DOI: http://dx.doi.org/10.26483/ijarcs.v13i5.6895

Volume 13, No. 5, September-October 2022

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

HYBRID ENCRYPTION USING LSB STEGANOGRAPHY AND RSA

K Manikandan*
Associate Professor (Senior) Scope (CSE)Vellore Institute Of Technology,
Katpadi, Tamilnadu, India –632014

M Narayana Royal
Student, Scope (CSE)
Vellore Institute Of Technology
Katpadi, Tamilnadu, India -632014

P Manohar Venkat
Student, Scope (CSE)
Vellore Institute Of Technology,
Katpadi, Tamilnadu, India -632014

Dommaraju Nikhil
Student, Scope (CSE)
Vellore Institute Of Technology
Katpadi, Tamilnadu, India -632014

Malayam Rajesh
Student, CSE Department
Vellore Institute Of Technology Katpadi,
Tamilnadu India -632014

Abstract: Computers and the internet are the two main communication tools used today to link the entire world together as one virtual space. So we can easily exchange lots of information within seconds of time, but the confidential data that needs to be transferred should be kept confidential. Thus, in order to aid this, we have proposed a new encryption technique by combining Image steganography (LSB) with the cryptographic RSA algorithm for providing more security to our data as well as imperceptibility. The expected outcome would be a properly secure combination of encryption models that uses steganography to hide the message content in a cover image, and also encrypts the message using the cryptographic algorithm, as an additional security layer, in case the content was retrieved from the cover image.

Keywords: AES, RSA, LSB, Steganography

I. INTRODUCTION

The basic need of every growing area in today's world is communication. This communication needs to be safe and secure. We use many insecure pathways in our daily life for transferring and sharing information using the internet or telephonically, but at a certain level it's not safe. Steganography and cryptography are two methods which are used to share information in a concealed manner. Cryptography includes modification of a message in a way such that is in an encrypted form guarded by an encryption key which is known only by the sender and receive. But in cryptography it's always clear to an intermediary that the message is in an encrypted form, whereas in steganography the secret message is hidden in a cover image so that it isn't clear to any intermediary that whether a message is hidden in the information being shared. The cover image containing the secret message is then transferred to the recipient. The recipient extracts the message with the help of the steganography algorithm.
It is a challenging process which will lead us to combine two technologies, one of them is an algorithm from cryptography, namely RSA, and the other is the LSB algorithm from steganography. Our research has been concentrated on developing a method for securely transferring and sharing critical data. All the reputed organizations while sending business documents over the internet always use encryption of the data to protect leakage of information about their organization from their rivals or imposters. We have used LSB and RSA to create a secure steganography algorithm which is far more secure than many systems being used for the purpose of secretly sending data.

II. PROBLEM ANALYSIS

A. RSA Algorithm

An asymmetric encryption method, the RSA algorithm needs both a public key and a private key. The concept of RSA is based on the fact that big integers are challenging to factor. The public key is made up of two numbers, one of which is the product of two enormous prime numbers. The same two prime numbers are also used to create the private key. Therefore, the private key is compromised if someone is able to factorize the huge integer.

B. AES algorithm

A symmetric block encryption algorithm with a block/chunk size of 128 bits is the AES Encryption algorithm, sometimes referred to as the Rijndael algorithm. These distinct blocks are converted using keys that are 128, 192, and 256 bits long. It then connects these blocks to create the ciphertext after encrypting each one separately. It is founded on an SP network, sometimes referred to as a substitution-

permutation network. It comprises of a number of interconnected processes, some of which involve bit shuffles and others involve substituting inputs with certain outputs (substitutions) (permutations).

Here we are using only RSA algorithm but not AES as it is asymmetric and has both the public key as well as private key. Which is helpful for storing encrypted data in image format which is secure. We need the data to be more secure than faster in this case.

C. LSB Steganography

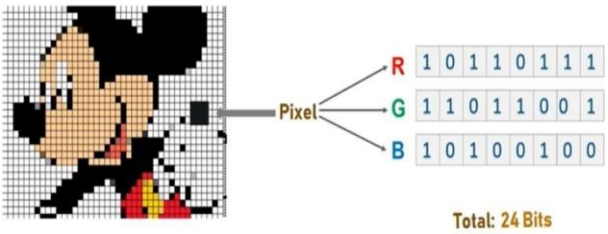
Image-based Steganography is based on a fairly straightforward concept. Digital data (pixels) that make up images define the contents of the image, typically the colours of all the pixels. Since each pixel in an image comprises three values and is the building block of every image (red, green, blue).

D. Encode the data:

Ascii values are used to translate each byte of data into its 8-bit binary equivalent. Now a set of three pixels with a total of 9 values are read from left to right. Binary data is stored in the first 8 values. If 1 happens, the value becomes odd; if 0 occurs, it becomes even.

E. Decode the data:

To decode, three pixels are read at a time, till the last value is odd, which means the message is over. Every 3-pixels contain a binary data, which can be extracted by the same encoding logic. If the value is odd the binary bit is 1 else 0.



III. LITERATURE SURVEY

1. High Capacity data hiding using LSBSteganography and Encryption

The main goal of this paper is to offer high capacity and resistance to visual and statistical attacks. They suggest a high-capacity data embedding method that combines cryptography and steganography. The method they used are transposition ciphers. The procedure involves encrypting a message using the transposition cypher method before using the LSB insertion method to embed the encrypted message inside an image. The security of the embedded data will be improved by combining these two techniques. The capacity, security, and robustness requirements for secure data transmission over an open channel will be met by this combinational methodology.

2. An Analysis of LSB & DCT basedSteganography

This paper presents analysis of Least Significant Bit (LSB) based Steganography and Discrete Cosine Transform (DCT) based Steganography. This paper implements LSB based steganography, DCT based steganography and computes PSNR ratio. PSNR is the peak signal to noise ratio, in decibels, between two images. This ratio is used as a quality measurement between two images.

3. RSA Public Key Cryptography Algorithm – A Review

This Paper aims to review RSA, consider its advantages and disadvantages, and offer fresh remedies to the disadvantage. One of the most effective cryptographic algorithms currently in use for ensuring secure network communication is RSA (Rivest, Shamir, and Adleman).Paper discuss about RSA algorithm as the most widely used PKC algorithm , looks at current usage of RSA, also highlights the strengths and weakness of RSA, and briefly discusses the recommendations to mitigate some of the identified drawbacks.

4. RSA and ECC: A Comparative Analysis

After comparing the RSA and ECC ciphers, the ECC has proved to involve much less overheads compared to RSA [4]. Due to its capacity to offer the same level of security as RSA while utilizing smaller keys, the ECC has been demonstrated to have numerous advantages. Its lack of maturity, however, may even mask its beauty because mathematicians felt that not enough research had been done on ECDLP. Also, we believed that even though both systems are valid, the RSA is better than ECC for now, as it is more reliable because its security can be trusted more. However, the future of ECC looks brighter than that of RSA as today's applications (smart cards, pagers, and cellular telephones etc) cannot afford the overheads introduced by RSA.

5. A Secure Image Steganography based on RSA Algorithm and Hash-LSB Technique

In this paper we have proposed a new technique of image steganography i.e., Hash-LSB with RSA algorithm for providing more security to data as well as our data hiding method. The proposed technique uses a hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of the cover image. This technique makes sure, that the message has been encrypted before hiding it into a cover image. A secured Hash based LSB technique for image steganography has been implemented. An efficient a steganographic method for embedding secret messages into cover images without producing any major changes has been accomplished through Hash-LSB method.

6. Combination of Steganography andCryptography: A short Survey

In this paper, the major aim is to review several ways of combining steganographic and cryptographic techniques to achieve a hybrid system. Moreover, some of the differences between cryptographic and steganographic techniques were presented as well. They make a comparison study between the science of Cryptography and Steganography

7. A Study on Modified RSA Algorithm in Network Security

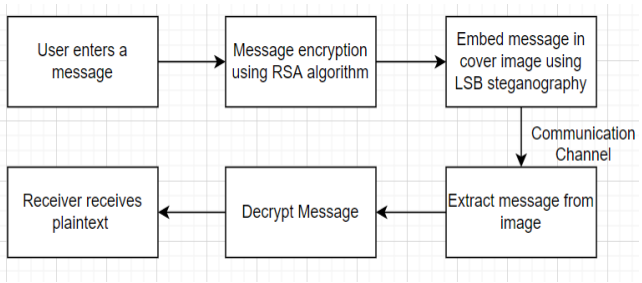
This research paper aims to endeavours modified method of RSA algorithm so the more secure RSA algorithm can be developed. In this research various modifications arepresented and compared to figure out new approaches of RSA cryptosystem, which try to improve the security and speed up the time of key generation encryption and decryption process. Researchers tried to performed a more secure RSA algorithm thus, the study of this paper figures out, that every day new approaches are developed which try to improve the security and speed up the time of key generation, encryption and decryption process.

8. A Review of Comparison Techniques of Image Steganography

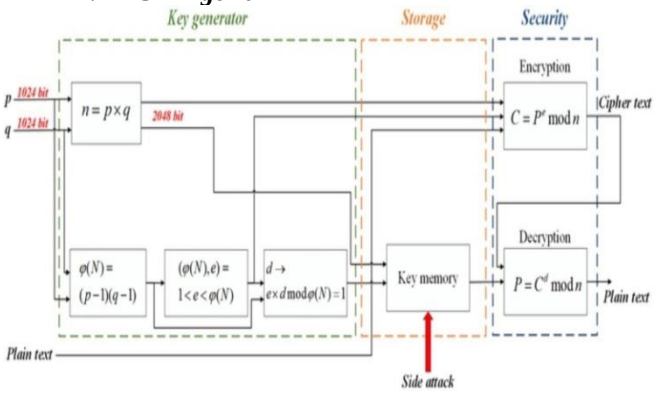
This paper deals with hiding text in an image file using Least Significant Bit (LSB) based Steganography, Discrete Cosine Transform (DCT) based Steganography and Discrete Wavelet Transform (DWT) based steganography. In this paper, analysis of LSB, DCT & DWT methods has been successfully implemented and results are delivered. The MSE and PSNR of the methods are also compared and also this paper presented a background discussion and implementation on the major algorithms of steganography deployed in digital imaging. The PSNR shows the quality ofimage after hiding the data.

IV. PROPOSED ARCHITECTURE

The basic structure of the algorithm is very simple. The user enters a text to send to the receiver, the text is then encrypted and embedded using LSB steganography in an image which is sent to the receiver and the embedded bits are decrypted to read the original message.



A. RSA Algorithm



- Generate the RSA modulus
- The initial procedure begins with selection of two prime numbers namely p and q, and then calculating their product N: N=p*q
- Consider number e as a derived number which should be greater than 1 and less than (p-1) and (q- 1). The primary condition will be that there should be no common factor of (p-1) and (q-1)except 1
- The specified pair of numbers **n** and **e** forms the RSA public key and it is made public.
- Private Key **d** is calculated from the numbers p, q and e. The mathematical relationship between the numbers is as follows –

  ed = 1 mod (p-1) (q-1)
- The above formula is the basic formula for ExtendedEuclidean Algorithm, which takes p and q as the input parameters.

For encryption

- Consider a sender who sends the plain text message to someone whose public key is **(n,e).** mC = Pe mod n

For decryption

- The decryption process is very straightforward and includes analytics for calculation in a systematic approach. Considering receiver **C** has the private key **d**, the result modulus will be calculated as −
  - Plaintext = Cd mod n

B. LSB Steganography

- Import all the required python libraries
- Define a function to convert any type of data into binary, we will use this to convert the secret data and pixel values to binary in the encoding and decoding phase.
- Write a function to hide secret message into the image by altering the LSB

- Define a function to decode the hidden message from the stego image
- Function that takes the input image name and secret message as input from user and callshideData() to encode the message
- Create a function to ask user to enter the name of the image that needs to be decoded and call the showData() function to return the decoded message.

V. RESULTS AND ANALYSIS

Receiver's side:

As you can see in the below image that the receiver side decrypted data is same as the data that we used in sender side normal text data. So here the image (stegimg.png) is used to store the encrypted data from the cover image.

```
Do you want to generate a new public and private key? (y or n) n
Would you like to encrypt or decrypt (e or d) d
What would you like to decrypt?

Enter image name (with extension): stegimg.png
Decrypting...
17271 761847
17271 761847
72101
121
Hey
```

Sender side:

```
Do you want to generate a new public and private key? (y or n) n
Would you like to encrypt or decrypt (e or d) e
What would you like to encrypt?
Hey
Enter the file name that stores the public key: public_keys.txt
Enter image name (with extension): mainimg.png
Enter the name of new image (with extension): stegimp.png
Max data encoded: 97864.66666666667
Encrypting...
Encrypted message is:  17271 761847
```

Cover Image 1 Stego Image 1

Cover Image 2 Stego Image 2

Cover Image 3 Stego Image 3

VI. CONCLUSION

From the aforementioned analysis, it can be observed that the combination of cryptography and steganography provides good and positive results. Imperceptibility is maintained while at the same time even if the data falls into the wrong hands, it is encrypted. Since in this project, only the RSA algorithm was used for encryption future work may include comparing the same implementation with different algorithms to find the most suitable one. Future work may also include creating a GUI web based or app-based application to allow users in the real world to communicate with each other safely and securely.

VII. REFERENCES

[1] Laskar, S. A., & Hemachandran, K. (2012). High Capacity data hiding using LSB Steganography and Encryption. International Journal of Database Management Systems, 4(6), 57.

[2] Walia, E., Jain, P., & Navdeep, N. (2010). An analysis of LSB & DCT based steganography. Global Journal of Computer Science and Technology.

[3] Nisha, S., & Farik, M. (2017). Rsa public key cryptography algorithm–a review. International journal of scientific & technology research, 6(7), 187-191.