Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# An Information Security Technique Using AES-RSA Hybrid and SLSB: Review

[1]Renu Yadav, [2]Dr Nasib Singh Gill
[1]Mtech Student, [2]Professor
[1, 2,] Department of Computer Science and Application, M.D University,
Rohtak, Haryana, India

***Abstract: Cryptography and Steganography plays a very important role as security tools. Cryptography is the art of converting the readable information into an unreadable form. Steganography is a tool used to hide information inside a media files such as images, audio and video etc. In this paper a combined technique of both cryptography and steganography is proposed for the better security of the data. The message is initially encrypted with AES and the keys of AES are encrypted with RSA then the hybrid of both AES-RSA is embedded inside an image with help of SLSB image steganography. Results of the technique provide a stronger security. The encryption time is also faster.***

***Keywords: AES; RSA; Hybridization; SLSB; Steganography;***

## I. INTRODUCTION

Cryptography is an effective way for protecting sensitive information .it is a method for storing and transmitting data in form that only those it is intended for read and process.The evolution of encryption is moving towards a future of endless possibilities. Stenography is the art of passing information through original files.

Steganography is a technique which hides data inside other data. Stenography refers tinformation or file that has been concealed inside a picture,video or audio file.The difference between Cryptography and steganography is cryptography keep the message secret and steganography keeps the existence of the message secret . The aim of both Cryptography and Steganography is keep the data safe from unwanted parties. So, for providing the Complete Security to the data we are using the concept of two layer of security i.e. Cryptography along with Steganography. Here in this paper we are using the crptography with AES ,RSA and Steganographic SLSB (Selected Least Significant Bit) algorithm for hiding the secret message inside the image.

## II. OVERVIEW OF EXISTING ALGORITHM

There are various types of cryptography algorithm exist in market. Main goal of these algorithms is to protect data and application from unauthorized access. So we are going to discuss some existing algorithms.

### *A. RIVEST SHAMIR ADLEMAN (RSA)*

RSA based on a public key system that is generated by Ron **R**ivest, Adi**S**hamir, and Leonard **A**dleman in 1978 [1]. Three basic steps are required to complete the process of RSA operations that are; key generation, encryption and decryption. First, messages are converted to numbers (integers), and then the numbers are manipulated according to the prescribed encryption scheme. Here is the description of the RSA cryptosystem. For the implementation of RSA we have to follow following steps [2]:

**Step 1** Firstly Choose two prime number p and q.
**Step 2** Then compute value of n= p x q.
**Step 3** Chooses $e$ with (e, $(p-1)(q-1)) = 1$ and computes $d$ with
$de \equiv 1(\text{mod}(p-1)(q-1))$.
**Step 4** Makes n and e public and keeps p, q, d secret.
**Step 5** Sender encrypts $m$ as $c \equiv m^e \pmod{n}$ and sends $c$ to Receiver
**Step 6** Bob decrypts by computing $m \equiv c^d \pmod{n}$.
In this set up, the integer n is called the RSA modulus, e is called the encryption exponent and d is called the decryption exponent.

### *B. ADVANCED ENCRYPTION STANDARD*

Advanced Encryption Standard (AES) algorithm is not only for security but also for great speed. Both hardware and software implementation are faster still.New encryption standard is recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10, 12and 14 round are depending on key size as shown in Figure 4. It can be implemented on various platforms especially in small devices. It is carefully tested for many security applications.

 

Algorithm Steps*:* These steps used to encrypt 128-bit block
1. The set of round keys from the cipher key.
2. Initialize state array and add the initial round key to the starting state array.
3. Perform round = 1 to 9: Execute Usual Round.
4. Execute Final Round.
5. Corresponding cipher text chunk output of FinalRound Step.

**Encryption** *:*Each round consists of the followingfour steps:

1 **SubBytes**: The first transformation, SubBytes, isused at the encryption site. To substitute a byte,we interpret the byte as two hexadecimal digits.

2 **ShiftRows**: In the encryption, the transformationis called ShiftRows.

3 **Mix Columns**: The MixColumns transformationoperates at the column level; it transforms eachcolumn of the state to a new column.

4**AddRound Key**: AddRound Key precedes onecolumn at a time. AddRoundKey adds a roundkey word with each state column matrix;theoperation in Add Round Key is matrix addition.The last step consists of XORing the output ofthe previous three steps with four words from the keyschedule. And the last round for encryption does notinvolve the "Mix columns" step.

**Decryption**: Decryption involves reversing all thesteps taken in encryption using inverse functionslike a) Inverse shift rows, b) Inverse substitutebytes, c) Add round key, and d) Inverse mixcolumns.

The third step consists of XORing the output ofthe previous two steps with four words from the keyschedule. And the last round for decryption does notinvolve the "Inversemix columns" step.

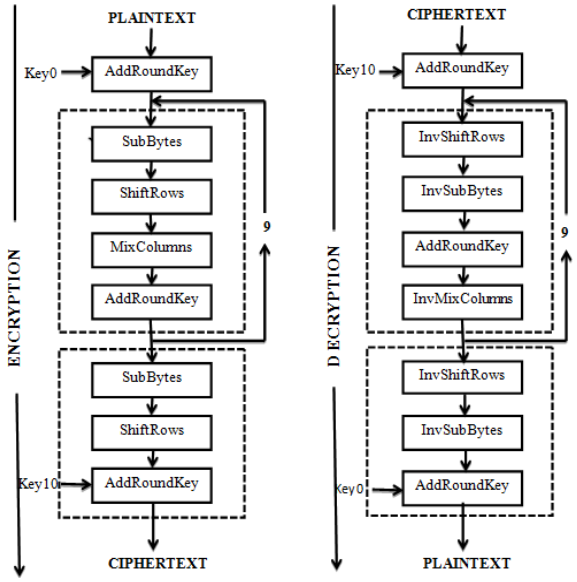


Fig- Encryption and Decryption Standard

### *C. SLSB ALGORITHM*

SLSB (Selected Least Significant Bit) is improves the performance of the recently most popular algorithm for data hiding LSB (Least Significant Bit).The LSB algorithm hide single bit of information in least significant bit of each color pixel.But this method is not effective when the Statistical Analysis like Sample Pair [6], Reed Soloman Analysis [7] is applied. When we are updating three colors of a pixel then the large distortion is occurs in the resulting image. The SLSB hides the data in only one of three (Red, Green, Blue) colors at each pixel of the carrier image. For choosing the color to hide a data, SLSB algorithm performs the sample pair analysis and selects the color with higher ratio because it shows higher diversity. The choice of sample pair analysis in SLSB algorithm is because of the work of ker in the field of hidden data detection. If we uses the sample pair analysis technique the color chosen with greater distortion and when we hide data in that area is less detectable. The following examples shows how the distortion is minimize using LSLB algorithm.

Ex.1) If the pixel of the carrier image are(Red-Greenblue)9E8C7A. In Binary 10011110-10001100-01111010 and we have to hide a message 111.

**By LSB Algorithm**:

It hides the each 1 bit into the least significant bit of each color pixel i.e. 10011111-10001101-01111011

Table 1: Result obtained by LSB

| | HexadecimaL | DECIMAL | RED | GREEN | BLUE |
|---|---|---|---|---|---|
| OriginalPixel | 9E8C7A | 10390650 | 158 | 140 | 122 |
| UpdatedPixel | 9F8D7B | 10456443 | 159 | 141 | 123 |

 

The table shows the distortion between original and updated color are of 65793 color

**By SLSB Algorithm:**

It hides the all data into a single color selected by the sample pair analysis i.e.10011111-10001100-01111010. Here data hide into the Red color.

Table 2:Result obtained by SLSB

| | HexadecimaL | DECIMAL | RED | GREEN | BLUE |
|---|---|---|---|---|---|
| OriginalPixel | 9E8C7A | 10390650 | 158 | 140 | 122 |
| UpdatedPixel | 9F8D7A | 10456186 | 161 | 140 | 122 |

The table shows the distortion between original and updated color are of 65536 color on color scale. This is less than LSB method.

## III. OBJECTIVE OF PROPOSED ALGORITHM

A. Two layer security by cryptography and stenography using SLSB algorithm to make information more secure.
B. AES and RSA are used for cryptography to provide hybrid cryptography and then SLSB algorithm is used with stenography.
C. AES is applied on plaintext with private key generated by RSA and then SLSB is applied for stenography and AES is also implemented with standard process and then slsb is applied for stenography, both the results are then compared

## IV. PROPOSED METHODOLOGY

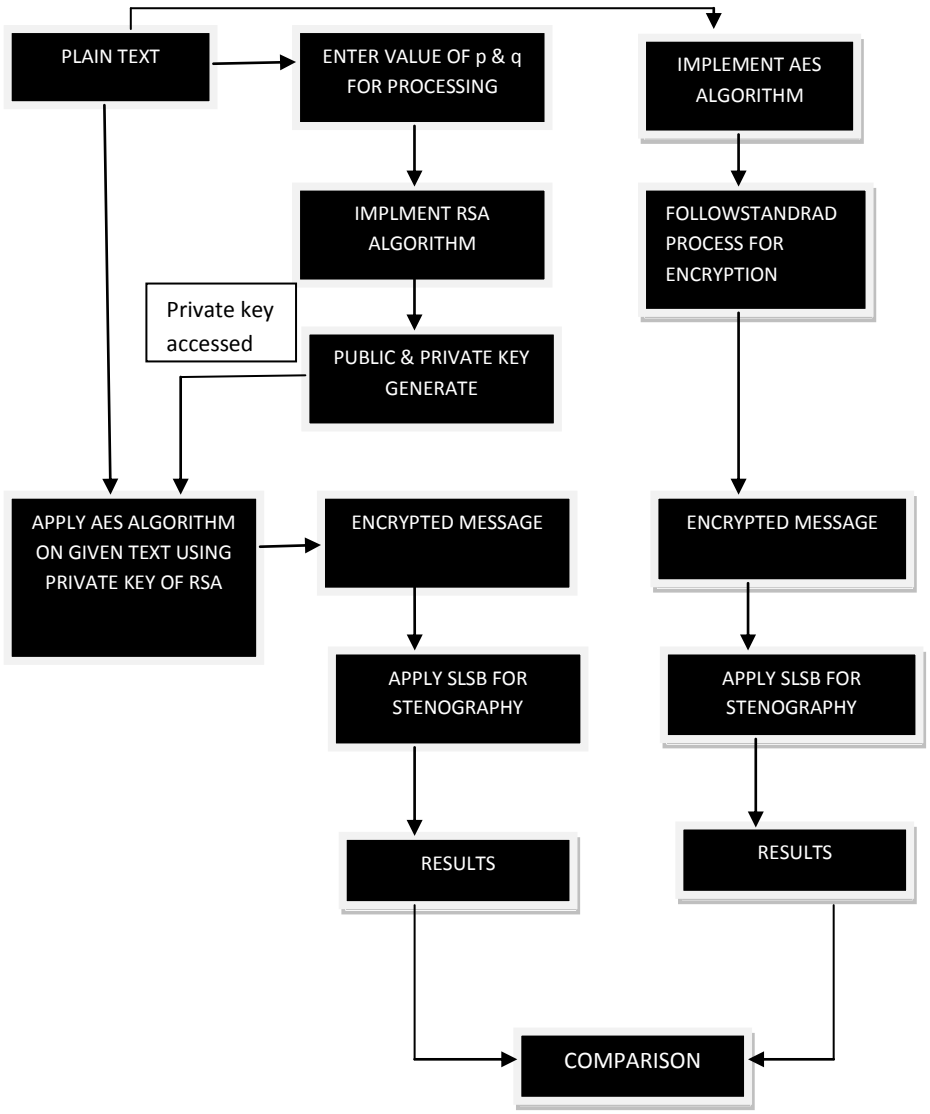


Fig- Proposed method used for cryptography and stegnography

 

## V. ADVANTAGES USING SLSB ALGORITHM

A. Although the concept of SLSB based on LSB it hides information effectively than LSB.
B. Uses Sample Pair Analysis for selecting best color from the possible three for data hiding.
C. Uses Pixel Selection Filter to select best area in image for hide the data.
D. Uses LSB Match to decrease difference between original image pixel and steganographic image pixel
E. Resist to histogram comparison, as the frequency of steganographic image is nearly similar to original image.
F. Resist to statistical analysis, as two colors for each pixel are unchanged. So, the final analysis ratio nearly similar to the original

## VI. CONCLUSION

Today many technologies are emerging in the area of information Security.Cryptography and Stegnography are also part of them**.**In this paper the two layer security by Cryptography and SLSB Steganography algorithm are used to make the information secure. By combining two techniques it immune to many attacks. AES and RSA are used for cryptography to provide hybrid cryptography and then SLSB algorithm is used with stenography. Due to use of SLSB algorithm the difference in the carrier image and the Steganographic image is negligible. We are using the Selected Least Significant Bit algorithm which is faster and reliable and compression ratio is moderate compared to other algorithm.

## REFERENCES

[1] Saurabh Singh and Gaurav Singh, **"Use of image to secure text message with the help of LSB replacement"**International journal of applied engineering research ,Dindigul Volume 1, No1, 2010.
[2] B. Padmavathi, S. Ranjitha Kumari, **"A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique**" International Journal of Science and Research (IJSR), Volume 2 Issue 4, April 2013
[3] Suraj J. Warade, Pritish A. Tijare , Swapnil N. Sawalkar, "**Data Security Using Cryptography and SLSBAlgorithm"** International Journal of Research in Advent Technology, Vol.2, No.4, April 2014
[4] Sandeep Singh, Aman Singh, "**An Information Security Technique Using DES-RSA Hybrid and LSB"** International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS) March-May, 2014, pp. 187-192
[5] Rishabh Jain, Rahul Jejurkar, "**AES Algorithm Using 512 Bit Key Implementation for Secure Communication"** International Journal of Innovative Research in Computer and Communication EngineeringVol. 2, Issue 3, March 2014
[6] Suraj J. Warade, Pritish A. Tijare, Swapnil N. Sawalkar ,"**Data Security Using Cryptography and SLSB Algorithm"** International Journal of Research in Advent Technology, Vol.2, No.4, April 2014
[7] **Anil Kumar, Rohini Sharma ,"A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique"** International Journal of Advanced Research in Computer Science and Software Engineering 3(7), July - 2013, pp. 363-372
[8] Jasleen Kour, Deepankar ,"**Steganography Techniques –A Review Paper***"* International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5) May 2014
[9] Atallah M.Al-Shatvani, "**A New Method in Image Steganography with Improved Image Quality"** Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 – 3915
[10] Atul Kahate (2009), **Cryptography and Network Security**, second edition, McGraw-Hill.
[11] Ajit Singh, Swati Malik **"Securing Data Using Cryptography and Steganography"** IJARCSSE Volume3, Issue 5, May 2013.
[12] Swati Tiwari, R. P. Mahajan**, "***A Secure Image Based Steganographic Model Using RSA Algorithm and LSB Insertion***",** International Journal of Electronics Communication and Computer Engineering (IJECCE), Vol. 3, Issue No. 1, 2012.
[13] Deepesh Rawat, Vijaya Bhandari, **"***A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image*", International Journal of Computer Applications, Vol. 64, Issue No. 20, Feb., 2013.

 