International Journal For Technological Research In Engineering
Volume 4, Issue 2, October-2016 *ISSN (Online): 2347 - 4718*

PARALLEL IMPLEMENTATION OF CRYPTOGRAPHIC ALGORITHM FOR IMAGE ENCRYPTION

Saurabh Khatri[1], Dr. Ajay Mathur[2], Dr. Swati Sharma[3]
PhD Scholar, Computer Science & Engineering, Jodhpur National University, Jodhpur, India
HOD, CSE, Govt. Polytechnic College, Jodhpur (Rajasthan)
Associate Prof. Dept. of Electrical Engg.,Jodhpur National University, Jodhpur, India

Abstract: This paper gives a review of one of the basic structures of RSA algorithm and also summarizes its role in solving issues related to image encryption and decryption. The algorithm is widely deployed, has better industry support and composed of numerous parts, each having a specific function within the algorithm. The most obvious and widespread use of RSA is on the Internet, where e-commerce is a driving force behind the need for a secure way to communicate.
Keywords: RSA, Encryption, Decryption, Cryptology

I. INTRODUCTION

Cryptography is the defensive part of cryptology, its activity field being the design of cryptosystems and of used rules. Cryptographic techniques allow a sender to disguise data so that an intruder can gain no information from the intercepted data. This paper includes various factors such as size of images and show how parallelism implementation reduces computation speed. Cryptography provides the mechanisms necessary to implement accountability, accuracy, and confidentiality in communications. As the need of security in communication increase, the use of cryptography will also increase. This paper gives introduction RSA algorithm and summary of issues. It also includes RSA algorithm and its implementation in sequential and parallel with varying different parameters.

RSA Algorithm: The RSA algorithm can be used for both key exchange and digital signatures. Although employed with numbers using hundreds of digits, the mathematics behind RSA is relatively straight-forward. To create an RSA public and private key pair, the following steps can be used:

a) Choose two prime numbers, p and q. From these numbers you can calculate the modulus, n = pq
b) Select a third number, e, that is relatively prime to (i.e. it does not divide evenly into) the product (p −1) (q −1), the number e is the public exponent.
c) Calculate an integer d from the quotient (ed-1)/(p-1)(q-1) .. The number d is the private exponent.
d) The public key is the number pair (n, e). Although these values are publicly known, it is computationally infeasible to determine d from n and e if p and q are large enough.
e) To encrypt a message, M, with the public key, creates the cipher-text, C, using the equation:

$$C = M^e \text{ Mod } n$$

f) The receiver then decrypts the cipher-text with the private key using the equation:

$$M = C^d \text{ Mod } n$$

Block Diagram of RSA Algorithm:

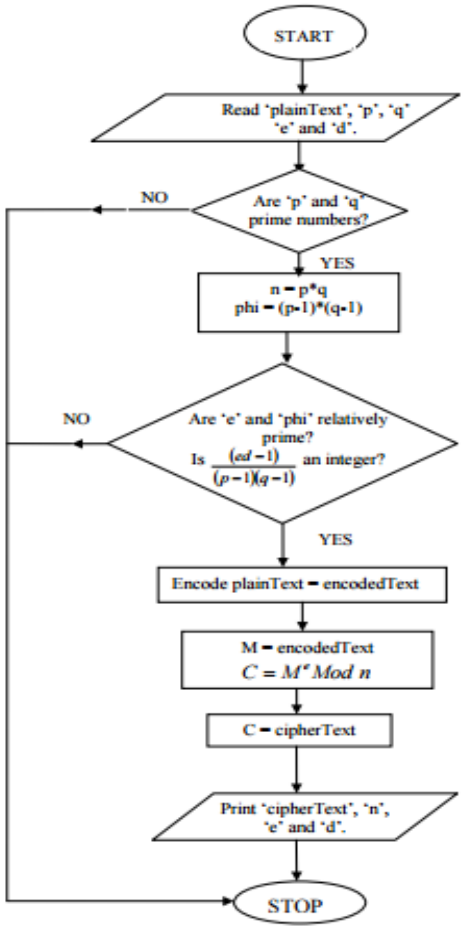

Figure 1: Block diagram of RSA algorithm

Encryption/Decryption:
To encrypt a message using RSA, firstly the message should be segmented into integers $0 \le m \le 2n-1$, i.e. $n-1$ bits length, then performing the equation:

$$\boldsymbol{c = m^e mod n}$$

Thus, c represents the encrypted message which is n bits in length. However, to retrieve the original message m from the encrypted message c, this calculation should be performed:

$$\boldsymbol{m = c^d mod n}$$

II. RESEARCH WORK

There are many issues and challenges in image encryption so many scholars are attracted to research on these issues in this domain. This section summarizes some of the research work done that uses RSA algorithm and give solution for these problems

[13]This paper includes the comparison of the three major algorithms used for cryptography on the basis of its encryption and decryption time. These three algorithms are implemented first and their encryption and decryption times are compared and after that an analysis on the basis of results has been made. The present work focus on combination of cryptography and steganography to secure the data while transmitting in the network. Firstly the data which is to be transmitted from sender to receiver in the network must be encrypted using the encrypted algorithm in cryptography.

The following technique has been implemented on CUDA considering host and device interaction process. Thus, to make the algorithm more efficient we parallelize the algorithm using CUDA block and grid methodology.

Limitations*:* Just like C, CUDA has a recursion-free, Function-pointer-free support.

- Texture rendering is not supported.
- The latency and bus bandwidth between the GPU and the CPU may be limited.

Secondly the encrypted data must be hidden in an image or video or an audio file with help of stenographic algorithm like LSB substitution technique.

Thirdly by using decryption technique the receiver can view the original data from the hidden image or video or audio file. Transmitting data or document can be done through these ways will be secured.

This paper include Modified Advanced Encryption Standard (MAES) for image encryption. It provides great security for digital image. The image to encrypt is converted in to a matrix of scale values. The matrix is divided into sub matrices which are shuffled in a random order. This random order serves as the shared secret between the two communicating person and then it is transmitted on a secure channel using Encryption techniques. On the receiver side sub matrices are shuffled back to original positions. It uses four steps for encryption

1. Substitute bytes
2. Shift rows
3. Mix columns
4. Add round key

And for decryption it uses

1. Inverse shift rows
2. Inverse substitute bytes
3. Add round key
4. Inverse mix column

Mohammad Ali BaniYounes and AmanJantan have presented a block based transformation algorithm based on the combination of image transformation and encryption decryption algorithm called Blowfish. [38]

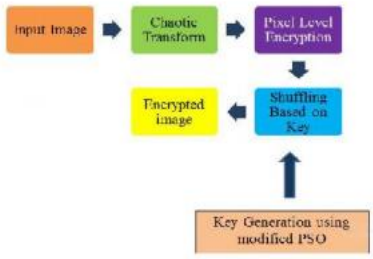

Figure2: Block Diagram

In 1st step it uses chaotic transform to original image. In the second step each pixel in the transformed image is converted into an equivalent 8 bit binary value. This binary value is shuffled based on the predefined key value [39].

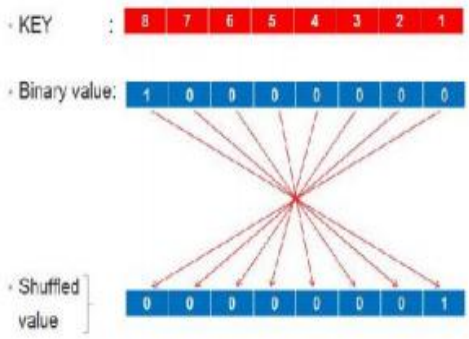

Figure 3: Pixel Level Encryption

[40]This paper introduces a secure communication system that employs both cryptography and steganography to encrypt and embed the secret message to be transmitted over a non-secure channel. The following algorithm describes these stages

Algorithm:

Input: Embed the message.

Output: Message is embedded safely in an image and reconstructed properly.

Begin

1. Message.
2. Encrypting message.
3. Implementing DWT based steganography
4. Embedding data.
5. Stego image.
6. Extraction of embedded message.
7. Encrypted message generation.
8. Decryption.
9. Original Message.

End

A detailed analysis of symmetric block encryption algorithms is presented on basis of different parameters. The main objective was to analyze the performance of the most popular symmetric key algorithms in terms of avalanche effect, integrity checking, Flexibility, Reliability, Robustness, Scalability, Security, and to highlight the major weakness of the mentioned algorithms, making each

algorithm's strength and limitation transparent for application.

III. LIMITATION

Blowfish: Blowfish is a very secure algorithm but Initial 4 rounds of blowfish are observed unprotected from 2nd -order differential attack.

AES: No any such kind of weakness has been observed in AES. Some initial rounds of AES are observed unprotected i.e. initial round can break by square method.

CAST128: by means of a known plain text attack Key of CAST 128 can be known by linear cryptanalysis. It can be broken by 2^17 chosen plaintexts along with one related-key query in offline work of 2^48.

DES: because of short key length brute force attack can crack easily by implementing brute force attack. Hence, Weak key is the major problem of DES. It doesn't protect data against linear and differential attacks.

IV. CONCLUSION

The concept of RSA Algorithm is being used in many areas. RSA algorithm provides a secure way for image encryption and decryption. Thus, to make the algorithm more efficient we parallelize the RSA algorithm.

REFERENCES

[1]. International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064 "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique" B. Padmavathi, S. Ranjitha Kumarihttp://www.ijsr.net/archive/v2i4/IJSRON120134.pdf

[2]. Ms. NehaYadav, Mr. Alok Kumar Singh" A NEW IMAGE ENCRYPTION APPROACH USING THE INTEGRATION OF A SHIFTING TECHNIQUE AND THE MAES ALGORITHM" ISBN-978-81-932074-4-4 Available at:http://data.conferenceworld.in/ICRTESM3/P1388-1394.pdf

[3]. M. Ali BaniYounes and A. Jantan, "Image encryption using block-based transformation algorithm" in IAENG International Journal of Computer Science, Volume 35, Issue 1, 2008.

[4]. C. Li, S. Li, G. Alvarez, G. Chen and K. T. Lo. "Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations". Physics Letters A, 2007.

[5]. SalehSaraireh "A SECURE DATA COMMUNICATION SYSTEM USING CRYPTOGRAPHY AND STEGANOGRAPHY" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013 http://airccse.org/journal/cnc/5313cnc10.pdf

[6]. YoussoufMahamatkoukou, SitiHajar Othman, Maheyzah MD Siraj. HerveNkiama"Comparative Study Of AES, Blowfish, CAST-128 And DES Encryption Algorithm" IOSR Journal of Engineering (IOSRJEN) ISSN (e): 2250-3021, ISSN (p): 2278-8719 Vol. 06, Issue 06 (June. 2016), http://www.iosrjen.org/Papers/vol6_issue6%20(part-1)/A066010107.pdf

