ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Advanced Text to Image Encryption by Using Selective Encryption Technique with C# (AES Encryption and CFB Mode)

Sadhana Singh, Ashish Agrawal and Priyanka Pradhan

Assistant Professor, Dept. of I.T., SRMSCET, Bareilly, India

Assistant Professor, Dept. of CSE., SRMSCET, Bareilly, India

Assistant Professor, Dept. of CSE/I.T., MJPRU, Bareilly, India

ABSTRACT: Image applications have been growing in modern years. In this paper novel Advanced Encryption Standard (AES) encryption image schemes based on secret key cipher block and BitMap (BMP) image file format are proposed. We have to encrypt or decrypt any data or image for providing the network security. This paper simply describes the images protection when we transmit from one place to another. AES encryption technique is one type of selective encryption. The AES algorithm is always worked with the Cipher Feedback (CFB) mode. While transferring the image from one place to other, there is a problem occurred with the size of the image or the resolution of the image, in this condition we simply compress the image by using the lossless image compression technique. In this paper, we use the Huffman lossless image compression technique for compressing the image which is generated by the text to image encryption. In this paper, we take a text and convert it into image with C# for providing the network security.

KEYWORDS: Huffman Coding, Image Encryption, Image Decryption, AES, CFB.

I. Introduction

Network security is an important factor in communicating and transferring the data from one public network to another. The information security is based on four basic principles: Confidentiality, Authentication, Integrity and Non-repudiation. In confidentiality, sender and receiver can access the contents with their secret keys whereas authentication helps in the proof of the identities. Integrity focuses on the originality of the content. Non-repudiation says particular information should not be sent again and again. In this paper we made an effort for making information sharing more secure with the use of AES technique of cryptography and C# language. Table 1 shows some basic concepts of cryptography.

Table 1. Cryptographic Process for any Text

Plain Text: Original / readable text	**Encryption:** Conversion of message
Cipher Text: Encrypted text / Cryptogram.	**Decryption:** Getting back the original message.

Public Key Encryption: Here, both the sender and receiver know about the keys. We use the pair of different keys for encrypting and decrypting the data. Public key is distributed to everyone for communication. Every user has public and private key pair. Public key encryption is slower as compared to the private key encryption.

Private Key Encryption: Here, one single key is used for encryption and second key is used for decryption. Both the senders and receiver share the same key. If the sender encrypts the message by one key then receiver decrypt the message by the same key. Systematic key management or the transfer of key is a major concern while using private key encryption [4]. In this paper we use the block cipher system for the encryption and the decryption of the information.

AES Algorithm: AES Algorithm is based over a cryptographic technique “Rijndael” which is a block cipher technique developed by Joan Daeman and Vincent Rijmen [5]. This algorithm is very flexible and it supports 128, 192,

DOI: 10.15680/IJIRCCE.2016. 0408103

and 256 bits of the combined data and their size. The plain text must be 128 bit long and which is divided into the four main blocks on which we performs the operations. These block functions work with an array of the size 4x4 matrix. For getting the complete encryption, the numbers of cycle's repetition are occurred: 10 cycles of the repetition defined for 128-bit keys; 12 cycles of the repetition defined for 192-bit keys;14 cycles of the repetition defined for 256-bit keys.

These repetitions achieve the following transformations:

Subbyte Transformation: This transformation is the linear byte Substitution step. Substitution is done with the help of the substitution table or S-box. Affine Transformation and multiplicative inverse are the basic building blocks for designing the substitution table [2]. In this one byte is replaced with another byte by using the substitution table.

Shift rows Transformation: This is the simple Transposition technique for bytes. In this transformation bytes is in the last three rows of any state are shifted at regular intervals and equalize of the left shift varies from one to three bytes.

Mix columns Transformation: This transformation is based on the matrix multiplication of the columns in which each column is multiplied by a fixed matrix. In this bytes are always treated as the polynomials rather than the numbers [2].

Add round key Transformation: This transformation is defines the simple bitwise XOR function between the round keys and the working state of the keys. In this the sub key is working together with the state.

Inverse Substitute Bytes: This is the reverse process of the Substitutes Bytes transformation. In this we use the inverse of the S-box for each byte of the state. Inverse is obtained by the inversion of the affine transformation by using the multiplicative inverse.

Inverse Shift rows: This process is the inversion of the Shift rows transformation. In this the first row of the state always same or not changed. The bytes of the second, third and fourth rows of the state are shifted cyclically by one, two and three bytes to the right respectively [2].

Inverse Mix columns: This process is the inverse of the Mix columns transformation. In this every column of the state considered as a polynomial. Modulo x4+1 is multiplied with the fixed polynomial and the result is generated corresponding to the column of the output state [2].

Table 2. AES algorithm with bytes and words

Number of Key Sizes of AES algorithm	**Bytes**	**Words**
AES-128 bit	16	4
AES-196 bit	24	6
AES-256 bit	32	8

AES algorithm can easily encrypt any text or image as compared to the DES (Data Encryption Standard), so there is no type of weaknesses are found. AES is the block cipher technique and this is extremely fast as compared to the other block cipher techniques. In the fig. 1 [16], we see the algorithm of AES encryption algorithm.

Cipher Feedback Mode: Cipher Feedback mode is the block of mode cipher operation. This is used as a random number generator.

In CFB mode we encrypt the block of plain text and generate the cipher text in the form of the block, and then the previous cipher text is encrypted with the help of the XORed function. This process is works when the final output block is not generated. For first time encryption of the plain text in the block, we use the Initialization Vector (IV). If we calculate Cipher Text from the Plain Text then we use the equation 1.

$$C_i = E_K(C_{i-1}) \oplus P_i \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

If we calculate the Plain Text from the Cipher Text then we will use the equation 2.

$$P_i = E_K(C_{i-1}) \oplus C_i \ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Initially we initialize the Initialization Vector which is shown in the equation 3.

$$C_0 = \mathrm{IV} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

All the three equation 1, 2 and 3 [6] are important for calculating the Plain Text and the Cipher Text of the information.

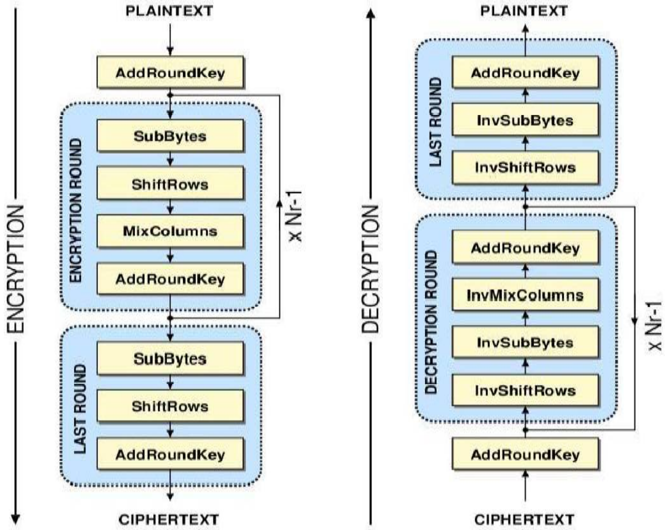


Fig. 1. AES Encryption and Decryption Algorithm

Huffman Algorithm: Huffman coding is an entropy encoding algorithm used for lossless data and image compression. The term refers to the use of a variable- length code table for encoding a source symbol (such as a character in a file) where the variable-length code table has been derived in a particular way based on the estimated probability of occurrence for each possible value of the source symbol. It was developed by David A. Huffman. Huffman Algorithm is discussed in [15].

II. RELATED WORK

This paper is based on the work done by Ahmad Abusukhon and Mohammad Talib [7]. In their Algorithm, the data is encrypted in two levels. In first level Text-To- Image Encryption is done which is designed by the authors of this paper while in second level Image-Shuffle Encryption is done which is based on efficient digital encryption algorithm based on matrix scrambling technique [8].

In their proposed algorithm they used AES encryption stage in which encryption of image uses a key following the AES algorithm, the AES has been extensively adapted for encryption of data but now a day's frequently used in encryption of images as well [2]. Praveen.H.L, H.S. Jayaramu, M.Z.Kurian [9] has developed a model which encryptions of the images are obtained from satellites. To prevent this error free encryption, scheme is proposed in On-Board. They states that AES provides an error-free encryption system and error are much more reduced even in radiation in satellites.

Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari and Hamida Almangush [10] has used AES algorithm for encryption of image in which firstly they have rotated the plain image to generate another image with the help of magic cube. Jawad Ahmad and Fawad Ahmed [11] have compared the two encryption algorithms namely Advanced Encryption Standard (AES) and Compression Friendly Encryption Scheme (CFES). They have explored the security estimations of AES and CFES for digital images against differential attacks, statistical and brute-force the calculated results are used to test the security of these algorithms for digital images shows some weaknesses in CFES. Manoj. B, Manjula N Harihar [12] states that Encryption and Decryption of image using AES can be designed and implemented to protect the confidentiality of image data. P. Radhadevi, P. Kalpana [13] has presented the encryption & decryption of an image using AES algorithm, they have concluded that the AES can be used very efficiently to secure image transmission.

P.Karthigaikumar , Soumiya Rasheed [14] has used AES algorithm in simulating of image encryption, they have implemented the AES algorithm in MATLAB on Xilinx platform, Timing simulation is performed that verifies the functionality of the designed circuit. Sourabh Singh and Anurag Jain [2] have used the AES algorithm for substitution of RGB for encrypting Text to image. They have implemented the AES algorithm in JAVA. In this paper they have encrypted the text into image in the PNG format which is the lossless compression format. This is the drawback of this paper.

III. PROPOSED ALGORITHM

In this section we describe the proposed model for the encryption and decryption. This algorithm is designed to improve the algorithm given by the Sourabh Singh and Anurag Jain [2]. In this paper we show the text to image encryption in the BMP file format which is lossless. BMP files are found in the uncompressed form, and so we need to compress the image. The main drawback of their algorithm is that they used

.png formatted image which is lossy. Figure 2 shows the proposed model or proposed algorithm for text to image encryption.

From sender side we firstly generate a random number N. Random number N is matched in the Combination Database (CD). Then we transfer the random numbers for each character. In the proposed model R1, R2… R36 are the random numbers for encrypting the text into image. Random numbers are generated with the help of the Cipher feedback mode.

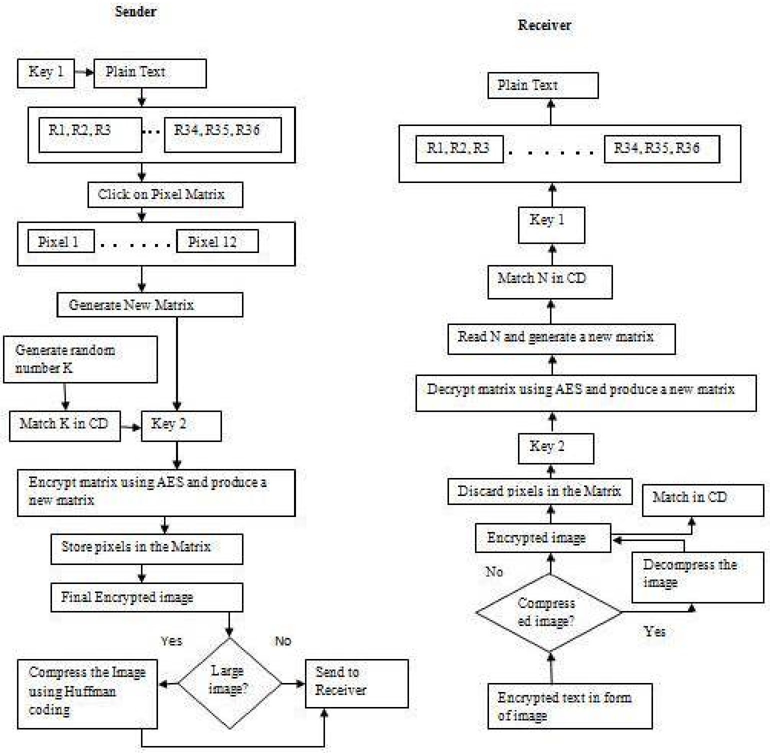
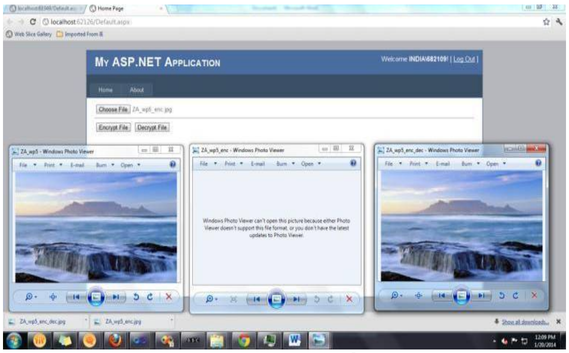


Fig. 1. Proposed Algorithm for Text to Image Encryption

IV. IMPLEMENTATION AND RESULTS

In this paper we use the encryption and decryption of the images or the text to image is shows. We use the .NET framework for the implementation and use the C# language. For encryption and decryption of the image we simply take a one image which is in the JPEG form and then we encrypt and decrypt the images. This is shown in the figure 3. In the figure 4, 5, 6 and 7 we show the text to image encryption and in this we take the text “I am Sadhana A Master of Technology student”. For the encryption we firstly made the text file and then we encrypt it with the help of the key. For the encryption we define the image in the form of the BMP, in this condition we need to compress the image and then decompress the image. For the decryption process we firstly took out the same image. For the second time we take the text for the encryption and decryption is the abstract of my paper. In this we also took out the same procedure for the encryption and decryption. In figure 8 we see the final decrypted image after performing the compression because

BMP image file formats are large in size.



Windows Photo Viewer can't open this picture because either Photo Viewer doesn't support this file format, or you don't have the latest updates to Photo Viewer.

Fig. 2. Image Encryption and Decryption

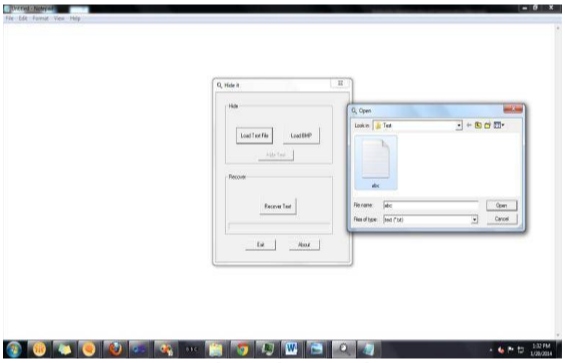


Fig. 3. Choose the Text File

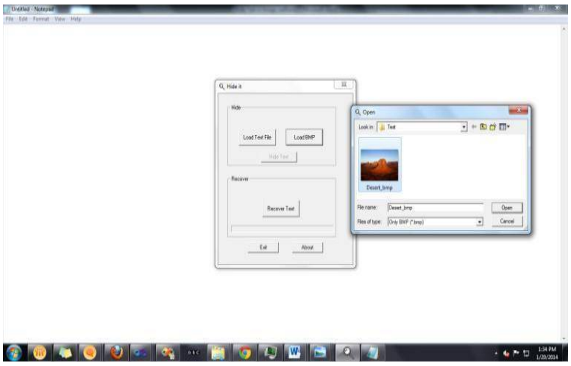
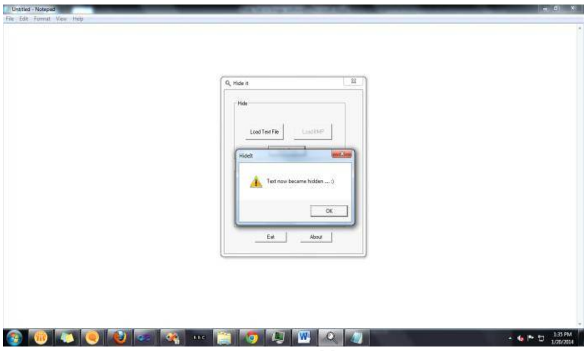
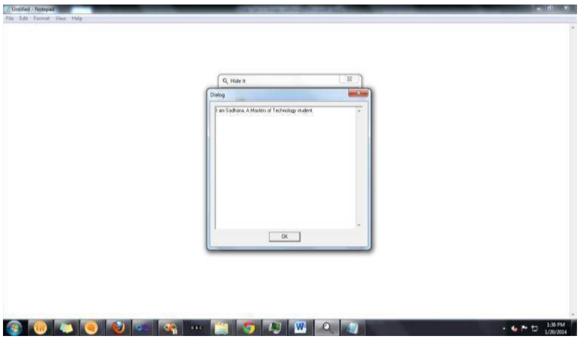


Fig. 4. Text to Image Encryption



Text now became hidden .... :)

Fig. 5. Text is Hidden



I am Sadhana. A Masters of Technology student.

Fig. 6. Decryption of Image to Text

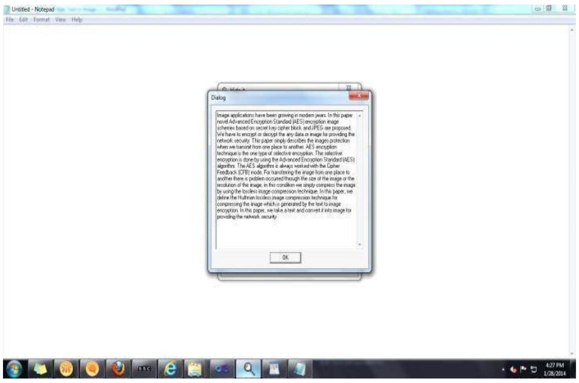


Image applications have been growing in modern years. In this paper novel Advanced Encryption Standard (AES) encryption image schemes based on secret key cipher block, and JPEG are proposed. We have to encrypt or decrypt the any data or image for providing the network security. This paper simply describes the images protection when we transmit from one place to another. AES encryption technique is the one type of selective encryption. The selective encryption is done by using the Advanced Encryption Standard (AES) algorithm. The AES algorithm is always worked with the Cipher Feedback (CFB) mode. For transfering the image from one place to another there is problem occured through the size of the image or the resolution of the image, in this condition we simply compress the image by using the lossless image compression technique. In this paper, we define the Huffman lossless image compression technique for compressing the image which is generated by the text to image encryption. In this paper, we take a text and convert it into image for providing the network security.

Fig. 7. Decryption Process

V. Conclusions and Future Scope

In this paper we encrypted the text to image by using the AES algorithm. We use the key size for the text to image compression in this paper is 256 bits. We also use the cipher feedback mode for the encryption and decryption in the block form. In this paper we show the image encryption and decryption on the JPEG file format. And for the text to image encryption and decryption with the help of the BMP file format. So for this we define the Huffman compression on the image. In future we work on the different image formats for encrypting the text into image. Different image formats like gif, tif, etc, or we also implement text to image with other techniques.

References

1. Atul Kahate, Cryptography and Network Security, Second Edition, Tata McGraw-Hill Edition-2008.
2. Sourabh Singh, Anurag Jain, "Combination of RGB Substitution for Text to Image Encryption Technique using AES", Proceedings of ICRTES'13 Organized by SPVRYAN, Nashik, Maharashtra, India.
3. Stalling, W. (2005) "Cryptography and Network Security Principles and Practices, 4th Edition Prentice Hall". Available at: http://www.filecrop.com/Cryptography-And-Network-Security-4th Edition.html.
4. Dr. Mahesh Motwani, "Cryptography and Network Scurity", Balaji Learning Book.
5. AES.pdf http://www.facweb.iitkgp-ernet.in/~sourav/AES.pdf.
6. http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Cipher_feedback_.28 CFB.29
7. Ahmad Abusukhon Mohammad Talib "A Novel Network Security Algorithm Based on Private Key Encryption" IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012.
8. Kiran Kumar, M., Mukthyar Azam, S., and Rasool, S. (2010) "Efficient digital encryption algorithm based on matrix scrambling technique". International Journal of Network Security and its Applications (IJNSA), 2(4).
9. Praveen.H.L, H.S Jayaramu, M.Z.Kurian "Satellite Image Encryption Using AES" International Journal of Computer Science and Electrical Engineering (IJCSEE), Vol-1, Iss-2, 2012.

10. Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari and Hamida Almangush “A Novel Image Encryption using an Integration Technique of Blocks Rotation based on the Magic cube and the AES Algorithm” International Journal of Computer Science Issues (IJCSI); Vol. 9 Issue 4, p41 Jul2012.
11. Jawad Ahmad and Fawad Ahmed “Efficiency Analysis and Security Evaluation of Image Encryption Schemes” International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 12 No: 04.
12. Manoj.B, Manula N Harihar “Image Encryption and Decryption using AES” International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249– 8958, Volume-1, Issue-5, June 2012.
13. P. Radhadevi, P. Kalpana “Secure Image Encryption Using AES” International Journal of Research in Engineering and Technology Volume: 1 Issue: 2.
14. P.Karthigaikumar Soumiya Rasheed “Simulation of Image Encryption using AES Algorithm” IJCA Special Issue on Computational Science - New Dimensions & Perspectives” NCCSE, 2011.
15. http://en.wikipedia.org/wiki/Huffman_coding
16. http://www.scribd.com/doc/159903373/An-Enhanced-Text-to-Image-Encryption-Technique-using-RGB-Substitution-and-AES
17. Vadivel, R and V. Murali Bhaskaran,’Energy Efficient with Secured Reliable Routing Protocol (EESRRP) for Mobile Ad-Hoc Networks’, Procedia Technology 4,pp. 703- 707, 2012.

BIOGRAPHY

Sadhana Singh is a Assistant Professor in the Information Technology Department, Shri Ram Murti Smarak College of Engineering and Technology, Bareilly. She received Master of Technology (M.Tech) degree in 2015 from SRMSCET, Bareilly, India. She has more than 25 publications including international journals and international conferences. She has qualified the GATE 2012. She has 02 years of teaching experience. Her research interests are Image Processing, Software Engineering, Fuzzy Logic, Genetic Algorithm, Information Technology, etc.

Ashish Agrawal is a Assistant Professor in the Computer Science and Engineering Department, Shri Ram Murti Smarak College of Engineering and Technology, Bareilly. He received Master of Technology (M.Tech) degree in 2015 from SRMSCET, Bareilly, India. He has more than 25 publications including international journals and international conferences. He has more than 20 publications including international journals and international conferences. He has 03 years of teaching experience. His area of interest includes Software Engineering, Agile Development, Information Technology, etc.

Priyanka Pradhan is a Assistant Professor in the Computer Science and Engineering/Information Technology Department, MJPRU, Bareilly. She received Master of Technology (M.Tech) degree in 2015 from SRMSCET, Bareilly, India. She has more than 7 publications including international journals and international conferences. She has 01 years of teaching experience. Her research interests are Image Processing, Software Engineering, Information Technology, etc.