IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. IV (May-Jun. 2014), PP 01-05
www.iosrjournals.org

Selective Encryption of Plaintext Using Multiple Indexing

Soumya Balachandran[1], Sangeeta Sharma[2]
[1]*(Department of CSE, Lovely Professional University, India)*
[2]*(Assistant Professor, Department of CSE, Lovely Professional University, India)*

Abstract: *Selective Encryption is one of the encryption algorithm in the field of multimedia security. They are used for the purpose of hiding image, video or audio files. The main feature of selective encryption is that the resource and time taken to encrypt the files is lower than any other encryption algorithm. We propose an algorithm that will exploit this feature of selective encryption to encrypt plaintext instead of multimedia file. Our purpose is to design an encryption algorithm that will be computationally faster than any hard encryption algorithm such as Advanced Encryption Standard (AES) while providing the basic cipher complexity.*

Keywords: *Advanced Encryption Standard; Cipher Complexity; Linear Congruential Theorem; Prime Number indexing; Pythagorean Theorem; Selective Encryption*

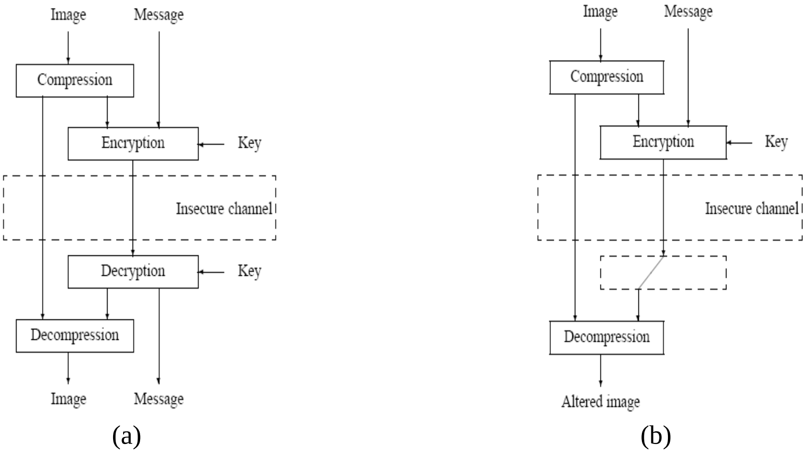
I. Introduction

Today's world is under the craze of newer and smarter technologies that provides them every service that a laptop or computer provides. As per the market demand the electronic companies are expected to develop electronic items that are smaller, faster and consume less resource. But this demand also has put constraint on the encryption algorithms that must meet the requirement of the smaller technologies that is ruling the market. Keeping this in mind we propose an algorithm that takes lesser time for computation than any hard encryption while simultaneously providing necessary security.

Selective Encryption is often recognized as a soft encryption in the field of multimedia security. The important characteristic of Selective Encryption is that it is computationally faster than AES. This is achieved by encrypting only a subset of data from file. Here subset of data is selected based on how vital the data is as compared to whole data. Presently, this algorithm is designed for encrypting multimedia files only. If this algorithm is used for simple plaintext, it gives faster computation but it does not provide necessary security. Overcoming this limitation, we aim to design an algorithm that will be computationally faster than AES without compromising the requirement of security.

II. Selective Encryption

The basic selective encryption works as follows. Firstly compression is done on the image. Then the algorithm encrypts only subset of bitstreams with a strong encryption algorithm. Moreover we can add message to this process. For full compatibility assurance with a decoder, only those bitstreams are encrypted that does not compromise the compliance with the original data. This is known as format compliance [1]. Now the encrypted data can be sent through unsecure channel where at the other end the receiver will decrypt the altered image with key and then decompress it to retrieve the message and the original image.



(a) (b)

Figure 1. (a) Selective encryption mechanism (b) When decryption is unknown to receiver [2]

Main features of Selective Encryption are the following

- Time taken to encrypt the subset of data is lower as compared to whole data.
- It encrypts only that subset of data that are very crucial as compared to whole data.
- It conserves resources and power.
- It is format compliant.
- For encryption of data, it can use any encryption algorithm that user wants.
- The cipher appears only as distorted image or video.
- Compression is done on them to make it more distorted.

a) Classification of Selective Encryption

Selective Encryption Algorithms are classified based on following approaches [3]:

1) Precompression

In Precompression method, the compression is done after the encryption. They are inherently format compliant and irrelevant for lossy compression. But drawback of using this method is that it causes bandwidth expansion and adversely impact compression efficiency. Hence this method is not compression friendly

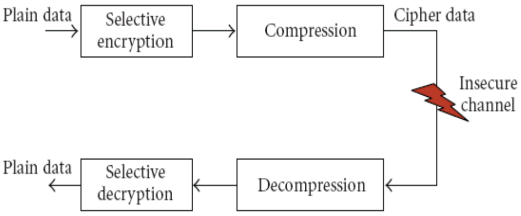


Figure 2: Precompression Approach[3]

2) Incompression

In Incompression based algorithms, both encryption and compression are jointly performed. But in this approach the format compliance and compression friendliness are adversely impacted.

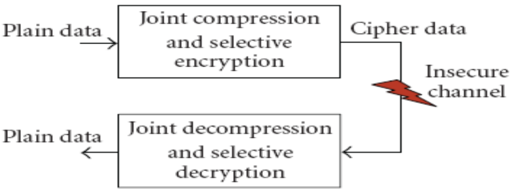

Plain data
Joint compression and selective encryption
Cipher data
Insecure channel
Plain data
Joint decompression and selective decryption

Figure 3: Incompression Approach[3]

3) Postcompression

In Postcompression based algorithms, encryption is done after the compression. This approach is compression friendly. Encryption and decryption does not need any modification at encoder or decoder sides. Moreover, it is nonformat compliant.

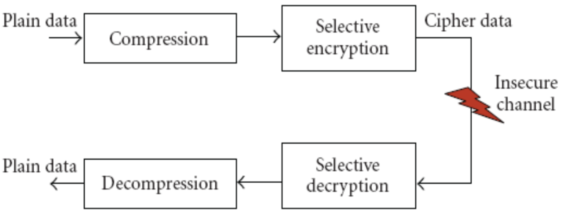


Figure 4: Postcompression Approach[3]

III. Proposed Algorithm

From extensive research and study, it is clear that on using the existing selective encryption on the simple plaintext, it produces cipher faster that the AES but it will not provide necessary security or a strong cipher. We designed an algorithm that overcomes this weakness by applying multiple rounds of selective encryption on plaintext with the help of indexing methods.

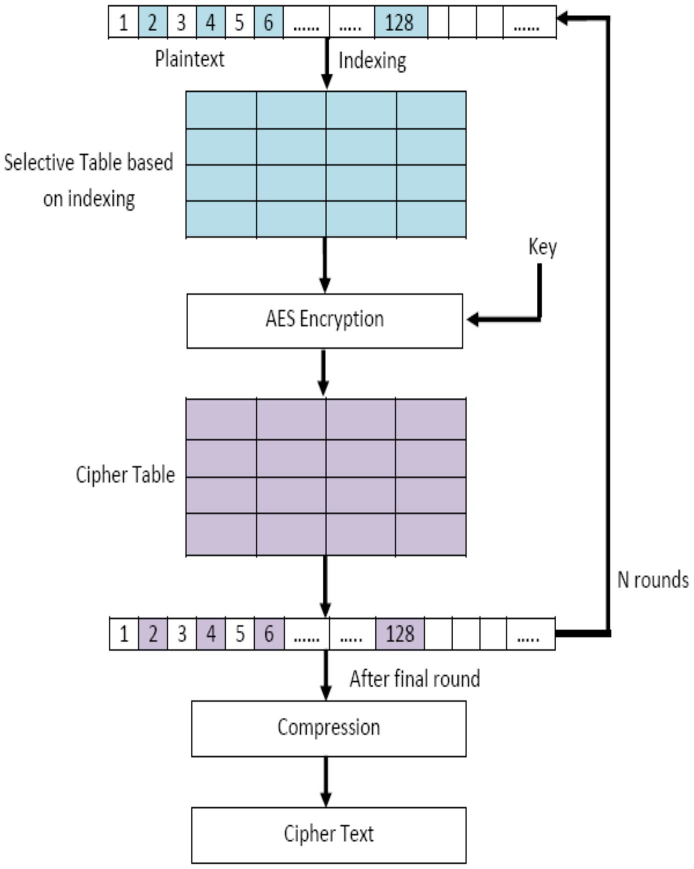


Figure.5. Block Diagram of Selective Encryption of Plaintext using multiple indexing

For encryption technique, we decided to use 128bit AES. Since 128bit AES has 10 rounds we proposed to have maximum number of rounds be 10 rounds. In addition to this, we propose that maximum number of rounds for the proposed algorithm be based on the security level or we can refer it as cipher complexity. Based on different security level as per user requirement, the maximum number of rounds can be selected.

Table 1. Relation Between the Cipher_Complexity and Number of Rounds

Cipher_Complexity	**No. Of Rounds (N)**
Low	3
Medium	6
High	10

Steps of proposed algorithm for encryption

1) Select any one of the indexing methods and generate a list of N index numbers depending on Cipher_Complexity or Number of Rounds.
2) Let X be the first index number for the first round.
3) All the elements in plaintext that is in position of multiples of X are selected to form a string.
4) Since we are using 128bit AES encryption technique we do necessary padding to form multiple Selective Table each of 128bit size.
5) On each Selective Table 128bit AES is applied with the help of key.
6) The generated cipher is replaced to its original position in plaintext.
7) Then next index number is selected for next round and steps 3-6 is repeated until N rounds are completed.
8) After N rounds, the new generated cipher is compressed to reduce the filesize.

We propose three different indexing methods

a) Prime Number Indexing Method

Prime number is an old and famous numbers that are generally used in field of cryptography. They are considered distinctive because on multiplying prime number with any number generates unique and distinctive number. Because of this distinctive feature we decided on prime number as one of the indexing method. For maximum number of 10 rounds list of prime numbers are 2, 3,5,7,11,13,17,19,23 and 29. Example, For first round 2 is the index number and all elements at position of multiples of 2 i.e. 2,4,6,8,10… are selected and encrypted with AES. In this round itself we can assume that the time taken to encrypt half of the elements will be approximately as half as time taken by AES. Similarly for index number 3, it may be approximately one-third of AES. For cipher security, we explain it with help of example of LOW cipher_complexity and as shown in Fig.6. From the figure itself we can conclude that the some elements are encrypted thrice.

b) Random Generator Indexing Method

Random generator is a device that generates a sequence of number that has no pattern. Because of this distinctive feature we decided this as second method for random generator indexing method. For our proposed algorithm, we thought to use basic random generator i.e. Linear Congruential Theorem as explained in [3]. It uses four parameters.

m	the modulus	$m>0$
a	the multiplier	$0<a<m$
c	the increment	$0<=c<m$
X_0	the starting value	$0<=X_0<m$

The sequence of random numbers $[X_n]$ is obtained via the following iterative equation:

$$X_{n+1} = (aX_n+c)\bmod m \qquad (1)$$

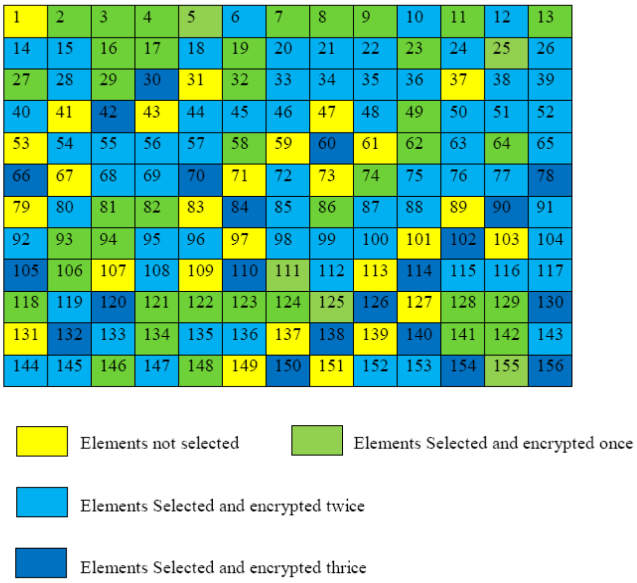

Elements not selected
Elements Selected and encrypted once
Elements Selected and encrypted twice
Elements Selected and encrypted thrice

Figure.6. Elements encrypted in Plaintext while using Prime Number Indexing Selective Encryption method when Cipher_Complexity is Low

c) Mathematical Equation or Series Indexing Method

We can use any mathematical equation or series as the third indexing method. We decided on simple Pythagoras theorem i.e. Pythagoras equation is $H^2 = B^2 + P^2$ where H: Hypotenuse, B: Base, P: Perpendicular. In our algorithm we proposed to use Pythagoras equation with the parameters mentioned in (2).

$$X= \sqrt[2]{(\text{cipher\_complexity})^2 + (\text{prime}[i])^2} \qquad (2)$$

where prime[i] = 2,3,5,7,11,13,17,19,23 and ‘i’ is the i^{th} round.

IV. Conclusion

The main advantage of selective encryption is that it is computationally faster than any hard encryption algorithm such as AES while preserving a level of cipher complexity. Our proposed algorithm is based on exploiting this advantage of selective encryption on simple plaintext. The main application of using the proposed algorithm is that it can be used in mobile nodes, sensor nodes where there is constraint on resource, power consumption and scalability. Our algorithm can meet the requirements of such mobile nodes, sensor nodes without violating the constraints.

The merits of the proposed algorithm are the following.

- Faster Computation than AES.

- Encrypted filesize will be lower than the AES.
- Number of encryption done on some elements of plaintext will be equivalent to maximum number of rounds.
- The algorithm to a limit is dynamic as total number of rounds is not fixed for every new encryption. It is decided by user.

Our future work is the time analysis of the proposed algorithm in java and to do comparative analysis of time complexity and cipher complexity with that of AES. Based on comparison analysis we can find best indexing method. Moreover, we also want to do crypt analysis of the proposed algorithm.

References

[1] W. Zeng, J. Wen, M. Severa , Format-compliant selective scrambling for multimedia access control, Proc. of the International Conference on Information Technology: Coding and Computing, 2002 , p. 77.

[2] Marc Van Droogenbroeck and Raphaël Benedett, Techniques for a Selective Encryption of Uncompressed and Compressed images, Proc. of Advanced Concepts for Intelligent Vision Systems, September 9-11, 2002

[3] A Massoudi**,** F Lefebvre**,** C De Vleeschouwer**,** B Macq and J-J Quisquater **,** Overview on Selective Encryption of Image and Video: Challenges and Perspectives**,** *EURASIP Journal on Information Security,Vol.2008,Article id.17929, 2008*

[4] Stallings,William, Cryptography and Network Security: Principles and Practice(Pearson, 5th Edition,2006, p. 226)