REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES BY RESERVING ROOM BEFORE ENCRYTPION

Sonia Bhandi[#1], Amritdas Vaishnav[#2], Kamesh Phegade[#3,] Prof. S.P. Joshi[#4]

[#]*Information Technology Department, Mumbai University*
Mumbai, Maharashtra, India

soniabhandi@gmail.com

vaishnavamrit1@gmail.com

kameshcr7@gmail.com

spjoshi@acpce.ac.in

[*]*A.C. Patil College of Engineering*
Navi Mumbai, Maharashtra, India

Abstract*— Security of tip has always been a serious issue from the hobbies to this time. It has always been the interested topic for researchers to develop secure techniques to send data without revealing it to anyone apart from the receiver. Therefore from time to time researchers have developed many techniques to satisfy secure transfer of knowledge and cryptography with steganography is one among them. The system proposed during this study uses a canopy object, image specifically to cover the message to be sent. Before a message is embedded within the image, the message is first encrypted using RSA encryption algorithm. After the message has been encrypted, the method of embedding or hiding the message within the image is carried on. Least Significant Bit (LSB) technique is used to embed the message into the image. If in any case the cipher text got revealed from the duvet image, the intermediate person apart from receiver can't access the message because it's in encrypted form. The results show that high security and robustness is achieved when cryptography is combined with steganography.

I. INTRODUCTION

The basic need of each growing area in today's world is communication. Everyone wants to stay the within information of labor to be secret and safe. We use many insecure pathways in our lifestyle for transferring and sharing information using internet or telephonically, but at a particular level it isn't safe. Steganography and Cryptography are two methods which could be implemented together to share information during a concealed manner. Cryptography includes modification of a message during a way which might be in digesting or encrypted form guarded by an encryption key which is understood by sender and receiver only and without using decryption key the message couldn't be accessed or decrypted back to normal form. But in cryptography it's always clear to intermediate person that the following message is in encrypted form, whereas in steganography the message is hidden in cover image so that it couldn't be clearer to any intermediate person that whether there's any message hidden within the information being shared. The cover image containing the key message is process and secret key provided by the sender. This study is however designed to figure in image steganography using RSA algorithm and LSB insertion for android based smartphones.

II. LITERATURE REVIEW

[1] Y. J Chanu, T. Tuithung, and K. M Singh proposed system based on steganalysis. In this system all strong and weak points are mentioned very clearly and by analyzing steganalysis techniques a better steganography techniques can be developed. The main disadvantage of the system is that it is not able to detect the secret message.

[2] S. Manoharan proposed system based on LSB, RS analysis and low colour images. The method is Effective in all cases such as random embedding with LSB replacement and random embedding for sequential for LSB matching. However this

Technique only applies to synthetic images with a small number of distinct colours such as logos and flags and it is not effective for big sizes images.

[3] J. K. Mandal, and S. Ghatak proposed system based on LSB, Visual Cryptography and Visual Steganography. The main drawback of this system is that it degrades the quality of the image during embedding.

III. Proposed System

The complete process of the model consists of six main steps. The first step as demonstrated by the model is the generation of public and private keys for encryption. The second step is the encryption step, which involves employing standard encryption algorithm, in this case, RSA algorithm to encrypt the text into binary data. In the third step, the appropriate frame is selected and the process of embedding is carried out using LSB insertion to hide the text in the image as the fourth step. In the fifth step, the encrypted text is extracted from the hidden frame and the seventh step applies the process of decryption using the private key to obtain the original text. Figure 1 depicts the proposed model.

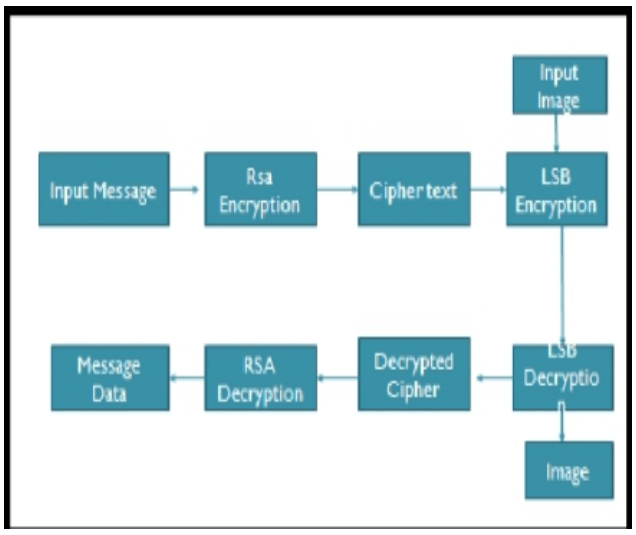


Fig.1. *Proposed Model*

IV. Implementation

Working of the system

The working of the system consists of two parts:
a. Encryption part: Hiding encrypted data within the given image.
b. Decryption part: Image retrieval with decryption of hidden data.

I. Steps and methods involved in Encryption part:

Embedding Algorithm:
Step 1: Choose a public key from generated list of keys for encoding .
Step 2: Enter the secret message & choose the duvet image.
Step 3: Encrypt the message using RSA algorithm.
Step 4: Find least significant bits of each RGB pixels from the duvet image.
Step 5: Embed the encrypted message into least significant bits(LSB) of RGB pixels of cover image.
Step 6: Text message is successfully hidden within the duvet image.

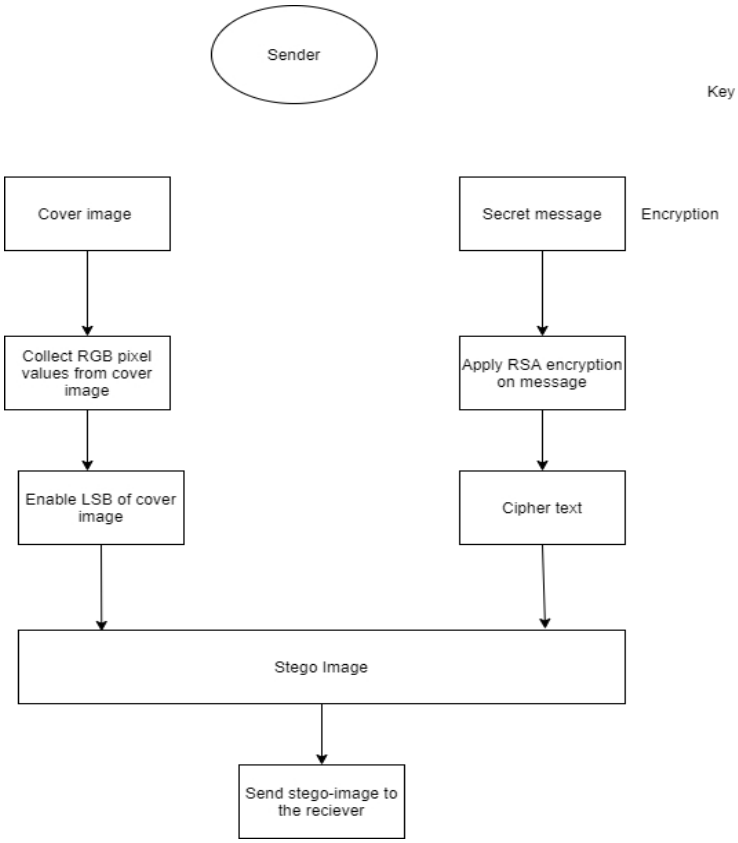


Fig.2. *Embedding part at sender side*

A. LSB Algorithm for image

LSB stands for Least Significant Bit. There are basically two methods for concealing messages inside an image: Least Significant Bits(LSB) and Discrete Cosine Transform(DCT). LSB method belongs to the spatial domain whereas the DCT method falls within the category of the frequency domain. the only and simplest way to implement in image steganography is LSB. In LSB, there's the encoding of the info to be hidden since the individual pixels of the least significant bits of the image are modified. Using a picture of 8bit, the least Significant Bit, thus the last bit is that the 8th number little bit of each byte of the carrier image becomes the bit which is taken into account because the secreted message. for twenty-four bit image, the colours of the each component like the Red, Green, and Blue (RGB) are changed.

For example: Assuming cover images has two-pixel values as (1010 0000 0010 0011 0100 0111) and (0101 1111 0011 1100 0111 1100).Let‘s also assume the key bits are 1101112, immediately the key bits are embedded, the pixel values also change. That pixel values are: (1010 0001 0010 0011 0100 0110) and (0101 1111 0011 1101 0111 1100). The underlined bits indicate the bits changed from the initial value and only three bits within the carrier image get changed.

B. RSA Algorithm for data encrytpion

RSA stands for Rivest–Shamir–Adleman, is an algorithm used by modern computers for encryption and decryption of file/text. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called as public key cryptography, because one of the keys can be given to anyone while the other key must be kept private. The 2 keys generated through this algorithm are called public key and private key. the public key is given to the sender of the info for encrypting the info using the subsequent public key while the private key is given to the receiver of the info for decrypting the encrypted data received from the sender.

The steps for generation of public and private keys in RSA are as follows:

1.Pick two large prime numbers p and q, such that p isn't equal to q;
2. Calculate n = p*q;
3. Calculate phi(n) = (p-1) (q-1);
4. Pick e, in order that gcd(e, phi(n)) = 1, 1 < e < phi(n);
5. Calculate d, in order that d*e mod phi(n) = 1, i.e. d is that the reciprocal of e in mod phi(n);
6 .Get public key as Ke= {e, n};
7. Get private key as Kd= {d, n};

II. Steps and methods involved in Decryption part.

Retrieval Algorithm:

Step 1: Choose the image obtained from the encryption part.
Step 2: Find LSB bits of each RGB pixels from the image.
Step 3: Retrieve the bits from the LSB of the image.
Step 4: Apply RSA algorithm to decrypt the retrieved data.
Step 5: Finally read the secret message and recover the original image.

C. LSB Decoding and RSA Decryption

In the decoding process we detect the positions of the LSB’s where the info bits had been embedded. When the position of the bits had been specified, the bits are then extracted from the position within the same order as they were embedded. At the top of this process we'll get the message in binary form which again converted into decimal form, and with same process we got the cipher text message. After retrieving the positions of LSB pixels that contain the secret message, the receiver will decrypt the secret message obtained, by using RSA algorithm. To apply RSA algorithm receiver will use his/her private key because the key data are encrypted by recipient public key. Using receiver private key

cipher text are going to be converted into original message which is in readable form.

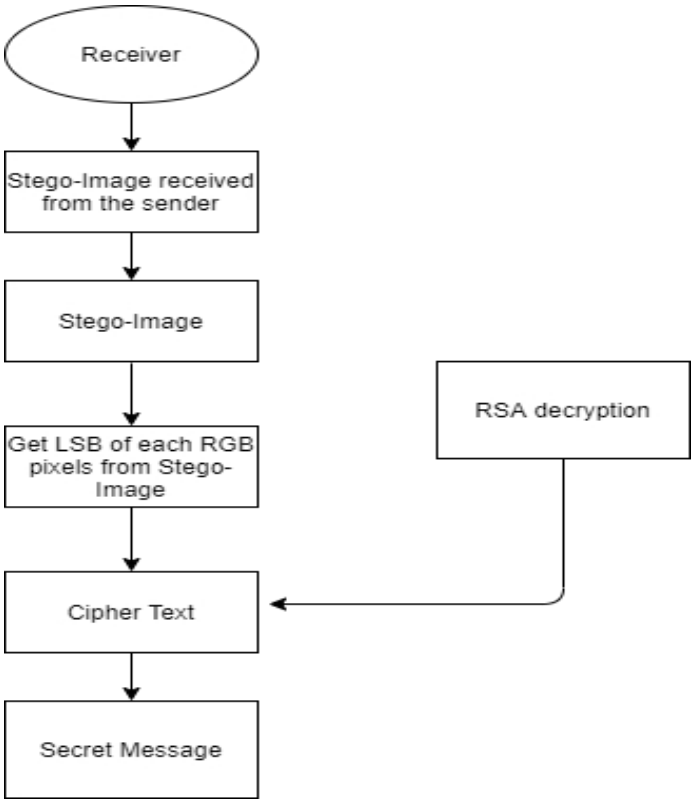


Fig 3. *Retreival part at receivers side*

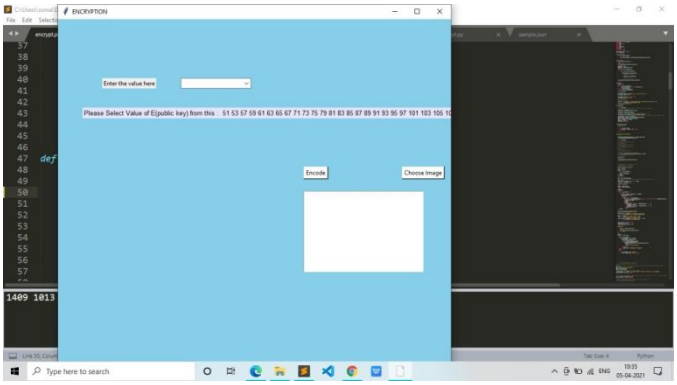
IV RESULT

A. ENCRYPTION PART

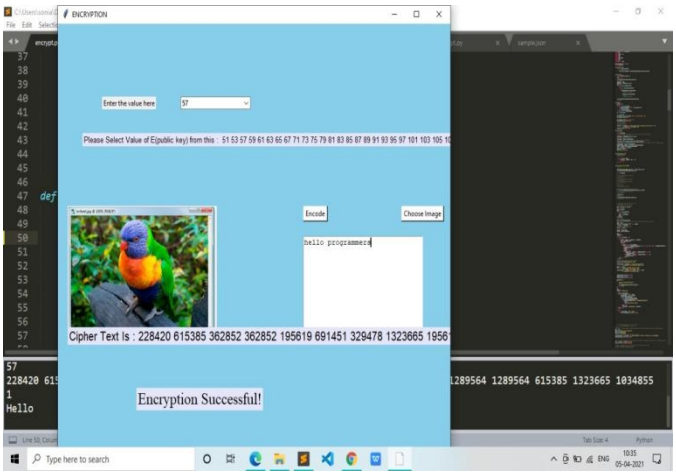
1. After opening GUI, user will be prompted with a list of public key(e).

2. The list of ‘e’ is generated by using any two large prime numbers(p & q) and through which phi(n) is obtained by applying standard RSA algorithm.

3. User will now select any value of ‘e’ from the list. The range of ‘e’ is set from 50-200 for ease of user and fast program processing. Larger the size of key more the time it takes to completes the given process.



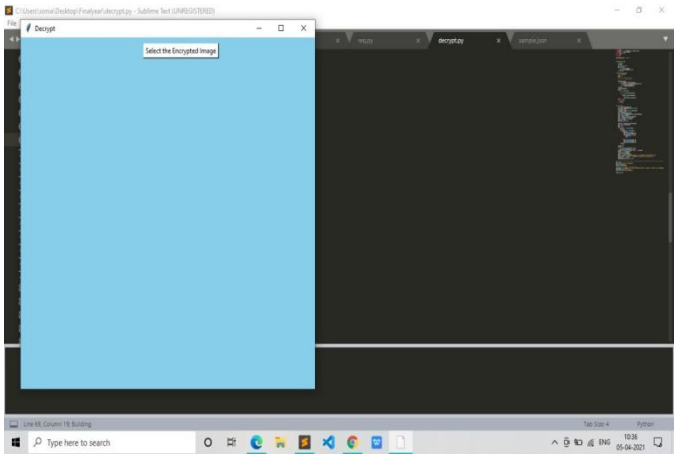
1. After selection of ‘e’, now choose a cover image by clicking on “choose image” button & also enter the text message in the given text box for hiding in cover image.
2. Click “Encode” button and text is encrypted by using public key and is hide inside LSB bits of image successfully.
3. A message is displayed “Encryption successful” after finishing the encryption part and the final image with hidden data is ready, known as “Stego image”



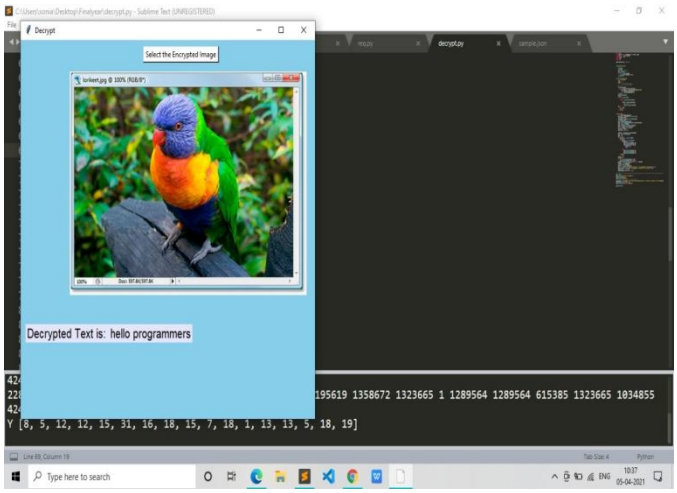
`

B. DECRYPTION PART

1. At decryption part user will be prompted to select the image for decryption.
2. User will select the image obtained from the previous encryption part. In this example it is saved as “encrypted_image.png”



1. After selection of image, encrypted data is retrieved from the image by selecting the LSB bits of image.
2. The encrypted data is now decrypted using private key(d), which is generated at the time of public key.
3. The data is now decrypted in user readable format and displayed on the GUI, and the image is also recovered without any change.



IV. Conclusion

A secured GUI software using Cryptographic(RSA) and Steganographic method has been implemented. RSA cryptography method is used for data encryption in order to provide more security to data from attacks, And an efficient steganographic method for embedding secret messages into cover images without producing any major changes has been accomplished through LSB method.There is less chance for degradation of the original image. More information can be stored in an image.

Acknowledgment

Me and my group members would like to express our special thanks for gratitude to our guide Mrs. S.P. Joshi for their guidance and their assistance in completing our project. They always helped us by showing us the right path for the project and clearing our doubts whenever approached by us at the various stages of the project.

References

[1] Mirza Abdur Razzaq., and Mirza Adnan Baig., 2017, “Digital Image Security: Fusion of Encryption, Steganography and Watermarking”, IJACSA, Vol 8, No. 5, pp. 224-228.

[2] Markandey, A., Moghe, S., 2014, “An Image Encryption Mechanism for Data Security in Clouds”, 2014 IEEE GHTC – SAS, pp. 227-231.

[3] Somaya AI-Maadeed, Afnan Al-Ali., and Turki Abdalla, 2012, “A New Chaos-Based ImageEncryption and Compression Algorithm”, Journal of Electrical and Computer Engineering, Vol 2012, pp.
.

[4] Helei Cui., Xingliang., and et al., 2017, “Harnessing Encrypted Data in Cloud for Secure and Efficient Mobile Image Sharing”, IEEE Transaction on mobile computing, Vol. 16, No. 5, pp. 1315 – 1329.