Secure Data using 2-steps Encryption and Steganography to avoid Data theft.

Joshi Siddharth Jayesh
Department of Computer Science Somaiya Vidhyavihar University Mumbai,India

Shaikh Mohammad Bilal Naseem
Assistant Professor, Dept of Computer Science/IT Somaiya Vidyavihar University Mumbai, India

Abstract— Data Security is the most important concern in the terms of modern communicating era. Encryption is the best and the effective way to provide data security and privacy. Most of the modern encryption systems are based on only one step of encryption and decryption which have some drawbacks of data theft but in this application, we have used two step encryption and decryption for better security. In this application, we have used one custom encryption and decryption method and also Advance Encryption Standard. Advance Encryption Standard is based on a principle known as a substitution–permutation network, and is very use full in hardware and software. We have also used Steganography it is the technique which is used to hide the secret data into an ordinary or non-secret file to avoid detection. Steganography can be combined with encryption technique to provide an extra step for protection. In this application we can ide a secret message into an ordinary image and also do text encryption and decryption.

Keywords— Encryption,Decryption,Steganography,Secure,Data,Two Steps,AES.

Figure no. 1 Encryption and Decryption process

I. Introduction

Cryptography is a study and technique of protecting information and securing communications through the use of codes, so that the information can be access by the only person who is authorized to read it. The native meaning of the word Cryptography is that its prefix says "crypt-" means "hidden" or "vault" and the suffix "-graphy" stands for "writing"[1]. More generally, it's all about developing and analyzing the different protocols which are used to overcome the influence of the adversaries. There are various aspects of the cryptography in data security such as data authentication, integrity, confidentiality, and non-repudiation. Cryptography in the modern age was effectively prior synonymous to encryption, which converts an information from a readable form to nonsense form. The person who is encrypting should share the information of the decrypting process to the recipients, thereby precluding the process from the unwanted person. The ancient cryptography focused on the confidentiality of the message. According to it the message was converted into an incomplete format and then it was converted back into the complete form at the receiver end. This process was done by the people who had knowledge about ancient cryptography [2].

A. *Aspects of Cryptography:*

- *Data Confidentiality: - The Information should only be accessible to whom it is intended and should not be accessible to any other person.*
- *Data Integrity: -The information cannot be modified during the storage or transmission between the sender and the recipient.*
- *Data Non-repudiation: - The Sender of the information is not allowed or cannot deny the intention of his/her for sending the information at later stages.*
- *Data Authentication: - The identification of the Sender and Recipient should be confirmed and also the destination or the origin of the information should also be confirmed.*

B. *Encryption and Decryption:*

- *Encryption is the process in which we convert the plain text (normal message) into a nonsense or meaningless form.*
- *Decryption is the process in which we convert the nonsense or meaningless form of message into its original form (normal message).*
- *Most of the modern application are only based on the one step of encryption & decryption.[3]*

II. Problem Statement

To ensure the better security of data and to keep highly confidential which will not be access by an unauthorized person, there is need of advance security than one step encryption.

III. Advance Encryption Standard (AES)

Advance Encryption Standard (AES) is a technique which is based on “substitution-premutation network". It is also known as “Rijndael”. It is used to encrypt the electronic data. It was established by the U.S. National Institute of Standards and Technology in 2001.[4]. It computes all the operation in bytes rather than bits. So, if there is plain text of 128 bits it will treat it as a plain block of 16 bytes. In the AES encryption there are 4 steps Byte Substitution, Shift Rows, MixColumns and Addroundkey and for the Decryption process it is vice versa. It offers various features such as security, cost and implementation. It is widely used for protecting data at rest. Figure no.2 shows the step by

step encryption and decryption in AES.

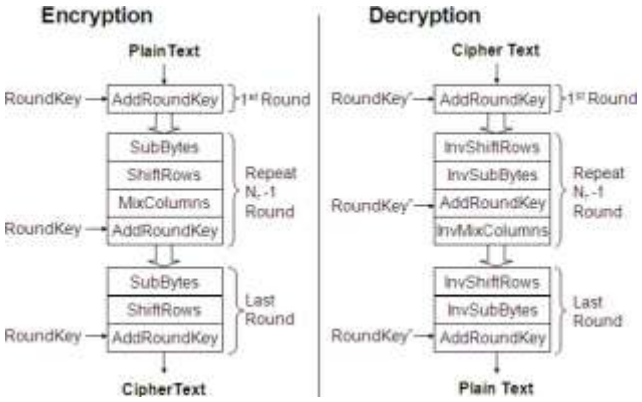

Figure no. 2 Advance Encryption Standard

IV. Steganography

Steganography is the technique of obscuring any type of file, video or image within any other file, video or image. It is derived from a Greek word "steganós" which means "obscure or secret" and graphy which means "writing". Steganography when combined with cryptography provides an extra step of security [6]. Its main function is that it is use to hide the data from the unauthorized person because they will not be able to see anything as it provides a secret path, that it is invincible. It uses some method for protecting it from detection there by not degrading the quality of the image [7]. It is also used for copyright control of any material, to enhance the robustness of image search and also smart identity cards [8]. Figure no.3 shows the encryption and decryption in steganography.

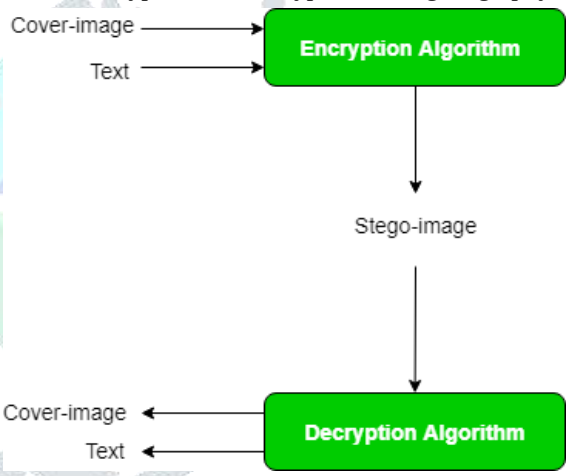

Figure no.3 Steganography

Digital Watermarking is also a part of steganography. It is the way of altering a multimedia into a host image to mainly show the copyright of the content. In this process it takes a host image and then insert the watermark image to it with help of some algorithm and key. In the figure no.4, it shows how media tv channels have their watermark in broadcasting.

Figure no.4 Media tv channels using their logo as watermark for broadcasting

V. Proposed Method

A. Image encryption

In the image encryption we have two methods that is encryption and decryption. We had used a library called as "Steganography.js". In the encryption part, first we have to select an image in which we want to hide any secret message or confidential data and then we have to type the message that we have to encrypt in it. When we select an image, it is displayed on the screen. By clicking on the encrypt button, we will get the encrypted image. We can download it and send it to the person whom we want to give that information.

Figure no.5 Original Image

Figure no. 6 Stegano Image

So, as you can see that after encryption the quality of the image is not downgraded. Figure no.5 was the original image and Figure no. 6 is the encrypted image with a message "Hello how are you".

Now in the decryption part we just have to select the encrypted image and then it will directly show the secret message. In figure no. 7 we can see the Stegano image and the message encrypted with it.

Figure no.7

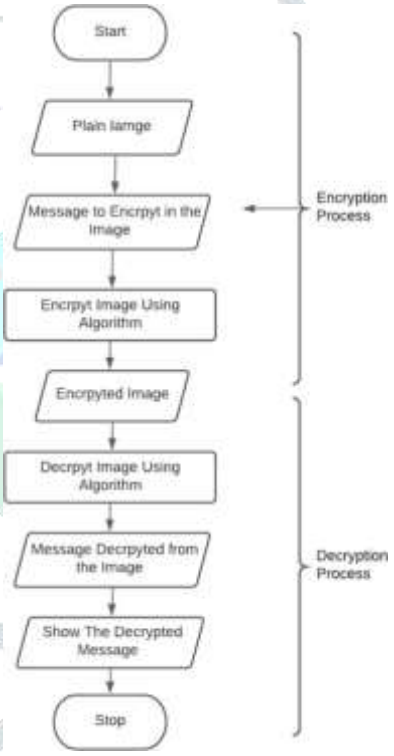

Figure no. 8

The figure no.8 shows step by step whole process of steganography.

B. Text Encryption

Figure no. 9

In text encryption we are doing two steps encryption which gives double security. So, firstly in this encryption part we have enter some text that we want to send someone and also enter the key. Then the given text is first encrypted using the custom method which we had created. In text encryption method the text goes under a "For Loop" where the whole text is divided into list of characters, we also have a switch case where we have assigned a particular value of our own to every alphabets and numbers. So, because of this method the encrypted message is not hackable unless someone has access to our source code. This was the first encryption and now in the second encryption, we have used Advance Encryption Standard (AES) with the help of the "Crpyto.JS" library. In the AES we encrypt the message which is already been encrypted using the custom method and the key entered by the user. Then the message which is encrypted using the AES is displayed to the users' screen.

Suppose if during the event of sender sending the encrypted message to the receiver, some unauthorized person gain access to it and then tries to decode it, he will get the encrypted message that was encrypted using the custom method. If the unauthorized person has no knowledge about that we have used two step encryption then there will not be any problem but if at all they know about the two step encryption then to they don't know about the custom method so still our data is safe . And for decryption process we have to enter the encrypted message which was displayed to the user and the provided key then it is decrypt's it using the AES and that decrypted message is now decrypted again using the custom method to get the original text. So, during this whole process the custom method is not displayed. So, this model provides us the better security then the applications which uses the one step encryption.

For better understanding we can see in the figure no.10, which shows the flowchart of the whole text encryption.

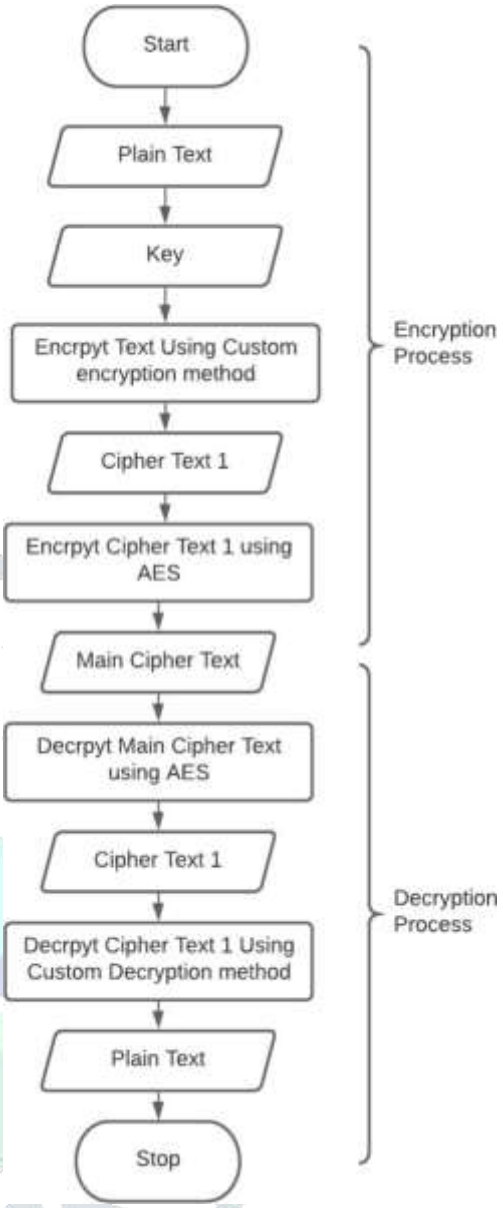

Figure no.10

VI. Acknowledgment

I would specially like to thank my **prof. Shaik Mohammed Bilal N** to encourage and guide me to do this research work on "***Secure Data using Two step Encryption and Steganography to avoid Data theft.***". The project received whole hearted assistance, inspiration, encouragement and valuable guidance in all phases.

VII. Conclusion

The main goal of this research paper is to give a better security which is essential in this modern communicating era. Our model of two step encryption will provide very higher level of security and using steganography, it will also be great way for communicating without any fear of detection. According to us the scope of this project is that it will be very helpful for the Government Intelligence and Defence organization for a secure communication.

VIII. Future Scope

The future scope is to add the different file encryption means documents, audio and video file encryption. Also, a high level of security to the web application. And also, to create system to communicate between the registered and authorized user directly via our application that will be a very major feature.

IX. References

[1] Design and Analysis of Multimedia Communication System - Scientific Figure on ResearchGate.
https://www.researchgate.net/figure/AES-Encryption-Decryption-Flowchart_fig2_221958203
[2] A Modified Side Match Scheme for Image Steganography
https://rb.gy/a7tz6f
[3] Information Hiding in Images Using Steganography Techniques
https://www.researchgate.net/publication/259893801_Information_Hiding_in_Images_Using_Steganography_Techniques
[4] Digital image steganography: Survey and analysis of current methods Abbas Cheddad , Joan Condell, Kevin Curran, Paul Mc Kevit
https://rb.gy/vdfzdt
[5] A Secure and Fast Approach for Encryption and Decryption of Message Communication
https://rb.gy/2emqat
[6] Analysis and Review of Encryption and Decryption for Secure Communication V. Agrawal, S. Agrawal, Rajesh Keshavrao Deshmukh
https://rb.gy/fvkvx7
[7] Cryptography
https://rb.gy/mmipe8
[8] Achieving Secured Group Data Sharing Using Key Aggregate Searchable Encryption
https://rb.gy/bchgln
[9] SerachSecurity Cryptography
https://rb.gy/xwbum1
[10] Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data
https://rb.gy/8589qn