International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
*ISSN (Online)*2349-6967 *Volume 2 , Issue 1(Jan-Feb 2015), PP1-5*

AES grade encryption on to Steganography

Farhan R. Patel[1], Dr. A. N. Cheeran[2]

[1] *(Department of Electrical Engineering, V.J.T.I. College, India)*

[2] *(Department of Electrical Engineering, V.J.T.I. College, India)*

Abstract:-With the increasing demand of wireless transfer of information through internet, security of data is becoming an area of prime concern. It is not only important to hide the actual data or information but also equally important to even hide the existence of the data from the real world. Although, there is a big difference among the two, but achieving both together is the need of the time in data communication. This increased the significance of data hiding and encryption for the purpose of data storage and data transmission. Design 128bit encoder using AES (Advance Encryption Standard) Rijndael algorithm for image encryption is proposed in this paper. AES was developed by National Institute of Standard and Technology (NIST) in the year 2001 and is widely accepted for encryption of the Stego image which carries the actual information and at the receiver side decryption of the same image retrieves the original content which is the actual message or information. Here, Steganography is achieved using LSB (Least Significant Bit) method and AES is then applied on to this Stego Image. MATLAB simulation will be developed to verify the functionality of the designed process.

Keywords:- Advance Encryption Standard (AES) algorithm, Cryptosystem, Encryption and Decryption, Least Significant Bit (LSB) method, S-box, Steganography.

I. Introduction

The emerging scenario of today's world exchanging data over the air needs an exceptional grade security, as over the air data can be easily attacked by an attacker, or it can be hacked by a hacker or intruder. The intruder or the attacker once get to know the existence of the message, can definitely try to corrupt the message or can modify its content thereby spoiling the actual content of it and finally resulting into error. User always desires an error free transmission and reception of the message. For this it is very important that not only the message contents but also the existence of the message must be hidden from the external world, when it is transmitted. These have emphasized the need for fast and secure digital communication networks to achieve the requirements for secrecy, integrity, and non reproduction of the exchanged information. Steganography provides means of hiding message content into an image. Cryptography provides us a method for securing and authenticating the transmission of information over insecure channelswith a guarantee that the unintended persons will never able to understand the content of message, till the time key is unavailable with him. In the paper we propose an algorithm which uses combination of both steganography and Encryption, where encrypting stego image which contains the hidden text is performed.

The reminder of this paper is organized as follows: Section II describes the conventional cryptosystem. Section III describes the concept of steganography. In section IV explains AES method of encryption. Following section V gives the information of proposed and expected work. In section VI, the results are explained and finally section VII, describing the conclusion of the paper.

II. Conventional Cryptosystem

The word cryptography is derived from two Greek words which mean "secret writing". Cryptography is the process of scrambling the original text by rearranging and substituting the original text making it unreadable for others. Cryptography is an effective way to protect the information that is transmitted through the network communication paths [1]. In general, cryptography is transferring data from source to destination by altering it through a secret code. The cryptosystems uses a plaintext as an input and generate a cipher text using encryption algorithm [2] making it unreadable for others. Cryptography is an effective way to protect the information that is transmitted through the network communication paths [1]. In general, cryptography is transferring data from source to destination by inserting it through a secret code. The cryptosystems uses a plaintext as an input and generate a cipher text using encryption algorithm [2].

III. Steganography

Steganography is an art of hiding and transmitting data through special carriers to conceal the existence of the data [3]. This can be achieved using different techniques such as LSB hiding, Jsteg analysis etc. and the art of detecting information through these algorithms is called as 'Steganalysis'. When steganography is applied to a text, the new image is called the "steganographic image". Now the text gets concealed by the image which forms a cover over the text, thereby hiding the text from the external world. Here, not only the data is hidden but also the existence of the data is also hidden from the external world and it is just the stego image which is visible to the human eye.
The important conceptssuch as LSB inserting, followed by the types of cryptosystem etc. are discussed in the following sections.

3.1 LSB (Least Significant Bit) inserting algorithm

LSB (Least Significant Bit) is an algorithm to implement steganography. It is the process of adjusting the least significant bits of the pixels of the carrier image behind which the confidential data is hidden. It is a simple approach for embedding message into the image [4].

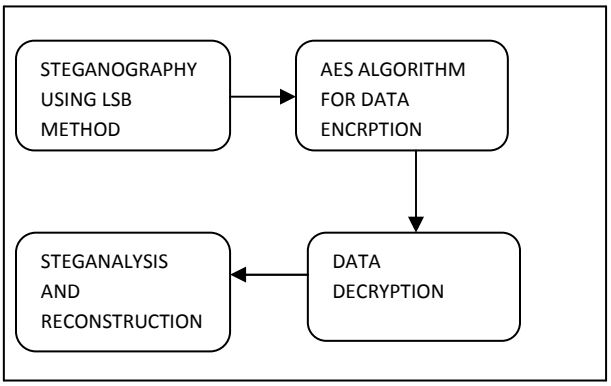


Fig.1: Transmitter and Receiver Block Diagram

3.3 Types of Cryptosystems

3.3.1) Symmetric Cryptosystem

3.3.2) Asymmetric Cryptosystem

3.3.1 Symmetric Cryptosystem

In this method of cryptosystem, symmetric key is used at the transmitter and the receiver side; it results into advantages such as fast processing of data, better security and less number of computations as compared to asymmetric cryptosystem.

Examples: AES, DES, 2DES, 3DES, Twofish, etc.

3.3.2 Asymmetric Cryptosystem

In this method of cryptosystem, asymmetric key is used at the transmitter and the receiver side, it results into some drawbacks when compared to symmetric key algorithm such as more number of computations, large size of the key is required in asymmetric method.

Examples: RSA, ECC algorithm, etc.

IV. Advance Encryption Standard (AES) algorithm

The AES algorithm is a kind of symmetric cryptosystem, a method in which same key is being used at both the transmitter and receiver side [6].

4.1 AES specifications

Datablocklength:128bits.

Keylength:128bits,192bitsor256bits.

It is an iterative algorithm where each iteration is called as a round and the total number of rounds may vary depending upon the size of the key.

The following are the variations of the key size and their corresponding rounds:

Key length(N_k)	Block size(N_b)	No. of rounds(N_r)
4x32=128bits	4x32=128bits	10
6x32=192bits	4x32=128bits	12
8x32=256bits	4x32=128bits	14

Table: 1: AES parameters

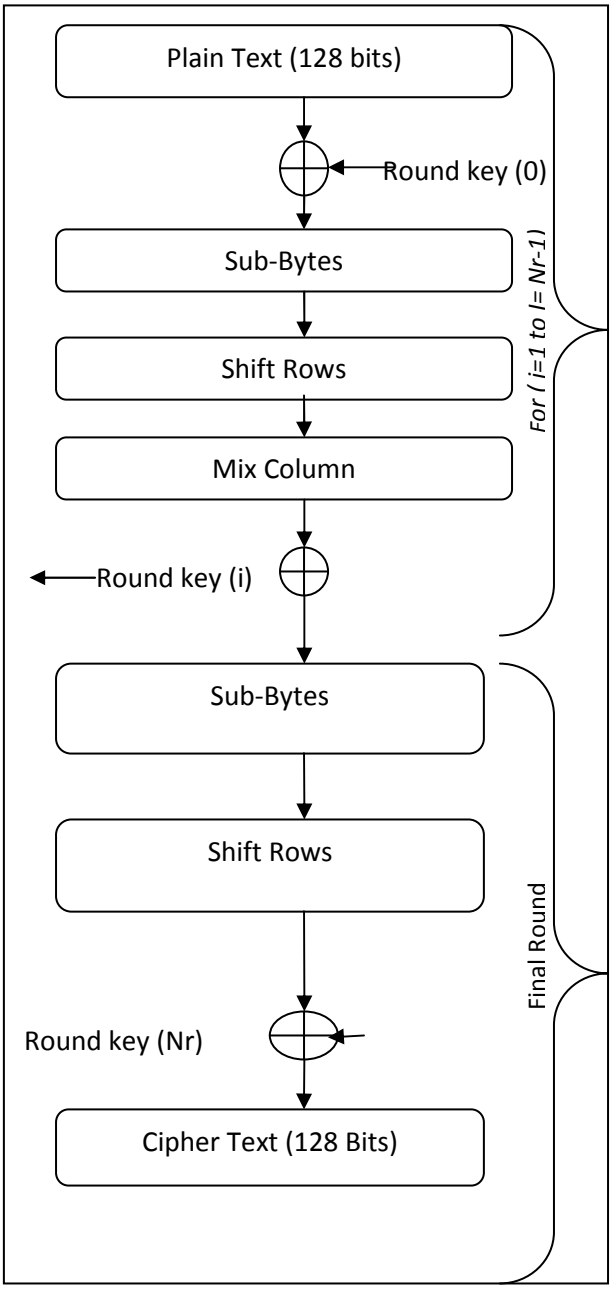


Fig.2: AES encryption block diagram

4.2 AES Encryption method

The 128bits size of N_b data block is first divided into 16 Bytes. These bytes are mapped into a 4x4 array called as "state". All internal operations of AES are performed onto this state.Now, as we know that the algorithm is iterative in nature with each iteration being named as the round wherein for each round 128 bit of data and 128 bit of key

isrequired. This implies that we require 4 words of the key for each round wherein the output of one round acts as input of the next round. Also if the input key is of fewer bits then it needs to be expanded using key expansion technique so as to get desired bit length key size depending upon the number of rounds. Now, since it is a method of symmetric cryptosystem hence it provides simplicity in design.

Now in this AES encryption method, there involves four kinds of transformation for every round of iteration. However, the last round of iteration involves only three transformations.The transformations can be summarized as follows:

Byte substitute Transformation

This method of substitution is a nonlinear byte substitution using S-box (substitution box). This transformation operates on each byte of the state independently. The transformation is achieved by multiplicative inverse, arithmetic over extended fields GF (2^8) and by using affine transformation. Thus the substitution of each byte is carried out by the corresponding byte from the S-box. Now, since this substitution is a byte oriented substitution and hence each byte of the state can be individually controlled. The input byte is used to index a row and column in the lookup table to receive the substituted value.

Shift Rows Transformation

It is again a byte oriented transformation. Cyclic shifting of the bytes in the last three rows of the state is achieved in this stage of the transformation. Different offsets are selected for achieving this shift in rows.

Mix Column Transformation

This mix column transformation is operated on each column independently. This substitution uses the method of arithmetic over the extended fields GF(2^8), where it is designed as a matrix multiplication. In this transformation, each byte of a column is mapped onto a new value which is a resulting function of all the four bytes in that column.This involves a perfect mixing of the bytes within that column which is coupled with the shift row transformation so as to provide a robust grade security in order to protect the data from the unintended person or hacker.

Add Round Key Transformation

In this stage, we perform a simple XOR between the output of the current stage and the round key. It is a self inverse transformation.

V. Proposed System

We perform the steganography that is hiding text into image using (LSB) least significant bit technique and then carry out encryption of this image using Advance Encryption standard (AES) technique in which we use 128 bit block size of data and 128 bit block size of the key. Thus our proposed technique isintegration of two methods of data security thereby resulting into a high grade security, whereas the existing systems implement these techniques individually.

In this paper we demonstrate an innovation of combining the two techniques LSB insertion and AES encryption. This combination ensures a high military grade security on to the data, as not only the data is being hidden from the external world but even the existence of the data can be hidden from the intruder or the hacker [5]. To achieve this we first start with the process of hiding the text into an image using LSB (least significant bit) insertion technique using the method of steganography. Once achieved this, we then apply encryption on to the stego image using AES thereby resulting into the encrypted Image.

Our proposed system involves two main stages:

(i) Embedding text into a grayscale image using Steganography.
(ii) AES based encryption on to the output of steganogrpahy that is on the stego object.

5.1 Embedding text into a gray scale image

The proposed system considers a file of text containing ASCII characters and the cover object which is a gray-scale image of size (256×256) pixels and the resultant output is stego-object which is a resulting image. The ASCII characters of the text are inserted into the cover image by the method of LSB insertion technique.

LSB (Least Significant Bit) insertion technique is the simplest and yet powerful method of steganography.

In this method, message bits are hided into the least significant bit of the cover image. This is possible as the human visual system exhibits psycho visual redundancy in terms of perception of vision and persistence of vision. Taking this into consideration, LSB method exploits psycho-visual redundancy and hence LSB of the cover image is used to conceal the text thereby providing a cover onto it without making the external world even having a doubt of this embedding of the text into it.

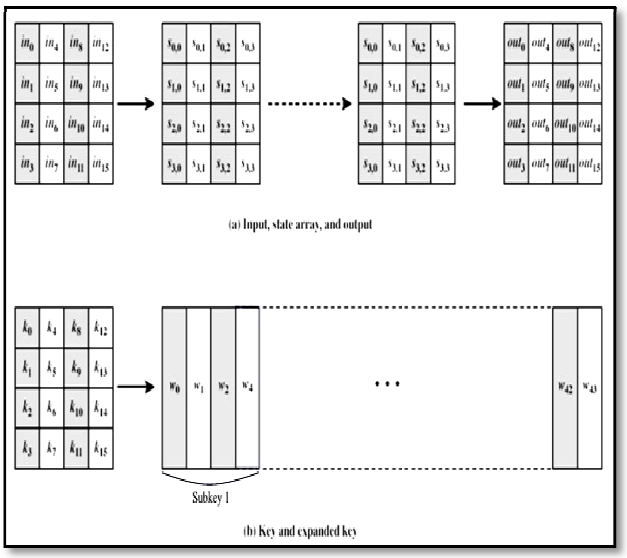


Fig. 3: Key Expansion

LSB Steganography can be classified by two methods LSB replacement and LSB replacement and LSB matching. The terminology of LSB replacement/LSB hiding was firstly discussed by T. Sharp[8]. Let us first consider LSB replacement, In this technique the last bit of the cover image is replaced by the bits of the message which is aimed to be hided. Now consider the second technique of LSB matching in which a secret key is used to generate the pseudo-random order pixel for each pixel of the cover image. In this if the LSB of the cover pixel matches the bit of secret data then no changes are done else a one is added or subtracted from the cover pixel value, at random. The complete algorithm of data hiding in an image is given in [7] as follows:

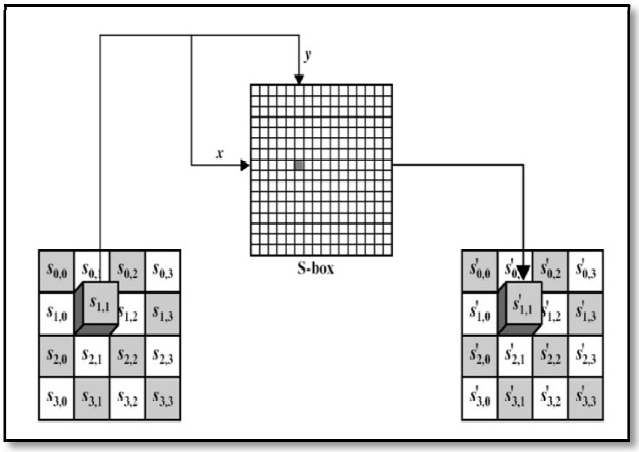


Fig. 4. S-Box Substitution

Let C be the original 8-bit grayscale cover-image of

$M_c \times N_c$ pixels represented as

$$C = \{X_{ij} \mid 0 \le i < M_c, 0 \le j < Nc$$

$$X_{ij} \in \{0, 1, \ldots\ldots\ldots, 255\} \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

M be the n-bit secret message represented as

$$M = \{m_i \mid 0 \le i < N, m_i \in \{0,1\}\} \ldots\ldots\ldots\ldots (2)$$

For embedding the n-bit secret message M into the krightmostLSBs of the cover-image C, thesecret message M isrearranged to form a conceptually k-bit virtual image M' which is represented as,

$M' = \{m'_{ij} \mid 0 \le i < n', m'_i \in \{0, 1, \ldots\ldots, 2k-1\}\} \ldots\ldots$ (3)Where, $n' < M_c \times N_c$.

The mapping between the n-bit secret message M = {mi} andthe embedded message M'= $\{m'_i\}$

can be defined as follows:

$$m'_i = \sum_{i=0}^{k-1} m_{i\times k+j} \times 2^{k-1-j} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

After that, a subset of n' pixels $\{x_{l1}, x_{l2}, \ldots\ldots\ldots x_{ln}\}$ is chosenfrom the cover-image C in a predefined sequence. Theembedding process is completed by replacing the k LSBs ofx_{li} by m'_i. Mathematically, the pixel value x_{li} of thechosenpixel for storing the k-bit message $m'_i$is modified to formthe stego-pixel x'_{li} as follows:

$x'_{li} = x_{li} - x_{li} \bmod 2k + m'_i$.

Also, Algorithm [5] for LSB Based embedding and extractingprocess is given as:

In the extraction process, given the stego-image S, theembedded messages can be directly extracted. Using the samesequence as in the embedding process, the set of pixels $\{x_{l1}, x_{l2}, \ldots\ldots\ldots x_{ln}\}$storing the secret message bits are selected from the stego-image. The k LSBs of the selected pixels areextracted and lined up to reconstruct the secret message bits.

5.2 Encryption based on AES standard

Designing Steps

State array

The input to the encryption algorithm is a single 128 bit block; now this block is required to be copied into a state array. State Array is a square matrix of bytes. This state array is modified at each stage of encryption.

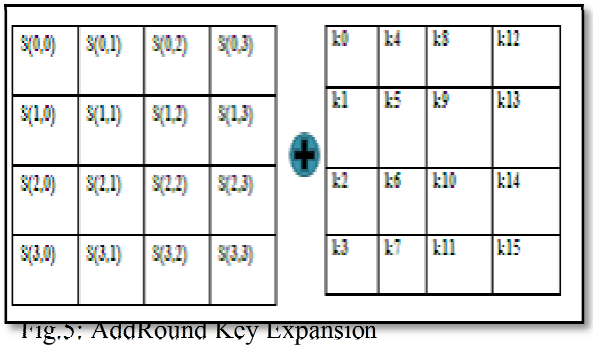


Fig.5: AddRound Key Expansion

Key Expansion

This stage is the most important stage for both encryption as well as decryption. The AES key expansion algorithm [5] takes as input a 4-word key and produces a lineararray of 44 words. Each round uses 4 of these words as shown in Fig.3. Eachword contains 32 bytes which means each subkey is 128 bits long.

The key is copied into the first 4 words of the expandedkey. The reminder of the expanded key is filled in 4 words at a time. Each added word w[i] depends on the immediately preceding word, w[i-1]and the word four positions back, w[i-4]. In three out of four cases, a simple XOR is used. For a word whose position in the **w** array is a multiple of 4, a more complex function **g** is used.

1. RotWord performs a one-byte circular left shift on a word. This means that an input word [b0, b1, b2, b3] is transformed into [b1, b2, b3, b0].
2. SubWord performs a byte substitution on each byte of its input word,using the S-box.
3. The result of step 1 and step2 is XORed with a round constant Rcon[j].

The round constant is for each round and is defined as Rcon[j] = (RC[j],0,0,0), with RC[1]=1; RC[j]=2*RC[j-1] and with multiplication over the field GF(2^8).

AddRound Key Expansion

The 128 bits of State array are bitwise XORed with the 128bits of the round key(4 words of the expanded key).The operation is viewed as a column wise operation between the 4 bytes of the State array column and one word of the round key (Fig. 5).

S-Box Substitution

Fig. 6 : Stego Image

AES defines a 16 x 16 matrix of byte values, called an S-box which contains a permutation of all possible 256 8-bit values. Each byte of State array is mapped into a new byte in the following way: The leftmost 4 bits of the byte are used as a row designated value and the leftmost 4 bits are used as a column designated value. These row and column designated values serve as indexes into the S-box to select a unique 8-bit output value.

Row Shifting

For the second row, a 1-byte circular left shift is performed. For the third row, a 2- byte circular left shift is performed. For the third row, a 3- byte circular left shift is performed. For the first row, no shifting isperformed.

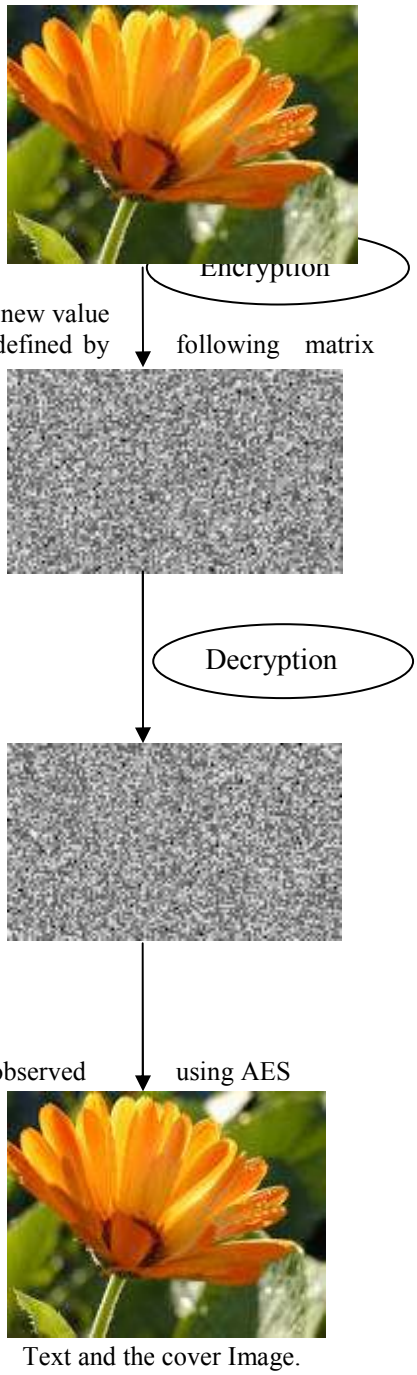
Column Mixing

It operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in the column. The transformation can be defined by following matrix multiplication on State array.

[02 03 01 01 [S(0,0) S(0,1) S(0,2) S(0,3)
01 02 03 01 ✖S(1,0) S(1,1) S(1,2) S(1,3)
01 01 02 03 S(2,0) S(2,1) S(2,2) S(2,3)
03 01 01 02] S(3,0) S(3,1) S(3,2) S(3,3)]

Resulting into
[S'(0,0) S'(0,1) S'(0,2) S'(0,3)
S'(1,0) S'(1,1) S'(1,2) S'(1,3)
S'(2,0) S'(2,1) S'(2,2) S'(2,3)
S'(3,0) S'(3,1) S'(3,2) S'(3,3)] ……..(5)

Each element in the product matrix is the sum of products ofelements of one row and one column.In this case,individualadditions and multiplications are performed in GF(2^8).The MixColumn transformation on a single column j (0 <= j <= 3) of Statearray can be expressed as
S'(0,j) = (2.s(0,j)) xor (3.s(1,j)) xor (s(2,j)) xor s(3,j))
S'(1,j) = (s(0,j)) xor (2.s(1,j)) xor (3.s(2,j)) xor s(3,j))
S'(2,j) = (s(0,j)) xor (s(1,j)) xor (2.s(2,j)) xor 3.s(3,j))
S'(3,j) = (3.s(0,j)) xor (s(1,j)) xor (s(2,j)) xor 2.s(3,j))



VI. Results

On performing MATLAB simulations, we observed that a high grade security is observed using AES encryption technique onto steganography.

Now, Secret message is the same text file for both the images. Using the method of LSB insertion technique, we first convert the secret information into ASCII representation and then each code is converted into 8 bit binary and then each bit is inserted into the last LSB of each pixel cover image, resulting into Stego image.

Text and the cover Image.

VII. Conclusions and Future Scope:

AES is the most promising encryption algorithm which is being used these days. Our paper shows a technique to implement AES onto Steganography. The present existing systems in the domain of steganography has some flaws or inconsistencies such as, less amount of security in encryption of the data, the sender of the data is not validated,

neither the receiver of the data is authenticated to view the secret data behind the image. Our system is expected to remove such inconsistencies of authentication as it will involve symmetric key with both the transmitter and the receiver. Encryption of the message over the process of the steganography will further ensure that even when decrypted, message is not seen instead cover image of the message is seen. This further opens the challenges to implement this system with different formats of the cover image such as .bmp, .jpg, etc. and to study different performance based parameters based on to it.

References:

[1] "*Introduction to computer security*" -Bishop, M., Pearson publications.

[2] "*Cryptography and Data Security*", Dorothy Elizabeth Rob, Ling Denning, Purdue University.

[3] Neil F. Johnson, ZoranDuric, and Sushil Jajodia, "*Information Hiding:*
Steganography and Watermarking - Attacks and Countermeasures", MA, Kluwer Academic Publishers, 2001.

[4] B.B. Githe, Divya Choksey, Mahesh Jambulkar, R. Ramnath " *Data Hiding Using Steganography And Authentication Using Digital Signatures And Facial Recognition*"

[5] P.Karthigaikumar and S.Rasheed "*Simulation of Image Encryption using AES algorithm*", *IJCA special issue on computational science-new dimensions and perspectives" NCCSE 2011.*

[6]M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki "*A Modified AES Based Algorithm for ImageEncryption*" World Academy of Science, Engineering and Technology 27, 2007

[7] Chan, C.K., Cheng, L.M., 2004. "*Hiding data in imagesby simple LSB substitution*". *Pattern Recognition 37(March), 469–474.*

[8]. T. Sharp, "An implementation of key-based digital signal steganography," in Proc. Information Hiding Workshop*,vol. 2137, Springer LNCS, 2001, pp. 13–26.*

[9] A.A.Zaidan, B.B.Zaidan, Anas Majeed, *"High Securing Cover-File ofHidden Data Using Statistical Technique and AES EncryptionAlgorithm*", World Academy of Science Engineering and Technology(WASET), Vol.54, ISSN: 2070-3724, P.P 468-479.

[10] M. Abomhara, Omar Zakaria, Othman O. Khalifa .A.Zaidan, B.B.Zaidan, "*Enhancing Selective Encryptionfor H.264/AVC Using Advance Encryption Standard* ", International Journal of Computer and Electrical Engineering (IJCEE), ISSN: 1793-8198,Vol.2 , NO.2, April 2010, Singapore..

[11] A.W. Naji, Shihab A. Hameed, B.B.Zaidan, Wajdi F. Al-Khateeb, Othman O. Khalifa, A.A.Zaidan and Teddy S. Gunawan, " *Novel Framework for Hidden Data in the Image Page within Executable File Using Computation between Advance Encryption Standared and Distortion Techniques*", International Journal of Computer Science and Information Security (IJCSIS), Vol. 3, No 1 ISSN: 1947-5500, P.P 73-78,3 Aug 2009, USA.