Security Enhancement using a modified AES algorithm

R.Bala[1],
Research Scholar,
Bharathiar University, India.
Ph: 9943901200
rbalasenthil@gmail.com

NP.Gopalan[2]
Professor,
NIT,Trichy,India.
Ph: 9952951745
npgopalan@nitt.edu

ABSTRACT
Security is an important issue for storing data and communicating it over Internet. Secret and private information is also being carried out through the Internet. This common usage of the Internet provides excellent platforms for online communications. Internet has also become an active platform for hackers and crackers. A challenge of experts is to develop systems to ensure protection of the data sent through the Internet. Here, we propose an innovative approach for enhancing security to conceal message using CrypticSteganography by integrating cryptography and Steganography to provide confidential communication. Cryptography and Steganography are different in their way of approach towards securing data, but yet seems to provide unify security solutions when it comes to protecting confidential data. Cryptography makes the information unintelligible whereas Steganography ensures that no clue to finding information exists. In cryptography we used modified AES algorithm to encrypt data and in steganography we implemented reversible texture synthesis to hide the data.

Keywords: Cryptography, Steganography, modified AES, Texture Synthesis

1. INTRODUCTION
Cryptography is a branch of information security. It provides security to the data concerned with storing and transmitting the information untouched over the insecure medium like Internet by encoding text data into a form unintelligible format with the help of various algorithms for encrypting process and only the particular user can decrypt it into original text. Cryptography does not have the capacity to hide the presence of data alone and it cannot protect data effectively. Any intruder can easily detect the encrypted data existed in a medium and can try numerous attacks in order to get the source data. So in order to further improve the security we implement a two layered approach for providing an enhanced and greater security. Steganography is also concerned with securing transmitted data but with a different objective. Steganography allows people by hiding the data within data over communication medium.

ICIA '16, August 25-26, 2016, Pondicherry, India
© 2016 ACM. ISBN 978-1-4503-4756-3/16/08…$15.00
DOI: http://dx.doi.org/10.1145/2980258.2980264

2. LITERATURE REVIEW
Feng et al. in their paper [1] purposed a modern approach of binary image steganography. They also implemented texture reduction technique. Complement, Rotation, parallel texture patterns of invariant were received from the steganographic image. They implemented the practical measurement and experimental results have high quality of stego image and embedding capacity was also high in their steganographic approach.

Islam et al. [2] implanted a enhanced version of LSB image steganography based on efficient filtering technique using status bit and for encryption they used AES algorithm to provide security. Due to uncompressed nature of bitmap images, they used it for hiding data in the part of steganography. Here they implemented encrypted secret data with AES algorithm and next step is to encrypt secret data that was embedded into image using steganographic practice. Filtering algorithm to embed more secure data in bitmap image was used by them. Further they used the status bit to check the insertion and extraction procedure of secret messages and experimental results shows that this method has peak embedding capacity while comparing to LSB algorithm. The high value of PSNR with high quality of stego image was maintained.

In Liu et al. [3] introduced a steganography algorithm which is adaptive based on block complexity and matrix embedding. Here they used the patch-based method to embed a confidential message through the synthesizing procedure. To extract the source texture for the purpose of reversibility, a message extracting procedure were used. They implements Histogram shifting (HS) technique for Reversible of data hiding (RDH).They presents a common model to construct Histogram Shifting - based RDH system used for shifting and embedding functions.

Otori and Kuriyama [4] established the effort of synthesizing pixel based concept of texture to combine the coding data. Secret messages were covered and being encoded into colored dotted patterns which are straightly painted on a empty image. To apply data-detecting process, they photographed the extracted messages in printout of stego-synthesized texture image. Pixel-based algorithm cover the remaining pixels by using the texture synthesis process based on pixels method, thus disguise the reality of dotted patterns. The capacity based on the quantity of dotted patterns and little error rate while extracting the message were occurred.

Ni et al. [5] presented a reversibility of data hiding algorithm for extraction of the source image without any alteration of the image after extracting the hidden data. They used histogram with zero or the minimum level of points in an image and slightly modify the grayscale values of pixels for embedding the data in the image. Comparing the available previous reversible method of data hiding algorithms, more embedding capacity of data were

achieved by them. The algorithm applicable to a broad range of images such as frequently used images, health check up images, above ground images and all texture images. They implemented a method that embedded a large amount of data along with keeping a same time and a superior quality of all natural images, particularly; the comparative value of PSNR is guaranteed as higher than the value of 48 dB. They projected lossless method of data hiding in still images and videos. The terms of pseudo code were used for the progression of embedding and extracting data.

Han et al [6] proposed algorithms based on the pixel values of synthesized image pixel by pixel and used spatial region for comparisons to choose from the sample texture and the most related pixel of output pixel. In every output pixel is decided from the earlier synthesized pixels and any incorrectly synthesized pixels in the process results to cause propagation of errors.

Mondal and Maitra [7], were tried to modify the already available algorithm to make novel algorithms that helps to boost security which has small encryption time. Here they used modified AES algorithm that gives added security with a small encryption time with 128- bit of key were used to encrypt. Here a technique uses randomized key to be hidden into an encrypted image by means of the basics concepts of cryptography, digital watermarking. They implemented cost effective approach for encryption is appreciable.

Wadi and Zainal [8] examines the Advanced Encryption Standard and they add two modifications of their image encryption technique to further improving the performance and the hardware requirements were reduced in AES algorithm. They first modified instead of 5 rounds in MixColumn transformation to 10 rounds, and the second they modified S-box and reverse of S-box in original AES algorithm as mingled into one simple S-box for both the process of encryption and decryption.

Kamali et al. [9] presents a Modified Advanced Encryption Standard to replicate a peak point protection and fine quality of image encryption. They had done a change in the Shift-Row Transformation. Their experimental results also showed that while comparing to original AES encryption algorithm, the modification done in the AES algorithm gives improved encryption results against statistical attacks to provide security.

Deshmukh and Kolhe [10] used a common technique to maintain security in multimedia content for encryption. They used MPEG of video stream which is different from usual textual data due to inter frame dependencies existed in the MPEG video. Specialized algorithms are required for MPEG video encryption due to its nature of special characteristics, such as coding format and massive data amount. The performance of calculating algorithm of AES was modified to reduce and encryption performance was improved.

3. PROPOSED MODEL

Here we proposed a novel approach for securing data over insecure medium by CrpticSteganography. Here in the part of cryptography we used new AES algorithm and in steganography side we used reversible texture synthesis. First the source file of text or image can be taken as input and it will be encrypted using new modified AES algorithm. After encrypting the source text or image file it will be used for further processing of steganographic steps such as reversibility of synthesizing a texture to hide the encrypted source data. Next the hidden data is transmitted over an insecure medium. No one can analyze it that the image contains hidden data. In the receiver side the hidden data will be recovered and further decrypted to get the original source data.

3.1 Steps Of new AES algorithm:

The AES algorithm has static S-box and a constant mix column matrix. The possible secret key were tried to crack the algorithm was 2128 for AES (128) algorithm. The algebraic attacks such as differential and linear cryptanalysis are complicated due to their nature of large amount of plain text and cipher text was needed. Theoretically shown that the possibility to break AES algorithm using XSL attack using multivariate equations. Due to static nature of S-box it is likely to construct these equations that were nearly 256! ≈ 2 1638 S-boxes, if we create any one of them, which is a key dependent S-box, it becomes very tricky to attack the AES algorithm. The mix column matrix has 16-byte entries with a static 4 × 4 matrix and a 79 key dependent mix column matrix if we constructed then cryptanalysis still becomes more complicated. AES operations are all same except for mix column matrix non-singular condition necessary to be satisfied.

3.2 Steganography :

In steganography [11] a reversible texture synthesis samples a small size of texture image that produces a original texture image with resembling emergence and the size also arbitrary. Then merge the texture synthesis procedure in steganography to cover up secret messages. Here we implemented texture synthesis process to hide and embed the source image of texture and covert messages. Stego image provides to recover covert messages and the resource texture. The implemented approach by us provides several advantages. No one can defeat our approach. The capacity of embedding information is proportional to the stego texture image size. Otori and Kuriyama [4] implemented pixel based concepts that receives error rate. Finally, the reversibility option gives functionality that allows recovering the source texture.

4. METHODOLGY

4.1 Cryptography:

In [8],AES with S-Box of cipher key dependent is block cipher in which the length of block has three alternatives of keys such as 128,192, or 256 bits in AES with block length has 128 bits. Here we considered a 128 bits key length because of its wide usage. The process of encryption and decryption in AES has dynamic S-box which are cipher key dependent with same number of rounds like 10, 12, 14 with 128, 196, 256 key length and data bit length have 128 bits. The round function is similar in AES except for 5 stages of block operations instead of 4 stages. The fifth stage in the proposed work was named as Dynamic S-box generation round after SubBytes( ) was introduced in the original AES for encryption. All the remaining stages in AES rounds are same. RevDynamic S-box round along with 4 stages is followed for decryption process. The configuration of proposed modified AES with its each round process of encryption is in figure 1 and decryption is figure 2.

The proposed algorithm uses AES Static S-box remains same irrespective of key and key dependent Dynamic S-box value was generated. In subbytes( ), the entry in the S-box was replaced in each byte the state.

$$X_{ij} = \text{S-box}\ (Y_{ij})$$

This function provides the non-linearity in the decrypted text.

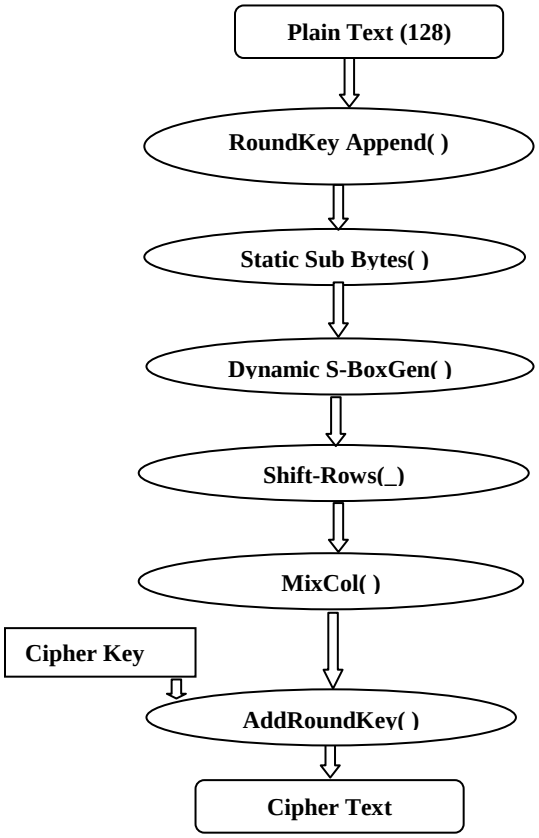


Figure 1. Modified AES Configuration for Encryption

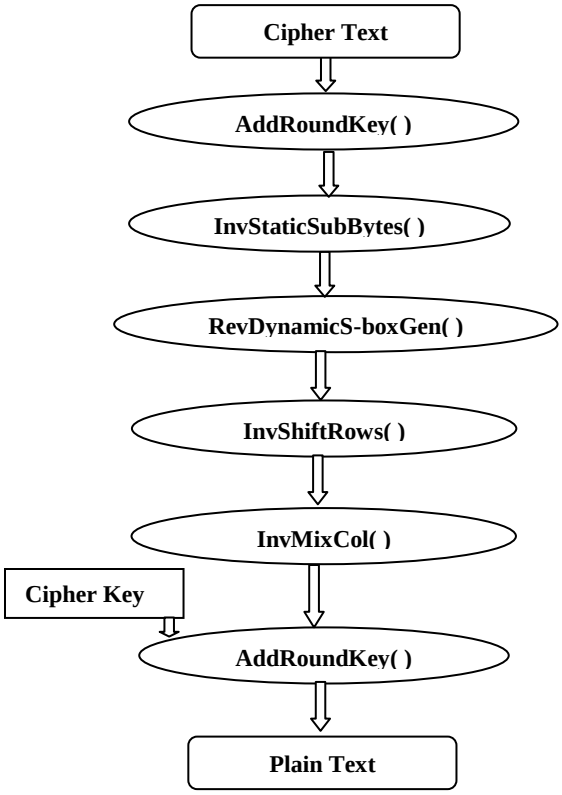


Figure 2. Modified AES Configuration for Decryption

Based on the multiplicative inverse over GF (28) used S-box is derived which provides good non-linearity. We require main S-box to make dynamic S-box which has sixteen rows starting from (00 to FF). The RevDynamicS-boxGen( ) receive value from the static S-box which is XORed to generate index value. From this index value we can get the row and column index which are to be interchanged. In this way we receive dynamically index value to decide either row shifting or column shifting.

4.2. Embedding procedure in Steganography:

In steganography the patch based algorithm is used to process it. Source texture image was taken as the input image is either being photographed or drawn images of texture. Next one empty image from the source texture is to be created as workbench to paste the patches. Save the bits of message data into separate patch and arrange the image.

First index table were generated to store the location of source path information of synthetic structure. Totally index table provides access and retrieval of source texture. To generate index table one must provide secret key for authentication process.

table permit us to get the synthetic texture as well as texture source perfectly. To generate the index table we have to provide the secret key to authenticate. The dimensions of the index table were determined by ($ST_w \times ST_h$), the parameters ST_w denotes the width and and ST_h denotes the height of the synthetic text structure. The entries level numbers in the index table can be determined by using the following equation

$$ST_{np} = ST_w \; X \; ST_h$$

$$= \left[\frac{TXT_w - PAT_w}{PAT_w - PAT_d} + 1\right] X \left[\frac{TXT_h - PAT_h}{PAT_h - PAT_d} + 1\right]$$

ST_{np} represent the patch numbers in stege-synthetic texture and TXT_w, TXT_h, PAT_w, PAT_h, and PAT_d, are the integer values entries. The encrypted secret message is written into patches on the location information determined in index table. For that select the patch based on the entry in the index table and also it provides which patch to select and where to paste in the blank image. Patches are identified by patch number and the entries in the index table were changed by using the patch number. Then stick the patches in the workbench. Construct a synthesized image of grouping from different patches.

The image which was synthesized is to create based on proper candidate patches must be chosen from patch list. The entries indicate the positions of the blank image to paste the patch that contains a secret message. Second step is to construct the stego-synthetic texture image. Here the message is converted into 8 bits of bytes and that will be taken for input of message oriented process in texture synthesis. Then both the source image of texture and composition image is considered as input to this procedure.

Third step is image decomposition procedure in patch based algorithm, we extract the original message from the image. The suitable patch is taken out from the composed image. The patch contains a encrypted data. This process is done with the help of index table. It provides where the patch is to be extracted from

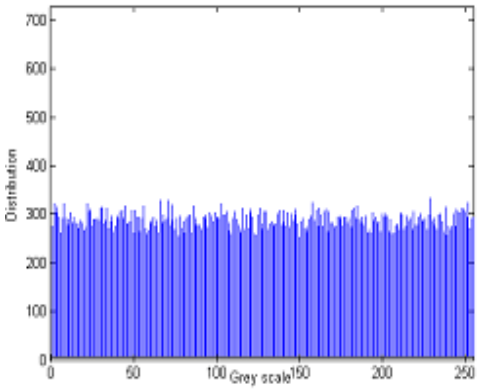
the composed image. After the patch was extracted then decrypt the encrypted message using our modified AES algorithm.

5. EXPERIMENTS AND RESULTS

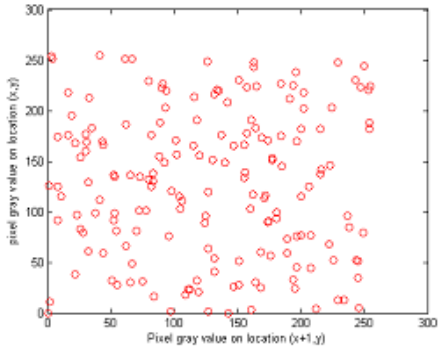
The modified AES algorithm has been designed to encrypt and decrypt any type of file formats such as .txt, bmp, and .wav files.

Source image

Encrypted Image



Histogram



Correlation

Figure 3. Encryption and Decryption process of image.

Figure 3 Shows that the sample source image was encrypted using the new modified AES to produce the encrypted image. Example Text files are decrypted it produces exact source message, but if any of the bits in key value changed caused the encrypted message in unreadable form because of its ASCII conversions takes place while decrypting a text file. High authentication, robustness and recoverability were achieved by using this method.

6. CONCLUSIONS

The integration of cryptography and steganography were employed results in high degree of security. In cryptography the slight changes in AES of dynamic S-Box provides better encryption results to enhance security against statistical attacks along with the reduction of time complexity. In Steganography the reversibility method implemented provides integrity of message in source texture recovered from the synthetic texture. Real reversibility was achieved and also without any distortion of image quality.

7. REFERENCES

[1] Feng, W. Lu, and W. Sun. "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture", IEEE transactions on Information Forensics and Security, 2015.

[2] M. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal and M. D. Hossain. "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography", IEEE International Conference on Informatics, Electronics & Vision (ICIEV) ,Dhaka, Bangladesh, 2014.

[3] X. Li, B. Li, B. Yang, and T. Zeng. "General framework to histogram shifting-based reversible data hiding", IEEE Trans. ImageProcess", 2013.

[4] H. Otori and S. Kuriyama. "Texture synthesis for mobile data communications," IEEE Comput. Graph. Appl, 2009.

[5] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su. "Reversible data hiding", IEEE Trans. Circuits Syst. Video Technol, 2006.

[6] C. Han, E. Risser, R. Ramamoorthi, and E. Grinspun. "Multiscale texture synthesis," ACM Trans. Graph, 2008.

[7] Subijit Mondal, Subhashis Maitra. "Data security - modified AES algorithm and its applications", ACM SIGARCH Computer Architecture News, 2014

[8] Salim Muhsin Wadi, Nasharuddin Zainal. “High Definition Image Encryption Algorithm Based on AES Modification”, Wireless Personal Communications, 2014.
[9] S.H.Kamali, R. Shakerian, M. Hedayati, M. Rahmani. “A new modified version of Advanced Encryption Standard based algorithm for image encryption”, IEEE International Conference on Electronics and Information Engineering (ICEIE), 2010.
[10] P. Deshmukh, V. Kolhe. “Modified AES based algorithm for MPEG video encryption Information” IEEE International Conference on Communication and Embedded Systems (ICICES), 2014.
[11] Wu, Kuo-Chen, and Chung-Ming Wang. "Steganography Using Reversible Texture Synthesis", IEEE Transactions on Image Processing, 2015.
[12] Dara, Mona, and Kooroush Manochehri. "Using RC4 and AES Key Schedule to Generate Dynamic S-Box in AES", Information Security Journal A Global Perspective, 2014.
[13] www.sersc.org
[14] www.ijarcst.com
[15] Garja,Nikhil,Shamsuddin.S.Khan,and Pradnya Rane. "Private cloud Security : Secured user aouthentication by using enhanced hybrid algorithm",International Conference on advances in communication and computing Technologues(ICACACT 2014),2014.
[16] research.ijcaonline.org
[17] data.conferenceworld.in

APPENDIX

A. HEADINGS IN APPENDICES

A.1 Introduction

A.2 Literature Review

A.3 Proposed Model

A.3.1 Steps Of new AES algorithm

A.3.2 Steganography

A.4 Methodology

A.4.1 Cryptography

A.4.2. Embedding procedure in Steganography

A.5 Experiments and results

A.6. Conclusions

A.7 References