Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 9, September 2017, pg.21 – 27

Performance Enhancement of RSA Algorithm Using Artificial Neural Networks

[1]Yousif Elfatih Yousif, [2]Dr. Amin Babiker A/Nabi Mustafa

[1]Department of Communications, Faculty of Engineering, AL-Neelain University, Khartoum, Sudan
[2]Department of Communications, Faculty of Engineering, AL-Neelain University, Khartoum, Sudan
[1] yousifsiddiq@gmail.com, [2] amin31766@gmail.com

Abstract— Cryptography is a technique to encrypt simple message into cipher text for secure transmission over any channel , An Artificial Neural Network (ANN) is an information processing paradigm that is inspired by the way biological nervous systems, one of the challenges to implement cryptography algorithm is execution time , An Artificial Neural Network (ANN) is a promising technique to improve the performance of RSA cryptography algorithm , In this paper we explore the implementation of RSA cryptography algorithm using ANN to reduce the execution time. This paper provides a fair comparison between normal RSA and ANN RSA .

Keywords— Cryptography, Artificial Neural Network, nervous, execution time, RSA

I. INTRODUCTION

A neural network is a machine which is designed for modelling the way in which the brain performs a particular task. The network is implemented by using electronic components or it is simulated in software on a digital computer. A neural network is a parallel distributed processor which is made up of simple processing units. These units have a natural propensity to store the experimental knowledge and making it available for use. Neural networks, with their remarkable ability to derive meaning from complicated or imprecise data, can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computer technique. Cryptosystems are commonly used for protecting the integrity, confidentiality, and authenticity of information resources [1]

In addition to meeting standard specifications relating to encryption and decryption, such systems must meet increasingly stringent specifications concerning information security. A neural network is a machine that is designed to model the way in which the brain performs a particular task. The network is implemented by using electronic components or is simulated in software on a digital computer. A neural network is a massively parallel distributed processor made up of simple processing units, which has a natural propensity for storing experimental knowledge and making it available for use. It resembles the brain in two respects:

1. Knowledge is acquired by the network from its environment through a learning process.
2. Interneuron connection strengths, known as synaptic weights, are used to store the acquired knowledge.

Neural networks, with their remarkable ability to derive meaning from complicated or imprecise data, can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computer techniques. Other advantages include:

1. Adaptive learning: An ability to learn how to do tasks based on the data given for training or initial experience.
2. Self-Organization: An ANN can create its own organization or representation of the information it receives during learning time.

3. Real Time Operation: ANN computations may be carried out in parallel, and special hardware devices are being designed and manufactured which take advantage of this capability.[2]

Cryptography refers to the tools and techniques used to make messages secure for communication between the participants and make messages immune to attacks by hackers. A cryptosystem is simply an algorithm which converts the input data (known as plaintext) into something unrecognizable (known as cipher text) and converts the unrecognizable data back to its original form.[3]

There are two types of cryptosystems; symmetric cryptosystems and asymmetric cryptosystems. Symmetric cryptosystems use the same key for encryption and decryption. On the other hand, asymmetric cryptosystems use two different keys; a public key for encryption and a private key for decryption.[4]

II. RSA Algorithm

The RSA cryptosystem was first published more than 30 years ago by Ronald Rivest, Adi Shamir and Leonard Adleman RSA is one of most used asymmetric key encryption algorithm .RSA uses multiple keys for encryption and decryption leading to secure transmission of messages. [5]

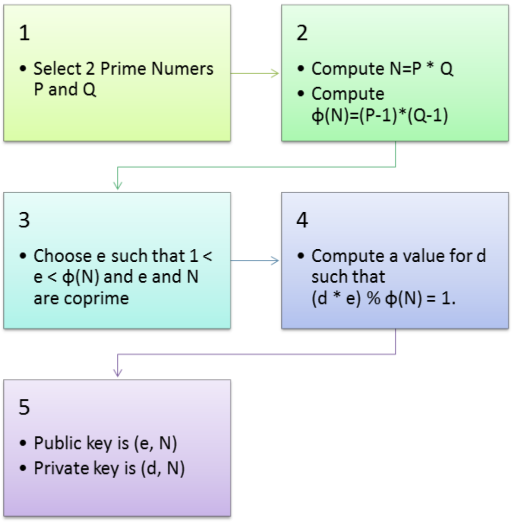
1
• Select 2 Prime Numers P and Q
2
• Compute N=P * Q
• Compute ϕ(N)=(P-1)*(Q-1)
3
• Choose e such that 1 < e < ϕ(N) and e and N are coprime
4
• Compute a value for d such that (d * e) % ϕ(N) = 1.
5
• Public key is (e, N)
• Private key is (d, N)

Fig. 1 The RSA steps

- The RSA is a block cipher whereby the plaintext and ciphertext are integers between 0 and n-1, for some n.
- A typical size for n is 1024 bits.
- In the RSA algorithm, one party uses a public key and the other party uses a secret key, known as the private key. Each station randomly and independently choose two large primes p and q number, and multiplies them to produce n=pq. This is the modulus used in the arithmetic calculations of the RSA algorithm (Rivest, Shamir, & Adleman, 1978).
- The process of the RSA algorithm is as described below:

1. Select p and q (both should be prime numbers)

2. Calculate n=pq

3. Calculate z= φ (n)= (p-1)(q-1)

4. Select integer D which is relatively prime to z.

Gcd φ(n) D=1(φ9n)=z)

5. Calculate ED mod(φ(n))=1

6. For Encryption: C=PE mod n

7. Where P is Plaintext, C is Cipertext (encryption)

8. For Decryption : P=CD mod n

Requirements

- It is possible to find values of e, d, n such that M^{ed} mod n= M for all M<n.
- It is relatively easy to calculate M^e mod n and C^d mod n for all value of m<n.
- It is infeasible to determine d given e and n.

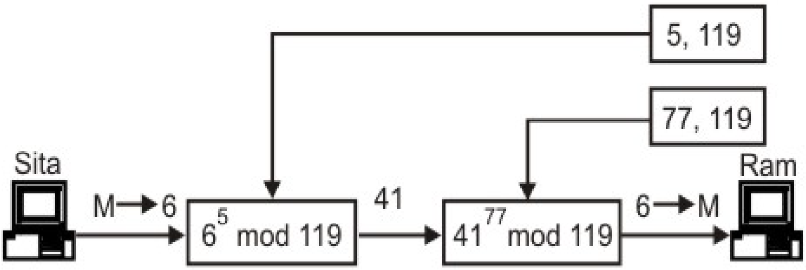

Fig.2 The RSA public key encryption

III.TYPES OF NEURAL NETWORKS ARCHITECTURES

There are three network architectures:

1. Single Layer feed forward networks – In this layer, the input layer consist of source node that results the output in the form of neuron. It is feed forward type of network.
2. Multilayer feed forward networks – It only adds an extra layer known as hidden layer. Because of this hidden layer higher level of statistic is obtained.
3. Recurrent Network – This network contains at least one feedback loop. In this loop, output of a neuron is fed back into its own input which increases learning capability. And it also increases performance [6]

IV.BACKPROPAGATION

There are so many restrictions in single layer feed forward network. So we use backpropagation to reduce the errors. The errors for the units of the hidden layer are determined by back-propagating the errors of the units of the output layer. This method is Backpropagation learning rule. It can also be considered as generalization of delta rule for multilayer function.[7]

V. PROPOSED DESIGN OF RSA ALGRITHM BASED ON ANN

In this design, it was merged ANN with RSA In this design we used a neural network called feed forward network , These types of networks are somehow straight forward and associate inputs with outputs. This kind of organization is also referred to as bottom-up or top-down. The learning algorithm used here is the Backpropagation method in feed forward network architecture. The input is plain text that is encrypted by NN-using RSA algorithm and output of NN is Cipher text .

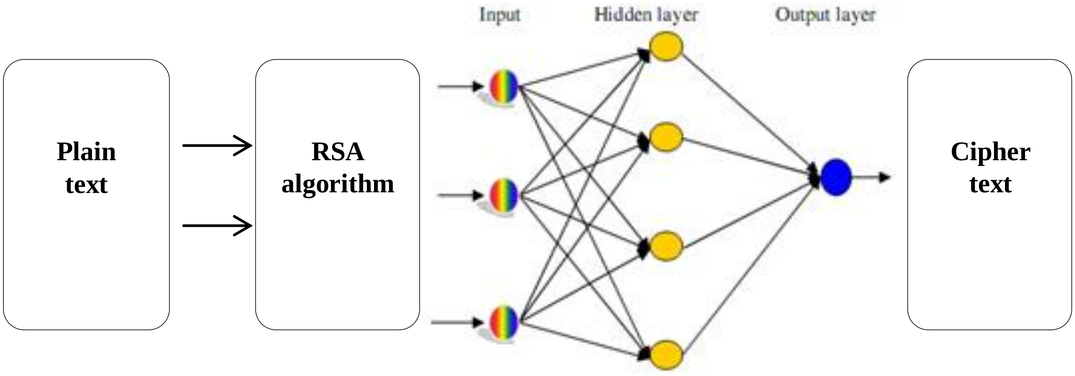

Fig. 3:Propsed Architecture of cryptography based on Neural network

VI. RESULTS AND PERFORMANCE ANALYSES

The implementation results reported in this section makes the comparison between the normal RSA and AAN RSA. In this paper, normal RSA and ANN RSA implementation in the environment of MATLAB

Table 1. Execution Time of AES algorithm for encryption

NO	Input file size in Kb	Time required for Encryption In seconds	
		(RSA)Normal	(RSA)ANN
1	3	0.30902	0.18968
2	6	0.58713	0.39061
3	9	0.93354	0.62498
4	12	1.19556	0.79482
5	15	1.57600	1.06395
6	18	1.94071	1.35826
7	21	2.23180	1.59249
8	24	2.59254	1.88571
9	27	2.98135	2.21400
10	30	3.29384	2.57629

Table 1 shows the execution time required by different size text files for encryption process. Here we reported two types of results. First of all, we show the execution time for different input plaintext size, in normal RSA implementation. Afterwards, we show the result of ANN RSA implementation for same input plaintext size.

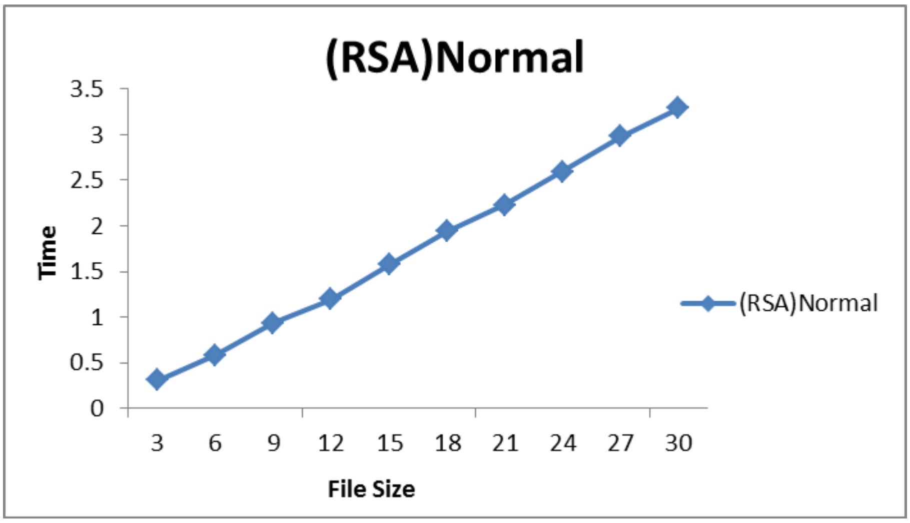

Fig.4 Execution Time for Normal RSA for encryption

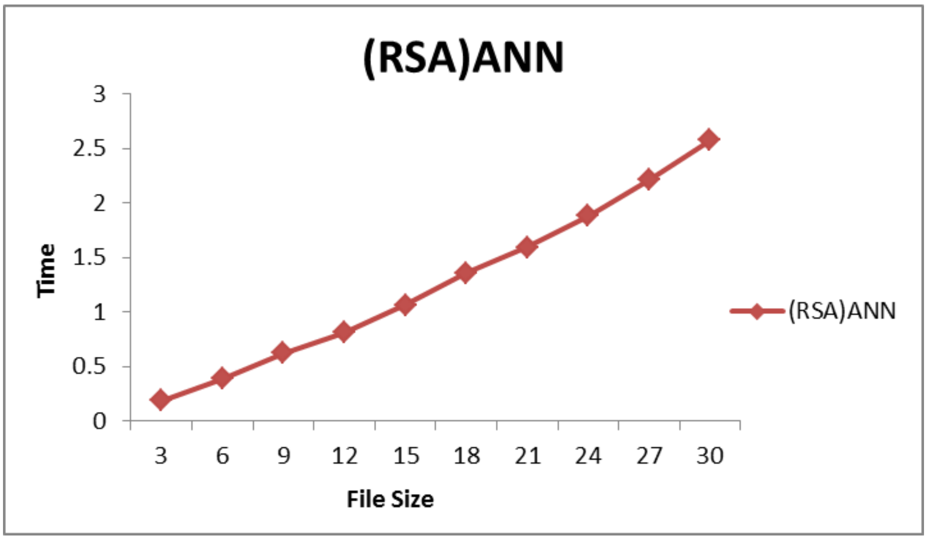

Fig.5 Execution Time for ANN RSA for encryption

Fig. 4 shows graphical representation of time for encryption process in normal RSA implementation, Fig. 5 shows graphical representation of time for encryption process in ANN RSA implementation .

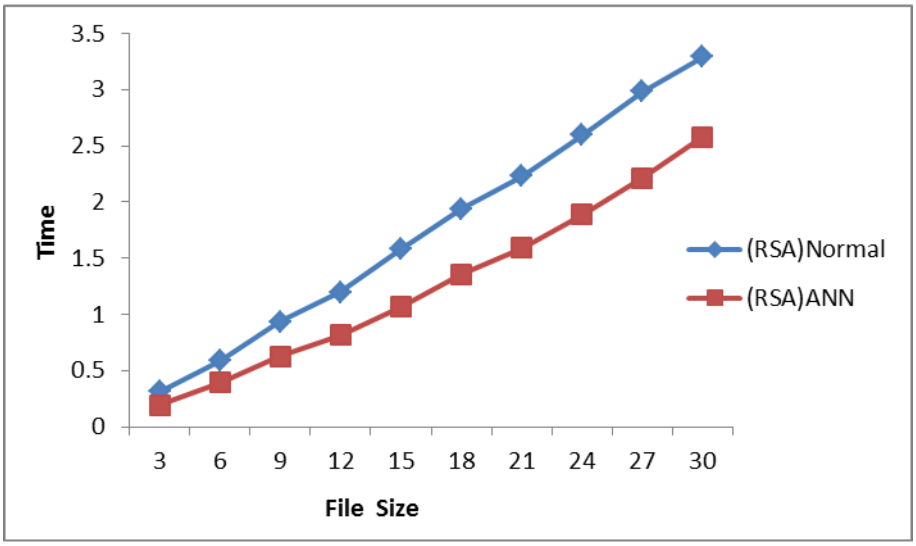

Fig.6 Comparison of Execution Time for Encryption

Fig.6 shows graphical representation of time for encryption process. In this graph blue line shows the encryption time for normal RSA implementation and the red line shows the encryption time for ANN RSA implementation. Graph shows the difference in execution time for normal RSA and ANN RSA implementation for encryption process. Here we can see the performance improvement in the ANN RSA implementation.

Table 2. Execution Time of AES algorithm for decryption

NO	Input file size in Kb	Time required for Decryption In seconds	
		(RSA)Normal	(RSA)ANN
1	3	1.3583	0.68566
2	6	2.51742	1.2104
3	9	3.72623	1.95209
4	12	4.69161	2.73458
5	15	5.84318	3.40464
6	18	7.21027	4.34889
7	21	8.59601	5.25521
8	24	9.82022	6.18592
9	27	11.4323	7.26192
10	30	12.86967	8.42446

Table 2 shows the execution time required by different size text files for decryption process. Here we reported two types of results. First of all, we show the execution time for different input plaintext size, in normal RSA implementation . Afterwards, we show the result of ANN RSA implementation for same input plaintext size.

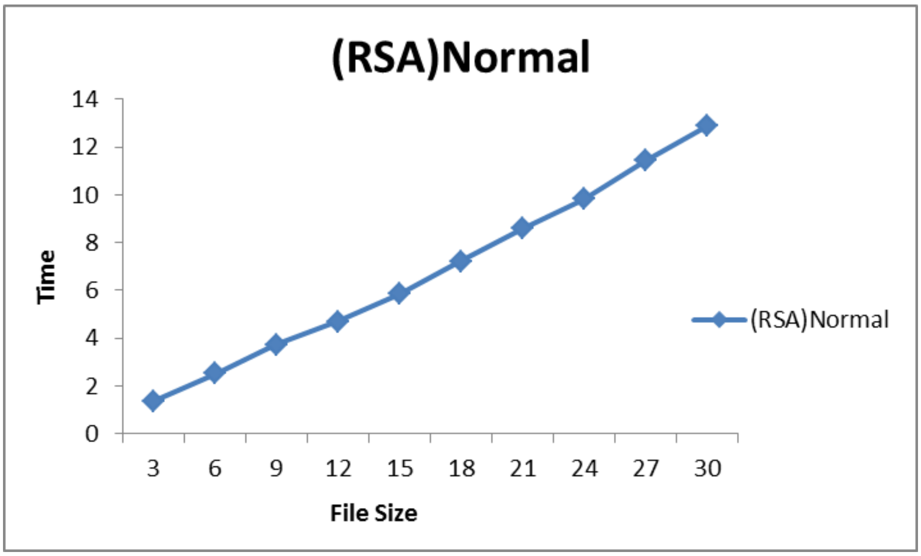

Fig.7 Execution Time for Normal RSA for decryption

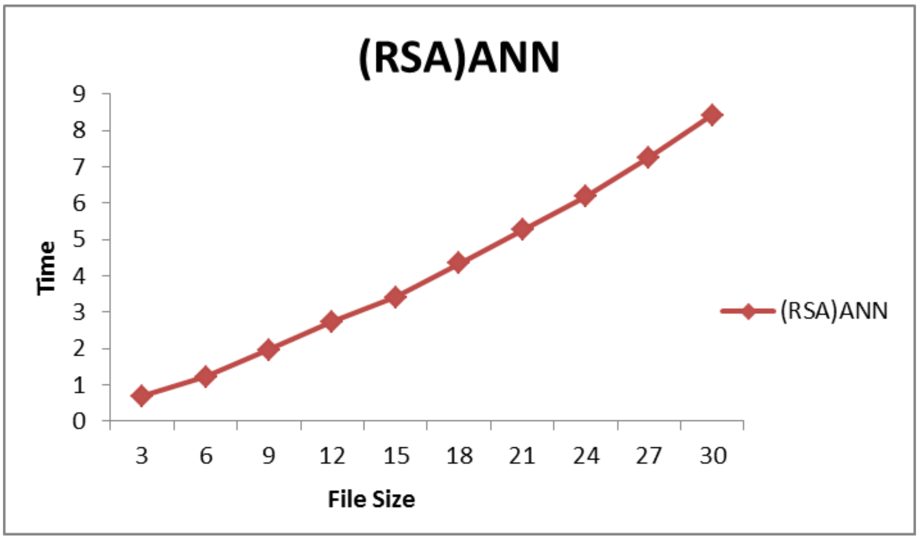

Fig.8 Execution Time for Normal RSA for decryption

Fig.7 shows graphical representation of time for decryption process in normal RSA implementation, Fig.8 shows graphical representation of time for decryption process in ANN RSA implementation.

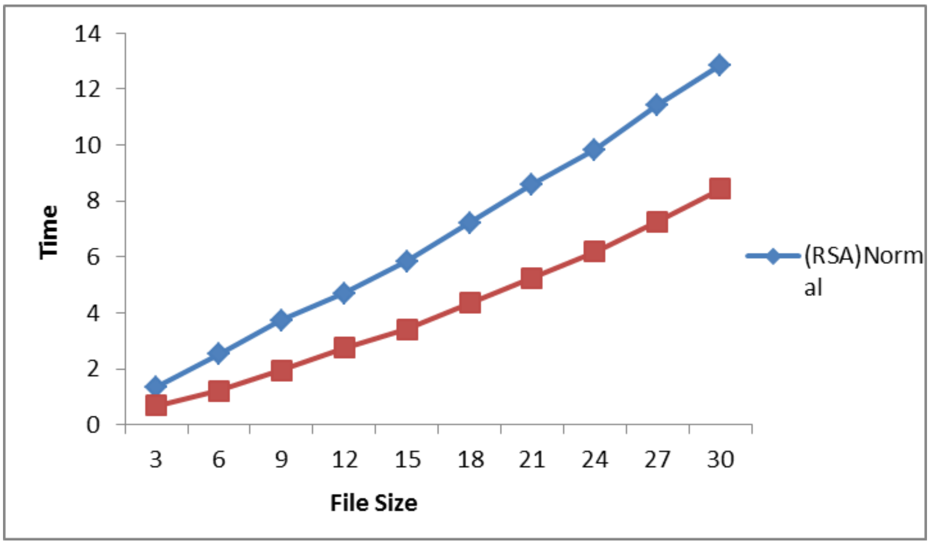

Fig.9 Comparison of Execution Time for decryption

Fig.9 shows graphical representation of time for decryption process. In this graph blue line shows the decryption time for normal RSA implementation and the red line shows the decryption time for ANN RSA implementation. Graph shows the difference in execution time for normal RSA and ANN RSA implementation for decryption process. Here we can see the performance improvement in the ANN RSA implementation.

VII. CONCLUSIONS

In this paper, we have designed and implemented of RSA algorithm by using An Artificial Neural Network (ANN), we provided an extensive quantitative evaluation of execution time for both normal RSA and ANN RSA implementation. After evaluation of execution time, we reported that ANN implementation of RSA takes less time for performing the encryption and decryption than the normal implementation. Overall, we can conclude that An Artificial Neural Network (ANN) provide an efficient and reliable way to implement RSA cryptography algorithm.

REFERENCES

[1] Tope Komal , et al.; " Encryption and Decryption using Artificial Neural Network" , IARJSET , Vol. 2, Issue 4, April 2015 pp. 81-83

[2] Yousif Elfatih Yousif, Dr.Amin Babiker A/Nabi Mustafa, Dr.Gasm Elseed Ibrahim Mohammed" Review on Comparative Study of Various Cryptography Algorithms",IJARCSSE , Volume 5, Issue 4, April- 2015, pp. 51-55

[3] William Stallings, "Cryptography and Network Security: Principles and practices, Dorling Kindersley (india) pvt ltd., 4th edition(2009).

[4] Yousif Elfatih Yousif, Dr.Amin Babiker A/Nabi Mustafa, " Cryptography Techniques based on Neural Networks",IJARCSSE , Volume 7, Issue 4, April- 2017, pp. 308-311

[5] Ajay Pal Singh , Parvez Rahi " Performance Enhancement in Public key Cryptosystems for Security using RSA Algorithm " , IJARCCE , Vol. 5, Issue 11, November 2016 , pp. 359-362

[6] Oludele Awodele, Olawale Jegede" Neural Networks and Its Application in Engineering ", InSITE, 2009

[7] Andrej Krenker, Janez Bešter and Andrej Kos " Introduction to the Artificial Neural Networks", Methodological Advances and Biomedical Applications