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

EFFICIENT DATA HIDING BY USING AES & ADVANCE HILL CIPHER ALGORITHM.

N.Lalitha[1], P.Manimegalai[2], V.P.Muthukumar[3], M.Santha[4]

[1](M.Phil) Department of Computer Science, Vivekanandha College of Arts and Sciences for Women, Namakkal, lalitha91mar@gmail.com
[2](M.Phil) Department of Computer Science, Vivekanandha College of Arts and Sciences for Women, Namakkal, kp.manimegalai@gmail.com
[3]Assistant Professor, Vivekanandha College of Arts and Sciences for Women, Namakkal, rajiperisamy@gmail.com
[4]Assistant Professor, Vivekanandha College of Arts and Sciences for Women, Namakkal, Shanthaa30@gmail.com

Abstract

In this paper we propose a data hiding technique using AES algorithm.Steganography and Cryptography are two popular ways of sending vital information in a secret way.Cryptography was introduced for making data secure. But alone cryptography cannot provide a better security approach because the scrambled message is still available to the eavesdropper. There arises a need of data hiding. So here we are using a combination of steganography and cryptography for improving the security. There are many cryptography techniques available; among them AES is one of the most useful techniques .In Cryptography, I have using AES algorithm to encrypt a message using 128 bit key the message is hidden . In this proposed technique, we use advance hill cipher and AES to enhance the security level which can be measured by some measuring factors. The result of this work shows that this advance hybrid scheme gives better results than previous techniques.

Keywords: AES Algorithm, cryptography, Hillcipher++, AES, data hiding.

1. Introduction

Cryptography is a part of information security. Presently we have very secure methods for both cryptography and Steganography – AES algorithm is a very secure technique for cryptography and the Steganography methods, which use frequency domain, are highly secured. Data hiding is a technique that is used to hide information in digital media such as images, audio, video etc. This idea is to apply both of them

together with more security levels and to get a very highly secured system for data hiding. This paper mainly focuses on to develop a new system with extra security features where a meaningful piece of text message can be hidden by combining security techniques like Cryptography and Steganography. The performance of a reversible data embedding algorithm is measured by its payload capacity, complexity, visual quality and security.

2. Cryptography

Cryptography encodes information in such a way that nobody can read it, except the person who holds the key. More advanced crypto techniques ensure that the information being transmitted has not been modified in transit.There is some difference in cryptography and steganography, in cryptography the hidden message is always visible, because information is in plain text form but in steganography hidden message is invisible

2.1 AES algorithm for Cryptography

This standard specifies the Rijndael algorithm**, a symmetric block cipher** that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. The input, the output and the cipher key for Rijndael are each bit sequences containing 128, 192 or 256 bits with the constraint that the input and output sequences have the same length. In general the length of the input and output sequences can be any of the three allowed values but for the **Advanced Encryption Standard (AES) the only length allowed is 128.**

A) Advantages of using AES algorithm

- Very Secure.
- Reasonable Cost.
- Flexibility, Simplicity

2.2 *AES* Image Encryption

The original image is in uncompressed format. Firstly, if the image is a color image, then encrypt each red, green and blue channel otherwise convert it into a gray scale image with each pixel value ranging in between [0-255] represented by 8 bits and then encrypt the image. The pixel bits are represented as $b_{i,j,0}$, $b_{i,j,1}, \ldots . b_{i,j,7}$. AES is a substitution-permutation network, which is a series of mathematical operations that uses substitutions and permutations such that each output bit depends upon every input bit. The AES algorithm consists of a set of processing steps repeated for a number of iterations called rounds.

SubByte: each byte of the block is replaced by its substitute in the substitution box(S-box).

ShiftRow: bytes in last three rows are cyclically shifted left over different number of offsets

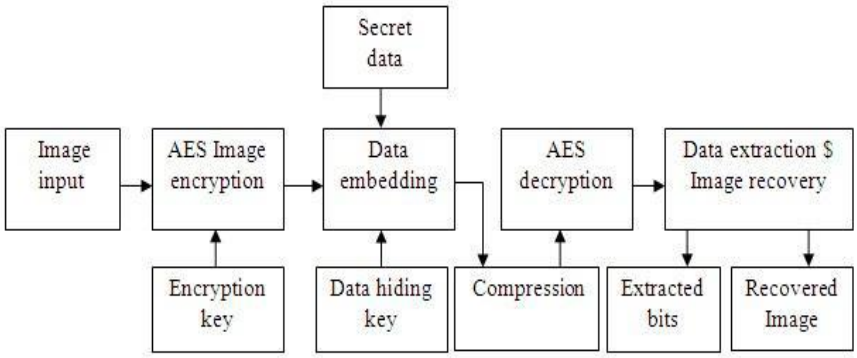


Figure 1. Block Diagram

Mix Column: Each column is multiplied with a known matrix. Multiplying by 1 means leaving unchanged, by 2 means shifting byte to the left and by 3 means shifting to the left and then performing XOR with the initial unshifted value.

AddRoundKey: XOR with the actual data and the sub key. In final round there is no Mix Column step. These steps are done for 10 rounds. Thus it becomes difficult for the attacker to obtain any information about the original content from the encrypted image.

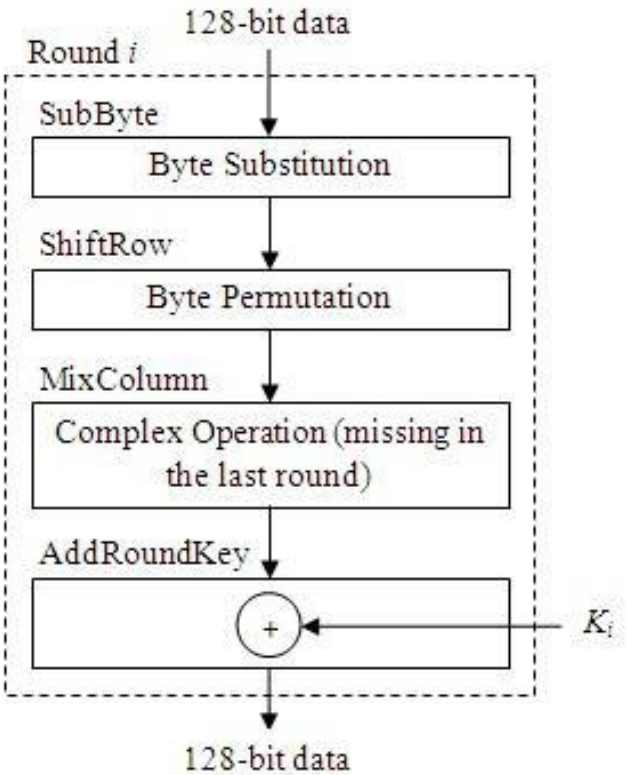


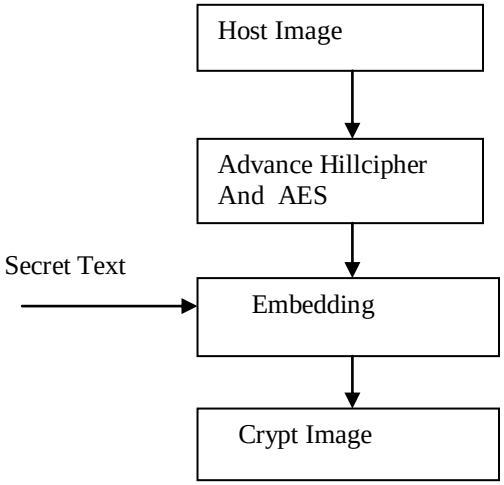
Figure 2. AES Encryption

2.3 Security design

Security is the major need to prevent our secret text data from unauthorized access while using internet to transfer the information .this proposed enhanced scheme use advance hill-cipher &DES encryption schemes & generate a crypt-image where secret text can be hide.we can divide our design into different moduleds.

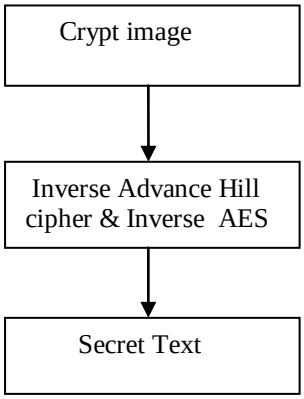
- Crypt Module
- Security Module
- Decrypt Module

Crypt Module:



Here we first select the original image and apply advance hill cipher to generate a cipher & add one more algorithm that is AES to generate key. Then secret text can be embedded with the original image and it gives crypt image where our secret data is being hidden in encrypted form.

Decrypt Module*:*



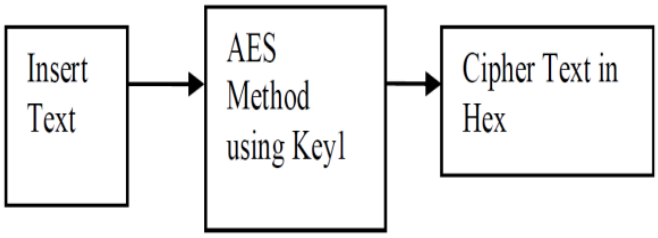
Here we select our encrypted image and apply inverse advance hill cipher & AES to retrieve the secret data.

3. Hiding the Text

Crypto Module:

Crypto Module the following steps are considered for encrypting the data.

- Insert text for encryption
- Apply AES algorithm using 128 bit key(key 1)
- Generate cipher text in hexadecimal form.



3.1 Data Extraction and Image Recovery

The image is decrypted using AES decryption. The steps are AddRoundkey, inverse subbyte using inverse S-box, inverse shiftrow where the bits are cyclically shifted towards right, inverse mixcolumn step using inverse P-box, and AddRoundkey. The decrypted image is segmented into blocks. The sum total of pixel values of each block is found then. For each block, if this value is greater than the threshold value then the data is hidden in that block and is extracted by xor-ing the original bits with the decrypted bits. Finally combine the extracted bits to obtain the secret data and collect the recovered blocks to form the original image.

4. Conclusion

In this paper, we proposed a secret text hiding approach, which is Enhanced Approach using Advance Hill cipher & AES techniques for securing confidential data from unauthorized access .we have presented a new system for the combination of cryptography and Steganography using four keys which could be proven a highly secured method for data communication in near future . The main advantage of this Crypto/Stegno System is that the method used for encryption, AES, is very secure and the DCT transformation Steganography techniques are very hard to detect. The hidden data is then extracted with the data hiding key and the original image is recovered. This work may be applicable where both the hidden data and the cover media are highly confidential.

REFERENCES

1. Domenico Daniele Bloisi , Luca Iocchi: Image based Steganography and cryptography,Computer Vision theor and applications volume 1 , pp. 127-134 .
2. William Stallings:" Cryptography and network Security: Principles and Practices"
3. Advance Encryption Standard, [Online], Available: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.
4. Deven N. Shah:"Information Security: Principles and Practice".
5. M. M Amin, M. Salleh, S. Ibrahim, M .R. Katmin, and M. Z. I. Shamsuddin, " Information Hiding using Steganography", IEEE 0-7803-7773-March 7, 2003
6. D.R. Stinson, Cryptography: Theory and Practice, Boca Raton.
7 . Provos, N. and Honeyman, P. (2003). Hide and seek: An introduction to Steganography. IEEE SECURITY & PRIVACY
8. Bender, W., Gruhl, D., Morimoto, N. & Lu, A., "Techniques for data hiding", IBM Systems Journal, Vol 35, 1996