Steganography Using AES Algorithm

Animesh Kumar, Deepak Idnani, Kaushal soni, Nitin Taneja, Rounak Shrivastava
Ajeenkya D.Y Patil University, Pune, Maharashtra, India,

Abstract :
Steganography is the method of hiding the data where sharing of data is present, by hiding data in other data. Steganography is becoming one of the most necessary as more people are joining the revolution of the cyberspace. In comparison to cryptography, it is used to keep strangers from knowing about the hidden data but it is to keep strangers from thinking that the data is even existing. Steganography consists of an array of secret connection methods that hide the data from being identified or seen. For hiding secret information in the image, there exist a huge number of methods of steganography methods some of them are even more complex than strangers all the graphical user interface have there some of the loose points or stronger points. Different application really needs absolute mortality of the secret information, while different application needs a huge secret data to be hidden. In this proposal, the report brings out the intends to give just an overview of image steganography, its uses, and different methods and also in additional security to both the information hidden and that image carries the data. Security is made available by encrypting the information that is transferred in the image and again encrypting the image that has the data using the AES algorithm. This method provides a double security layer to the data.

I. Introduction

Nowadays sharing and receiving images on the network is increasing in large numbers. The security of the network is a major concern as the number of information that is being interchanged is increasing day by day. Therefore the data hiding and data authorization are really very important for defending against unauthorized penetration and use. This is the main cause that resulted in the growth of the data hiding field. Data hiding in the field of hiding information in a way that no person other than the actual receiver of the data and the sender of the data can gain access to it. It hides information which can consist of images, videos, text, and audio files. This technique is also called steganography where the data is hidden in the image. The data that is hidden in the image can be the image itself. The hidden data should be recoverable. Volatile data hiding was firstly deployed for authentication and its important the feature is volatile, it hides the secret data in the digital image in such a way that only the certified person could decrypt the information and backup the original image. Many data hiding methods have been brought out. The performance of a volatile data enclosed algorithm is configured by its payload capacity, complexity, visual quality, and security.

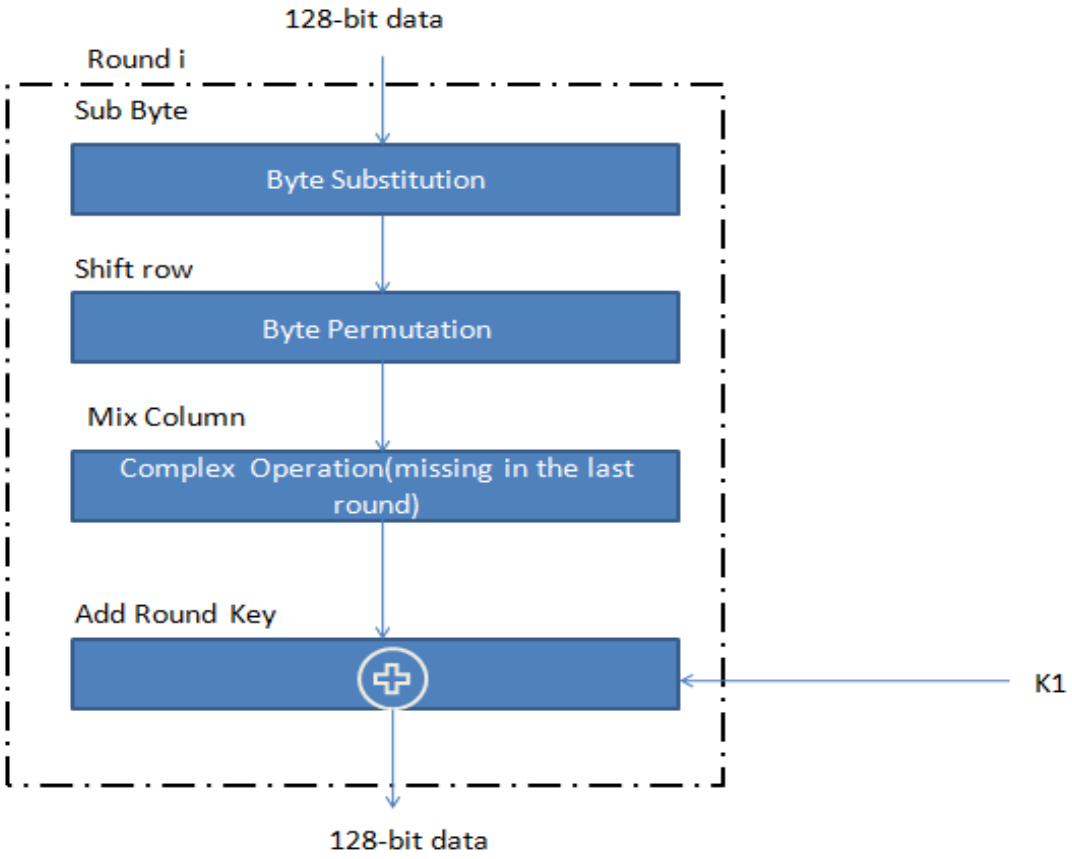
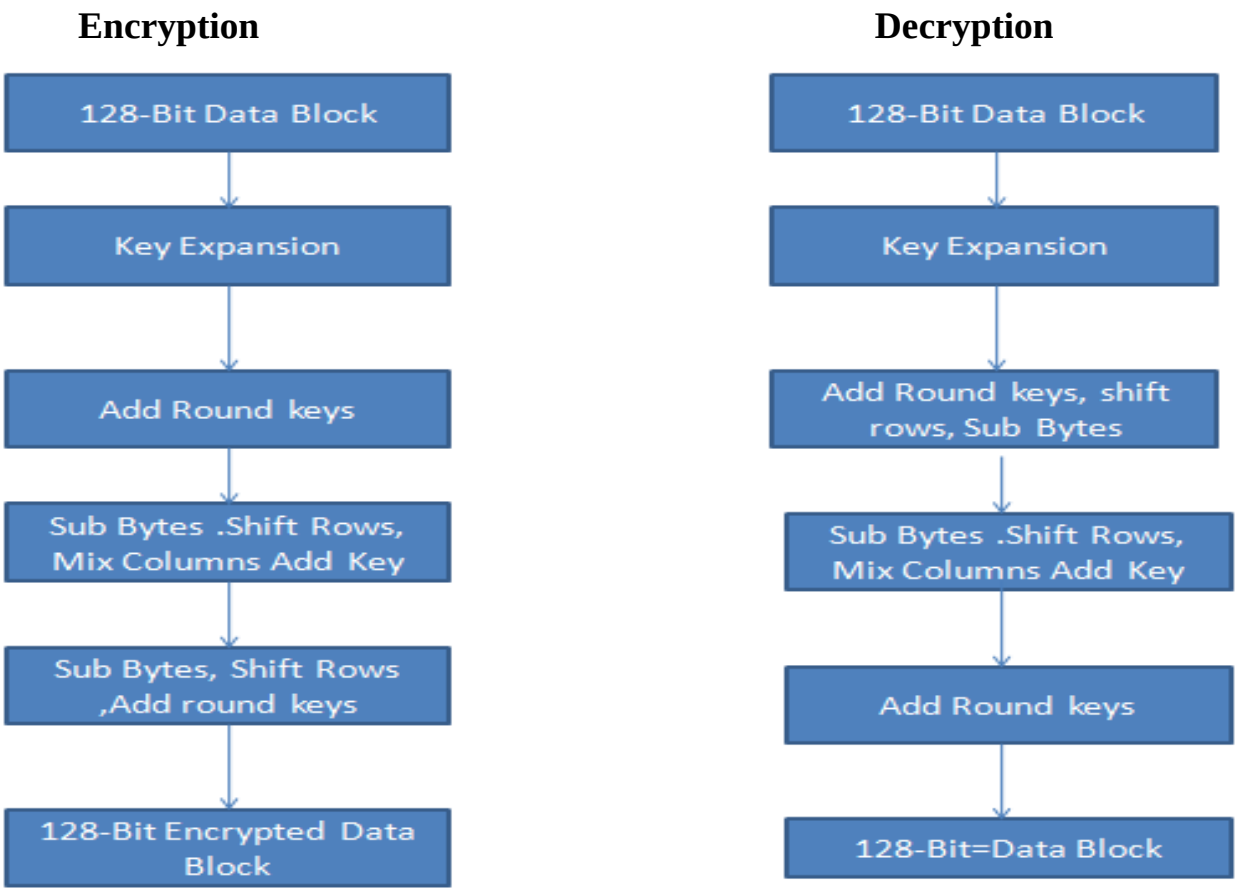


Fig. 1: Aes Encryption

II. Advance Encryption Standard (AES) Encrypption

It is a Symmetric Key Block Cipher that broadly takes on Symmetric Key encryption nowadays. It Comes for the alternative of Des as the size of Des was too small. For the Encryption and Decryption Purposes, it is applicable for the Block size of 128 Bits of size. The number of loops decides the Key Size. It uses 10 loops for 128-bit of keys,12 loops for 192-bit of keys and 14 loops for 256-bit of keys. In general, 4 functions used to encrypt the data and gives ciphertext as output and it includes Sub Bytes, Shifts rows, Adds keys and Mix Columns. The Components of Aes are cost price of memory is very less, high-speed algorithm procedure. I

Steps for encryption and Decryption



III. Existing system

The current system uses the histogram of the image to enclose the data. This method also enhances the contrast of the image. The image build-up is accomplished by histogram equalization. The highest crests in the histogram are taken. The bins between the crests are unchanged while the outer bins have deviated outwards so that each of the two crests can be split into two adjoining bins. To increase enclosed capacity, the highest two bins in the altered histogram can be farther chosen to be divided, and so on until a satisfactory compose improvement effect is achieved. For the restoration of the original image, the location map is enclosed into the host image, in sync with the carrier message bits and other side data. The generation of image histograms is a hard and a huge time-consuming process. But the diverge of the image is build up. The information is only hidden in the image where the level of security is on a beginner level. Since the information is hidden and if the process of restoring is known to the intruder than he will be able to retrieve the image easily without any major effort.

3.1 Disadvantages in Existing system

1. Computing time is very high.
2. Complexity in algorithm.
3. High Distortion.
4. Because of the Use of single key in whole processes, it is less secure.

IV. Proposed System

The symmetric key encryption called as stream cipher is encrypt the original image by using crypto key, With this that image is become unbreakable. Every bit of information is encrypted with every bit of key. There are two different key is used for information hiding and image encryption one is encryption key and data hiding key. Data Hider constrict of selected bits collecting from the encrypted image to

make the data confidential.The receiver is used encryption key and decrypt the confidential data and get the original image by using a distributed source decoder. The expected result is appeared without loss of information or image. Thus in our project, the security of the encrypted information and the image in which the data is hidden is increased. The receiver should have three keys to retrieve the data (i.e.) the decryption key of the information and image, and last the retrieving key of the data from the image.

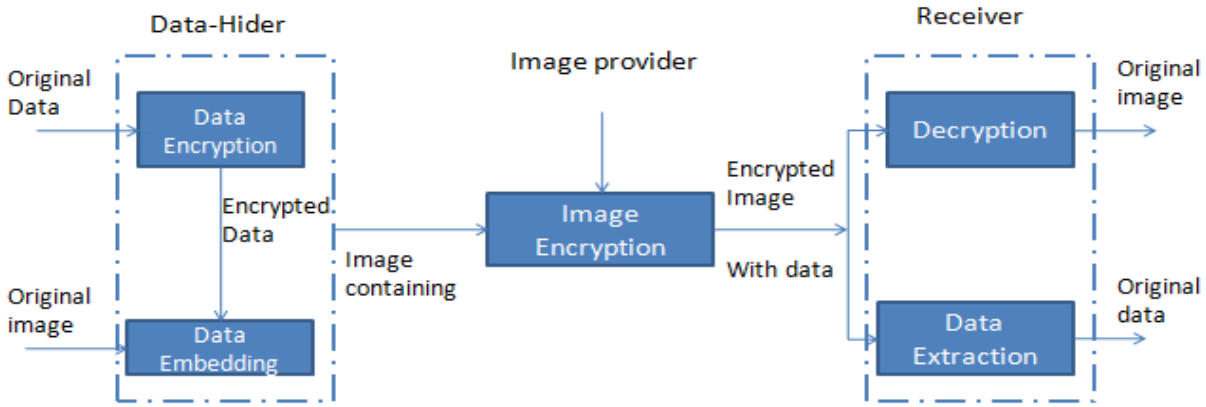


Fig. 3: Architecture diagram of proposed system

4.1 Modules involved

4.1.1 Data Hiding

Data hiding is used in OOP's concept to hide the internal data. It is a software based method.The data and the image which is enciphered has to be selected by client. It is called as summing up of data and data hiding.

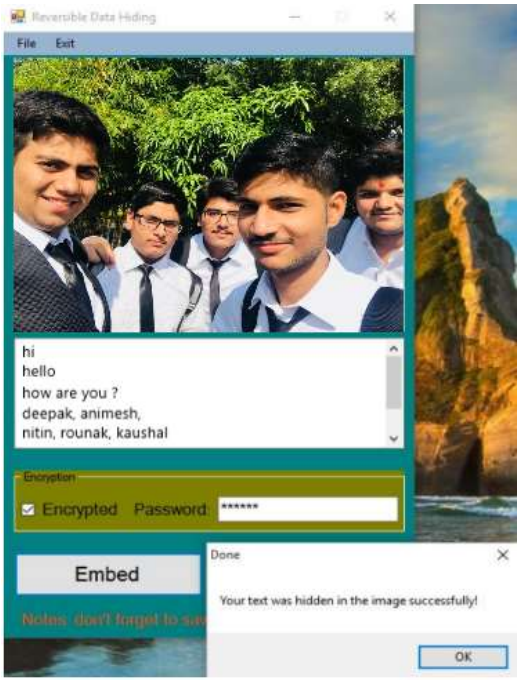


Fig. 4: The data is encrypted and hidden in the image

4.1.2 Image Encryption

In this module the image is encrypted and that encrypted image has to be saved in the local disk with a extension .png (Portable Network Graphics). Image hiding is a procedure of encrypting the confidential image with the help of some encryption algorithm by which the unauthorized user can not access that image.

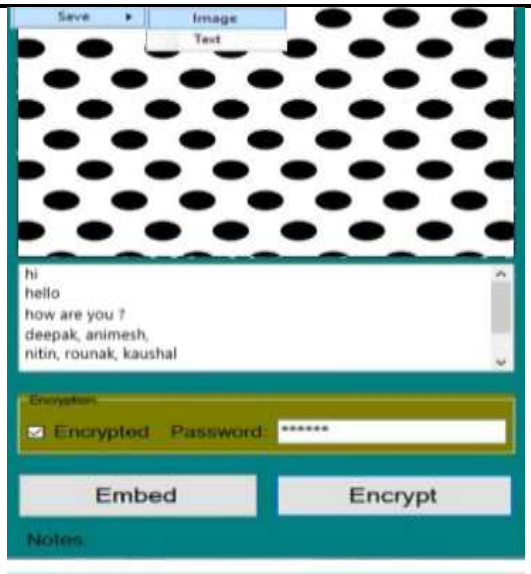


Fig 5 : The image is encrypted and it is saved

4.1.3 Retrieving Data And Image

The data is encrypted by using AES algorithm and that data is kept inside the hidden image. The receiver which has both keys information hiding and encipher key only able to open same image. First the information is de-ciphered and get that information from the image.

Fig. 6 : Decrypt Image and Extract the data from the image

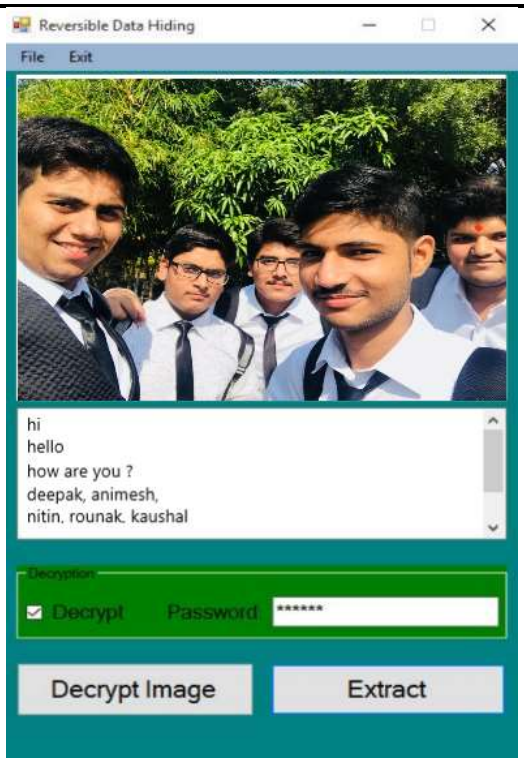


Fig. 7: Decrypt data and retrieve the original data

V. Conclusion

As the intruder does not Know about the Data that is hidden in the image it will increase the Security of the system. So the intruder can only able to access the data if he or she will have access permission. But he won't be able to know the data since there will be no proof of data that is hidden in the image. Only the certified person will be able to access both the original data and the image. Thus this system can be used in different domains where the image and its similar data have to be transmitted in a secure way. For example, in the field of medical science where the patient report with its outcomes has to be sent to the doctor securely, this system can be used.

Acknowledgment

We are really very thankful and we will also like to display our sincere recognition for our Head of the Department Dr.Shabnam Sharma and our supervisor Ratan Singh for the guidance, support and continuous encouragement in making this Research possible. Their Valuable guidance from initial to final level helps us to achieve to complete this research paper. Our sincere thanks to all the faculties who helped us to complete this and gave their valuable advice and made to easy to complete this.

VII. Refrences:

[1] https://pdfs.semanticscholar.org/f9ce/755c34e6e933755e2bac0630197ac25e Be0e.pdf
[2] https://pdfs.semanticscholar.org/0623/88583d1fe0d31cca939ba2911d34773e 7595.pdf
[3] https://ieeexplore.ieee.org/abstract/document/6850714/.com
[4] http://sci-hub.tw/https://www.sciencedirect.com/science/article/pii/S1877050 916304665
[5] https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm
[6] https://www.slideshare.net/atheistprince/aesadvanced-encryption-standard
[7] http://ijsetr.org/wp-content/uploads/2016/04/IJSETR-VOL-5-ISSUE-4-919-923 .pdf
[8] https://cloud.google.com/files/security-features-for-connect-for-anthos.pdf
[9] https://www.simplilearn.com/ice9/pdfs/agenda/lvc/AWS_Solution_Architect_Brochure.pdf
[10]https://olbolui.olbenefits.ml.com/publish/content/application/pdf/GWMOL/FedFundWireTransfer_04242014.pdf