International Journal of Engineering & Technology, 7 (3.34) (2018) 674-677

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Encryption and Decryption of an Image Data – a Parallel Approach

[1]Raghu M E., [2]K C Ravishankar

[1]Dept. of C S and E. Govt. Engineering College, Hassan, Karnataka , India
[2]Dept. of C S and E. Govt. Engineering College, Hassan, Karnataka , India,.
**Corresponding author Email: rme@gechassan.ac.in[1], kcr@gechassan.ac.in[2]*

Abstract

Multimedia data has been essential part of our lives, from instant messaging application to social media. Instant messaging applications like WhatsApp uses AES 256 bit key for security purpose. The security measures are taken so as to protect the data from unauthorized access and to ensure privacy. This paper mainly considers image data as source for encryption and decryption. Along with text, AES algorithm is used for image cryptography, in its suitable way. The AES algorithm is chosen because of its highly secured way of encryption and decryption. Time required for the procedure of encryption and decryption is also measured. Present use of Internet, mobile and socialmedia made images considerable value in our daily life. Securing multimedia data is becoming an important issue in communication and storage. Secured communication of digital images is needed in many areas, such as electronic commerce,medical imaging systems, mobile check deposit, online photograph album, military image communication, etc.., There is a need of developing fast encryption methodologies for such communication

Keywords*: Cryptography, Encryption, Decryption, Parallel, Threads*

1. Introduction

Recent developments in Internet technology, distribution of multimedia content through the Computer network is enormous. However the increased multimedia documents, image processing tools, easy and cost minimized availability of Internet access and social media created lot of scope for multimedia data encryption in faster and cost effective way. A major challenge is to protect the confidentiality of multimedia content in transmission of data in networks.

Multimedia data may be text, audio, images, video and different graphical objects. Securing all these type of data is essential today, because of use of these multimedia data in different fields. These data may be used in military applications, medical, engineering, education, entertainment etc.., Securing and communicating the multimedia data in fast and using available hardware in now essential.

There are different techniques to securemultimedia data. One way to secure traditionally isby converting plain text (data) to cipher text (data) called encryption and reconverting cipher text (data) to plain text called decryption. Generally called as cryptography an art of securing data.There are different techniques available for data security -a symmetric algorithms like Data Encryption Standard (DES), Advanced Encryption Standard (AES) etc., and an asymmetric algorithms like RSA,ECC etc., The cryptography algorithms proceed without distinguishing the nature of data as either text, image or video. If the input data is not a real timedata it can be treated as a regular bit stream data and any conventional algorithmic technique can be used for securing it. If any constraints are present on available data then itmay be difficult to secure multimedia data.

Nowadays, image encryption scheme include two processes such as substitution and diffusion. The substitution stage permutes all the pixels as a whole, withoutchanging their value. In the diffusion stage, the pixel values are modified sequentially so that a tiny change in a pixel spread to as many in the cipher image as possible.

1.1 Type of Cryptography:

The cryptography algorithms are classified based on the way the key is used for encryption and decryption. Further categorized on application and use of an algorithms, typesof cryptographicalgorithms are:

***Private Key(SymmetricKey) Cryptography*:**Algorithm on this type uses only one key for both encryption and decryption.E.g. DES, AES

***Public Key (Asymmetric key) Cryptography*:**Algorithm on this type uses one key for encryption and second key for decryption.E.g. RSA

***Hash Functions*:**Algorithm on this category uses a mathematical functions tosecure or encrypt the information.

In private key encryption input data is always a block sized, single key is used by both sender and receiver for encryption and decryption respectively. The sender uses some key (or procedure) to encrypt block sized input data and sends the encrypted data to the receiver. The receiver applies the same key used by sender (or procedure) to decrypt the encrypted datato get original input data. Because same key is used for encryption and decryption it is also called symmetric encryption.

In public key cryptography one key is used forby sender to encrypt the input data and another key is used by the receiver to decrypt the cipher data to get the original input data. Because both sender and receiver uses the different keys for encryption and decryption, it is also called as asymmetrickey cryptography.

In hash Functions a mathematical transformation is used to irreversibly convert the input data into unreadable form and reverse the operation to convert unreadable form to original input

data. This method is basically used in message integrity.

2. Literature Survey

Literature surveyshas been done with respect to cryptography, image encryption, different methods for image data encryption, parallel approach for text and image data encryption.

J. Ahmad, S. Oun Hwang and A. Ali [1] proposed comparative analysis of Advanced Encryption Standard (AES), compression friendly encryption scheme, chaotically Coupled Chaotic Map Encryption Scheme and a Bernoulli Map Based Encryption Scheme.

R. Yadavi, M. Beg2 , M. Tripathi [2] in their paper proposed literature review on multimedia data taking an image as an input for encryption using differenttechniques and also introduced the general information about images and an imageencryption with its advantages and disadvantages

R. Pakshwar, V. Kumar Trivedi and V. Richhariya [3] the researchers presented a survey of over twenty five different research papers which gives details of imageencryption techniques. They also proposed the importance of encryption and multimedia data. Many of the methods uses pixel as a basic element for encryption.

J. Shah and V. Saxena [4] elaborated classification of various image encryption schemes and analyzed each of them withvarious parameters like compression friendliness,encryption ratio, tunability, visual degradation, formatcompliance, speed and cryptographic security

Sivaguru J, Manikandan G,Karthikeyan S, Sairamn [5] proposed a parallel system for cryptography. Authors conclude that the parallel system enhances the speed of encryption and decryption. They have used the "**slice and merge**" concept to perform the parallel cryptography, they proved that performance is better than our traditional crypto algorithms.

Osama Khalifa [6] proposed the need for enhancing the performance of existing cryptographicmethods, which are widely accepted and executed by many users. Here also the author proposed the use of parallel methods for securing the data. The result shows that the parallel method is better than the sequential method. Author conclude that the software as to move along with the improvement of hardware, and one should make use of the all functionalities of the hardware without extra cost.

Salem Sherif Elfard[7] proposed the need for cryptography in providing security services and cryptography is the one of the powerful method for many applications indata security. Author proposed the parallel way of encrypting the data using linear Fibonacci forms.

RavishankarK C and VenkateshmurthyM G [8] proposed an image encryption based on the region permutation. This method gives the dis-orderness in the visibility of an image. The randomness is main intension in disordering the image. This method may be parallelized using existing hardware.

3. Proposed Parallel Encryption Using Aes

Any symmetrickey algorithm may be used to encrypt the input data. Here AES algorithm is used for encryptionwith 128 bit block size and samelength key size. The algorithm uses 10 rounds, where 9 rounds are with 4 stagesand 10^{th}round of 3 stages.

The four stages for encryption are,

1. Substitute bytes.
2. Shift rows.
3. Mix Columns.
4. Add Round Key.

The 10^{th}round without the 3^{rd}stage.

The first 9 roundsof decryption are same as encryption but only change is in the order of 1 and 2 stages of encryption.

1. Inverse Shift rows.
2. Inverse Substitute bytes.
3. Inverse Add Round Key.
4. Inverse Mix Columns.

The 10^{th}roundjust leaves 4th stage output as it is.

3.1 Encryption:

Here an image data is converted to cipher text in parallel using threads. At first read the input image from the specific location and images is split into number of parts of same dimension equal to number of threads created and assign each part of an image to the threads. Perform the encryption of each part of an image in parallel using AES algorithm. After the encryption output of each thread is saved to specific location. Later output of each thread is combined and stored as single output file. Threads are used to increase the performance as each thread can perform its task in parallel.

The performance measure of this approach is compared with the performance of conventional/sequential approach. The performance of parallel approach is better than the sequential approach.

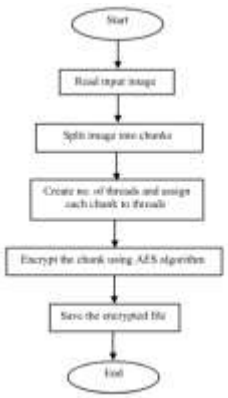

Fig 1: Encryption of an image using threads

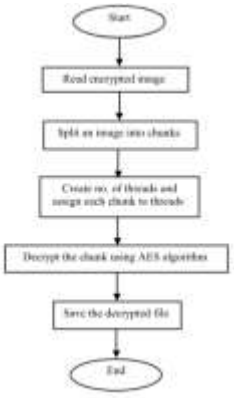

Fig 2: Decryption of an image using threads

Pseudo code for Encryption of an image using threads.
Begin
Step 1: Choose an image.
Step 2: Slice an image.
Step 3: Create number of threads.
Step 4: Assign each chunk to thread for encryption with the key.
Step 5: Encrypt the each chunk using AES algorithm.
Step 6: Merge all chunks to single file.
Step 7: Record time for encryption.
Step 8: Store the encrypted image.
End.

An encrypted image is decrypted in parallel by using threads. An image is split into number of equal parts and assign each parts of an image to the threads and decryption of each part of an encrypted image in parallel and the decrypted images are merged into single original image.

Pseudo code Decryption of an image using threads.
Decryption:
Begin
Step 1: Choose an encrypted image
Step 2: Slice an image into number of chunks.
Step 3: Assign each slice to thread for decryption with the key.
Step 4: Decrypt the each chunk using AESalgorithm.
Step 5: Merge all checks to file.
Step 6: Store the decrypted image.
End.

The image encryption is done with the help of AES algorithm. Encryption can be done either sequential way or in parallel. Main aim here is to minimize the time of cryptography. Hence whole process is done in parallel. As shown in the flowchart the image is

first sliced into chunks, each chunk is encrypted in parallel using AES. The time taken in the sequential and parallel process are compared.
Decryption is just a reverse process where the encrypted image is taken as input to get origin image. Here AES algorithm is applied with decryption procedure. Time taken by the algorithm with threads is compared with the sequential processing.

4. Results

4.1. Encryption:

The encryption and decryption of an image using threads is an approach to minimize the time required. Figure 3 shows an original input image, figure 4 shows the chunk of an image before the encryption process. Here each slice is converted into cipher data in parallel, output of each thread is shown in figure 5. Output is merged into one encrypted file (figure 6).

Figure 3: Input ImageFigure

Figure4: Image after dividing into chunks

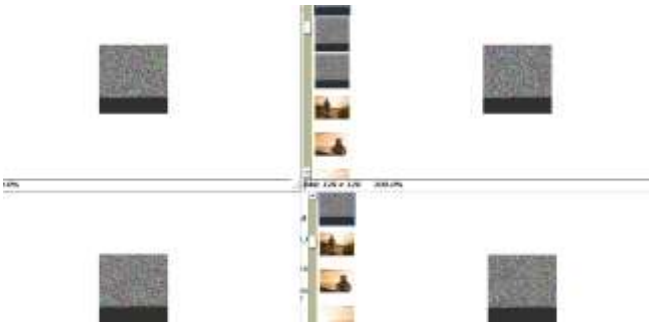

Figure5: Encrypted Chunks

Figure 6: Encrypted Image

4.2 Decryption:

Decryption is done on cipher data by taking the output of encryption. Figure 6 above is an input image for decryption. Here each chunk is decrypted in parallel using AES. Output of each thread is shown in figure 7. Each output is merged into one decrypted file (figure 8).

Figure 7: Decrypted Image with Slices

Figure 8: Merged Decrypted Image

5. Analysis

Time analysis is the important between sequential and parallel approach. Table 1 shows the time taken by both the approach for the same image. Time taken for different formats of the picture also various depends on the image format. All times are indicated in seconds.
First column indicate the name of the input image, second column indicate size of the image, third column specify the time taken for the encryption in sequential encryption and fourth and the last column indicate the time taken for parallel encryption. The time comparison indicate that the parallel approach takes almost the half the time of sequential approach.

Table 1: Time comparison

Image name	Image Dimension (W * H)	Sequential encryption time (sec)	Parallel encryption time (sec)
a.png	556 x 554	1.67	0.92
C1.png	238 x 239	0.34	0.20
CC1.jpg	556 x 554	1.70	0.94
CC.jgg	850 x 1280	6.07	4.02
Cute.jpg	479 x 780	1.98	1.02

6. Conclusion

Now a day's encryption of multimedia data is essential because of various applications like Video conferencing, VoD, WhatsApp, weather forecast etc. This paper gives an idea about how image data can be encrypted and decrypted using parallel mechanism with available hardware. The data can be encrypted and decrypted with minimum time compared with the traditional sequential method. It is also divide the image data into available cores and time taken for encryption and decryption can be minimized.

References

[1] J. Ahmad, S. Oun Hwang and A. Ali (2015),"An Experimental Comparison of Chaotic and NonchaoticImage Encryption Schemes", Wireless personal communication, Volume 84, Issue 2, pp 901–918

[2] R. Yadavi, M. Beg2 & M. Tripathi (2013), "Image Encryption Techniques: A Critical Comparison",International Journal of Computer Science Engineering and Information Technology Research(IJCSEITR) ISSN 2249-6831 Vol. 3, Issue 1.

[3] R. Pakshwar, V. Kumar Trivedi and V. Richhariya (2013), "A Survey on Different ImageEncryption and DecryptionTechniques, IJCSIT, Vol. 4 (1), 2013, 113 –116.

[4] J. Shah and V. Saxena (2011), "Performance Study on Image Encryption Schemes", IJCSIInternational Journal of Computer Science Issues, Vol. 8, Issue 4, No 1.

[5] Sivaguru J, ManikandanG,Sharman,Karthikeyan .S, "A Parallel Approach for Improving Data Security," Journal ofTPIT, Vol. 39 No.2, 15 May 2012, PP. no 119-125.

[6] Osama Khalifa, "The performance of cryptographic algorithms in the age of Parallel computing,", August-2011, Heriot Watt University School Of Mathematical and Computer Science.

[7] Salem Sherif Elfard. "University Bulletin – ISSUE," No. - 15 – Vol. 2- 2013

[8] RavishankarK C and VenkateshmurthyM G, "Pixel Compaction and Encryption for Secure Image Transmission,"NCIDAPD-2007, BIT Sathyamangalam, March 15-16, 2007