IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

Design of Image Steganography using Asymmetric Key Cryptography

G. Divya Sri[1*], A. Ramani[2], A. Jhansi Priya[3], B. Santhi[4], SK. Wasim Akram[5]

[1,2,3,4]Dept. of CSE, Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India
[5]Dept.of CSE, Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India

Corresponding Author: divyasri0717@gmail.com, Tel.: 9393577477

DOI: https://doi.org/10.26438/ijcse/v7i3.1922 | Available online at: www.ijcseonline.org

Accepted: 07/Mar/2019, Published: 31/Mar/2019

***Abstract*—** Technological advancements and the usage of internet have been increasing very rapidly in the modern society from day to day. These advancements are leading to many security threats and security issues. There is a need to provide security to confidential information which has been a major concern from the past to the present times. In order to arrest all these security challenges a novel approach has been provided using Steganography and Cryptography through which data security and confidentiality can be ensured. Steganography deals about hiding the data within an image, audio or video file whereas Cryptography is all about transforming the data into unreadable format. In the proposed system the secret message is encrypted using RSA and Column Transposition technique. Later the encrypted message is embedded into the image using the LSB technique. Whenever the combination of Cryptography and Steganography have been used then the level of security has been increased rather than using the Steganography alone.

***Keywords*-----**Steganography, Cryptography, Encryption, Decryption, Public key, Private key

I. INTRODUCTION

Today's world is surrounded by computer and internet. Internet is widely used across the world for the purpose of communication. As the internet usage has been increasing rapidly, there is a need to provide the security. In order to achieve data security, mechanisms must arise in order to prevent the data thefts and threats.

Steganography is the art of hiding the secret message into the picture or image [1]. This hiding of the messages can be done by using three different techniques: 1) Here only pure steganography is performed which means there won't be any secret key.2) In this a secret key will be shared among the communicating parties before sending the stego image.3) Public key steganography is used where public key and private keys are used before embedding and after extracting the messages to and from the images [2].

Embedding the message into the picture will be done by using the LSB least significant technique [3]. By using this technique changes made to the bit positions of the pixels corresponding to the image cannot be easily detected by the human eye as only negligible changes are made.

Cryptography is important to ensure security [4]. Encryption algorithms are categorized into two types asymmetric and symmetric. In the symmetric key cryptography only one key will be used for both encryption as well as decryption where as in asymmetric key cryptography we will be using different keys for encryption and decryption [5]. As we are using different keys it is difficult to predict the keys and decode the message being sent to the receiver. The techniques used for encrypting and decrypting the messages are: RSA algorithm and Column transposition techniques. By using these two techniques the message will be converted into unreadable format.

Rest of the paper is organized as follows, section I contains the Introduction of Image Steganography, Section II contains related work of Image Steganography, Section III contains Methodology related to Image Steganography, Section IV contains results and discussions of Image Steganography, Section V concludes the research work with the future directions.

II. RELATED WORK

According to Brij Mohan Kumar [6], the message which is to be hidden within an image is encrypted using the senders private key and then upon receiving the message the receiver will be using the sender's public key in order to decrypt the message. When this approach is used then there is a chance to easily know the message being communicated because the public key is known by everyone and by using it anyone can easily decrypt it. An approach has been proposed where the data is being embedded at the edges [7]. The pixel values at the edges of the image are retrieved first. Then the pixel values will be randomized in some random fashion. After this starting from the first value the data will be embedded into each pixel value. There is a need to traverse through all

the pixel values because all the edges have to be retrieved before embedding the text into the image which takes a lot of time. Another approach followed for secure transmission of data which is transposition technique [8]. By using the transposition technique alone enough security cannot be provided because there is a chance that the encrypted message can be decoded. With the help of anagrams there is a possibility to decode the message.

III. METHODOLOGY

As there are number of steganographic and cryptographic methods available. In the proposed work message will be encrypted by using two techniques namely RSA algorithm and Column transposition techniques. First the transposition technique is used to provide first level of encryption and then another level of encryption is performed using RSA algorithm. Then a encipher is produced. This encipher is embedded into the image using the LSB technique in which the cipher text will be placed at the Least Significant positions of each pixel. The reverse process is done in order to get back the plain text from cipher text. Detailed discussion about the techniques which have been used over here are as follows:

Cryptography Techniques used:

1)RSA algorithm
2)Column transposition technique.
Steganography technique used:

1)LSB technique
Detailed discussion about the techniques used:

RSA algorithm:
The ***RSA algorithm*** is named after three persons namely Ron Rivest, Adi Shamir and Len Adleman which was developed in 1977 this is the most generally utilized open key cryptography calculation. With this algorithm there is no need to exchange a key separately or secretly.

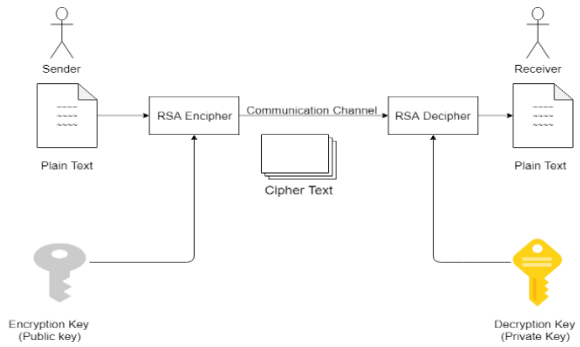

Figure 1: RSA algorithm

In this algorithm the message which is to be transmitted is first converted into non readable form so that it cannot be detected by any hacker. While encrypting the message the public key of the receiver is used and encrypted form of the message is produced. As we are using the public key of the receiver there is no need to share any key between the communicating parties as it is not necessary at all over here. The decryption to the message is done on the receiver side where the message is converted into its original form by using the private key of the receiver. Even the public key is known it is impossible to decode the message because the private key is confidential and is known only to the intended person. With this approach we can increase the confidentiality as well as security can be attained with this.

Column transposition technique:
This is one of the transposition techniques in which positions of the plain text are shifted according to some regular system so that cipher text can be formed by using different permutations. In the column transposition technique mixing up of the characters in the original message is done in order to form a cipher text which makes it difficult to decode the message. In the column transposition technique, the data will be written in rows and then the data is read into columns. These columns can also be chosen in any scrambled order without reading one after the other.

Depending upon the length of the text we can decide size of the matrix.

LSB technique:
LSB stands for Least Significant Positioning by which we can embed the data into the image in the LSB positions of each pixel. The number of bits to be changed in every pixel depends on the size of the message. Every pixel will be having a pixel number ranging from 0 to 255 and it can be represented in 8-bit format. The data will be inserted in last bits of every pixel with this even the values of the pixels are changes there will be only negligible changes which cannot be detected by human eye.

E.g.: Let us see how the Least Significant Positioning is done with an example.

8-bit pixel values (corresponding to image)

11101001 00110110 1001000 11001000
00110111 11001000 00100110 11001001 **……**

Text to be inserted in pixel representation (Let us take A for example and its value is 65)
01000001

Pixel values after performing the LSB Technique
11101000 00110111 10010000 11001000
00110110 11001000 00100110 11001001
In this way we will be embedding the required data in the LSB positions and while extracting the data we will be retrieving all those bits and decode the message by performing the reverse process.

IV. RESULTS AND DISCUSSION

This project can be developed using MATLAB. Over here it has been demonstrated in detail about how the keys are generated for RSA as well as working with the column transposition technique and RSA for encryption and decryption and also how has it been embedded into the secret image and how the extraction is done using LSB and original message is retrieved. Detailed discussion about how all this process will be done by combining the cryptography and steganography. Over here the input has been given and then the procedure has been observed. We can also observe how the cipher text has been generated from the original message and how RSA encryption and decryption has been performed and how the outputs have been generated. All this has been shown in detail over here:

```
Implementation of RSA Algorithm
-----------------------------------
The value of p: 11
The value of q: 13
-----------------------------------
Generated values :
The value of (N) is: 143
The public key (e) is: 7
The value of (Phi) is: 120
The private key (d)is: 103
-----------------------------------
Enter Message:
```

Figure 2: Taking input

Initially 2 prime numbers are given as input which generates N value, Public key(encryption), Phi value, Private key(decryption) and a prompt is displayed to enter the message to be sent.

```
-----------------------------------
Enter Message:hi
The message to be transmitted is : hi
-----------------------------------
column transposition technique : h-i-
ASCII Code after column transposition :
    104

     45

    105

     45

Cipher Text after RSA :
     91

    111

    118

    111

-----------------------------------
```

Figure 3: Generating cipher text

The message is given as input after which column transposition technique and RSA algorithm are applied to get the encrypted message.

Figure 4: After embedding in image

The ASCII values are embedded in the image. These are the images before and after steganography.

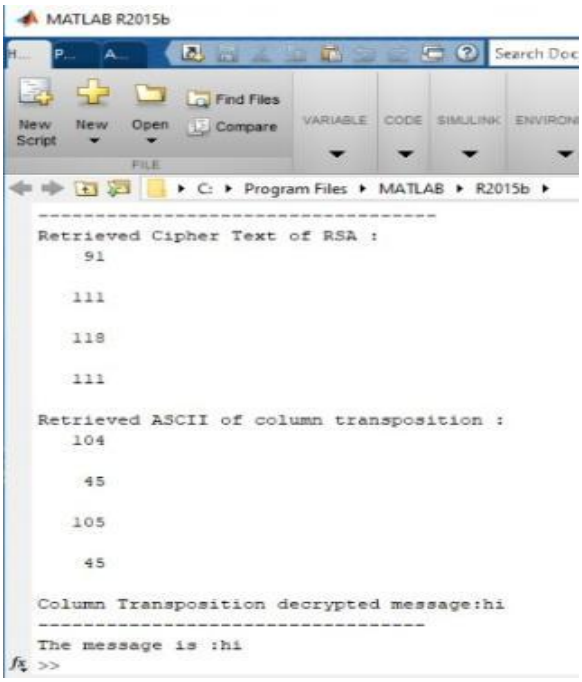

Figure 5: original message

The embedded data is extracted in the reverse order from the image and original message is displayed.

V. CONCLUSION AND FUTURE SCOPE

This paper proposed a new method where the security can be enhanced for the data being sent over the communication channel. A new approach for hiding the information has been provided here with less variations in image bits with LSB technique. By using the combination of RSA algorithm and Column transposition technique better security and

confidentiality has been provided to the data which is being transmitted between the sender and receiver. Moreover, without a key it is not possible either to encrypt or decrypt the message. The future work of the proposed work might be development of an android application where the users can be able to encrypt and decrypt the messages to and from the images by which a new way of communication can be established by sending the images to each other over email, WhatsApp etc.

REFERENCES

[1] Swati Nimje, Amruta Belkhede, Gaurav Chaudhari, Akanksha Pawar and Kunali Kharbikar,"Hiding Existence of Communication Using Image Steganography " in International Journal of Computer Science and Engine and Engineering(IJCSE), Volume-2, Issue-3 ,E-ISSN: 2347-2693.Mar-2014.

[2] Unik Lokhande, A.K.Gulve "Steganography using Cryptography and Pseudo Random Numbers" in an International Journal of Computer Applications (0975 – 8887) Volume 96– No.19, June 2014 .

[3] M. S. Sutaone,M.V. Khandare,"Image Based Steganography Using LSB Insertion Technique" in 2008 IET International Conference on Wireless, Mobile and Multimedia Networks.

[4] Arati Appaso Pujari,Sunita Sunil Shinde,"Data Security using Cryptography and Steganography" in IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. V (Jul.-Aug. 2016), PP 130-139.

[5] Pooja Rani, Mrs. Preeti Sharma,"Cryptography Using Image Steganography" in an International Journal of Computer Science and Mobile Computing, Vol.5 Issue.7, July- 2016, pg. 451-456.

[6] Miftah Ul Uroos, Sukhvinder Kaur ,Muheet Ahmed Butt , "Steganography: A Comparative Survey Conducted on Digital Images" in IOSR Journal of Engineering (IOSRJEN) ISSN (e): 2250-3021, ISSN (p): 2278-8719 Vol. 08, Issue 10 (October. 2018), ||V (I) || PP 52-61 .

[7] Sneha Arora, Sanyam Anand "A Proposed Method for Image Steganography using Edge Detection" in an International Journal of Engineering Sciences, Issue June 2013, Vol. 8.

[8] Shamim Ahmed Laskar, Kattamanchi Hemachandran ,"High Capacity data hiding using LSB Steganography and Encryption" in an International Journal of Database Management Systems(IJDMS) Vol.4, No.6, December 2012.

