Data Abstraction & Encryption Using Various Techniques (Cryptography)

Mr. Amit S Hariyani
Department of Computer Science, Bhavnagar
Maharaja Krishnakumarsinhji Bhavnagar University,
Sardar Patel Campus, Gardi Gate, Bhavnagar

Mr. Bhavesh S Hariyani
Shree Swaminarayan College of Computer Science,
Maharaja Krishnakumarsinhji Bhavnagar University,
Sardarnagar, Bhavnagar

Abstract— Data abstraction is a technique by using which we can hide information inside other information in such a way that it is unable to recognize the existence of any data whereas encryption means converting data in some other form such that only intended people can access it. So many carriers available for data abstraction but one of the most popular is using image. Now a days to provide security for personal data it is quite difficult. Here by using some cryptographic techniques data can be abstracted and encrypted. For example any secrete image will be converted into a text file, and an encryption done into a cipher text by using security password based encryption algorithm and at last it will be embedded into cover image. This process done by inserting secrete bits of message into cover image only for selected pixels. This makes it infeasible for other party to retrieve the hidden data.

Keywords— Data abstraction, cover image, encryption, security

I. INTRODUCTION

In previous years people were facing lots of problems because of less security and loss of private data, but now a days lot many techniques are available which are using cryptography to secure data. Cryptography is used to send encrypted data by providing a private key that allows decryption at the other end, and we can send our secrete data safely whether it is any audio file, video file or any image etc.

II. WHY DATA ABSTRACTION REQUIRED?

There are lots of terminologies available for data abstraction one of which is "Generating codes that allow information to be kept secret". This technique of converting data from human readable format to non-understandable format allows secure sending and also converting back into original one at the other end. The converted text in data abstraction always show a static data of input text. There are so many techniques available that follows their own strategy, but they all uses some patterns. This pattern based idea used to decrypt the encrypted data. Data abstraction is a one type of science and art of hiding data and thus it embeds hidden data in other cover media so as no one can stole it. In ancient years people were using indistinguishable ink or hidden tattoos to dispatch hidden content. But now a days so many network technologies developed that provides easy to use communication channels for data abstraction. Actually the data abstraction process begins by recognizing the cover image's unrequired bits (those which can be removed without losing the image's integrity). The merging process defines one medium by replacing those repeated bits with data from hidden information.

III. ENCRYPTION OF DATA WITH ABSTRACTION

The encryption of data with abstraction includes embedding or hiding sender's private information in a file (package) that does not give any clue about the existence of the information when it will be viewed by someone. To perform this process any type of media files like .bmp, .jpg, .gif, .mp3, .doc etc. can be used as a container which acts as a carrier for the sender's information. The information here is hidden inside container and the carrier is transferred to the other end. This operation uses both logical and technical methodologies to perform the task. Generally the encryption algorithms takes secrete information and a container as an input and it gives the carrier message as output which includes embedded information. The container will never give any information to receiver about the data or information it contains until or unless it revealed by the receiver with tools that are used for encryption by sender. These techniques of data abstraction and encryption are mostly used in militaries for secured transmission of data and to hide information. Some of the examples of data abstraction techniques includes identification and authentication, watermarking and transferring passwords which are highly used.

IV. DATA HIDDING BEHIND IMAGE

Here we have demonstrate how to hide data behind image with example. To hide the information behind the image we can follow given steps:

A. ***Choosing one image that can be used for data hiding :*** Here we can use any type of image file such as .jpg, .bmp, .png etc.

B. ***Merge Data file with an image by using winRAR :*** In this step we place the data files that you want to hide in same folder path where the intended image placed and then after by using winRAR create .rar file of the data, that means the data should be zipped in one file say data.rar (do not include image in this .rar)

C. ***Hide data (.rar) behind Image :*** Now using command prompt and performing some commands on our .jpg and .rar file we can hide the data for that we need to follow given below steps:

a. CD <space> <filepath> (where both files are placed)
b. COPY /b <imgname.jpg> + <data.rar> <space> <newimgname.jpg>

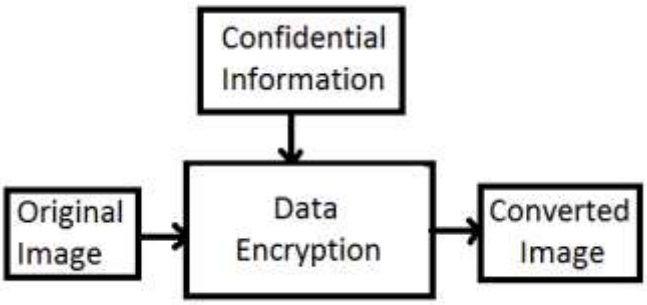
Here, by using above two steps we can easily hide our data behind the image. In first step we move towards the file location where both files are placed (.jpg and our .rar file) and in second step using COPY command we are generating new image file that includes our data.rar file behind it and works as a normal image file. It means when you double click on it, it will be opened in image viewer and we can see the original image but if you open it with WinRAR than you can extract it and we receive two files our original .jpg file and data.rar files. This is the way we can hide our information behind the image file.

ORIGINAL IMAGE
DATA FILE
CONVERTED IMAGE

The other way of data encryption is hiding the image behind the video file. For example if we hide image of 2mb behind the video having size of 200mb than it may not possible to understand the confidential information is hidden behind the video but incase if we hide the video of size 200mb behind the image file having size only 2mb then it can be easily recognized that there should be some information hidden behind the image so, we need to care about it at the time of hiding the data. The file size is also important in this process. This data abstraction technique merges the hidden information in ordinary cover image so than no one can easily recognize it.

V. DATA ENCRYPTION TERMINOLOGY

Data encryption refers to the converting the data from one form into another one using some techniques. For example the information that we hide behind the image file may also be converted into another form before abstraction or else if we consider the image file, at the time of abstraction its bits at least significant position are changed so we can consider it as another type of encryption.



Data Encryption using encryption algorithm

VI. RSA ALGORITHM

The RSA algorithm is one of the example of data encryption. It takes two different keys one is called Public Key and other is called Private Key. The Public Key is publically given to anyone where as Private Key is kept secret. Below given example demonstrates how Public and Private Keys are generated.

A. ***Generating Public Key:***

a. Select any two co-prime numbers say P=59 and Q=53 and calculate N = P*Q = 3127.
b. Calculate exponent such that it must be an integer and not be factor of N. Here 1<e<**Φ**(n). For example, e=3.
c. So for public key here in this example here we have N=3127 & e=3.

B. ***Generating Private Key:***

a. First of all **Φ**(n) will be calculated where **Φ**(n) = (P-1) * (Q-1). So **Φ**(n) = 58*52 = 3016.
b. Now the private key will be calculated, that is d = (k * **Φ**(n) + 1) / e for any given integer k.
c. If we consider k=2 then we get value of d=2011.
d. So from above steps we get d=2011 as a private key.

C. ***Encrypting and Decrypting Data based on generated Private and Public Keys:***

Here suppose we want to encrypt and decrypt the number 89 by using our private and public keys :

Encryption is done as $C= 89^e \bmod N$.

$C= 89^3 \bmod 3127$.

$C= 1394$

Decryption is done as $C^d \bmod N = C^{2011} \bmod 3127 = 89$.

VII. FEW POINTS THAT MUST BE REMEMBERED FOR DATA ABSTRACTION

A. ***Indistinguishable :*** The people must unable to distinguish the original data and the converted image.

B. ***Capability:*** The image must be of high defination such that it should not loss its originality or else the quality of image must not be decreased after conversion.

C. ***Durability:*** This referese to the level of difficulty faced to destroy the converted information without destroying the container.

VIII. TYPES OF DATA ABSTRACTION

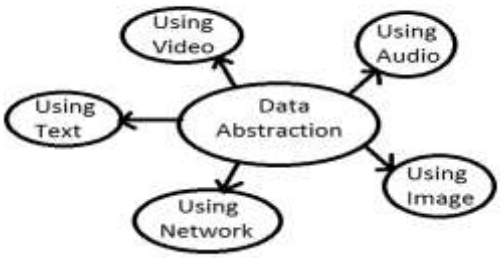
A. ***Text Abstraction :*** In this type of data abstraction technique mostly whitespaces are used to abstract the actual data.

B. ***Image Abstraction :*** To hide our data behind the image, high defination image is required, such that it can not loss its sharpness after encryption. For that mostly 8 to 24bits size images are used.

C. ***Network Abstraction :*** This includes hiding our information by using some network protocols such as IP, TCP, UDP etc. In Open System Interconnection model lots of layers using carriers to send data on different layers.

D. ***Audio Abstraction :*** We can convert the analog data into digital form as well as digital data into analog vice verca. Here, the digital form of the voice data is used for encryption and abstraction where we can hide our information by modifying the digital signal.

E. ***Video Abstraction :*** This can be performed by replacing pixels at least significant bit positions of the video in such a way it should not loss the originality of video.



IX. CONCLUSTION

Data abstraction and encryption techniques are used in many places to keep data secrete at the time of transmission, mostly it is used for military purpose to hide the confidential information with the help of encryption techniques such as by using some watermarks or special symbols so that no one can identify the actual information until or unless it decrypt the message with the same technique.

X. REFERENCES

[1] https://ieeexplore.ieee.org/document/7087159/
[2] https://searchsecurity.techtarget.com/definition/RSA
[3] https://en.wikipedia.org/wiki/Steganography
[4] A research paper on Cryptography Encryption and Comparision techniques by Sunita Kumar.
[5] Stegonography Techniques – A review paper Jasleen Kour Deepankar Varma.