outputs used to state. The learning algorithm used for this network is an inverse (back) propagation algorithm and also a sigmoid function is the transfer function within the concealed layer. For the implementation of the sequential machine, a serial document and a sequential decoder are used.

(b) Cryptography obtained from Artificial through an artificial neural network depends on a sequential machine of n states

As Michel I. Jordan can implement a sequential machine employing a neural network, so the information is successfully encrypted and decrypted. In this state, the initial state of the sequential state machine will act as a key. The data is employed to train the neural network [10,12].

(c) Cryptography obtained from a chaotic neural network.

The cryptography theme was designed by a chaotic neural network [4]. A network is recognized as a chaotic network if its weights and biases are evaluated by a chaotic sequence. Especially in digital signal encryption we use a chaotic neural network [8].

V. Simulated Test Result

(a) Sequential Machine

A sequential machine of general status n. For example, the serial adder was executed using this machine.

Input 1	Input 2	Current State	Output	Next State
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

Table 1: State table of the Serial Adder

Table 1 shows the serial adder status table: the current state represents any previous carry that may exist, while the next state represents the output carryover. The data of the serial adder status table is entered in the program. The following command window implemented in MATLAB shows several execution steps.

A sequencing machine N is implemented and training data is entered. First, it asks the user to enter the entry, exit and status here, enter 2 entries, 1 exit and 2 states.

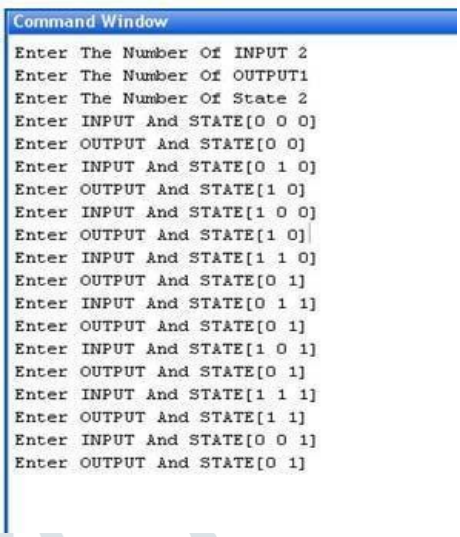

Figure 4: Enter the training data in the n-State sequential machine

With the help of the backward propagation algorithm, to minimize the error function by updating its weights with the same biases.

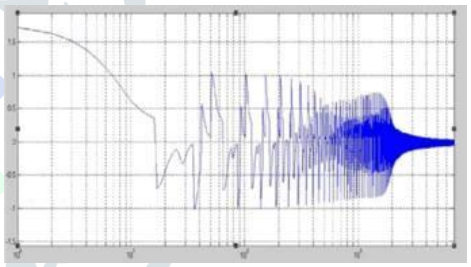

Figure 5: Shows the plot of the error function against the number of iterations

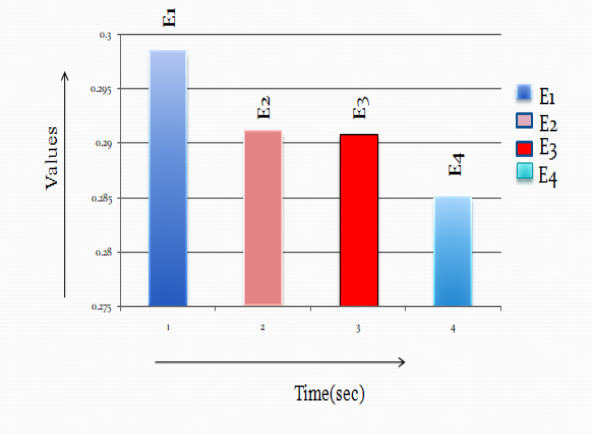

Figure 6: Representation of errors in graphical form

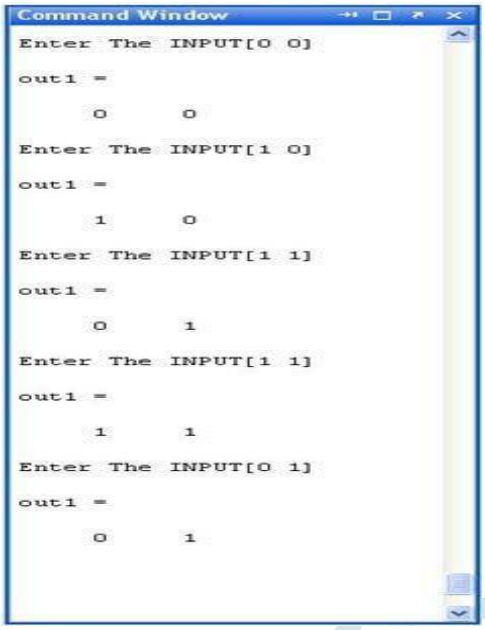

Figure 7: Final output of sequential machine

The command window above shows the final result of the sequential machine implemented as a serialize. There is an initial state informing the user to add the input bits. The output is the sum and the carry bit. Once the execution of the program is completed, it automatically jumps to the new transport status. This output is considered as a previous transfer status.

(b) Cryptography using chaotic neural network

A chaotic network is a neural network whose weights depend on a chaotic sequence. The chaotic sequence highly depends upon the initial conditions and the parameters, **x(0)** = 0.75, and ,μ = 3.9 are set. It is very difficult to decrypt an encrypted data correctly by making an exhaustive search without knowing **x(0)** and μ.
Here a sequence of ten numbers is used for encryption and the initial parameters for the chaotic network are used as mentioned. The output or the encrypted data is then used for decryption. It can easily be seen that the output is in a chaotic state.

Input	Output with x(0) = 0.75 & μ = 3.9	Output with x(0) = 0.55 & μ = 1.5	Output with x(0) = 1.32 & μ = 4.7
36	190	64	219
3	150	17	252
7	153	15	248
43	167	47	212
85	248	87	170
52	95	53	203
236	60	236	19
98	98	98	157
79	44	79	176
10	217	10	10

Table: 2 Same Input Encrypted with Different Initial Conditions (Values of $x(0)$ and μ)

Input	Output with x(0) = 0.75 & μ = 3.9	Output with x(0) = 0.55 & μ = 1.5	Output with x(0) = 2.43 & μ = 5.4
190	36	218	65
150	3	132	105
153	7	145	102
167	43	163	88
248	85	250	7
95	52	94	160
60	236	60	195
98	98	98	157
44	79	44	211
217	10	217	217

Table: 3 Encrypted Data of Table 1 (Column 2) Decrypted Using Same and Different Initial Conditions

Input	Output with x(0) = 0.55 & μ = 1.5	Output with x(0) = 3.65 & μ = 6..5	Output with x(0) = 0.75 & μ = 3.9
64	36	191	218
17	3	238	132
15	7	240	145
47	43	208	163
87	85	168	250
53	52	202	94
236	236	19	60
98	98	157	98
79	79	79	44
10	10	10	217

Table: 4 Encrypted Data of Table 1 (Column 3) Decrypted Using Same and Different Initial Conditions

Input	Output with	Output with	Output with
= 0.55 & 219	36	65	155
252	3	105	248
248	7	102	249
212	43	88	212
170	85	7	170
203	52	160	203
19	236	195	19
157	98	157	157
176	79	211	176
10	10	217	10

Table: 5 Encrypted Data of Table 1 (Column 4) Decrypted Using Same and Different Initial Conditions

It is clear from table 2, 3 and 4 that we can decrypt an encrypted data correctly by knowing the exact values of $x(0)$ and μ otherwise we get the wrong data as shown in column 3 and 4 of table 2, 3 and 4.

This technique succeeded to encrypt different types of data (texts, signals type wav and binary images) and gave another advantage, when re-encrypting the same input data sample we obtained different encrypted data.

When output with $x(0) = 0.75$ and $\mu = 3.9$

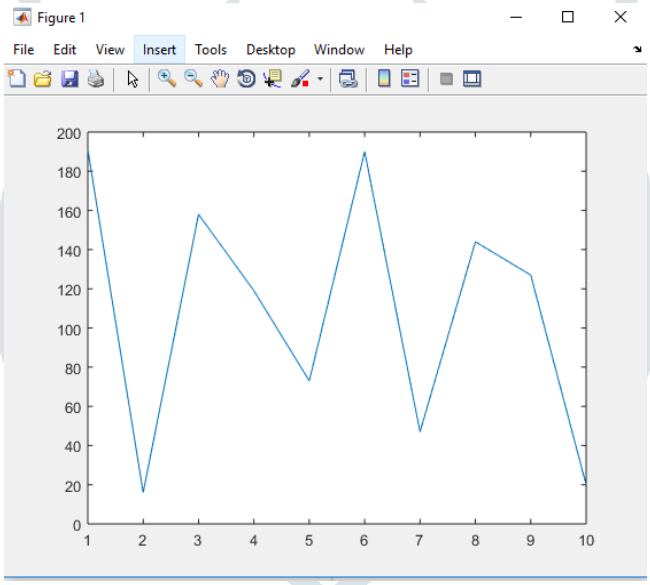

Figure 8: Input vs output graph in encryption

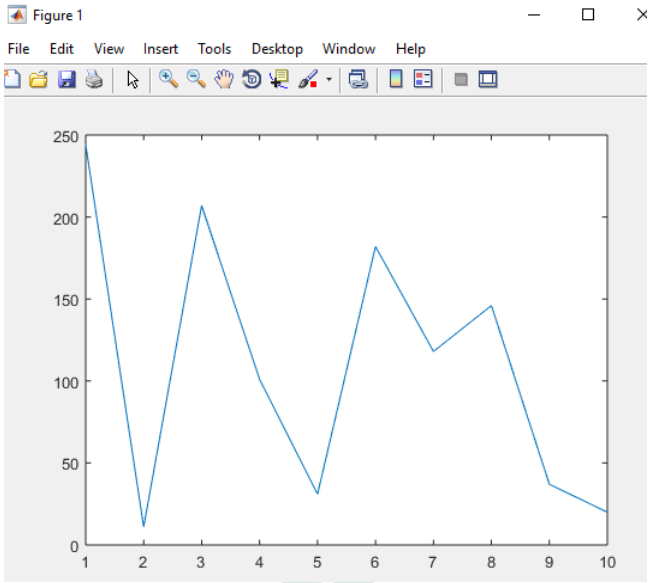

Figure 9: Input vs output graph in decryption

A neural network based cryptography technique has been implemented to study encryption and decryption techniques. Accuracy is enhanced by proper selection of network topology and parameters in the training algorithm.
Decryption data by using the weights which obtained from hidden layer to output layer and consider these weights as a private key. This technique succeeded to encrypt different types of data and gave another advantage, when re-encrypting the same input data sample we obtained different encrypted data.
Related model has been simulated for various input problems. Finally, the accuracy has been demonstrated in form of Tables (table 2, table 3 and table 4).

VI. Conclusion

From the above results, it is concluded that the sequential machine has been successfully implemented (trained) with the help of back propagation algorithm, to minimize the error function and thus reduces the training time as well as the number of neurons.
Chaotic system produces the same results if given the same inputs, it is unpredictable in the sense that you cannot predict in what way the system's behaviour will change for any change in the input to that system.
Simulated results and related graph clearly identified parameter on which training time reduces. Therefore, the artificial neural network will be used as a replacement methodology of encrypting and decrypting the data.

VII. References

1. D.R. Stinson, "Cryptography: Theory and Practice", CRC press, 1995.
2. Toru Ohire, "Toward encryption with neural network analog" Bruges (Belgium), 26-28 April 2000, D- Facto public, ISPN 2-930307-00-5, pp. 147-152.
3. Amera I., "Using Hebbian Network for cipher", Thesis in computer and mathematical sciences university of Mosul/Iraq, 2003.
4. S. Lian, A block cipher based on chaotic neural networks, Neurocomputing 72(4) (2009) pp. 1296-1301.
5. S. Wen, Z. Zeng, T. Haung, Q. Meng, W. Yao, Lag synchronization of switched neural networks via neural activation function and applications in image encryption, IEEE Trans. Neural Network system, 26 (7) pp. 1493-1502, 2015.
6. N. Bigdedi, Y. farid, K. Afshar, A novel image encryption/decryption scheme based on chaotic neural networks, Eng. Appl. Artif. Intell. 25(4), pp. 753-765, 2012.
7. T.A. Fadil, S.N. Yaakob, B. Ahmad, "A hybrid chaos and neual network cipher encryption algorithm for compressed video signal transmission over wireless channel, in: Electronic Design (ICED), 2nd International Conference on, IEEE, pp. 64-68, 2014.
8. S. Chatzidakis, P. Forsberg, L.H. Tsoukalas, " Chaotic neural network for intelligent signal encryption, in Information Intelligence, Systems and Applications, IISA, The 5th International Conference on, IEEE, pp. 100- 105, 2014.
9. V.R. Kulkarni, Sulabha Apte and Shaheen Mujawar, "Hash function implementation using Artificial Neural Network", IEEE Trans., pp. 1-8, 2010.
10. Salan Sarairen, " Secure Data Communication System by using Cryptography and Stenography", International Journal of Computer Network and Communication, vol. 5 pp. 125-137, may 2013.
11. Shipra Sahu, Jai Singh, Javed Ashraf, " Encryption & Decryption of Text Data with RSA cryptography using MATLAB", International Journal of Science & Engg., vol. 3, pp. 104-110, 2015.
12. K. Kiron, B. Srinath, and Pochamreddy Satishwar Reddy, "Performance Evaluation of sequential Adder using neural network", International Joutrnal of Science & technology, vol. 9, pp. 1-5, Oct. 2016.E.C.Laskari,G.C.Meletiou,D.K.Tasoulis,M.N.Vrah atis, "Studying the performance of ANN networks on problems related to Crypto," Non linear Analysis: Real World Applications, vol.7, pp. 937-942, 2006.
13. Daniel J. Bernstein·Johannes Buchmann Erik Dahmen,"Code Based Crypto", National Institute for Research in Computer Science and Control,2009.
14. T.Godhavari, 'Cryptography using neural network', IEEE Indicon 2005 Conference, Chennai, India, 1113 pp., 258-261, Dec. 2005.
15. M. E. Smid and D. K. Branstad, "The Data Encryption Standard: Past and Future," Proceedings of The IEEE, vol. 76, no. 5, pp. 550559, 1988.
16. Bataineh, Mohammad Hindi. "ANN for studying human performance." MS (Master of Science) thesis, University of Iowa, 2012.
17. William Stallings, eds. "Cryptography and Network Security" from principles and practices, by Pearson Education Pte. Ltd...
18. T. SCHMIDT, dept. of computer science, ryerson university, canada - a review of applications of artificial neural networks in cryptosystems
19. http://www.garykessler.net/library/crypto.html.
20. http://www.wikipedia.org.