INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

REVIEW OF IMAGE ENCRYPTION TECHNIQUE BASED ON AES

Rufina Tresa Mendez[1], Dr. V.S Jayanthi[2], P. Geetha[3]

[1]*PG Scholar, Department of Electronics and Communication Engineering, HICET, Coimbatore.*
[2]*Professor, Department of Electronics and Communication Engineering, HICET, Coimbatore.*
[3]*Assistant Professor, Department of Electronics and Communication Engineering, HICET, Coimbatore.*

HINDUSTHAN COLLEGE OF ENGINEERING AND TECHNOLOGY, OTTHAKALMANDAPAM, COIMBATORE, INDIA

Abstract

Encryption of images has become a necessity in today's world to protect a confidential image from unauthorized access. Various methods have been proposed and developed in spatial, frequency and hybrid domains to encrypt the image securely. Encryption could either be a full encryption or partial encryption based on the security requirements. In this paper we present an overview of various image encryption techniques based on AES.

Keywords- AES, Image Encryption, Security, Cryptography

1. Introduction

Cryptography is as old as human history. Introduction of digital computation has made information exchange fast and simple. Maintaining confidentiality is a challenge in modern communication. Most crypto-algorithms rely on mathematical problems that are considered very difficult to solve.

The first widely used encryption algorithm was Digital Encryption Standard (DES). It made use of 56 bit cipher keys and hence the possible number of keys was 2^{56}.

AES is a symmetric key encryption algorithm and represents the evolution of DES .It was defined in 2000. Cipher keys of 128 bits[2] are adopted and the possibility of brute force decryption is made practically impossible.

AES due to the following strengths is considered suitable for image encryption [15] [16].

- It is resistant to known attacks and mathematically sound.
- AES is faster compared to other block ciphers; however there is a tradeoff between size and speed.
- The algorithm is suitable across a wide range of hardware and software systems.
- The algorithm is simple and compact.

- AES is fully self-supporting. It does not use S-boxes or bits from Rand tables.
- AES is designed to be compliant to pipelining
- The parallel design of round transformation is useful in dedicated hardware as it allows faster computation.

2. AES Algorithm

AES is a block cipher with block length of 128 bits [15]. AES allows three different key lengths of 128, 192 or 256 bits. Encryption consists of 10 rounds of processing for 128 bit keys, 12 rounds for 192 bit keys and 14 rounds for 256 bit keys. Except for the last round in each case, all other rounds are identical. Each round of processing includes one single byte based substitution step, row wise permutation step, a column wise mixing step and addition of round key. The order in which these four steps are executed is different for encryption and decryption.

Each round of processing works on the input state array and produces and output state array. The output state array produced by the last round is re-arranged into a 128 bit output block. AES varies slightly from the Rijndael Cipher algorithm as it requires the block size to be 128 bits, whereas the Rijndael cipher works with any block size that is a multiple of 32 as long as it exceeds 128. AES uses a substitution –permutation network. Each round of processing in AES involves byte level substitutions followed by word level permutation.

Prior to the round based processing for encryption, the input state array is XORed with the first four words of the key schedule. The same process happens during decryption, except that the cipher text state array is XORed with the last four words of the key schedule.

AES is a suitable scheme for encryption of images. On integration with other techniques the image becomes more secure

We present here the various image encryption techniques based on AES

J. M Rodrigues et al [1] proposed a selective encryption scheme for color image based on AES stream ciphering using Variable Length Coding (VLC) of the Huffman's vector. The non-zero AC coefficients in Huffman's bit stream from highest to lowest frequencies are used to build the plaintext vector. The vector is encoded with AES in CFB mode. The original Huffman's bit stream is substituted with ciphered information. These operations are made separately in each quantized DCTed block. The main advantage of this method is the progressive decoding of a particular area of the image. The proposed scheme allows decryption of a specific region of image and results in significant reduction in encrypting and decrypting processing time. AES-CFB mode is used as this optimizes the decryption process. Only previous block is necessary to decrypt the current one. This method works in the entropy encoding process during the creation of Huffman's vector. Experiment shows that this scheme provides satisfactory PSNR, sufficient security and acceptable and selective confidentiality results.

Mohammed Benabdellah et al [2] proposed a hybrid approach for encryption –compression which is based on the AES encryption algorithm of the dominant coefficients, in a mixed scale representation, of compression by Faber-Schauder Multi scale transform (FMT). On comparison with Quad tree AES and DCT partial encryption it showed good performance. In the case of FMT transformation, on each scale, the value of each pixel is given by the calculation of the difference with its neighboring pixel of the preceding scale. Thus the areas which present a local peak for these differences correspond to a strong luminous transition for the values of grey, while the areas, where those differences are invalid, are associated with an area, where the level of grey is constant. The information of the transformed image is concentrated in the outline region of the initial image. The AES encryption is carried out after the stage of quantization right before the stage of entropic coding. The principle advantage of this method is the flexibility and the reduction of processing time of coding and decoding. The processing time can be varied according to the desired degree of safety.

Y. Ou et al [3] proposed a region based selective encryption scheme to achieve secure access for medical images. It employs AES to encrypt a certain region's data in the code stream. The size of the encrypted bit-stream is not changed and there is no compression overhead generated.

Z Brahimi et al [4] proposed a partial encryption technique based on AES where some sensitive precincts corresponding to parts of JPEG2000 code stream are encrypted. The protected code stream format is compliant to JPEG2000 code stream. The percentage of data subjected to encryption while maintaining high confidentiality is significantly reduced as compared to full encryption. Less that 30% of the data is encrypted. The scheme does not decrease the compressibility and does not increase the complexity of the JPEG2000 coder. It keeps file format and compression ratio unchanged and does not degrade the original error robustness. This scheme works with any standard ciphers and introduces negligible computational cost. Packets are the most fundamental building blocks of JPEG2000 code stream. A packet is identified by 4 parameters namely C (Component), R (resolution level), P (Precinct) and L (Layer quality). They can be sorted into these 4 parameters in 5 progression order: LRCP, RLCP, RPCL, PCRL and CPRL. In this method, code blocks are collected into larger groupings called precincts. Only some sensitive precincts of the entire image are encrypted. The code stream is parsed to select only packets containing code-blocks which belong to the selected precincts. The remaining packets are sent without encryption. For a color image, precincts are selected from each component (Y, C_b, C_r)

N. A. Flayh et al [5] proposed a partial image encryption scheme where the Embedded ZeroTree Wavelet (EZW) algorithm was used in the compression step. In encryption step, AES and permutation cipher are used. Only part of the original data is encrypted resulting in significant reduction in encryption and decryption time.

S.H Kamali et al [6] proposed a modification of the AES algorithm, MAES, to reflect a high level security and better image encryption. The modification is done by adjusting the Shift Row transformation. If the values of the first row and columns are even, the first and fourth rows are unchanged, and each byte in the second and third rows is shifted to the right, cyclically. On the other hand if the first and the second rows are unchanged, each byte of the second and fourth rows is shifted to the left. However security is compromised when entropy reaches maximum value. Results proved that it provides better encryption than the original AES algorithm.

Ju-Young Ho et al [7], proposed an expansion of the AES –Rijndael, named as Selective Encryption Algorithm, with five criteria namely compression of plain data, the second is size of block, third is selectable round, fourth is optimization of software implementation and fifth is the selective function of the whole routine. The compressed image as input data not only gets high security but also reduces more than 35% of average execution time than the original AES algorithm.

R Subramanyan et al [8] proposed an algorithm based on AES key expansion, in which the encryption process is a bit wise exclusive OR operation of a set of image pixels along with a 128 bit key which changes for every set of pixels. The keys to be used are generated independently at the sender and receiver side based on the AES Key Expansion process. Hence only the initial key is shared rather than sharing the whole set of keys. Experimental results show that this algorithm offers good resistance against brute force attack, key sensitivity tests and statistical crypt analysis

Jignesh et al [9] proposed a hybrid based 128 bit key AES-DES encryption algorithm. In this method, the input image is converted initially into 128 bit plain text. This 128 bit text is further divided into two sets of 64 bit plain text data. This 64 bit plain text is given as input to the DES algorithm. Two such encrypted 64 but texts are then merged as single 128 bit encrypted data, which is further applied to AES algorithm for further encryption. This hybrid model gives a better non linearity when compared to the plain AES. There is better diffusion as it is merged with DES. The possibility of an algebraic attack on the hybrid model is reduced.

A. Bashir et al [10] proposed an encryption technique based on integration of shifted image blocks and basic AES, where the shifting algorithm technique is used to divide the image into blocks. Each block consists of a

number of pixels and these blocks are shuffled by using a shift technique that moves the rows and columns of the original image in such a way to produce a shifted image. The shifted image is then used as an input to the AES algorithm to encrypt the pixels of the shifted image. Experimental results show that the new integration technique has satisfactory security and more efficient than using AES algorithm alone without the shifting algorithm.

A. Bashir et al [11] proposed an encryption algorithm based on rotation of faces of magic cube. The original image is divided into six sub-images and these sub-images are divided among a number of blocks and attached to faces of a magic cube. The faces are then scrambled using rotation of the magic cube. The rotated image is fed to the AES algorithm which is applied to the pixels of the image to encrypt the scrambled image. The algorithm was shown to withstand exhaustive, statistical and differential attacks. The rotation algorithm and the AES algorithm use the original image to generate three encrypted images.

a) a ciphered image using AES algorithm
b) a rotation image using a rotation process
c) a rotation image encrypted using AES algorithm.
This technique presented an inverse relationship between the number of blocks and correlation. There exists a direct relationship between the number of blocks and entropy. It can encrypt large data sets efficiently.

Nazneen M.G et al [12] proposed a selective bit plane encryption using AES to provide secure image transmission in low power mobile environment. An 8bit/pixel image is considered to be in the form of 8 bit plane, where each bit plane is associated with a position in the binary representation of the pixels. Using the Selective or Partial (SE) approach only a subset of the bit planes is AES encrypted, starting with the bit plane containing the most significant bit (MSB) of the pixel. The minimal percentage of data to be encrypted is 12.5% increasing in steps of 12.5% for each additional bit plane encrypted. Encryption of MSB bit plane alone is not secure enough, whereas encryption of four bit planes provides high confidentiality. There is a reduction in computation due to selective encryption. The image is considered as a two dimensional array of pixel values. The 8 bit data is a set of 8 bit planes. Each bit plane may have a value of 0 or 1 at each pixel, but together all the bit planes makeup a byte with value between 0 and 255. In the SE approach, AES is used to encrypt a subsequent number of bit-planes only, starting with bit-plane containing the most significant bit (MSB) of the pixels. AES implementation with block size 128 bit and a 128 bit key is used. The 128 bit block is filled with a quarter of a bit plane. The encrypted bit planes are transmitted together with the remaining bit-planes in plaintext. If there are identical plaintext quarter-lines directly situated above each other, which also adhere to the AES block border (that is starting at pixel position 0,128, 256 or 384), these data produce identical cipher text blocks. Identical blocks of Cipher text are again arranged as identical quarter-line thereby generating the barcode effect. The histogram of the ciphered image obtained by this method is fairly uniform and is significantly different from original image. Also there is no loss of image quality.

Tanvi [13] proposed an image cryptosystem that encrypts the digital image by first dividing them into blocks, and then the pixel values of the blocks are scrambled. The scrambled blocks are then randomly passed through the AES algorithm. The algorithm gave decreased correlation and increased entropy when compared with only using the original AES algorithm for encryption. AES algorithm cannot be successfully applied to the digital images that are having major portion as a single color. The digital images have high correlation among the neighboring pixels. To lower the correlation a transformation algorithm is proposed in which the image is broken into square blocks of size n*n and then the blocks are transformed based on a key. Then the blocks are randomly fed to the AES algorithm. Using this method the entropy was found to be around 7.9.

Harleen Kaur et al [14] proposed a modified version of the AES algorithm which requires less encryption time, less computational power requirement and maintains sufficient level of security. Various modifications were made in the transformation step. In this algorithm, if the first element of state array is even, then the shifting is same as that of original AES algorithm. But, if the first element of the array is odd, then first and fourth rows of the state array are kept un-shifted and second and third rows are shifted cyclically to the left. In this method the Rcon value is

not constant, but is formed from the initial key itself .This improves the reliability of the algorithm. The strength of the algorithm is justified by the fact that even a single bit change in the encryption and decryption key, will not allow the decryption to be successful.

4. Conclusion

In this paper we have given an overview of the various image encryption techniques based on AES algorithm. Few are modifications of the original AES algorithm while some techniques use an integration of other techniques along with AES for better security. Some techniques perform a full encryption while some perform a partial encryption of the digital image.

REFERENCES

[1] J. M Rodrigues, W. Puech, A. G Bors, June 2006, "*A selective Encryption for Heterogenous color JPEG images based on VLC and AES stream cipher, 3rd European conference on Color in Graphics, Imaging and Vision.*

[2] Mohammed Benabdellah, Mohammed Majid Himmi, Noureddine Zahid , Fakhita Regragui and El Houssine Bouyakhf, 2007 *" Encryption –Compression of Images based on FMT and AES algorithm, Applied Mathematical sciences*, Vol 1, , no. 45, 2203-2219.

[3] Y.Ou , C.Sur , K. H Rhee, 2007 ,"*Region based selective Encryption for Medical Imaging", 1st Annual International Workshop,* vol 4427, no. 4613, pp 62-73.

[4] Zahia Brahimi, Hamid Bessalah, A Tarabet, M.K Kholladi, Jul.2008 *,"A new selective encryption of JPEG2000 code stream for confidential images transmission", 5th International Multi-conference on Systems, Signals and Devices*, pp,1-4.

[5] N. A Flayh, R. Parveen,S. I Ahson, ,2009, *" Wavelet based partial encryption of compressed images", International Journal of Engineering Research and Industrial Applications (IJERIA),* Vol 2, No. III pp 89-98.

[6] S. H Kamali, R.Shakerian, M.Hedayati, 2010, "*A new modified version of Advanced Encryption Standard based algorithm for image encryption*", *International Conference on Electronics and information Engineering*", ICEIE, vol .1, pp 141-145.

[7] Ju-Young Oh, Dong-II Yang PhD and ki-Hwan Chon, PhD, Mar 2010 "*A selective Encryption Algorithm based on AES for medical Information", Healthcare informatics research,* vol 16, no. 1, , pp 22-29.

[8] R Subramanyan, Vivek M Chhabria, T G Sankar Babu, 2011 *" Image Encryption based on AES key expansion", Proceedings of Second International Conference on Emerging Applications of Information Technology, EAIT*, ISBN: 978-0-7695-4329-1, Pgs 217-220.

[9] Jignesh R Patel, Rajesh S Bansode, Vikas Kaul, Feb 2012, " *Hybrid Security Algorithms for Data Transmission using AES-DES", International Journal of Applied Information Systems(IJAIS),* ISSN: 2249-0868,Vol 2-No-2.

[10] Ahmed Bashir Abugharsa, Abu Samad Bin Hasan Basari, Hamida Almangush, Mar 2012. *" A new Image Encryption Approach using the Integration of a shifting technique and the AES algorithm", International Journal of Computer Applications* , vol 42-No.9,

[11] Ahmed Bashir Abugharsa, Abu Samad Bin Hasan Basari, Hamida Almangush, , 2013 "*A novel Image Encryption scheme using an Integration Technique of Blocks rotation based on the Magic cube and the AES algorithm, Centre of Advanced Computing technology.*

[12] Nazneen M.G, Sufia Banu, Zahira Tabassum, Khamer Fatima, Arshia Sharif, June 2013 "*Selective Bitplane Encryption For ecure Transmision of Image Data in Mobile Environment", International Journal of Science and Technology Research*, Vol2, Issue 6, ISSN 2277-8616.

[13] Tanvi, Oct 2013 "*An Image Cryptosystem based Pixel Scrambling and AES algorithm", International Journal of Computer Applications*, Vol 80-No.1.

[14] Harleen Kaur, Reena Mehla, Jul 2014 " *Image Encryption using AES with Modified Transformation",' International Journal of Science and Research"(IJSR),*ISSN: 2319-7064, Vol 3, Issue 7.

[15] www.iis.ee.ethz.ch/IS1.pdf IS1: CryptoFun, Fachpraktikum.

[16] P.Radhadevi, P.Kalpana, Oct 2012, "*Secure Image Encryption usinf AES", IJRET*, ISSN: 2319-1163, Volume 1, Issue 2.