# SECURE DATA ENCRYPTION AND DECRYPTION USING CRYPTO-STEGO

[1]Matcha Venkatesh, [2]T.Anitha, [3]G.Satish, [4] M.Sudarshan, [5]K.Ram Sudeep
[1]Student, [2]Assistant Professor, [3,4,5]Student
[1]Department of Computer Science & Engineering,
[1]Anil Neerukonda Institute Of Technology And Sciences, Visakhapatnam, India

***Abstract :*** Securing data encryption and decryption using Cryptography and Steganography techniques. This paper introduces a new kind of approach for covert communications between two private parties. The approach introduced in this paper makes use of both steganographic as well as cryptographic techniques. In Cryptography we are using Rivest-Shamir-Adleman (RSA). In Steganography we are using Image Steganography for hiding the data. And we also use Mutual Authentication process to satisfy all services in Cryptography i.e., Access Control, Confidentiality, Integrity, Authentication. In this way we can maintain the data more securely. We are using RSA for encryption of data and Steganography concept to hide the data in an image. Such that any other person in the network cannot access the data. Only the sender and receiver can retrieve the message from the data.

***Index Terms :*** **Rivest-Shamir-Adleman(RSA), Cryptography, Steganography.**

## 1. INTRODUCTION

Digital communication witnesses a clear and continuous development in many applications within the Internet. Hence, secure communication sessions must be provided. The security of data that is transmitted across a world wide network has become a key factor on the network performance measures. So, the confidentiality and integrity of transmitted data are needed to stop from accessing and using transmitted data. Steganography and Cryptography are 2 techniques that are provided for network security. The aim of this paper is to develop an approachto cover secret data in an image, by taking advantage of combination of cryptography and steganography.

### Cryptography

Cryptography is one of the secure method used to guarantee the privacy of communication between parties. This method is used for secret writing, which is used to encrypt the plaintext with a key into ciphertext to be transferred between parties on an insecure channel. Using a valid key, the ciphertext are often decrypted to the given plaintext. Cryptography provides a secure communication across an insecure channel, like: confidentiality, privacy, non-repudiation, key exchange, and authentication. There are two kinds of Cryptography techniques :

i) Symmetric / Secret Key Cryptography
ii) Asymmetric / Public Key Cryptography

### Symmetric / Secret Key Cryptography

The other name for Secret key encryption is symmetric-key, shared key, single-key, and eventually private-key encryption. By using the key we can encrypt the given plain text, similary by using the same key at receiver side we can decrypt the message to obtain the plaintext. The key will be known only by a people who are authorized to the encryption or decryption.

### Asymmetric / Public Key Cryptography

We can call this technique as asymmetric cryptography or public key cryptography, here we use two keys which are mathematically associated, used separately for encrypting and decrypting the information. In this technique, when we use the private key, there are no possibilities to obtain the data or simply discover the other key. The key used for encryption is public key, and the decryption key is private key.

### Steganography

It can be defined as the science of concealment and communicating data through apparently reliable carriers in attempt to hide the existence of the data. So, there is no knowledge of the existence of the message in the cover image. If an individual views the given cover which the information is hidden inside of he or she will have no clue that there is any covering data. The proposed model is a combinational of Rivest-Shamir-Adelman(RSA) and Image Steganography.

## 2. RELATED WORK

### 2.1 Rivest-Shamir-Adelman

Rivest-Shamir-Adelman(RSA) is an approach to public-keyCryptogrophy.

#### 2.1.1 Different Operations on RSA

Let P and Q be the two prime numbers. The operations are "e" and "d". Product of P and Q is considered as "n". Product of (P-1) and (Q-1) is considered as $\phi(n)$.

##### 2.1.1.1 Public Exponent

let "e " be the public Exponent, it can be calculated using GCD between e and $\phi(n)$ , e values varies from 1 to n. If Gcd of e and $\phi(n)$ is "1" then that value can be considered as "e".

##### 2.1.1.2 Secret Exponent

let "d" be the secret exponent and ed mod $\phi(n) = 1$. The Extended Euclidean is based on the formula $\gcd(e, \phi(n)) = 1$, where d should be equal to $s + \phi(n)$ in order to satisfy the ed mod $\phi(n) = 1$ condition.

#### 2.1.2 RSA algorithm

**a) Key Generation**

Inputs : 2 Prime Numbers p and q.

1. Select p and q such that both are the prime numbers, $p \neq q$.
2. Calculate n=p*q,
   (n) -> Euler's totient function
3. Calculate q(n) = (p-1)*(q-1)
4. Select an integer e such that gcd ( q(n), e)) =1 & 1< e < (n)
5. Calculate d; d= e-1 mod (n)
6. Public Key, PU= {e, n}
7. Private Key, PR ={d,n}

**b) Encryption**

Input : PlainText

1. Let the Plaintext be : "M".
2. Ciphertext be : "C".

C = M^e mod n, Where 1 < M > n.

**c) Decryption**

Input : CipherText

1. Ciphertext: C
2. Plaintext : M= C^d mod n

### 2.2 Steganography

It can be defined as the science of concealment and communicating data through apparently reliable carriers in attempt to hide the existence of the data. A secret message are often plaintext, an image, ciphertext, or anything which can be represented in form of a bitstream. After the secret data is embedded in the cover object, the cover object will be called as a stego object and the stego object sends to the receiver by selecting the suitable channel, where decoder system is used with the same stego method for obtaining original information as the sender would like to transfer .We are having 4 kinds of steganography , Text steganography, Image steganography, Video steganography, Audio steganography. In this paper we are using Image steganography.

**Encryption Algorithm**

Inputs: Image,Data,Key

1. Intially consider an Image
2. And consider Data and a Key.
3. Now hide the data in the given image by using the secret key.
4. Now send the Stego-Image to the Receiver.

**Decryption Algorithm**

Inputs : Stego-Image, Key

1. Consider the input be Stego-Image.
2. Using the Secrert Key ,Obtain the hidden message from the Stego-Image.

## 3. METHODOLOGY

In proposed model RSA , the inputs are two prime numbers P and Q , and a plain text. For Steganogtraphy the inputs are text, key and image.

### 3.1 Encryption

Inputs : Message, Prime Numbers, Image, Secret Key

1. Consider an Input , It can be :
   a) Text
   b) Image
   d) AudioVideo
2. Convert the input to Base-64 using Base-64 conversion Algorithm.
3. After converting into Base-64 we will be getting a String.
4. Store the entire string in a Text File and save the file.
5. From that file consider each character and apply Rivest Shamir Adelman(RSA).
6. For RSA we must generate two different prime numbers. Using that prime numbers, Calculate Eulers Toient and q(n).
7. Select integer e such that gcd ( q(n), e)) =1 & 1< e < (n), Where e is called as Public Exponent.
8. Now sender “A” will Encrypt the message using the Public Exponent.
9. Let the encrypted message be Cipher Text (cm).
10. Consider an image, And hide the encrypted message(cm) in the given image with the secret key Using Stegnography Algorithm.
11. And the secret key will be considerd from RSA algorithm.
12. Now send the Stegno-Image to the Receiver.

### 3.2 Decryption

INPUT : Stego-Image, key

1. Consider the input be Stego-Image.
2. Using the Secrert Key , Obtain the hidden message from the Stego-Image.
3. The Secret Key can be obtained using the RSA Algorithm.
4. And the obtained message is a Cipher Text. We must decrypt the message.
5. The Decyption of the message can be done using RSA Algorithm.
6. For Decryption the receiver will use the Secret Exponent.
7. And thus the receiver will decrypt the message and it is in the form of Base-64

Finally by using Base-64 algorithm the Base-64 text is converted into the original input, Which can be Text, Image, Audio, Video.

## 4. EXPERIMENT RESULTS

The above stated hybrid method was applied to the data such as image, video, audio as shown in figure(4). The cover image used for this process is shown in figure(3). Total process of entire method is shown in figure(5).

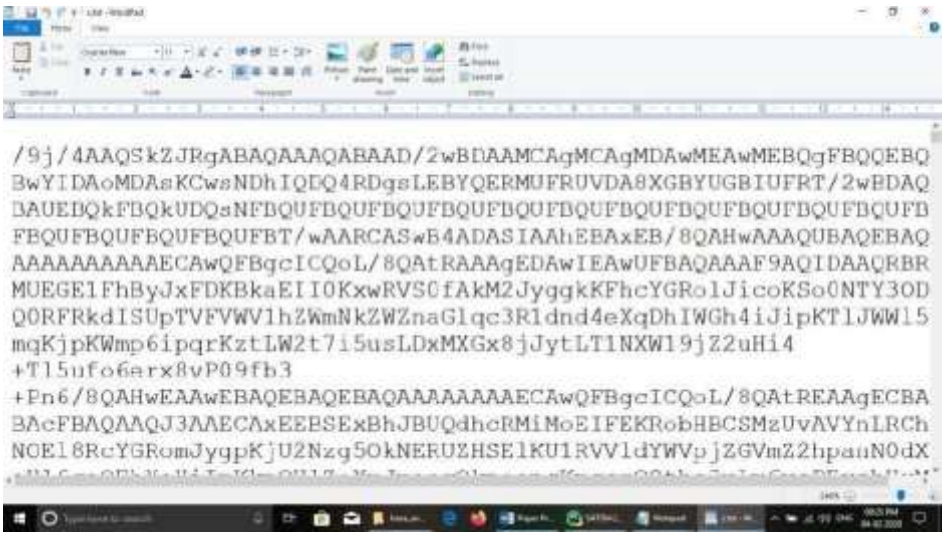


**Figure 1 : Image Encryption**


**Figure 2 : Rsa Encryption**

Figure 3 : Cover Image

Figure 4 : Encryption Data

Figure 5 : Stego_Object

## 5.FUTURE SCOPE AND CONCLUSION

In this project, we deal with the concepts of security of digital data communication across the network. This project is designed by using the steganography and cryptography features factors for better performance. We performed a new steganography method and combined it with RSA Encrption algorithm. We performed our method on image by implementing a program written in Python language. The method proposed has proved successful in hiding various types of text, images, audio and videos in colour images. We concluded that in our method the Image files and RSA Cryptography are better . Because of their high capacity. Results achieved indicate that our proposed method is encouraging in terms of security and robustness.

## 6. REFERENCES

[1] H.Abdulzahra, R. AHMAD, and N. M. NOOR, "Security enhancement; Combining cryptograhy and steganography for data hiding in images," ACACOS, Applied Computational Science,pp.978-960,2014.

[2] P. R. Ekatpure and R. N.Benkar, "A comparative study of steganography & cryptography,"2013.

[3] M. H. Rajyaguru, "Cryptography-combination of cryptography and steganography with rapidly changing keys ,"Interntional Journal of Emerging Technology and Advanced Engineering,ISSN ,pp.2250-2459,2012.

[4] D. Seth. L. Ramanathan, and A.Pandey, "Security enhancement; Combining cryptography and steganography," International Journal of Computer Applications(0975-8887)Volume,2010.

[5] J. V. Karthik and B. V. Reddy, "Authentication of secret information in image steganography," International Journal of Computer Science and Network Security(IJCSNS), vol. 14, no. 6. P. 58. 2014.