Volume 5, Issue 7, July 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: Research

Renu Yadav[1], **Dr Nasib Singh Gill**[2]
[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. As going through all the previous work, we come to know that the importance of hiding data in encrypted form is highly required in all manners for the global world communication. Study of previous work generates a problem statement for us. If we perform a single level encryption mechanism for the text, it would become a little easier for the decrypted end to make it visible to the user and hence a question can be put on the standard of encryption. In this research work we study about an invention on AES algorithm using SLSB technique and also RSA with AES+SLSB. In both approaches output of one technique will work as like input of sequential approach. AES is implemented in two ways one is using standard key and other using private key of RSA algorithm. SLSB is applied on both way of AES implementation. Main motive of this combined approach is to reduce time and enhance security. Finally we compare the both results.

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 RSA and Steganographic SLSB (Selected Least Significant Bit) algorithm for hiding the secret message.

A. RSA ALGORITHM

RSA is one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir andLeonard Adleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician, had developed an equivalent system in 1973, but it wasn't declassified until 1997.

A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. Breaking RSAencryption is known as the RSA problem. It is an open question whether it is as hard as the factoring problem.

RSA based on a public key system that is generated by Ron **R**ivest, Adi**S**hamir, and Leonard **A**dleman in 1978 . 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 $c \equiv m^e$ (mod 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.

C. SLSB ALGORITHM

In the following paragraphs, the explanation of the operations that are doing by the Segmented LSB (SLSB) will be given. Before listing the algorithm’s steps that describe the operations of (SLSB), some data structures that are using in the algorithm are defined follow:

1. MessageB: is a list that contains a binary representation (bits) of all characters in the secret Message. The number of elements (size) of this list is (n*8), where n is the number of characters in the secret Message.
2. DataB: is a list of the Least Significant Bit (LSB) of all pixels in the stego-image. The number of elements (size) of this list is (m), where m is the size of the Image and its equal (Width × Height × Palette).
3. SegmentLength: is a positive integer number between (2 … (n*8)/2) which represents the length of each segment (number of bits) in the SegmentList.
4. SegmentsList: is a list of segments that is created from the MessageB by splitting it to k segments, where k = (n*8) / SegmentLength. And each segment has number of bits equal SegmentLength.
5. SegmentIndex: is a list of indices, each index represents the first index of a sequence of bits in DataB that is having a best match with the bits of one of the segments in SegmentsList. We must note that there is no overlapping between the sequences of match bits in this technique.

```
Algorithm: Segmented-LSB (SLSB)
// Hiding Operation
(for embedding the characters of the secret Message in the Text Data)
Step1: Calculate the TotalSize (in byte) that is required to store:
        (1) Length of secret message (number of character)
        (2) SegmentLength
        (3) Size of SegmentList
Step2: For i = 1 To ( (n*8) / SegmentLength )
        {
        For j = ((TotalSize*8)+1) To m
        {
        x = 1
        BestMatch = 0
        BestIndex = -1
        w=j
        For w = j To ( j+ SegmentLength )
        {
```

```
Find the number of matched bits MBits in Segment[i][x] with the bits of DataB[w]
x = x+1
}
If (MBits>BestMatch)
{
BestMatch = MBits
BestIndex = j
}
}
SegmentIndex[i] = BestIndex
Substitute the bits of Segment[i] instead of the bits in ImageB starting at BestIndex
}
```

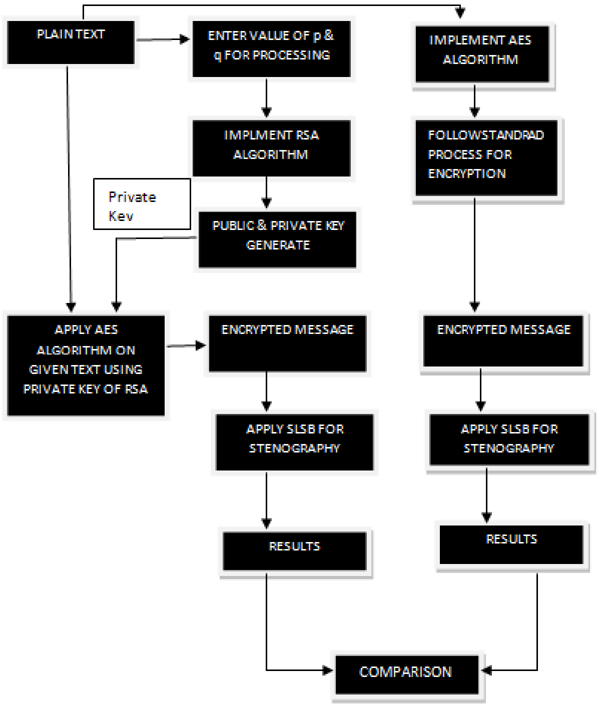
Step3: Store the bits representation of the above three information (in Step1) in the Least Significant Bit (LSB) at the start of the DataB list (from bit #1 to bit #(TotalSize*8)).

II. OBJECTIVE OF PROPOSED ALGORITHM

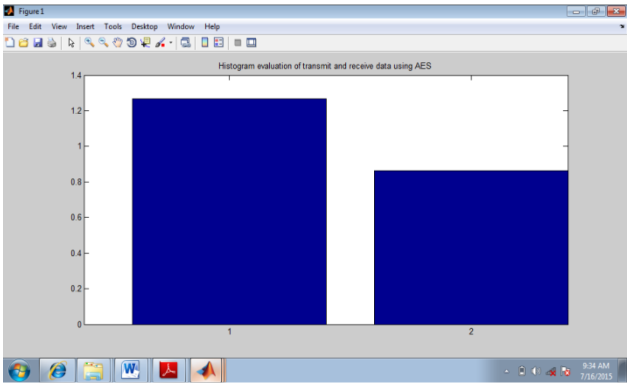
We shall follow these objectives as following:

1) Study cryptography concept in security mechanism.
2) Implement RSA algorithm on a plain text and this will generate public & private key.
3) Use private key of RSA as encryption key for AES algorithm.
4) Ciphertext generated by AES is taken as input of SLSB technique and encrypted text is further encrypted.
5) Now implement AES algorithm with standard key and generate encrypted text of plaintext.
6) This encrypted text is further as input of SLSB technique. SLSB generate final ciphertext of plaintext.
7) Compare the results of SLSB in both cases.

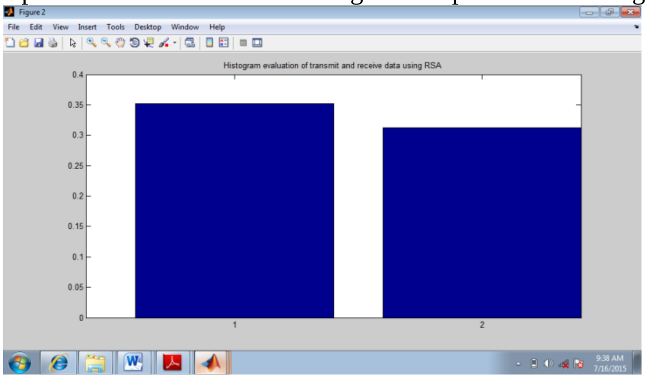
III. PROPOSED METHODOLOGY


PLAIN TEXT
ENTER VALUE OF p & q FOR PROCESSING
IMPLEMENT AES ALGORITHM
IMPLMENT RSA ALGORITHM
FOLLOWSTANDRAD PROCESS FOR ENCRYPTION
Private Key
PUBLIC & PRIVATE KEY GENERATE
APPLY AES ALGORITHM ON GIVEN TEXT USING PRIVATE KEY OF RSA
ENCRYPTED MESSAGE
ENCRYPTED MESSAGE
APPLY SLSB FOR STENOGRAPHY
APPLY SLSB FOR STENOGRAPHY
RESULTS
RESULTS
COMPARISON

IV. RESULTS



The histogram represents the timing of data receiving and transmitting after encoding in AES algorithm. In above window histogram 1 on x-axis represent transmit time and histogram 2 represents receiving time of AES algorithm.



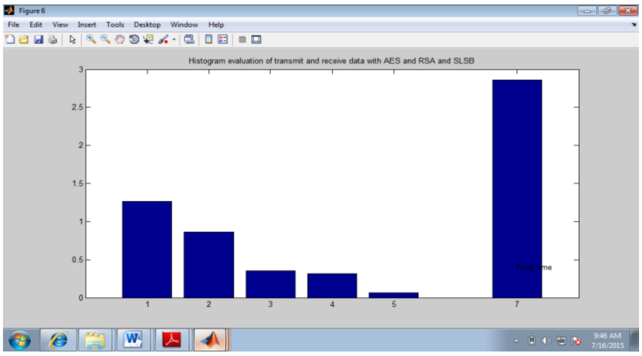


Table-I Comparative table for all techniques in combined approach (RSA+AES+SLSB)

Sr. No.	Technique Name	Transmit Time (ms)	Receiving Time (ms)
1.	RSA	0.35	0.31
2.	AES	1.29	0.78
3.	SLSB	0.1	Not Exist
4.	RSA+AES+SLSB	Total Time = 2.83	

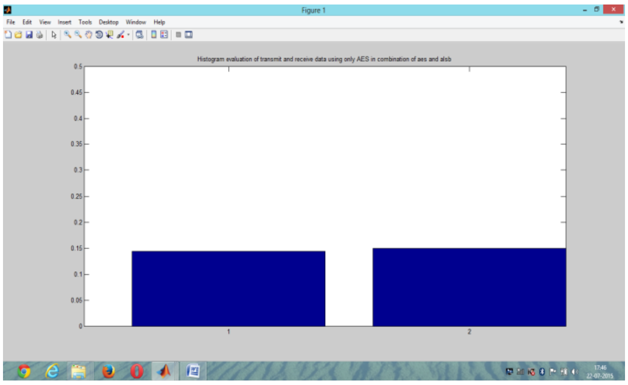


Figure 5.10: Time consume by only AES in combination approach of AES + SLSB

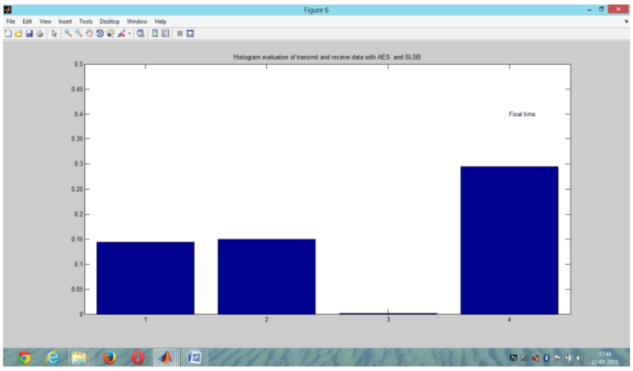


Figure 5.11: Histogram 3 represents time consuming by SLSB and histogram 4 represents total time consuming by combined approach AES+SLSB

Table-II Comparative table for all techniques in combined approach (AES+SLSB)

Sr. No.	Technique Name	Transmit Time (ms)	Receiving Time (ms)
1.	AES	0.9	0.7
2.	SLSB	0.1	Not Exist
3.	AES+SLSB	Total Time = 1.7	

Table-III Comparative table for combined approach (RSA+AES+SLSB)& (AES+SLSB)

Sr. No.	Technique Name	Total Time (ms)
1.	RSA+AES+SLSB	2.83
2.	AES+SLSB	1.7

V. CONCLUSION

With the implementation of AES algorithm with SLSB and combination of RSA+AES+SLSB, a conclusion is achieved that for better secureness of any text or image we can apply any techniques from these but combination of all three techniques will provide us more security as compared to combination of AES with SLSB. But in case time consuming AES with SLSB is better for use but less secure. For an illusion designing of this work we chose a text and apply AES algorithm on it with encryption key. We got some encrypted text and after that apply the SLSB then got an encrypted text that is very difficult to any other person to decrypt it and time saving. But secondly we apply RSA on same text and then apply AES on that encrypted code after that final technique SLSB is applied on the output of AES algorithm. Time consume in three combination technique is 2.83 ms and in two technique combination 1.7ms. This is achievement in our conclusion that makes a text more secure in not enough time.

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] **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

[4] 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

[5] Atallah M.Al-Shatvani, "**A New Method in Image Steganography with Improved Image Quality"** Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 – 3915

[6] Atul Kahate (2009), **Cryptography and Network Security**, second edition, McGraw-Hill.

[7] Sonalsharma, jitendrasinghyadav, parshantsharma," **Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm"**International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012 ISSN: 2277 128X.

[8] B. Persis Urbana Ivy, PurshotamMandiwa,Mukesh Kumar**," A modified RSA cryptosystem based on 'n' prime numbers**", International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume1 Issue 2 Nov 2012 Page No. 63-66.

[9] Mohammed AbuTaha, MousaFarajallah, RadwanTahboub, Mohammad Odeh," **Survey Paper: Cryptography Is the Science of Information Security",** International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (3): 2011.

[10] Diffie W. The first ten years of Public Key Cryptography, In Contemporary Cryptology: The Science of Information Integrity, Editor, Simmons G.J. IEEE Press, New York. p.p 135-175, 2003

[11] Gilles Cazelais**, "Numerical Example of RSA",** Typeset with LATEX on June 11, 2007

[12] M. Nordin A. Rahman, A. F. A. Abidin, MohdKamirYusof, N. S. M. Usop**," Cryptography: A New Approach of Classical Hill Cipher",** International Journal of Security and Its Applications Vol. 7, No. 2, March, 2013

[13] 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.

[14] 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.