IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Implementing AES Algorithm for Selective Encryption in Wireless Networks

Manjula G.[1], Dr. Mohan H.S.[2]

Associate Professor, ISE, SJBIT, Bangalore, India [1]

Professor & Head, ISE, SJBIT, Bangalore, India [2]

Abstract: The importance given to security in every Internet application is an unblemished spur to contribute in the turf of Information Safety. The evolution of digital data transaction in E-way is expanding, data safety is emerging with much more importance in data storage and broadcast. To defend the data against various attacks and eavesdropping we use a procedure known as Encryption which protects the data. To accomplish this, Encryption algorithms serve a fundamental role in proficient information security structures. Symmetric key algorithms are stereotypically effective and serve to be the fastest cryptosystem and hence have crucial applications in many territories. Selective cryptography is a novel drift in protecting the data. It targets at dropping the volume of data to be encrypted however it aims to attain a satisfactory and economical security. This methodology is predominantly anticipated in controlled communication such as in real time applications with delay limitations, mobile communication with restricted computational power and so on. In this paper, we present the perception of encryption using AES algorithm and selective encryption and the propose a new selective encryption method which is constructed on symmetric key. By exploiting a new probabilistic approach, a sender embraces appropriate ambiguity in the procedure of data encryption, so that only consigned recipient can recover the original data and other illegal systems have no acquaintance of the total conveyed communication. By reducing the amount of encryption i.e. Selective Encryption is a very useful method for the different data formats such as text, video and audio content. This paper discusses the importance of Probabilistic Selective Encryption, their role in ensuring the strength of a cipher system and finally describes a new approach of Encryption using enhanced AES based Selective Encryption.

Keywords: Encryption, Decryption, Cryptography, Advanced Encryption standard (AES), Symmetric Encryption, Asymmetric Encryption.

I. INTRODUCTION

In this rapidly changing Digital epoch, the means of communicating through multimedia components is very demanding and needs topmost security. Various data formats like text, multimedia etc is transmitted using different networking paradigm. Cryptographic practices are mainly utilized to deal with the safeguard of data together with the broadcasting of data over the communication network. With the growth of information technology and increasing demands for information security, the encryption methods have been attracted more and more attention is given on the utilization in recent years. Prevailing encryption systems are classified into three types such as symmetric encryption, asymmetric encryption, and Hash algorithms. Several methodologies are used for providing security amenities like Data Confidentiality, Data Integrity, and Data Validation to provide shield to counter the attacks, such as - discharge of input messages, reforming of message, masquerade etc. To resolve these flaws, the processdevised is known as Encryption which converts plaintext into unreadable format. In contrast, Decryption is the inverse method of the encryption where the encrypted data is converted back to original data. Cryptographic algorithms are classified into Symmetric (private) and Asymmetric (public) keys algorithms. In symmetric key algorithms, a private piece of data known as key is commonly shared between the sender and the recipient(s) throughout the duration of data communication; while, a pair of keys is used by asymmetric key algorithm namely Public Key and Private Key. The public key is normally disseminated, whereas private key is earmarked to be confidential. For a symmetric key algorithm, both the communicating parties would have recognized the common key well in advance, and utilize the same key for encryption and decryption. Clearly, such a key would be symmetric for both parties of the communicating parties. Nevertheless, the distribution of the shared key has to be very confidential; a secure method for key distribution and key management has to be devised. In contrast to symmetric method , an asymmetric key algorithm marks the practice of using two keys namely public key and private key which are dissimilar

The process of selecting a standard Encryption algorithm was initiated by the National Institute of Standards and Technology (NIST) which called for contenders to substitute the aging and antiquated Data Encryption Standard (DES) in the year 1997. NIST then proclaimed that Rijndael was the proposed Advanced Encryption

DOI10.17148/IJARCCE.2017.63149

Standard (AES) [1].The Symmetric Encryption category is significant in advanced cryptography, the purpose being it is more rapid as compared to the Public key Cryptosystem [2]. The usage of the images is tremendous in internet, social networks, medicine, and other aspects of life. [3]. The message should be conveyed at a faster rate and efficiently through the network and in a very secure way. Various algorithms have already been recommended for protecting the data over various network but any algorithm for doing this takes time to encrypt the data. To overcome the time limit for encryption it has been proposed that Selective encryption is a method of enciphering only few parts of a data file while leaving other parts of the data unencrypted. As information security is becoming a crucial civic concern now a days, data encryption is becoming pervasive for transmission of any type of crucial and sensitive data. The overhead incurred for data encrypting can be minimized by using an effective encryption method. The encryption algorithms are predominantly pragmatic in the jurisdictions of energy-efficient atmospheres. For multimedia communications, which involves real-time data transmission, stupendous multimedia content need to be conveyed securely? Selective Encryption algorithm diminishes the overall cost and time without negotiating the security of the system.

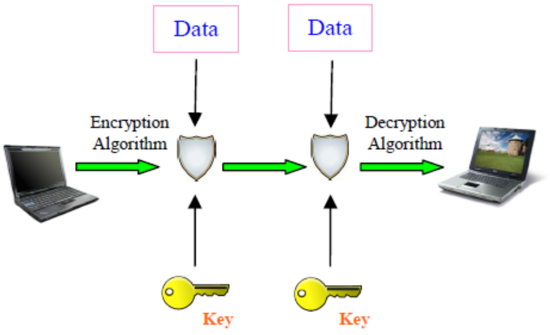


Figure 1 Encryption and Decryption Process

The concept of private key encryption and decryption procedure is illustrated in Figure 1. The mobile devices in a wireless network are commonly exhilarated with the use of batteries as their back up power supply and in general will have restricted computational power and the concept of saving energy is to be addressed first. Hence, an effective selective encryption algorithm would be a probable purpose to save substantial power for wireless devices, and to offer ample security for data communication [4].

II. THE ADVANCED ENCRYPTION STANDARD(AES)

AES is a popularly used block cipher technique that usually encrypts and decrypts data with data block of 128 bits. This algorithm uses 10, 12, 14 rounds of transformation. The key which is given to the algorithm is expanded into the 44 words each comprising of 4 bytes each. The key size used in the AES algorithm can be 128,192,256 bits and depends on the number of rounds AES supports the use of key lengths 128, 192, and 256 bits [5]. All rounds of encryption and decryption will pass through Nr rounds (Nr=10, 12, 14) [6] [7][8]. The following Figure 2 illustrates the structure of AES algorithm.

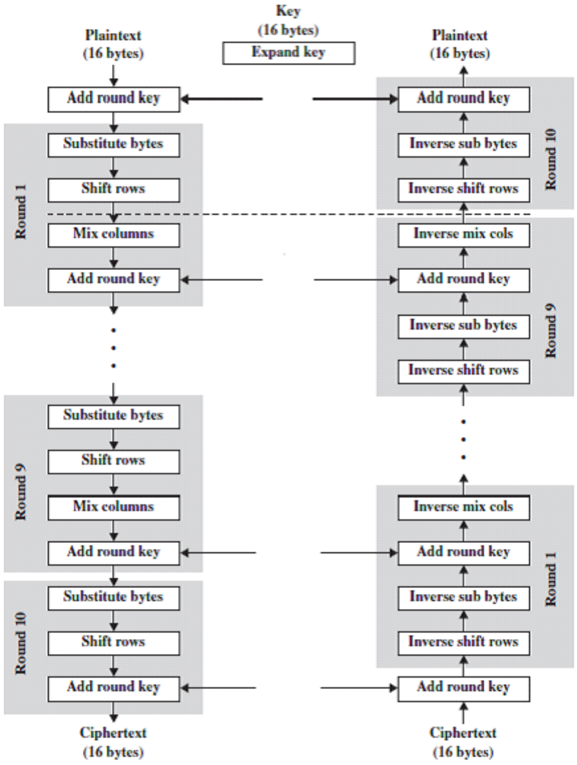


Figure 2: AES algorithm

III.THE SELECTIVE ENCRYPTION ALGORITHM AND DATA EMBEDDING

The perseverance of selective encryption algorithms is to encrypt limited slices of the original data with reduced overall calculation; on the other hand tolerable number of messages are encrypted to offer consistent protection to secure the message confidentiality [9]. By using selective encryption, it is not mandatory for all messages to be encrypted and the complete data communication can be observed to be secure. Hence the total processing time of encryption is reduced in Selective encryption practice. In the philosophy of selective encryption algorithms, ambiguity is tangled in the message encryption course to define the undefined form of encrypted messages and thereof it surges uncertainty which can boost the security of data communication, since all messages are acknowledged to possess indistinguishable prominence. Consequently, ambiguity turns out to be one of the governing issues when devising a selective-based cryptosystem. Generally, the existence of additional ambiguity makes cryptosystem most efficient. However, this technique can also decrease the complexity of the design. Figure 3 illustrates the procedure for selective encryption process

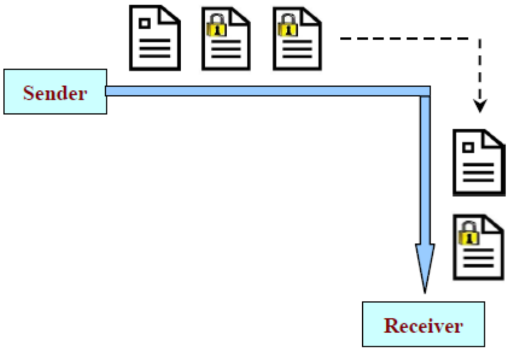


Figure 3 Selective Encryption and Decryption Process

In this paper improved method of AES algorithm is used. Here, the input size is increased from 4*4 matrix to 8*8 matrix. Rijndael was developed by Joan Daemen and Vincent Rijmen and is a block cipher. The AES algorithm supports any combination of data and key size of 128, 192, and 256 bits. Nevertheless, AES basically allows a 128 bit data block to be distributed into four basic operational blocks. These blocks function on an array of bytes and are structured as a 8*8 matrix that is termed the state array [6]. For complete encryption, the data has to be passed through Nr rounds (Nr = 10, 12, 14) .The purpose of using enhanced AES algorithm is to increase processing speed and to increase the volume of data to be directed in less time. The purpose is to encrypt messages with less energy consumption but at the same time data should be encrypted in order to secure data confidentiality [10]. The concept of selective encryption is briefly described in [11] and they have proposed a selective encryption algorithm which is probabilistically in nature and is based on symmetric key. This technique is termed to be one of the most encouraging and reliable solutions which reduces the overall cost of data protection in environments where energy plays a very important role such as MANETS and wireless networks. In order to increase the security, the encrypted data is implanted into image to enhance the security using lossless technique. Data implanting using images has exhibited incredible interest, which is done by using either lossy or lossless techniques. Since lossy techniques allows huge hiding capability, host image cannot be recuperated with great reliability.

IV. PROBABLISTIC SELECTIVE ENCRYPTIONALGORITHM

In the theory of probabilistic methodology, it is designed to achieve or obtain adequate uncertainty. In the method of delivering messages, the sender will arbitrarily generate a value which is used to designate the percentage of encryption, which signifies the number of messages that are determined to be encrypted from the total communicated messages. The sender then utilizes a probabilistic function which is used to select the previously determined quantity of messages to encrypt them. Figure 4 demonstrates the overall flow of the probabilistic selective encryption. We can conclude that more the ambiguity is involved in the probabilistic encryption algorithm more is the encryption achieved.

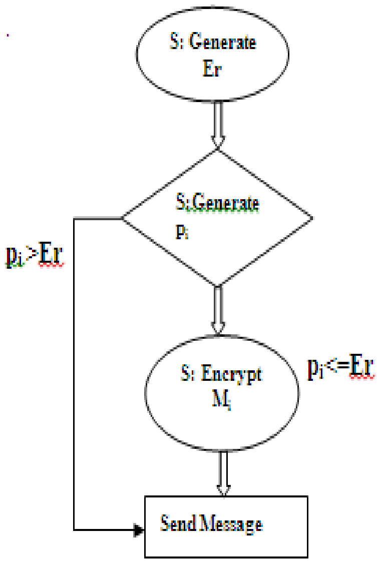


Figure 4:Flow chart of probabilistic approach

1) The sender/producer of transmitting nodeshas to first select a random number Er (Encryption Ratio) which is by generated by a random generator RNG andwhich governs the proportion of encrypted messages among the total messages. The generated encryption ratio should be such that it is greater than a pre-determined threshold value which confirms that a minimum number of messages are encrypted so as to create uncertainty.

2) Next the sender must install a probabilistic function PF to produce a possibility value for encryption pi to define if a message Mi will be encrypted or not.

3) Finally, the sender opts for the messages to be encrypted which is determined based on the above calculated encryption ratio Er. For example, the sender S will decide based the encryption probability pi whether to encrypt a message or not. If the value of pi generatedis less than or equal to the encryption ratio Er, then the message Mi will be encrypted using its secret key SK; else, this message will not be encrypted.

VI. DATA EMBEDDING

The main objective of embedding is to safeguard the message so that the opponent cannot perceive the existence of message inside the cover image. The quality of cover image and the process of embedded data security are two major concerns that are to be deliberated throughout the process of the data embedding. SDEM-DCT (Scramble Data Embedding in Mid-frequency range of DCT) Algorithm is used for the embedding purpose. In this adaptive mid frequency DCT coefficients substitution has been designed to hide the message data inside the cover image. In this method encrypted data and image are given as the input for the embedding purpose. Extracting the data is precisely the opposite of our embedding algorithm in addition; the receiver has to identify the keys for de-embedding process. The main aim is to make use of high and trusted Scramble and Descramble Algorithm which can hide data inside the mid frequency range of DCT matrices and achieve maximum security.

VII. EXPERIMENTAL RESULTS

This section discusses the experimental results obtained. The code was implemented using MATLAB. Figure 5 illustrates the cover image used for encryption and Figure 6 shows the secret image used to embed the encrypted image

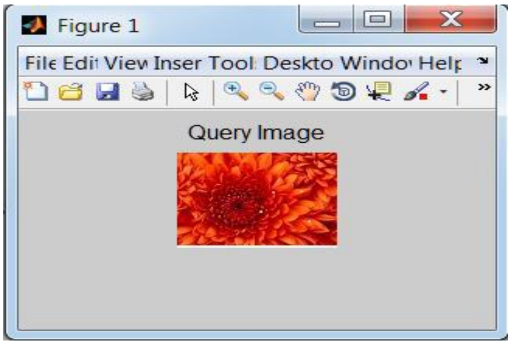


Figure 5 Cover Image

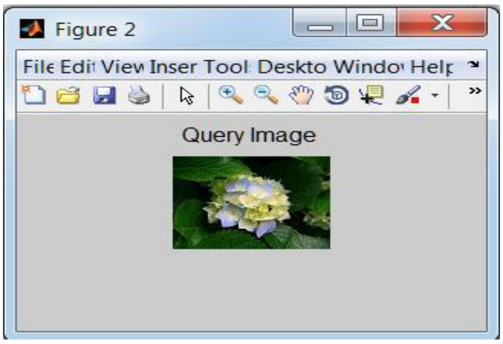
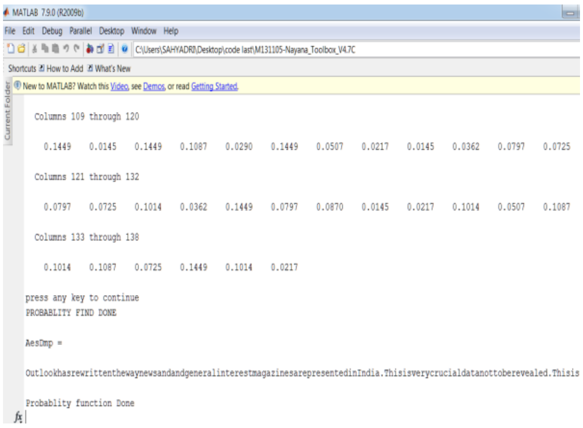


Figure: 6 Secret Image


MATLAB 7.9.0 (R2009b)
File Edit Debug Parallel Desktop Window Help
C:\Users\SAHYADRI\Desktop\code last\M131105-Nayana_Toolbox_V4.7C
Shortcuts How to Add What's New
New to MATLAB? Watch this Video, see Demos, or read Getting Started.
Current Folder

```
  Columns 109 through 120

    0.1449    0.0145    0.1449    0.1087    0.0290    0.1449    0.0507    0.0217    0.0145    0.0362    0.0797    0.0725

  Columns 121 through 132

    0.0797    0.0725    0.1014    0.0362    0.1449    0.0797    0.0870    0.0145    0.0217    0.1014    0.0507    0.1087

  Columns 133 through 138

    0.1014    0.1087    0.0725    0.1449    0.1014    0.0217

press any key to continue
PROBABLITY FIND DONE

AesDmp =

OutlookhasrewrittenthewaynewsandandgeneralinterestmagazinesarepresentedinIndia.Thisisverycrucialdatanottoberevealed.Thisis

Probablity function Done
fx
```

Figure 7: Probability calculation and encryption

A probability function is used to calculate the probability of every message and then is compared with the Encryption ratio to determine if the message is encrypted or not. The following screen shots shows the probability calculation, encryption and embedding of secret data.

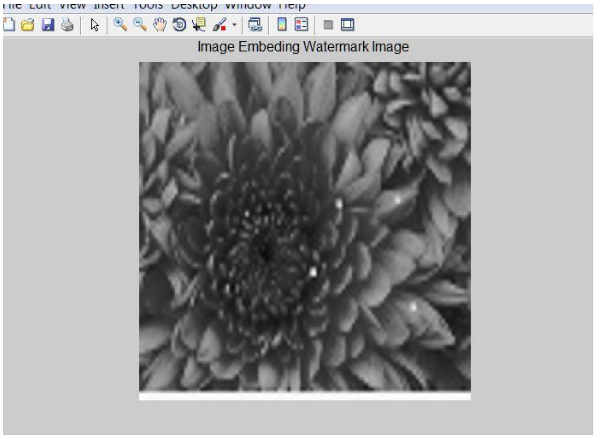

File Edit View Insert Tools Desktop Window Help
Image Embeding Watermark Image

Figure 8: Watermarked image

These screen shots shows de-embedding of original data from the cover image.

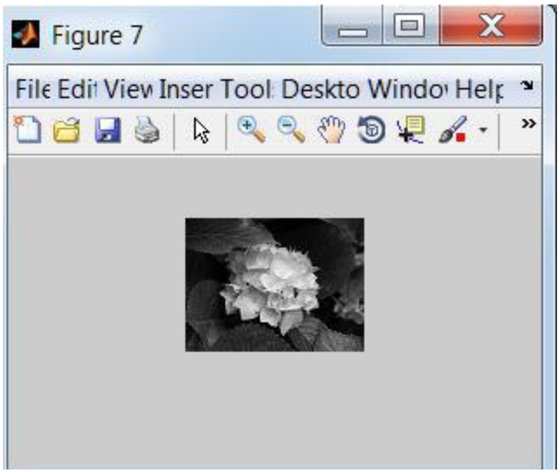
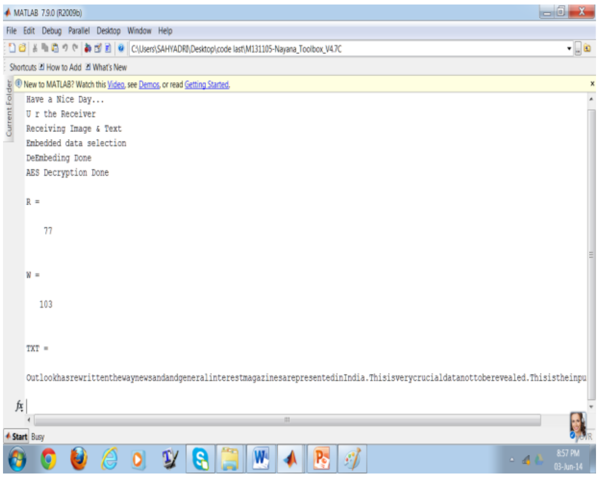


Figure 9: De-embedded image at the receiver side


MATLAB 7.9.0 (R2009b)
File Edit Debug Parallel Desktop Window Help
C:\Users\SAHYADRI\Desktop\code last\M131105-Nayana_Toolbox_V4.7C
Shortcuts How to Add What's New
New to MATLAB? Watch this Video, see Demos, or read Getting Started.
Current Folder
Start Busy
8:57 PM
03-Jun-14

```
Have a Nice Day...
U r the Receiver
Receiving Image & Text
Embedded data selection
DeEmbeding Done
AES Decryption Done

R =

    77



W =

   103



TXT =

OutlookhasrewrittenthewaynewsandandgeneralinterestmagazinesarepresentedinIndia.Thisisverycrucialdatanottoberevealed.Thisistheinpu
fx
```

Figure 10: De-embedded data at the receiver side

VIII. CONCLUSION AND FUTURE WORKS

Hypothetical results demonstrate that the proposed probabilistic selective encryption algorithm can be one of the most promising solutions in the area of information security which reduces the cost of data protection in wireless networks. The proposed approach is most suitable and gives better results when compared to other approaches. Thus, our solution delivers a realistic solution for protected wireless communication. Future work can be done to study the use of different packet sizes and the proposed method should be able to handle different kinds of data like videos, PDF etc.

REFERENCES

[1] Trappe, W. and Washington, L. C.: Introduction to Cryptography with Coding Theory. United States: Prentice Hall, (2002).

[2] C.S Lamba, "Design and Analysis of Stream Cipher for Network Security", Second International Conference on Communication Software and Networks, 2010.

[3] Rafael C. Gonzalez, "Digital Image Processing",2009.

[4] Yonglin Ren, Azzedine Boukerche and Lynda Mokdad," Performance Analysis of a Selective Encryption Algorithm for Wireless Ad hoc Networks" International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 183-188 The Society of Digital Information and Wireless Communications (SDIWC) 2012 (ISSN: 2305-0012)

[5] Daemen, J., and Rijmen, V.: The block cipher Rijndael. Proceedings of the Third International Conference on smart card Research and Applications, CARDIS'98, 1820, pp. 277-284, Berlin: Springer, (2000).

[6] Stallings, W.: Cryptography and Network Security, Prentice Hall, (2010).

[7] Daemen, J. and Rijmen, V.: The First 10 Years of Advanced Encryption. In IEEE Security and Privacy, vol. 8, pp. 72-74, November (2010).

[8] Federal Information Processing Standards Publications FIPS 197, Advanced Encryption Standard (AES), 26 Nov (2001).

[9] A. Boukerche, "Algorithms and Protocols for Wireless, Mobile Ad Hoc Networks", Wiley & Sons, 2008.

[10] Chi-Feng Lu , Fast implementation of AES cryptographic algorithms in smart cards; Yan-Shun Kao; Hsia-Ling Chiang; Chung-Huang Yang; Security Technology, 2003.

[11] Yonglin Ren, Azzedine Boukerche, Lynda Mokdad, "Performance Analysis of a Selective Encryption Algorithm for Wireless Ad hoc Networks", IEEE WCNC 2011-Network.

DOI10.17148/IJARCCE.2017.63149