ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 4, April 2016

Data Security Analysis using Image and Cryptography

Aditi Sengupta, Nabamita Debnath, Ritika Gupta

***Abstract*— It is necessary to maintain secrecy of information in various circumstances like sending confidential text files or passwords. This is when cryptography and steganography techniques are needed. The aim of this paper is to analyze how unwanted people can be prevented from accessing secret information using RSA algorithm, steganography and visual cryptography. In this paper, a secure communication is obtained which shows that Image Hiding is much more secure than Data Hiding.**

***Index Terms*— Data security, RSA, Steganography, Visual cryptography.**

I. INTRODUCTION

Steganography means hiding information in other information and using images as cover makes it difficult to access the hidden information as innumerable images are available in the internet.

Cryptography is the science and art of processing message in such a way that makes them immune from attacks and secures them by converting it into an unreadable format called cipher text. [1]

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading. It basically involves creation of shares & overlapping them to get original message.

In this paper we basically apply the layers of security (RSA encryption **[1]**, steganography & visual cryptography) in different sequence and analyze the image characteristics and resultant PSNR & MSE. We first performed simple preliminary information hiding by means of steganography and analyzed the MSE, PSNR & histogram of resultant output with input. We hide plain text without any encryption in image by means of steganography using LSB substitution technique.

Next we considered two case :(I) Image steganography followed by Visual Cryptography on image (i-2).**[3]** (II)Visual Cryptography on image(i-1) followed by Image steganography.

CASE 1:

(a) In first case we encrypted the message into cipher text using RSA and stored the private key. Next we hide the cipher text in a Cover Image 1 by means of steganography using LSB substitution **[2]** which gives resultant image(i-1).We again hide this image(i-1) in another Cover Image 2 using image LSB substitution steganography technique & gives the resultant image (i-2) which has image(i-1) hidden in it. Now we perform visual cryptography on image(i-2) and create 2 shares of image(i-2) which is then finally transmitted.**(See Fig-1(a))**

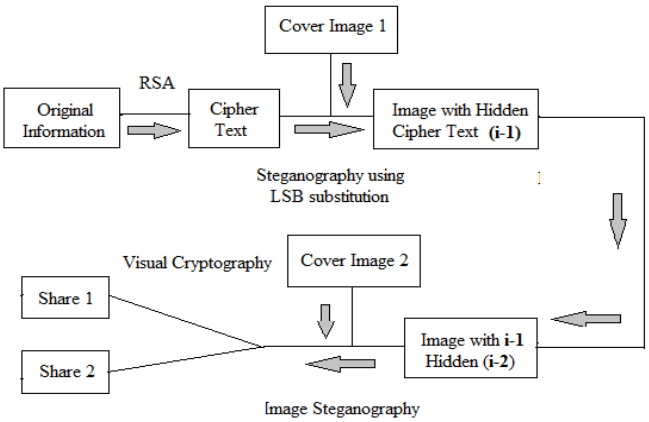

FIG-1(a)

(b) At receiver end for retrieving the original message, the 2 received shares are overlapped to reconstruct the image (i-2).Then extracting the image (i-1) using reverse algorithm of image steganography. Now from image (i-1) cipher text is extracted and

***Aditi Sengupta**, Assistant Professor in Electronics & Communication Engineering, Dr. Sudhir Chandra Sur Degree Engineering College Kolkata, India, 9126301101.*

***Nabamita Debnath**, B.Tech student in Electronics & Communication Engineering, Dr. Sudhir Chandra Sur Degree Engineering College, Kolkata, India, 9073064360*

***Ritika Gupta**, B.Tech student in Electronics & Communication Engineering, Dr. Sudhir Chandra Sur Degree Engineering College, Kolkata, India, 9088884707.*

finally RSA decryption performed to retrieve original message. **(See Fig-1(b))**

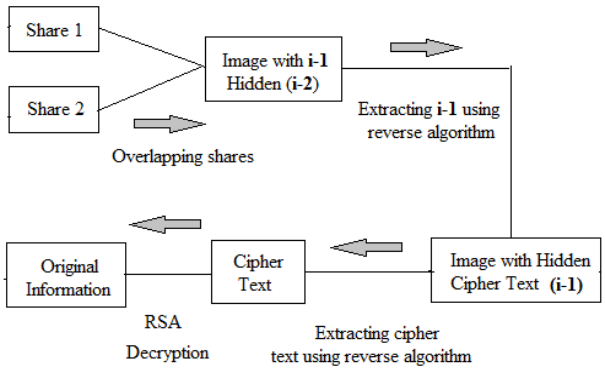

FIG-1(b)

CASE 2:

(a) In the second case same process is repeated. We encrypted the message into cipher text using RSA and stored the private key. Next we hide the cipher text in a Cover Image 1 by means of steganography using LSB substitution which gives resultant image (i-1).Now we perform visual cryptography on image (i-1) and create 2 shares. These 2 shares are hidden in Cover Image 2 by using same LSB substitution steganographic technique. The resultant image (i-3) has shares hidden in it which is transmitted. **(See Fig-2(a))**

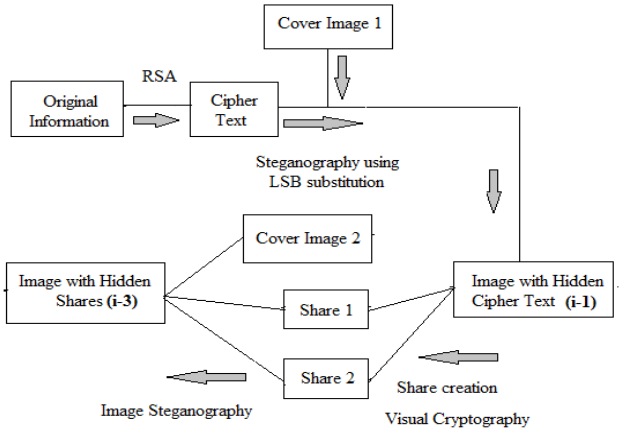

FIG-2(a)

(b) At receiver end the from the image (i-3) the two shares are extracted using reverse algorithm of steganography. These two shares are then overlapped to reconstruct the image(i-1) with hidden cipher text. The cipher text is decrypted using RSA decryption algorithm and original message is finally retrieved. **(See Fig-2(b))**

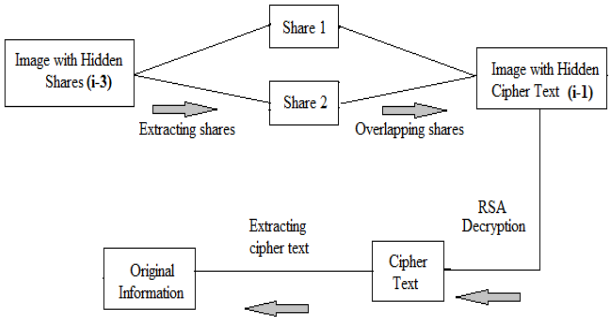

FIG-2(b)

II. ALGORITHMS

1) Hiding Cipher Text in Cover Image 1:

a] Embedding Process:

Step1: Use RSA algorithm to convert original text into cipher text.
Step2: Read cover image.
Step3: Find dimensions of the image.
Step4: Find size of the cipher text.
Step5: Compare the size of text with the size of the cover.

i) If size(text) > size(cover)
Abort.
ii) Else continue.

Step6: For each character in the text, find its ASCII value.
Step7: The red, green and blue pixel values are modified with the ASCII values such that only the least significant bits are modified.
Step8: Store the text and image size information in the cover.
Step9: Write the modified image into a new file.

b] Extraction Process:

Step1: Read the modified image file.
Step2: Calculate its size.
Step3: Retrieve the text and image size information.
Step4: Apply reverse algorithm to calculate ASCII values of text characters from the modified pixel values.
Step5: Find the cipher text from the ASCII values.
Step6: Decrypt cipher text to get the secret information.

2) Hiding modified image files in Cover Image 2:

a] Embedding Process:

Step1: Read the cover image and images to be hidden.
Step2: Find size of each image.
Step3: Compare total size of images to be hidden with that of the size of cover.
i) If size(Images to be hidden)> size(cover)
Abort.
ii) Else continue.

Step4: Store information about the number of images to be hidden and their size.
Step5: Take each image to be hidden separately and store in the same row matrix.
Step6: Use each element of the row matrix to modify the matrix of the cover image.
Step7: Reshape the modified matrix to get back the original dimensions.
Step8: Write the modified image in a separate file.

b] Extraction Process:

Step1: Read the embedded image file.
Step2: Retrieve information regarding the number of hidden images and their sizes.
Step3: In accordance with the retrieved dimensions, extract the hidden images using reverse algorithm.

3) Performing Visual Cryptography**[4]** :

a] Creation of Shares:

Step1: Read the input image .Store its size in i & j.
Step2: Choose number of shares you want to create in N. (In this paper we have created 2 shares). Select the range of random nos. 1:N accordingly.
Step3: Make a matrix [R] with same dimension as input image matrix and fill it with random numbers 1:N.
Step4: Create shares by equating each single number in R[i,j] matrix with image matrix and storing those image pixel values in new share matrices S for each bit plane. Repeat this step till as many shares as you chose in N is created .
Step5: Write each created share.

b] Overlapping of Shares:

Step1: Read each shares from the file.
Step2: And overlap the shares one upon another using image addition.
Step3: Write the overlapped output image.

III. RESULTS

Without RSA Plaintext Encryption:

i) MSE(:,:,1) = 0.001821
ii) PSNR(:,:,1) = 75.538853 dB

iii) MSE(:,:,2) = 0.001216
iv) PSNR(:,:,2) =77.452001 dB

v) MSE(:,:,3) = 2.5586e-004
vi) PSNR(:,:,3) =84.084803 dB

With RSA encryption:

i) MSE(:,:,1) = 0.009038
ii) PSNR(:,:,1) = 68.604154 dB

iii) MSE(:,:,2) = 0.001950
iv) PSNR(:,:,2) = 75.265457 dB

v) MSE(:,:,3) = 0.000584
vi) PSNR(:,:,3) = 80.502279 dB

Hiding i-1 into Cover Image 2:

i) MSE(:,:,1) = 0.090747
ii) PSNR(:,:,1) = 58.586461 dB

iii) MSE(:,:,2) = 0.162023
iv) PSNR(:,:,2) = 56.069036 dB

v) MSE(:,:,3) = 0.163947
vi) PSNR(:,:,3) = 56.017754 dB

Hiding share1 and share2 into Cover Image 2:

i) MSE(:,:,1) = 0.128917
ii) PSNR(:,:,1) = 57.061708 dB

iii) MSE(:,:,2) = 0.128369
iv) PSNR(:,:,2) = 57.080197 dB

v) MSE(:,:,3) = 0.159761
vi) PSNR(:,:,3) = 56.130101 dB

Creating Shares of i-2 and Overlapping:

i)MSE(:,:,1) = 0
ii) PSNR(:,:,1) = Inf

iii) MSE(:,:,2) = 0
iv) PSNR(:,:,2) = Inf

v) MSE(:,:,3) = 0
vi) PSNR(:,:,3) = Inf

ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 4, April 2016

Histograms

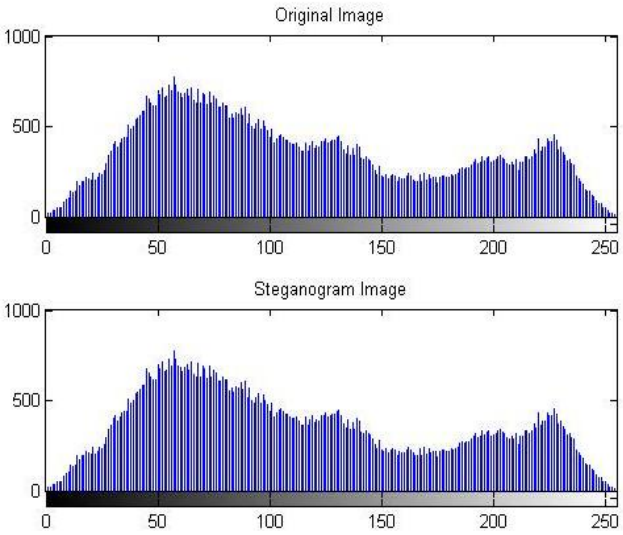

Fig-1: Without RSA encryption Steganography Histogram (grayscale)

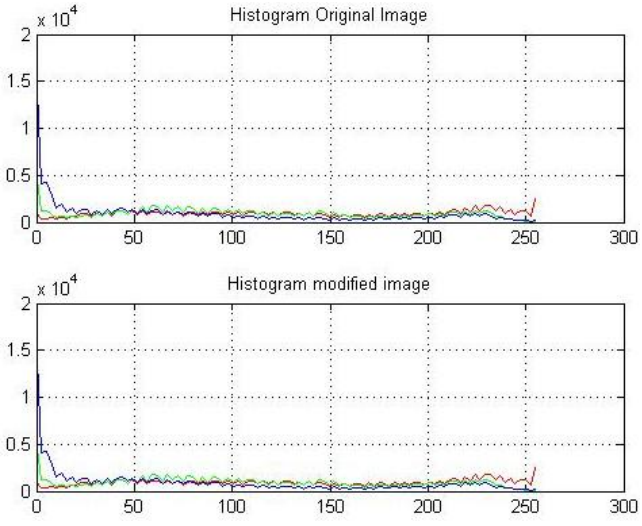

Fig-2: Without RSA encryption Steganography Histogram (RGB)

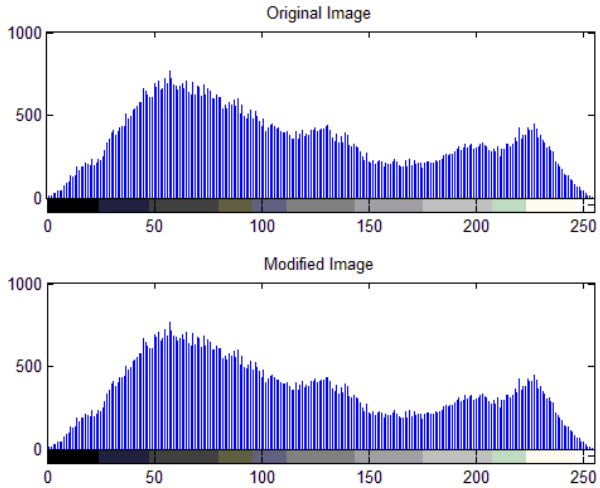

Fig-3: With RSA encryption Steganography Histogram (Grayscale)

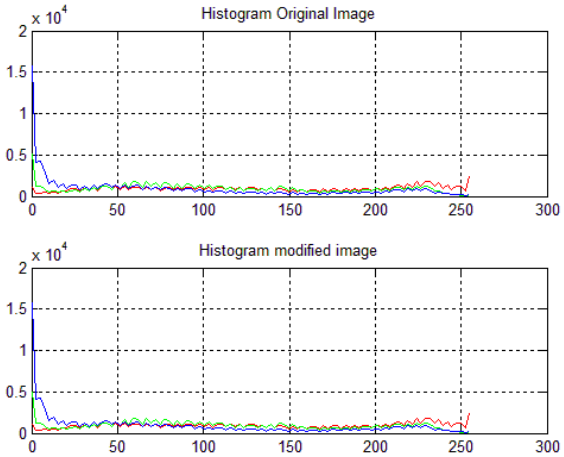

Fig-4: With RSA encryption Steganography Histogram (RGB)

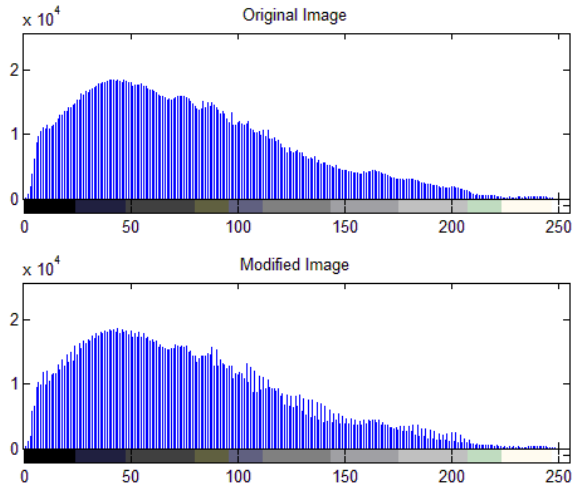

Fig-5: Hiding image (i-1) in Cover Image-2 Histogram (grayscale)

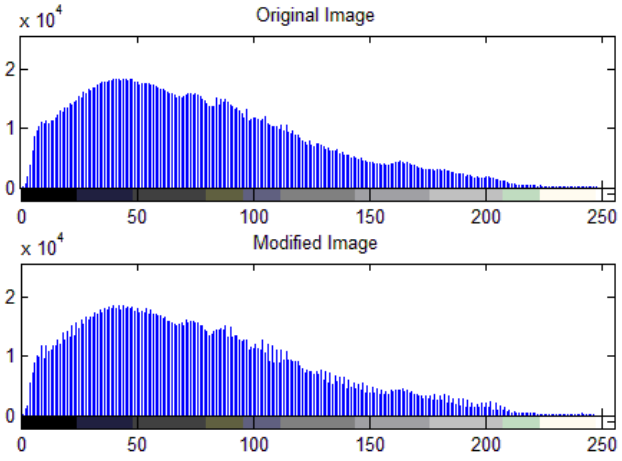

Fig-6: Hiding share1 & 2 into Cover Image-2 Histogram (grayscale)

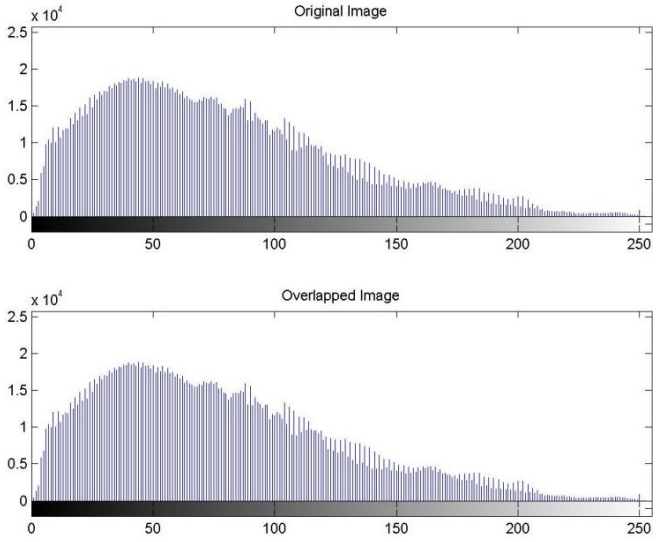

Fig-7: Creating shares image (i-2) & overlapping Histogram (grayscale)

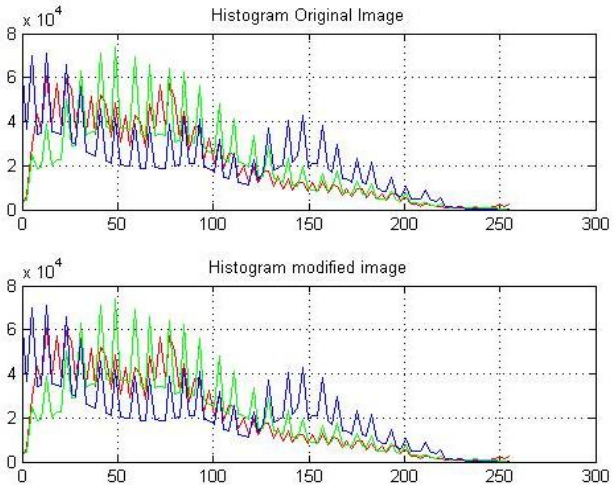

Fig-8: Creating shares image (i-2) & overlapping Histogram (RGB)

IV. CONCLUSION

Images are the most convenient means to be used as there are innumerous images available on internet which makes it difficult for people to identify which images have hidden information. By breaking our secret image into two shares before hiding the shares in the cover makes the system more secure as is evident from the histograms.

V. FUTURE SCOPE

We can enhance the security by applying genetic algorithm to modify the pixel values and thus will further improve the histogram of modified image. This will impose a greater challenge for the unwanted entities to extract the hidden information. We can also extend our work to include videos as cover.

REFERENCES

[1] Behrouz A. Forouzan, "Data Communications and Networking," Fourth Edition, McGraw-Hill, 2007, pp-931,949
[2] James C. Judge, "Steganography: Past, Present, Future," SANS Institute Infosec Reading Room, 2001
[3] George Abboud, Jeffrey Marean, Roman V. Yampolskiy,"Steganography and Visual Cryptography in Computer Forensics," Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering, *IEEE Computer Society, 2010*
[4] Rehana Begum R.D,Sharayu Pradeep , "Best Approach for LSB based Steganography Using Genetic Algorithm and Visual Cryptography Secured Data Hiding and Transmission over Networks," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4 Issue 6, June 2014.