Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 7, July 2015, pg.279 – 285

RESEARCH ARTICLE

Improvement in Performance of RSA Algorithm Using SLSB

Ms. Renu Yadav[1], Dr. Nasib Singh Gill[2]

[1]M.Tech Student, Department of Computer Science and Application, M.D University Rohtak, Haryana

[2]Professor, Department of Computer Science and Application, M.D University Rohtak, Haryana

[1] bhatotiarenu@gmail.com [2] nasib.gill@gmail.com

Abstract*: *Most companies and government agencies have a dire need for protecting sensitive information. Encryption, access restriction, and locking documents behind firewalls are some common techniques for protecting sensitive information. Encryption is an effective way for preventing an unauthorized person from viewing the content of a sensitive document. Nonetheless, once the document is decrypted for viewing using the secret key, an ill-intentioned authorized person can save, copy, print, or transmit the unencrypted document anywhere he or she wants without any major difficulty. Many algorithms are invented by researcher for avoidance of risk. One of them is RSA algorithm which play important role for better security. In this paper we use a hybrid approach using RSA algorithm with SLSB technique. This technique is applied directly on output of RSA algorithm. The results of hybrid approach compared with RSA.

Keywords: 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 to information 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 cryptography 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

$de \equiv 1(\mathrm{mod}(p - 1)(q - 1))$.

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 $m \equiv c^d$ (mod 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. 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-Green -blue)9E8C7A. In Binary 10011110-10001100-01111010 and we have to hide a message 111.

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

	Hexa decimal	DECIMAL	RED	GREEN	BLUE
Original Pixel	9E8C7A	10390650	158	140	122
Updated Pixel	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.

In the following paragraphs, the explanation of the operations that are doing by the 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. ImageB: 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 ImageB 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 stego-image Image)
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 ImageB[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 ImageB list (from bit #1 to bit #(TotalSize*8)).

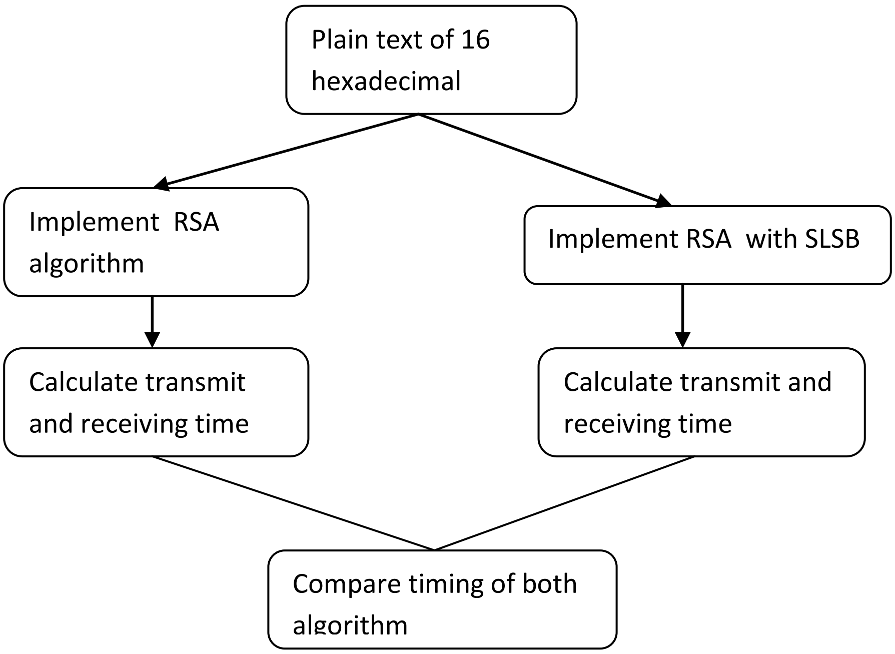
II. OBJECTIVE OF PROPOSED ALGORITHM

A. Two layer security by cryptography and stenography using SLSB algorithm to make information more secure.

B. RSA are used for cryptography and then SLSB algorithm is used with stenography.

C. RSA is applied on plaintext with private key generated by RSA and then SLSB is applied for stenography on the resultant and RSA is also implemented with standard process and both the results are then compared.

III. Proposed Methodology


Plain text of 16 hexadecimal
Implement RSA algorithm
Implement RSA with SLSB
Calculate transmit and receiving time
Calculate transmit and receiving time
Compare timing of both algorithm

IV. 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

V. RESULTS

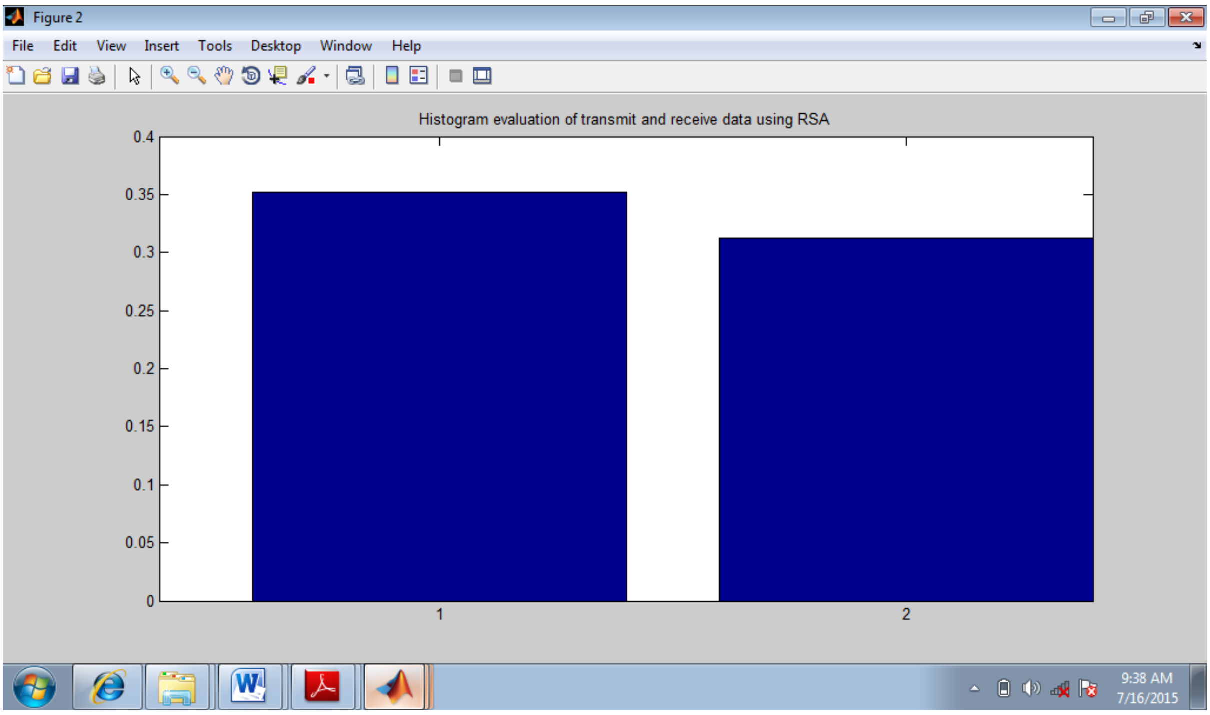


Figure 2
File Edit View Insert Tools Desktop Window Help
Histogram evaluation of transmit and receive data using RSA
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
1
2
9:38 AM
7/16/2015

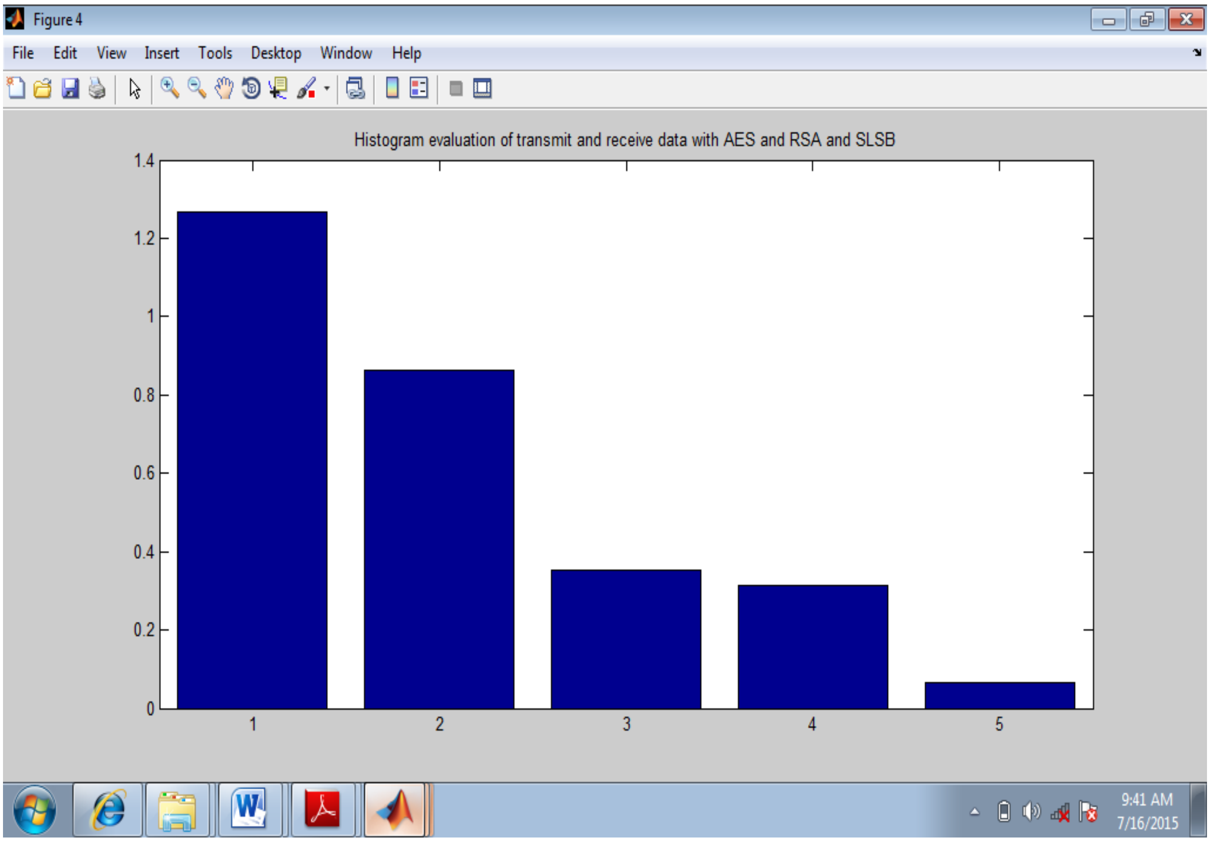


Figure 4
File Edit View Insert Tools Desktop Window Help
Histogram evaluation of transmit and receive data with AES and RSA and SLSB
1.4
1.2
1
0.8
0.6
0.4
0.2
0
1
2
3
4
5
9:41 AM
7/16/2015

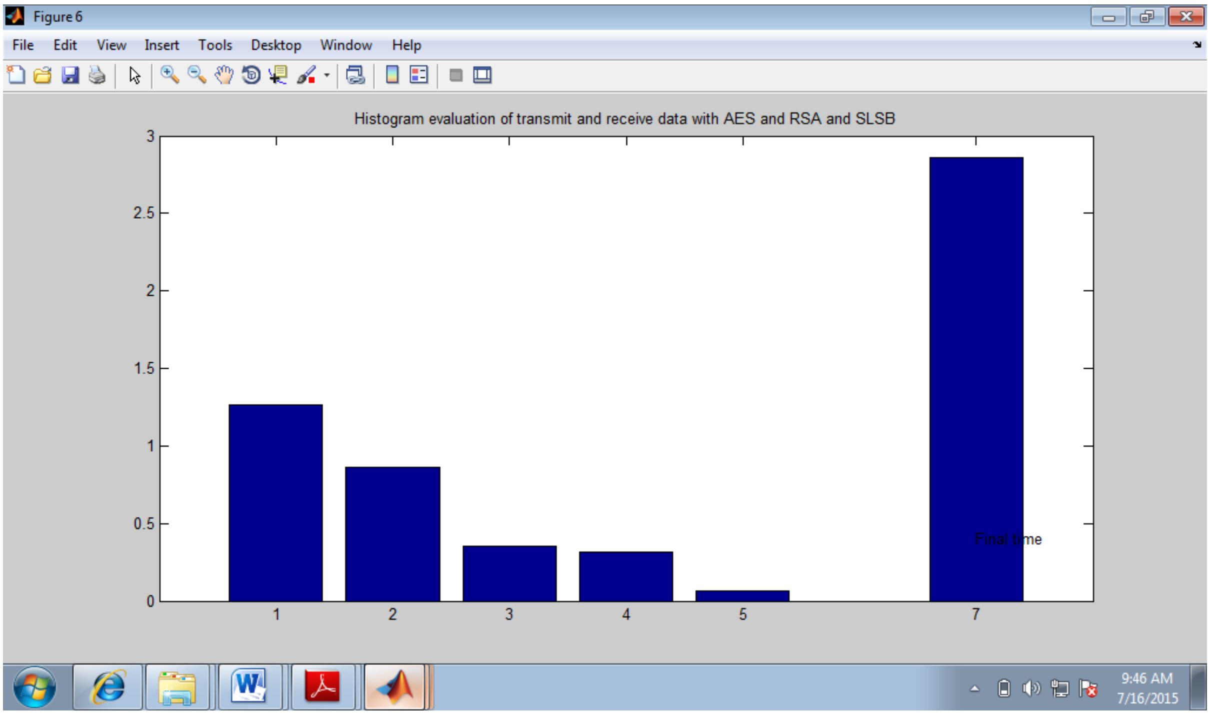


Figure 6
File Edit View Insert Tools Desktop Window Help
Histogram evaluation of transmit and receive data with AES and RSA and SLSB
3
2.5
2
1.5
1
0.5
0
1
2
3
4
5
7
Final time
9:46 AM
7/16/2015

VI. Encryption and Decrption Time

Sr. No.	Technique Name	Transmit Time (ms)	Receiving Time (ms)
1.	AES	1.29	0.88
2.	RSA	0.35	0.31
3.	RSA+SLSB	0.1	Not Exist

VII. CONCLUSION

With the implementation of RSA algorithm with SLSB, a conclusion is achieved that for better secureness of any text or image we can apply any two techniques one by one on each other that make it more secure like SLSB with RSA. For an illusion designing of this work we chose a text and apply RSA 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. This is achievement in our conclusion that makes a text more secure in less 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.