Steganography for Communication of Secure Data

Minal Aggarwal [1], Ishan Mehndiratta [1], Dr. Deepak Chahal[2]

[1]MCA Student, [2]Professor,

[1,2] Department of IT, Jagan Institute of Management Studies, Sector-05, Rohini, New Delhi, India.

Abstract

Nowadays, digital communication is used frequently and effective ways of data hiding are in need. One of the method of securing the data communication is Steganography. Steganography is method of concealing an image, audio, video or a message into another image, audio, video or a message. Dual Steganography is a technique which provides two level data hiding.

Keywords: *Data Hiding, Steganography, Dual Steganography, Cryptography, Steganography.*

Introduction:

As in ancient times during the wars, people used to send many secret messages. Slowly with time highly secure data is becoming a priority these days. So new methods for securing the data in need of the hour. Data transmission need major security in fielding of online banking, artificial intelligence companies, militaries, online companies and data privacy. Day by day increasing usage of the internet and mobiles where people keep their data online. Security of the data while storing and transmission is becoming important and methods like water marking, cryptography and steganography used for the same. Integrity of data refers to protecting information from falsely being modified by an unauthorized party. Information is valuable only if it is correct, tampered information could prove costly to both the sender and the receiver party [1].
Steganography is basically known as "cover writing". Steganography is technique of invisible data communication while hiding the private data within a normal looking cover.

The word steganography is derived from a Latin word *"steganographia"* which a combination of Greek words *"steganos"* means "covering" and "-graphia" means written text. Steganography is not same is cryptography, it is bit different.
As steganography focuses on concealing both the message and the fact that a secret message is sent, whereas cryptography is used only to protect the message content.

Steganography can be of various types: -
1) Text Steganography 2) Image Steganography 3) Video steganography 4) Audio steganography

- Text Steganography: - It is technique of hiding the data in text and various methods of this basic steganography are statistical and random generation of data and format based method.
- Image Steganography:-Images in steganography is used as covers .Various image steganography techniques are spread spectrum, masking technique, spatial domain method.
- Video Steganography: - Videos are basically combination of audios and various images in which data hiding is done in distortions and can be a large amount of data too. These distortions can easily get unobserved by humans because of continuous playing.
- Audio Steganography: - This method uses the scientific masking method of Human Auditory System (HAS). It is basically a masking property that renders a weak tone in the high and strong tone so there is just a little change in binary sequence of the audio file.

Steganography Vs Cryptography:

- In steganography, as there is way too much important and sensitive data, so hiding data with encryption is better approach. Whereas in cryptography the encrypted file or packets and easier to be marked and identify.

- Steganography is basically a "cover writing", whereas cryptography is more of "writing secretly".
- Steganography used the key for data securing, whereas cryptography doesn't have any specific methods like that.
- Steganography can be done on various types of files like images, audios, videos, whereas cryptography can be done on only the text files.
- Steganography is not practiced frequently as compared to the technique of cryptography.
- Steganography is basically used for achieving more secure and less detectable transition whereas cryptography is used to make a message in displaced form which can be read be the receive not the others.
- Steganography implicate factors like authentication and confidentiality, whereas cryptography imposes the factors like integrity, authentication and confidentiality and also non-repudiation.
- Various techniques for steganography are spatial domain, transform domain, distortion,and whereas in cryptography the techniques followed were asymmetric and symmetric key encryption.
- In steganography the hidden file which contains the data is not visible to the intruder whereas, in cryptography the intruder cannot understand the message which is encryption without the decrypting key.

Steganography Software:

- Various software are available like
  Xiao Steganography, StegHide, Crypture,
  SSuite Picsel, OpenStego, Hide'N'Seek.
- These type of steganography can be used to apply various types of functions that helps in hiding of the data which includes:-
  - Encoding of the actual data and hiding it in another file.
  - Keeping the tabs on the bits which carries the encoded data.
  - Encryption of the data bits that has to be hidden.
  - Also, extracting the data at the receiver's end.
- OpenStego is an open source used for steganography. It basically provides mainly 2 functionalities like:-
  - Data hiding:- It is method of hiding data into the image which acts as a cover.
  - Watermarking:- It is a method where the images have invisible signature which is used to identify the data stealing.
- Also, Xiao Steganography is used to hide the data in files like BMP images. It is a free Windows software. This software works as:-
  - Choose the file image file which is a cover file.
  - Then again choose the file that contain the information that need secrecy.
  - Then you can impose may advance features like password or editing the algorithm.
  - At the receiver's end the software should be installed also for to read that secured message.
- Crypture is a command like tool used for steganography. It accepts the BMP files as the cover file but there is a restriction that it has to be 8 times larger than the file containing the secret data.

Some Techniques of Image Steganography:

- Spatial Domain Technique:
  - It type of technique is also known to be as "substitution technique".

- It mostly works on the HVS (Human Visual System), where the changes are done on the bits of the cover image which most likely to be ignored according to the HVS.
- The data is mostly hidden in the LSB (least signifi9cant bits) of the image.
- The advantage of using the LSBs is that those bit become the random noise in the cover image and get unnoticed even when changes are made in image.

Fig 1 :-Spatial Domain Technique

- Transform Domain Technique:
  - It is technique of embedding data in the frequency domain of the signal.
  - These techniques are better the techniques using LSBs as the secure data is hidden at the parts of image where data compression, processing or cropping doesn't affect much.
  - Some Transform domain techniques are: -
    - JPEG compression
    - JPEG steganography
    - Wavelet transform technique

- Distortion
  - In this technique of steganography the "stego-object" is created using the sequences of the changes done in the cover image.
  - That sequence of the modifications are stored in the signal distortion.
  - Also the original cover image and to be stored with the distorted image, then only at the decoder's end, the difference can be tell in both the images to find the secret message.

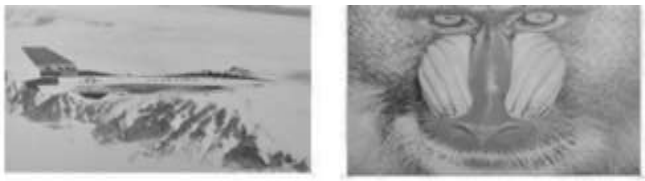
  Figure 3: there is an original image at the left corner and the image on right is image after distortion technique is applied on it. A focus is made on machines as machines cannot be understood by verbal communication it forms abstractions and concepts [2].

Dual Steganography:

Dual steganography is method of combining both steganography and cryptography. It is basically embedding of cryptography in the process of steganography. This method works embedding secret message in a cover first and then again embedding the stereographed-cover object in another object medium.

Dual Image Steganography Method in detail:

In dual steganography, the image steganography is demand over the internet. Method is following into 2 phases one is Data Hiding at sender level and another is Data Abstraction at receiver's level



(a) Mig (b) Atelidae

Table 1: DCT Transform Technique

COVER IMAGE	PSNR(db)	MSE(db)
MIG	55.6473	.420896
ATELIDAE	58.3766	.30740

Fig 2 : Transform Domain Technique.

1. **Data Hiding:**Taking 2 cover images and following the steps as follows
    1. Take the cover image 1 as cover object and dividing into planes.
    2. Secret Message is converted into the binary format.
    3. Storing the upper values in green planes and lower values in red planes.
    4. Assigning the stego key and storing in blue planes.
    5. Combing the planes of cover image1.
    6. Then embedding the cover image 1 is secret message in cover image 2 using above steps, which generates the end stego object.

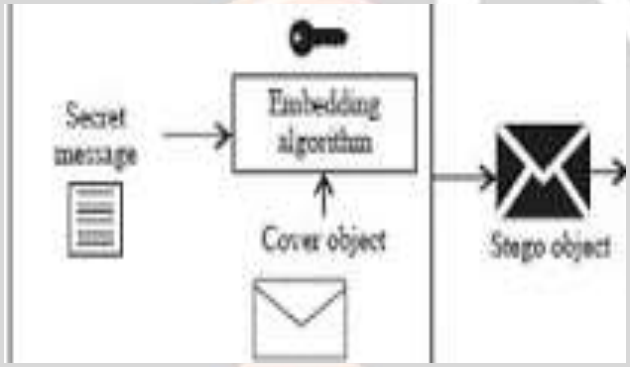


Fig 3 : Data Hiding At The Sender's End.

2. **Data Abstraction:** At the receiver end the stego image is taken and following steps are performed
    1. Take the stego image and diving into planes.
    2. The stego key act as passwordand verified with the stored key present in blue planes of cover image 2.
    3. If the key matches the upper and lower values obtained binary format of the cover image 2.
    4. Then the upper and lower values of cover image 1 is obtained to get the secret data message from cover image.

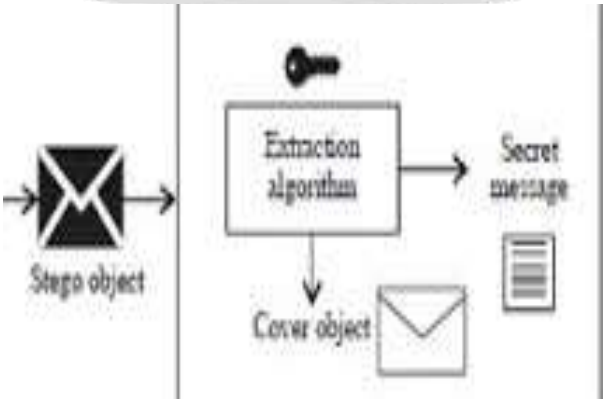


Fig 4: Data Abstraction At The Receiver's End.

Conclusion

In this paper, a brief explanation about the steganography is all about, comparing it with cryptography technique that how both are different. Also, some commonly software that are used in this technique of securing the data communication are there, some of the steganography techniques have been discussed also.

References

[1] Y. et al. A Survey on Cryptography, Encryption and Compression Techniques, International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 11 | Nov 2019.

[2] Kharb L.et al (2019) "Brain Emulation Machine Model for Communication" in International Journal of Scientific & Technology Research (IJSTR). pp 1410-1418.