Volume: 12 Issue: X Month of publication: October 2024

DOI: https://doi.org/10.22214/ijraset.2024.64629

“Four Wall Interlocking” May be the Solution

Rutvi H. Choksi[1], Shivangi Parmar[2], Mr. Arunkumar Kavad[3]
[1]B.Sc. Forensic science (sem-5, 3rd year), from Parul university Gujarat, INDIA
[2]Assistant Professor, Institute of applied science, Parul University
[3]Founder of FORENSIC TALENT INDIA LLP

I. INTRODUCTION

Cryptography scrambles data using encryption algorithms, making it unreadable to unauthorized parties. Imagine it as locking a message in a secure vault. Steganography hides the very existence of the data by embedding it within another file, like a secret message written in invisible ink within a picture. Both methods play a vital role in secure communication, especially when transmitting information over unreliable networks.

Cryptography utilizes a two-step process: (1) Encryption: The original, readable data (plaintext) is transformed into an unreadable format (ciphertext) using an encryption algorithm. Think of it as scrambling the letters in your message. (2) Decryption: The ciphertext is then converted back into its original form using a decryption key, akin to unlocking the vault with the correct key.

There are two main types of encryption algorithms: (1) Symmetric encryption: Both sender and receiver use the same secret key for encryption and decryption. Imagine a single key for both the lock and the vault. (2) Asymmetric encryption: This method utilizes a pair of mathematically linked keys: a public key (known to everyone) for encryption and a private key (kept secret) for decryption. Think of it as a public mailbox to deposit the message and a personal key to unlock your private mailbox.

By combining cryptography and steganography, we create a layered defence. Even if someone intercepts the data, they wouldn't know it contained a hidden message, let alone be able to decipher it. This enhances overall information security.

II. ADDITION OF NEW SYSTEM TO CS GRAPHY

With development of cryptography and steganography security towards confidential information increased and unauthorized exposer is avoided but its implement has not yet reached to that level. its application mostly involved in businesses at heigh scale , in military and other security purpose , in government system and many more .

It will become necessary to have one another form due to the advancement of technology and artificial intelligence, and “FOUR ALL INTERLOCKING” may be the solution

This system involved four steps in manner of maintaining content of cryptography which is hided inside steganography this are as :

A. AI Free or Humanitarian Access

With this intention we require to inbuild 1st layer as eyeball movement detection, fingerprinting and voice detection and heart rate

As this four factor will not be going to be cloned in AI, robots can’t be able to show that contraction as of realistic eye, even that pitch of voice layer vibration can’t be able to match that human frequency voice and finger printing was so earlier declared not to be casted to other digits or fingers according to now till analytical results says this.

1) Word hunt :

The word hunt is referring to finding or to type word security. This mechanism is of 2nd level involved to inbuilt password like security. That only to be known by a two or number of parties involved in communication. As it must involved some critical data shared only to near to individuals, something they share in common and not a cup of tea for other one to recognize it, should be added to this level.

In one word we can say “passcode” try to set pass code that none of third party or out of communication came to know about it.

It must contain some special characters like @,#,$,%,^,&,* and many more to make this more secure

More than 8 characters should be required to make this level complete.

Passcode must contain word or sentence known by both parties in communication. And no other person has any knowledge about it.

Pass code must contain two digits, limitations in digit is to make it short and accessible to authorized persons.

Must used one capital letter in passcode, used as identity.

2) Precise approach:

These levels of security provide system to add some number of questions for evaluation, which relates to content of data or it be set by formator according to requirement.

It will show that how much second party or receiver is near to information.

This system will work on principle of question and answer, sender will send message with some security question and receiver have to answer that question to unlock one wall of system.

This used to maintain confidentiality and MITM attack will be avoided.

Question will be framed in manner by sender that only receiver know how to answer.

With encoding of question answer for respective question should also selected, only on that manner unlocking of level will be done.

This system is case sensitive.

3) Immutability (block chain concept) :

As to maintain unchanged data transfer, it is mandatory to inbuilt immutability in networks; it was being one characteristic of block chain.

In some cases transparency in communication is needed but with security, in such condition block chain will play role.

Block chain is storing data in block and linked in chain, to store message transaction immutable and transparent in network of work space.

Points to be read

Might alteration is possible at requirement level but not in basic concept as it define whole point of security.

Levels of security are not being removed as all four layers are interlinked with each other.

Every level should be unlocked only in sequential manner.

No jump will be valid or possible.

This type of security levels are majorly made for crucial networking or data transfer, as it is so leisure for simple conversation.

Four wall interlocking system on applying on cryptography and steganography hybrid with intention to increase security to cope up with future developing cyber forms.

B. AI limitations

Artificial intelligence had able to work parallel with biological systems as found in human that nearly found to be next to impossible ,even though it came next to possible by advancing tech. Still many of crucial points are not being able to clone artificially in system.

That are eyes motions, contraction, voice pattern similar to human, that pitch can’t made it to match that stress available by nature.

This will be the point we take as block to build future require security. Make light on what is aforesaid data and evenly we have resolving problem of fingerprint casting is now not being done as many sensors having sweat recognition system.

That all this is mention in AI article given below

C. Reference

1) NIST(US) PUBLISHED PAPER ON AI
2) NAIAC national artificial intelligence advisory committee U.S.
   As per NAIAC, the development of AI is found on pivotal moment and have to work fast with maintaining balance between innovation and risk .
   This four wall interlocking system will definitely work to maintain fear of risk and obviously innovative steps towards AI.
3) Other point we must take in reference when we talk about NAIAC is GENERATIVE and NEXT GENERATION AI.
   This is large language model which will increases intelligence power on bases of past done activities or performed event, striking with permanence tendency of AI.
4) Under National AI initiative act 2020, require command on generative AI Wants to work on safety and assurance

D. Cryptography

Efforts towards improvement in cryptography

DES(data encryption standard) , which was released by NIST in 1977 but failed to meet the federal information processing standard’s (FIPS) need for a high level of protection .

Because our networking system is web- based and widely connects to different places. In order to maintain form of confidentiality that ensures the collaborative workplace between government, academia and industry, good form of landscape is thus essential for additional practical and integral protection.

This IT system is being access to every digital assistance to perform e-commerce and in bold to securing ‘’ top – secret federal data transfer through network.’’

In foregoing advancement cryptographic will definitely take turn when on QUANTUM COMPUTING became true dream. On other side of this development this will going to be at vast spectrum enhancing system.

E. Light Weight Cryptography

More about cryptography

On the date of July 27, 2022 quantum cryptography is introduced by international team of respective subject to make improvement of its core meaning, which is mention as follow by keeping in mind of four main pillar of cryptography:

Data Confidentiality,

Data Integrity,

Authentication and

Non-repudiation

1) QUANTUM CRYPTOGRAPHY

“System that prevented human intervention during network connection while encoding a message or text”

The Quantum cryptography is not what the way to replace traditional cryptography, using of large mathematical algorithm, instead of it making it more secure by usage of photons as physics principle described for transferring data more securely.

It uses 100 digit of factorizing encoding and decoding methodology which is next to impossible for any device to do in period of time works against algorithm.

F. Application of Quantum cryptography

QKD: for establishment of shared key between two individual associations by applying quantum communication.

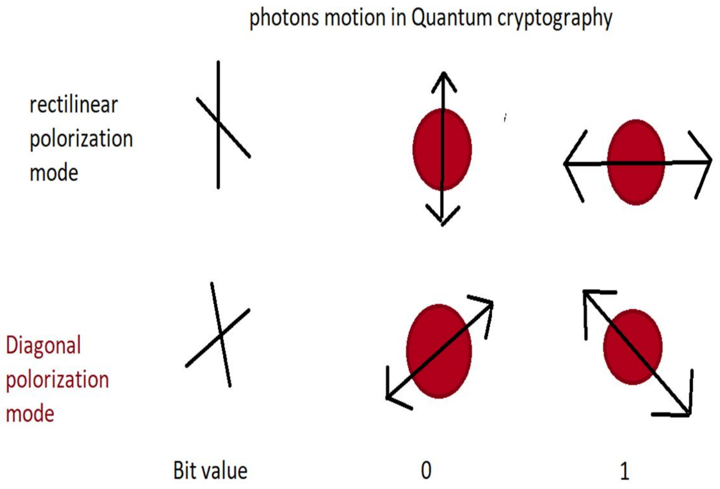
Quantum key distribution is just to apply confidentiality for key and not for any type of data transaction, key which used to attach with any encryption algorithm.

MISTRUSTFUL QUANTUM CRYPTOGRAPHY:

This concept can be easily explained through short story:

There are two parties working in collaboration wants to share some crucial information to third party and while conducting this purpose of communication, both having fear of confidentiality and both of them have mistrust to each other.

And for same quantum cryptography is conclusion.


photons motion in Quantum cryptography
rectilinear polorization mode
Diagonal polorization mode
Bit value
0
1

(fig. 1)

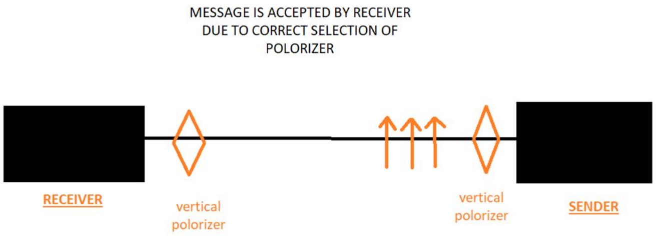
The above mentioned photons motions are regarding how binary numbers will be generated through Quantum mechanism and result in whole message encryption. That's why it found nearly to be impossible to decode message encrypted using quantum cryptography. At a time it is consider to be the best path to maintain four pillar of cybersecurity, may further changes update its credential.

1) Working Process

Process includes travelling of photons in one direction. Unit of photons carry one bit of data – either 0 or 1 and properties of photon involve oscillation, vibration, in certain way.

Polarizer is second stage, work as filter that allows certain amount of vibrating particle in single direction. If it states vertical stands for 1 bit translations and horizontal for 0 bit, one polarization works on only for either of one.

Now message or data is transferred using optical fiber and then second party will use polarizer randomly, irrespective of which polarizer used by first person or sender, then elimination of unnecessary polarizer is done, to make message readable.



(fig.2)

G. Four wall interlocking factors

1) Eyeball movement detection :

Eyeball tracker uses small range infrared light, this use to reflect in eyes and after reflection at some point, it will results in calculation and able to identify its movement.

This will protect messages from AI attack, as AI does not have capability to show eye movement like human

H. CIA PRINCIPLE

1) CONFIDENTIALITY :- ability to hide information from unauthorized person

Credential information including sensitive information is not remain unhide or unlock to entities who are not involve in communication.

Confidential information includes :-

Non- public data like:

Medical details of person

Financial information of individual and organizations

Business planning

Database of websites , applications , social media(this media include every platform of video ,audio, OTTS and movies) and other IT related stuffs

Research and education administration

Government administration information and military communication

Why is confidentiality required?

To create trustful environment

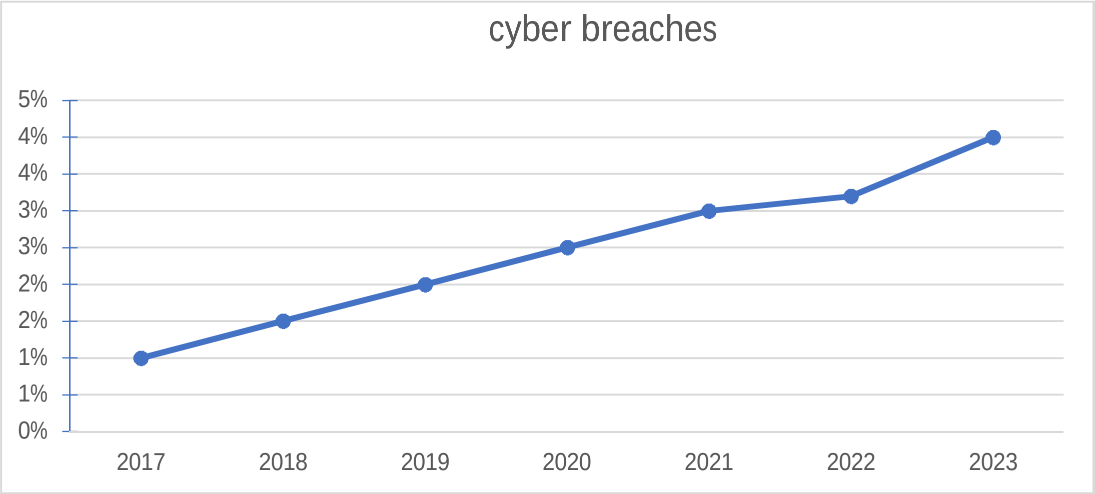
To prevent immoral use of information

To maintain dignity

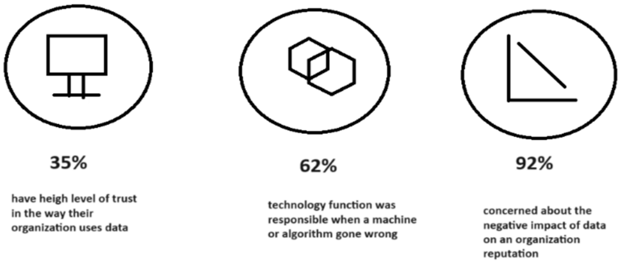
Abide IT laws

To provide non- interrupted communication base

What is breach?
When confidentiality breaks and third party able to access data without consent of authority.
Example :- MIAM, social engineering , putting private information on mass media spoofing , ransomware attacks , phishing ,etc.
CASE: - 1. BRITISH AIRWAYS found to be under threat of data breach which affected more than 400,000 customers, this took place in 2018 and affected both personal and credit card data .
CYBER BREACH :- (fig .3)



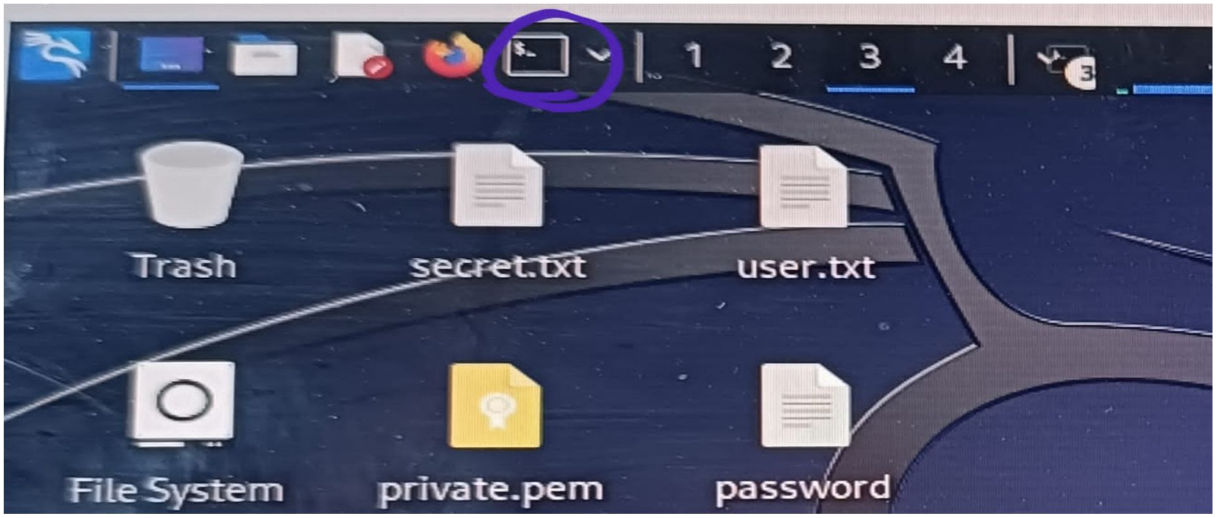
a) I: INTEGRITY: - the ability to ensure that data is accurate and unchanged
When some important or critical information is shared, the receiver must being assured about the message that received is not modified or manipulated.
Intentionally or unintentionally alteration in data or stealing of data is considered as data integrity breach.
CASE :
IN 2008 hackers infiltrate Brazilian government system.
IN 2010 stuxnet worm to make minor changes which result in destroying Iran's nuclear power program.


35%
have heigh level of trust in the way their organization uses data
62%
technology function was responsible when a machine or algorithm gone wrong
92%
concerned about the negative impact of data on an organization reputation

b) A : availability
After making data confidential and integrated it is required to make data accessible frequently. For example, if data is well secured and out of reach from unwanted individuals and even from authority, it seems to be useless and meaningless.
The third factor of CIA principle 'A' stands for availability of data.
DOS attack and flooding of report on site compromises availability and degrade trust of users trust.
Upgrading and staying update is primary solution of breaches and attacks which made services unavailable.

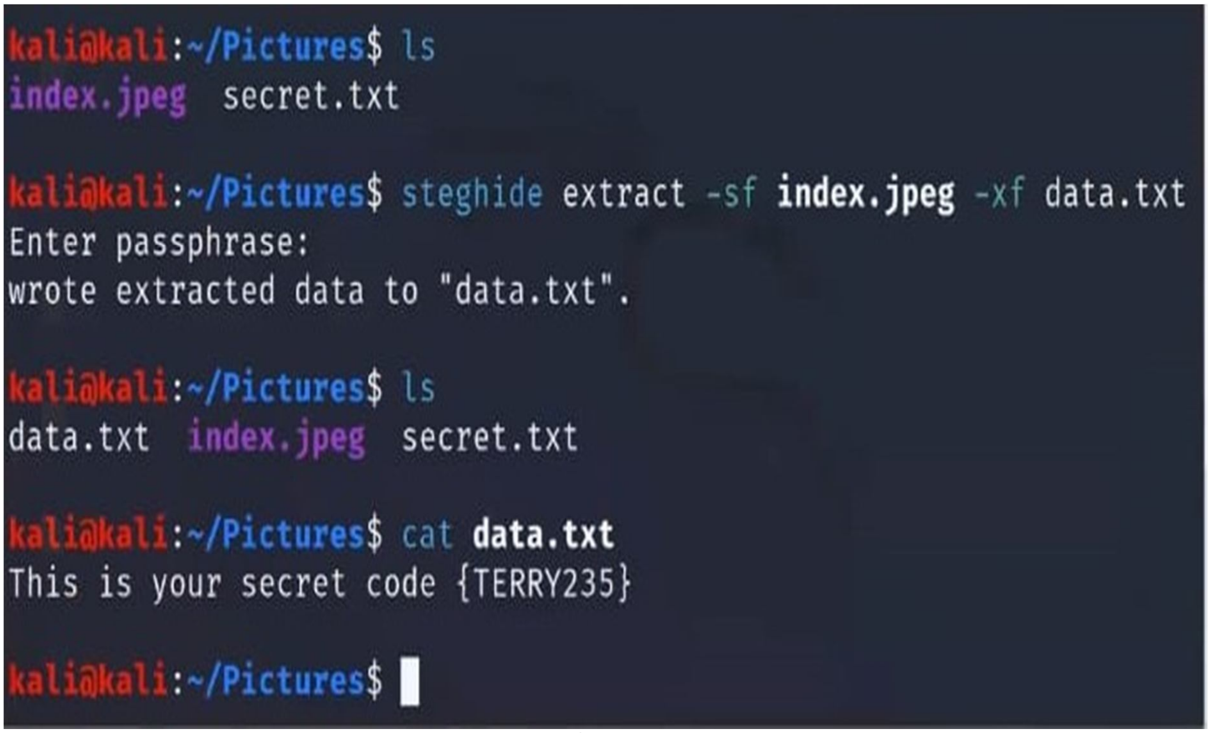
c) IMPORTANCE OF CIA PRINCIPLE
To deal with vulnerability and exploitation of data and information available at site, social media, communication, audio, video, graphics and text required should be protected during exchange or involved in transferring from one device to another.

Even in device CIA principle prevent exploitation and cracking of system, theft of data, mutation or modification
How to perform cryptography and steganography
Step 1: combination of both techniques is performed using kali Linux.
Open kali using VMware or virtual box oracle open, next to open terminal present on upper left corner on kali interface.



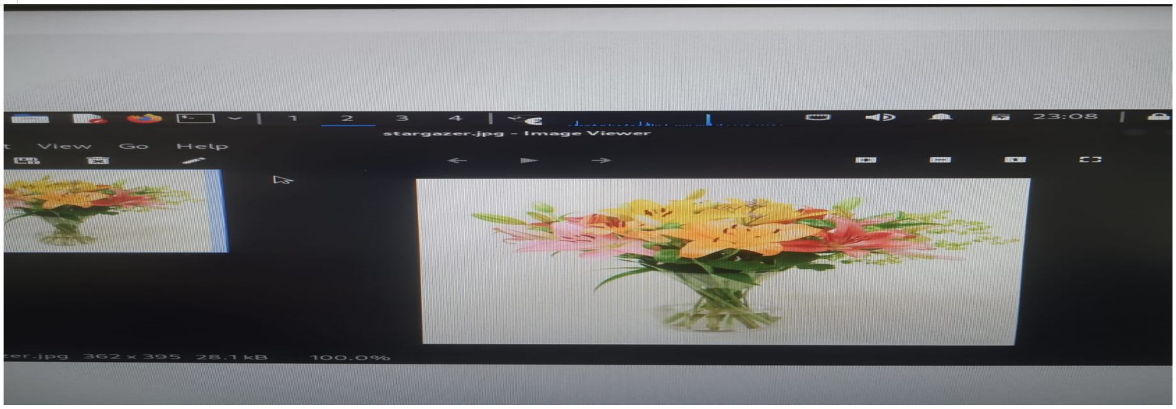
(fig.5)

Step 2: create new file with name as plain text and type some data inside file.
Open search engine like google and download image on Desktop
Here in image picture of flowers are visible.
Save this image in jpeg format.
Extract data from steg file as given below command in image



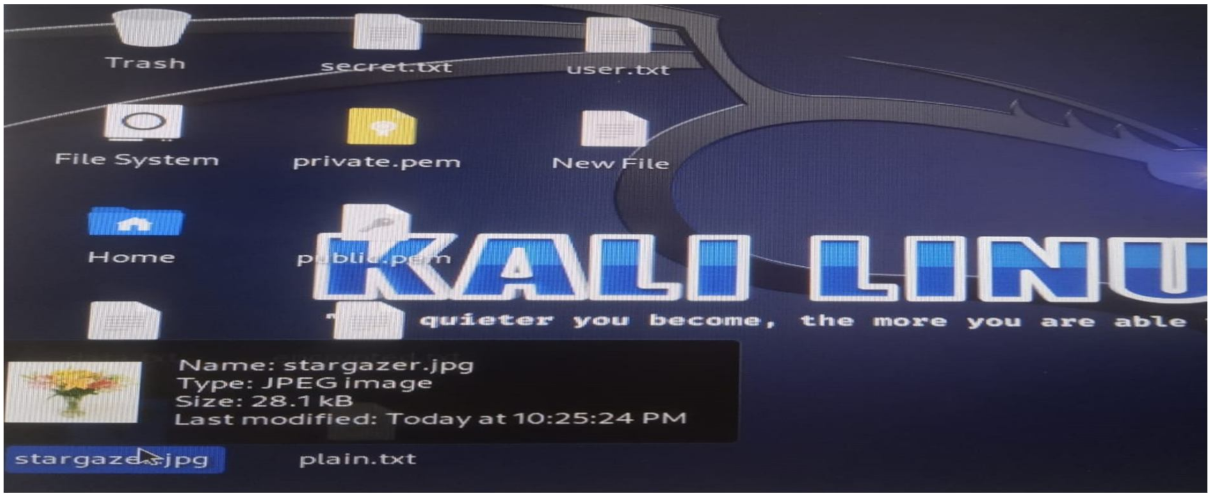
```
kali@kali:~/Pictures$ ls
index.jpeg  secret.txt

kali@kali:~/Pictures$ steghide extract -sf index.jpeg -xf data.txt
Enter passphrase:
wrote extracted data to "data.txt".

kali@kali:~/Pictures$ ls
data.txt  index.jpeg  secret.txt

kali@kali:~/Pictures$ cat data.txt
This is your secret code {TERRY235}

kali@kali:~/Pictures$ 
```

(fig.6)

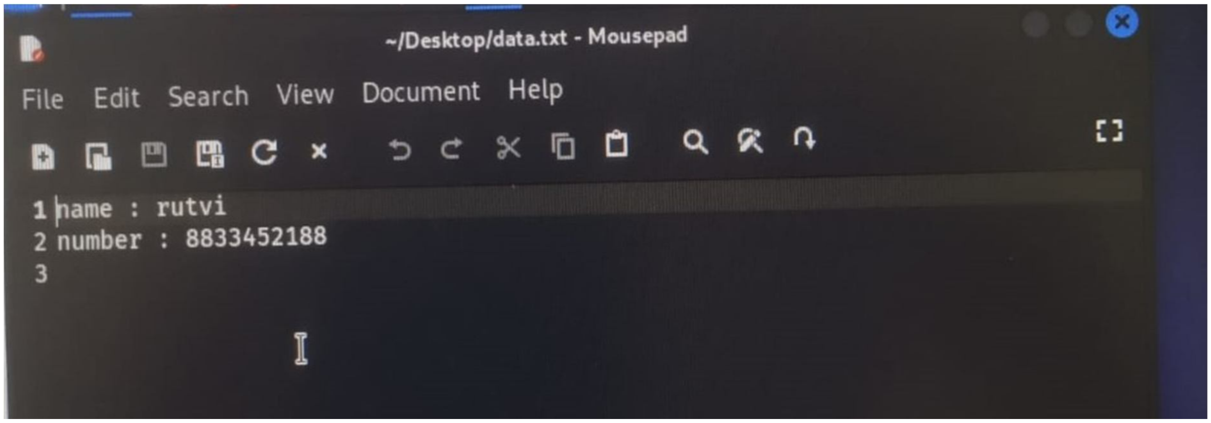


(fig.7)

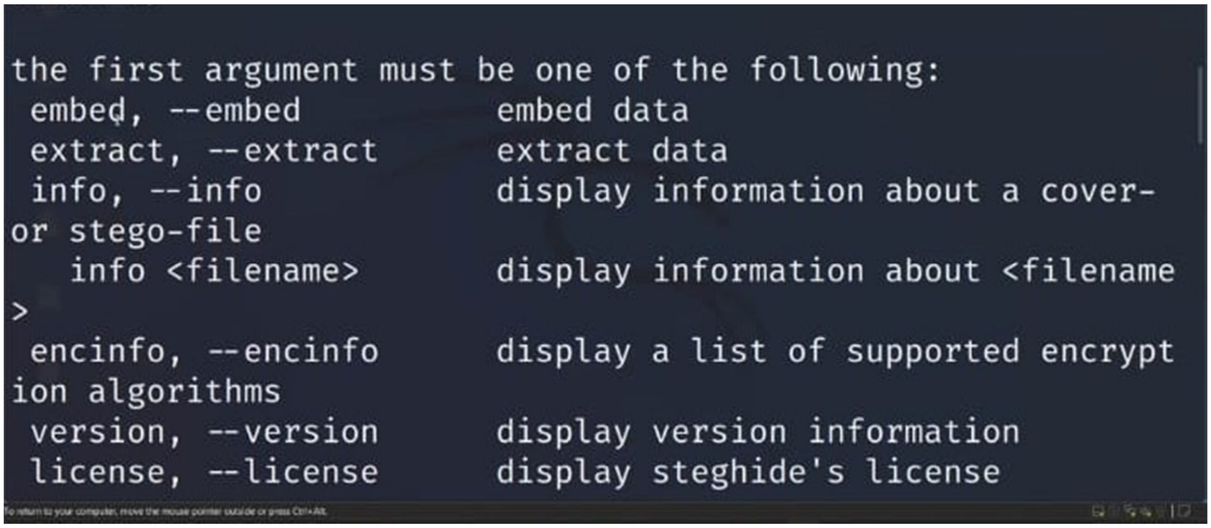
Step 3: open terminal and type command cd Desktop
Then press enter key you will be appear in Desktop and type ls
On command ls all files saved on Desktop
And give command steghid–help
All specific commands for steganography are present in help
Now give command steghideembed -ef plaintext.txt (name of file given) – cfstargazer.jpeg (name of image saved)
On pressing enter kali ask for passphrase, then re-enter passphrase
Embedding file in image is done.   (fig.7, 8, 9) as continue



Name: stargazer.jpg
Type: JPEG image
Size: 28.1 kB
Last modified: Today at 10:25:24 PM

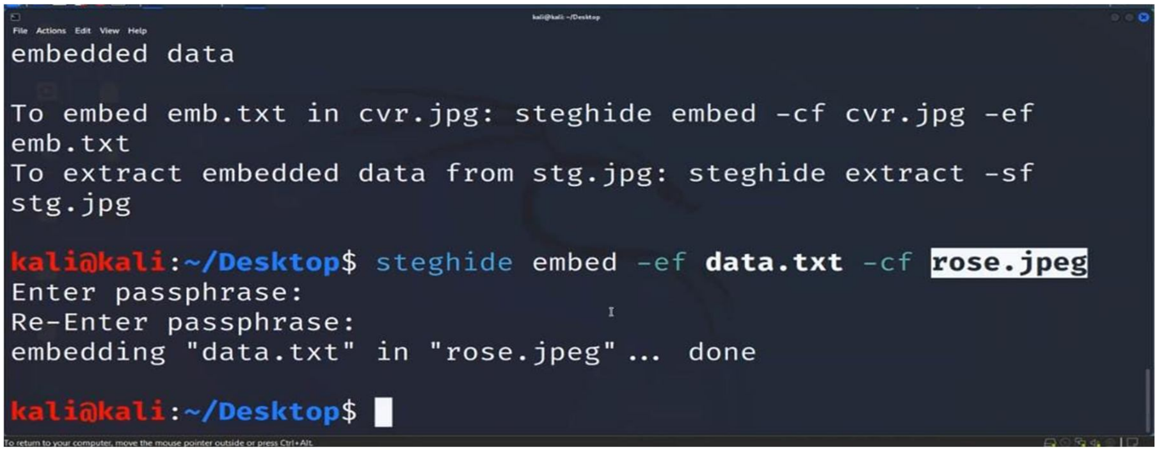


```
name : rutvi
number : 8833452188

```



```
the first argument must be one of the following:
 embed, --embed           embed data
 extract, --extract       extract data
 info, --info             display information about a cover-
or stego-file
   info <filename>        display information about <filename
>
 encinfo, --encinfo       display a list of supported encrypt
ion algorithms
 version, --version       display version information
 license, --license       display steghide's license
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.



kali@kali: ~/Desktop
File Actions Edit View Help

```
embedded data

To embed emb.txt in cvr.jpg: steghide embed -cf cvr.jpg -ef
emb.txt
To extract embedded data from stg.jpg: steghide extract -sf
stg.jpg

kali@kali:~/Desktop$ steghide embed -ef data.txt -cf rose.jpeg
Enter passphrase:
Re-Enter passphrase:
embedding "data.txt" in "rose.jpeg"... done

kali@kali:~/Desktop$ 
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

(fig.10)

After this process on opening of plain text embed image is visible on open it with some extra process with password data hide inside image is visible.

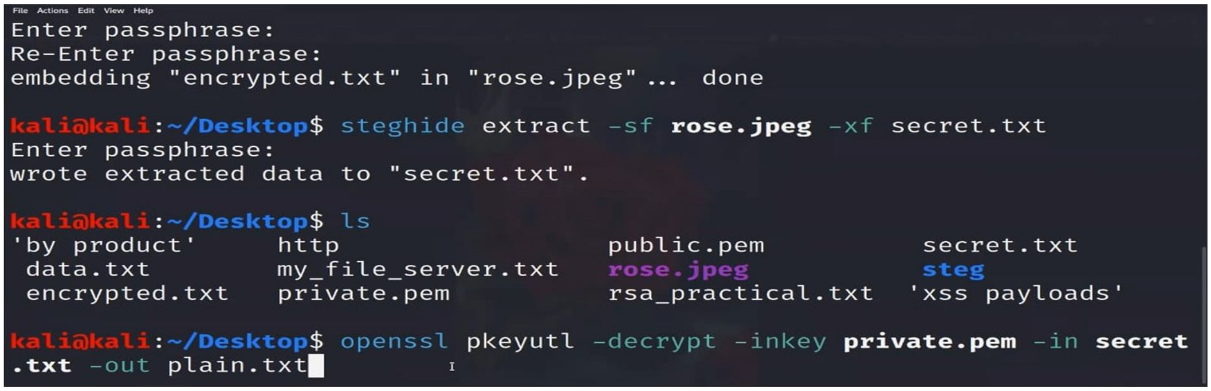
Step 4: for encrypting data or plain text give command as given below in terminal

/////////////

Opensslpkeyutl -decrypt -inkeyprivate.pem -in secret.txt (name of data file) -out plain.txt (fig.11)

I. Advantage and disadvantage of cryptography

Its advantage includes security of data but require tedious process and maintenance.



```
Enter passphrase:
Re-Enter passphrase:
embedding "encrypted.txt" in "rose.jpeg"... done

kali@kali:~/Desktop$ steghide extract -sf rose.jpeg -xf secret.txt
Enter passphrase:
wrote extracted data to "secret.txt".

kali@kali:~/Desktop$ ls
'by product'      http                  public.pem          secret.txt
 data.txt         my_file_server.txt    rose.jpeg           steg
 encrypted.txt    private.pem           rsa_practical.txt  'xss payloads'

kali@kali:~/Desktop$ openssl pkeyutl -decrypt -inkey private.pem -in secret
.txt -out plain.txt
```

Encryption and decryption is deep planned mechanisms so harder to crack it, but it is time consuming process.

Public and private key in symmetric and asymmetric cryptography is good locking system, but still it's require to protect from MAN IN MIDDLE ATTACK.

Hashing and mathematical algorithm make data unreadable but many sites are available and various commands in CLI will able encapsulate data.

Only text file are encrypted or hidden, video, graphic and audio require some alternate option.

1) Steganography to overcome drawback

In this technique encrypted data can also be hidden inside image file so it can overcome MAN IN MIDDLE ATTACK.

Steg file provide secret code foe encapsulating data present in file.

Steganography can be used to hide every form of data including text, video, audio, image, etc.

REFERENCES

[1] NIST – national institute of standardization and technology
[2] CPD online college (Evie Be)
[3] DNV - three pillar approach to cybersecurity
[4] RiskXchange– data security sensitive data
[5] BMC - Chrissy Kidd
[6] National security agency – quantum cryptography
[7] Institute of electrical and electronic engineering – cryptography using artificial intelligence
[8] Nist– blockchain overview