A Study on Different Approaches of Selective Encryption Technique

Saurabh Sharma
M.Tech Student (Computer Science)
Lovely Professional University
Phagwara, India
saurabh4362@gmail.com

Pushpendra Kumar Pateriya
Assistant Professor (Computer Science)
Lovely Professional University
Phagwara, India
pushpendra.mnnit@gmail.com

Abstract

Omnipresence of security in every application in Internet application is a clear motivation to contribute in the field of Information Security. Security is one of the most challenging aspects in the internet and network applications. Encryption is a process which is used to secure the data and the Encryption algorithms play a crucial role in efficient information security systems. Full encryption techniques are slow. Selective encryption is a technique to save computational power, overhead, speed, time. This technique also provides quick security by only encrypting a selected portion of a bit stream. Selective encryption technique is one of the most promising solutions to increase the speed of encryption as compared to the full encryption. Selective encryption is helpful for the multimedia content like images, video content and audio content. So this document discussed about Selective encryption technique which is used to increase the speed of encryption as compared to the full encryption.

Keywords: Selective encryption, Encryption, Decryption

1. Introduction

In this era, the communication through multimedia components is on demand. The data like text, images, video and audio is communicated through network. Cryptographic techniques are used to provide the protection of data and information while transmission of data over the network. The various algorithms are available for the security Services like Confidentiality, Data Integrity, and Authentication to protect against the attacks, for examples: - release of message contents, modification of message, masquerade etc. Encryption is the technique in which a plaintext message is converted into cipher text. Decryption is reverse process of the encryption in which cipher text is decrypted back into the original text. The algorithms in cryptography are categories into the two classes, Symmetric and Asymmetric encryption. In Symmetric encryption both the user shares the same secret key for encrypting and decrypting. The key should be kept secret to provide privacy. A symmetric algorithm does not consume too much computing power. Examples are: DES, Triple-DES (3DES), etc. In Asymmetric encryption the user use pairs of keys. One key is for encryption and another is for decryption. The decryption key is kept secret also called “private key” or “secret key”, while “public key” is send to all for encrypting messages. Everybody having the public key is able to send encrypted messages to the owner of the secret key. Examples are RSA, DSA, and ELGAMAL. The Symmetric Encryption class is important in modern cryptography, reason being the Symmetric encryption is faster as compare to the Asymmetric encryption cryptosystem [1]. The use of the image is seen in internet, multimedia systems, medical, and telemedicine, military for the purpose of communication [2]. The data should be transferred at high speed through the network even in secure manner. There are lots of algorithms already proposed for securing the data over the network but the standard algorithm takes time to encrypt the data. Selective encryption is the technique of encrypting some parts of a compressed data file while leaving other part of plain text unencrypted. As security is an increasing public concern these days, encryption is becoming popular for communication any type of sensitive data. The cost and time for data encrypting can be saved by an effective encryption scheme that will be the required by the companies, associations or individuals. In this paper, basically we focused on the Selective encryption technique. This paper is organized as follows: in section 2, we have
the literature review of the selective encryption algorithms and in section 3; we have the comparative analysis of different selective encryption technique. In the end in section 4, is providing the conclusion over the discussion given in the paper.

2. Literature review

Yonglin Ren, Azzedine Boukerche, Lynda Mokdad [3] presents the principle of selective encryption with a propose of probabilistically selective encryption algorithm. The algorithm was based on symmetric key. By make use of probabilistic methodology and stochastic algorithm, in the process of message encryption a sender includes proper uncertainty, so that the decryption of the ciphertext is done by only entrusted receiver and other unauthorized nodes have no information of the broadcasted messages on the whole.

S.Kala [4] implemented the idea of selective encryption algorithm for wireless ad hoc network with the Quadrature Mirror Filters and Lossless compression techniques. In a Toss A coin algorithm the half of the data is encrypted and another half is unencrypted i.e., 50% of data will be encrypted and left 50% will be unencrypted and, it is transferred as it is. It requires more bandwidth. Selective encryption is one of the most promising solutions to reduce the cost of data protection in wireless and mobile networks [5].

Priyanka Agrawal, Manisha Rajpoot [10], Selective encryption is one of the most promising solutions to reduce the cost of data protection in wireless and mobile network.

Pramod Kumar, Pushpendra Kumar Pateriya [6], Selective image after encryption becomes more secure against the attacks. There are lots of cryptographic algorithms are available and most like: RS DES, AES, Chaotic System, DCT, and DWT are proposed and used for image encryption and selective image encryption [7].

Kalpana Singh and Shefalika Ghosh Samaddar [9] have used the selective encryption technique in RSA based on singular cubic curve for the text based documents. The author(s) proposed to increase the speed of encryption by using selective encryption. Selective encryption [8] is a technique which uses subset of bit stream rather than entire bit stream. In the selective encryption used in [9], only a random (r) of whole message/plain text is encrypted rather than the whole text. It increases speed of encryption/decryption in case of any cryptographic algorithm.

3. Comparative study

In this section we have compared the different algorithm of selective encryption technique based on their result analysis. S.kala [4] has enhanced the Toss-a-Coin Selective Encryption Algorithm in which the message is divided in two groups i.e. the odd number messages and the even number messages. Messages $M_1$, $M_3$, $M_5$, ………., $M(2n-1)$ represent the odd number messages and messages $M_2$, $M_4$, $M_6$, … $M(2n)$ represent the even number messages. By using the toss-a-coin algorithm either the odd number messages are encrypted or even number messages are encrypted. Thus here half of the whole messages are encrypted.

**Figure 1: Selective RSA based singular cubic curve [9]**

M is a message or a plain text, R is a selected text and M-R is a rest message part. On the R the selective encryption is done in RSA based on singular cubic curve and M-R is encrypted by the DES algorithm with the use of AVK (Automatic Variable Key).
The rest of the data which was remaining unencrypted is taken as input and the QMF (Quadrature Mirror Filters) algorithm is applied to yield 48% of compression. The remaining unencrypted data is compressed and other data was encrypted. With this the dual benefits were given to the data like security and compression.

Priyanka Agrawal, Manisha Rajpoot [10] has proposed a selective encryption approach which uses the advantages of grid method. The main objective was to obtain satisfactory complexity in the selection of some parts of a multimedia data after conversion it into the bitstream. For the period of sending messages, the sender will convert the visual data into binary form, then the binary bit stream is arranged in grid structure and then transpose of each sub grid should be done. The compliment of the bits is done if the bits on any sub grid are same. These bits are the selected bits which are to be encrypted and the encrypted data will be further combined with the remaining original bits in the grid and broadcasted over the transmission channels to the receiver. The selective encryption will be done on the selected part of the image and then selected part will be encrypted as shown in the Figure 3b and the Figure 3a represents the original image.

They have taken the benefit of symmetric key algorithm to decrease the complexity of the operation and protect the data in a reasonable computational cost and these properties make the scheme suitable for real-time applications.
Pramod Kumar, Pushpendra Kumar Pateriya [6] has proposed the Selective Image Encryption using RC4 Enrichment Algorithm and they are encrypting the selected portion of the image by using selection algorithm. They have analyzed the result of selective image encryption and full image encryption by taking different sized images as input data. This paper uses the proposed algorithm to done the encryption over the selective portion of the image. And image selection is done by using the selection algorithm describes in this paper. The simulation is done by using matlab 9.

In Figure 4 first input the original image and then select the portion of the image and encrypt the selective portion of the image by using the selection algorithm and encryption algorithm. In this simulation, the author(s) used the 256* 256 KB and 80 bits image. In Figure 5 and Figure 6, the performance analysis of the selective and full image encryption over the different sized images data is done. The result of the analysis is selective image encryption takes less time than the full image encryption. This shows the selective image encryption is best to use from time concern.

4. Conclusion

In this manner, this paper describes the concept of selective encryption technique. Selective encryption technique is one of the most promising solutions to increase the speed of encryption as compared to the full encryption. Selective image after encryption becomes more secure against the attacks. Selective encryption is advantageous for the multimedia content like images, video and audio. Selective encryption is faster as compared to the full encryption of the data. For securing large visual data with requirements of real-time communication and use in resource constrained applications such method would be in demand in the future as well.
5. References


