Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 6, 2021, Pages. 2144-2159
Received 25 April 2021; Accepted 08 May 2021.

Types of Steganography for Secure Data Maintenance

Farhana Begum[1], Girija Rani Suthoju[2]

[1]Department of Information Technology, Vardhaman College of Engineering, Hyderabad, TS, INDIA,
farhanasattar@gmail.com
[2]Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation,
Hyderabad, TS, INDIA.
girijaranis@gmail.com

Abstract

The term steganography is derived from Greek words, where, Stegano(means hiding) and graph (means write).Steganography is a methodology used to encode one secret information into other information, in simple terms it is enclosed by the other messages. It helps to hide private information inside text, audio, image or video. Here, we will discuss various types of Steganography techniques. Steganography is suited to secure the data. In Cryptography, sender encode the information by using encryption key and send it to receiver, if receiver know the key then only it can decrypt the message, whereas Steganography will hide the presence of the communication.

Keywords: Steganography, Data Hiding, Cryptography, secret, information, encrypt*;*

1. INTRODUCTION

Now a days, the communication becomes an essential part of day to day life. We always want to secure the information while sharing that can be done by Steganography and Cryptography, where as in Cryptography sender encrypt the data with an encryption key and send it to intended receiver, if receiver knows the key then only it can decrypt the message, Steganography will hide the alive of communication. To deal with cryptographic techniques, steganography approach came into existence. Thus, Steganography hides the extant of data. So that someone can't detect its presence. In Steganography the procedure of hiding message content inside any multimedia data such as image, audio, video is referred as an Embedding. Steganography used in many applications, such as secure transmission of data between international and national governments, military, online banking security and intelligent agencies security and defense organizations.

BASIC TERMINOLOGIES

Message: The Secret message which has to be sent.

Cover-object: It is an object in which data is to be hidden. It would be image, audio and video

Stego-object: The object which carrying the secret message is known.

Stego-key: Encryption and Decryption can be done with the help of key.

Embedding algorithm: To hide the message in the cover, algorithm is used.

Extracting algorithm: An Algorithm which used to uncover the message from the stego object

Basically Steganography (figure 1) are divided into four types

I) Text Steganography

II) Image Steganography

III) Audio Steganography

IV) Video Steganography

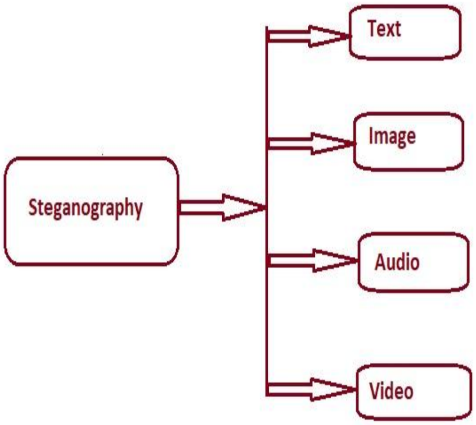


Figure. 1 Types of Steganography

TEXT STEGANOGRAPHY

Basically text steganography means data/message is hidden in text file as shown figure 2. It starts by a secret message in the cover text to create the stego key by applying the embedding algorithm. The stego key will be sent to the communication channel followed by the receiver in order to recover the secrets sent by the sender, the receiver should applied a recovery algorithm which are the parameters by the stego key to extract messages.

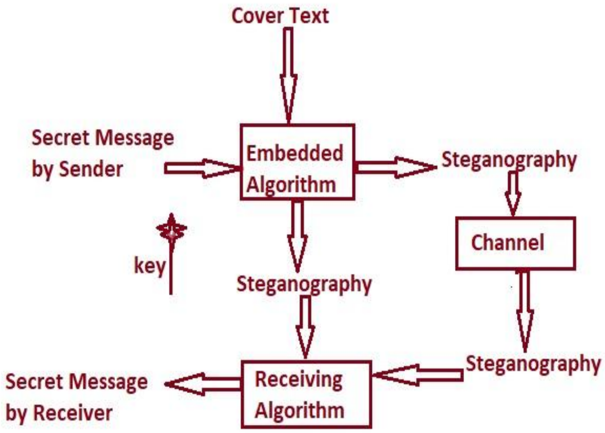


Figure. 2 Text Stego

Text steganography is classified into three types as shown in below figure 3..

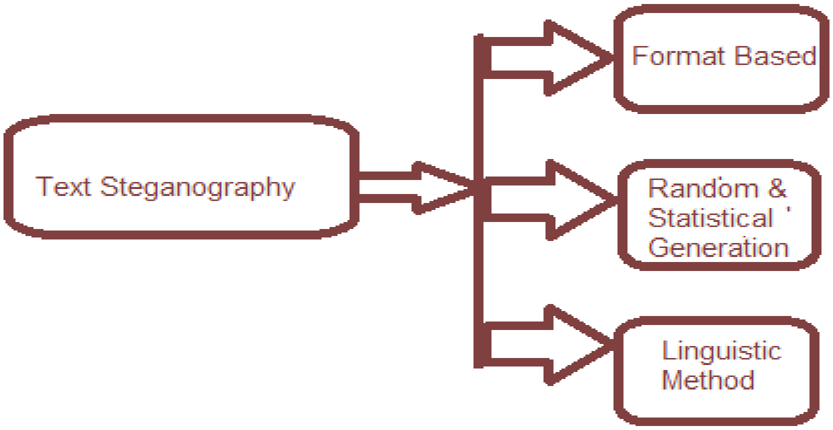


Figure. 3 Types of Text Steganography

A) Format Based Methods

This method succor to modify existing textby resizing the font size, inserting spaces between words or end of sentences or misspellings deliberately.

B) Linguistic Methods

In these methods, the syntax, and semantics are placed in order to hide the information. In syntactic methods, the punctuation marks like full stops or commas are used to hide the data.

It is part of information hiding which succor to hide secret messages by using written natural language.

C) Random and Statistical Generation method

In this method, it randomly change the order of character, if anyone intrudes the sequence message of the message will be displayed randomly. Another approach is statistical generation in which information is hidden in word order, for the purpose of encoding dictionary items are utilized.

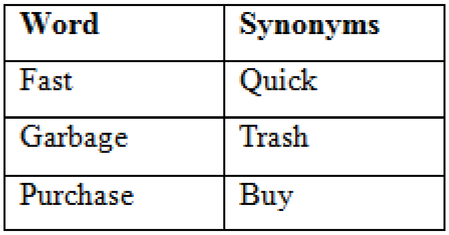
Text Steganography Methods

Line Shifting: It is used to shift the bits of the text vertically to encode the information

Word Shifting: It is used to shift the bits of the text horizontally to encode the information

Syntactic Technique: In this technique, changing punctuation as point (.) and comma (,) in the proper position to hide the information.

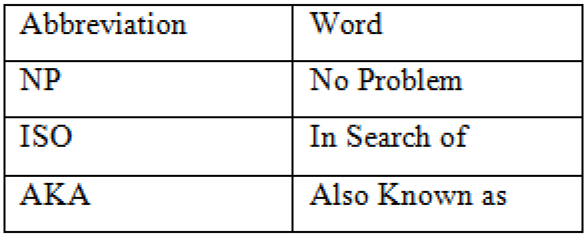
Semantic Technique: In this method message is hidden in synonyms/antonyms that exist in the document as shown in table 1.



Word	Synonyms
Fast	Quick
Garbage	Trash
Purchase	Buy

Table. 1 Semantic based hiding.

Abbreviation based hiding: This method is used to hide message in abbreviations as shown in Table 2..



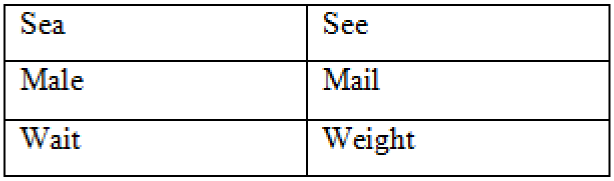
Abbreviation	Word
NP	No Problem
ISO	In Search of
AKA	Also Known as

Table. 2 Abbreviation based hiding.

White Spaces Hiding: In this Methods white space are used to hide the information because white space is usually ignored and if this method is used in huge amount of text would be very space consuming, there may be hidden information in white row.

Hiding data in paragraph: It is a method, message will be hidden at the beginning and ending Letters

Change of spelling: This method is applied to encode private messages in text format, and then embedded by describing alike but different words in spelling as shown in Table 3.



Sea	See
Male	Mail
Wait	Weight

Table. 3 Change of spelling

Feature coding: This method is used to change text feature, like text colour, text font.

2. IMAGE STEGANOGRAPHY

In this strategy, secret data could be enclosed in an image so that no one can identify hidden message and it is most widely used techniques. In this method, message is append at the border of the image. If the image is viewed in image viewer application, hidden message is ignored and message can be read if the image is viewed in the text editor.

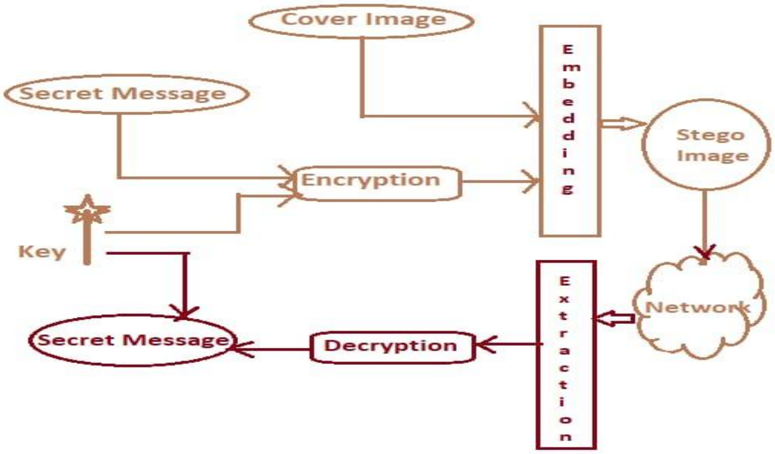


Figure. 4 Image Steganography

Image Steganography techniques broadly divided into two types

A) Spatial Domain Techniques

LSB Substitution Method

In this method, information is hidden in images Least Significant Bit (LSB) in this each byte of the eight bit will changed the secret message by one bit .

Optimum Pixel Adjustment Procedure:

In this approach, the stego image quality is improved without effecting the secret information, then it will be hidden the pixel value is adjusted in Optimal Pixel Adjustment Procedure (OPAP).

Inverted Pattern Approach (IP)

In this method, first it determines whether inverted or not inverted then enclosed each section of secret image.

IP method Using Relative Entropy:

In this method, instead of finding the mean square error,relative entropy is calculated for inverted pattern.

The proposed Hiding Streams of 1s and 0s

For hiding data this method uses alternatively 1s or 0s presence where the hidden data is convert into binary. The events of 1s and 0s are calculated and placed in the pel of the cover image, odd columns of the pixel represents occurrence of 1s and even columns represents occurrence of 0s.

Pixels Value Differencing (PVD)

This method provide a high quality stego image due to the number of inject bits is dependent on whether the pixel has edge area or smooth area. The difference between the adjacent pixels is less in smooth area and more in edge area.

The proposed mod method

This method provide high embedding capacity in which embedding is done by subtracting any remainder obtained from dividing with 10.

The proposed MOD10 based method

This technique, divide the gray value of pixel by 10, the remainder is obtained which depicts secret data. It determines whether the data is same as remainder or 10-remainder.

B) Frequency Domain Technique

Discrete Fourier transformation Technique (DFT)

This method is applied to each pixel value of spatial value f(x, y) for the image size M x N to get

Received 25 April 2021; Accepted 08 May 2021.

frequency component.

Discrete Cosine transformation technique (DCT)

This technique will convert a signal into elementary frequency components. It is mostly used in image compression.

Discrete Wavelet transformation technique (DWT)

In this technique wavelets are discretely sampled.

3. AUDIO STEGANOGRAPHY

Audio Steganography in secret information is enclosed in audio and robust in nature.

Working Flow of the System as shown in below figure. 5

Received 25 April 2021; Accepted 08 May 2021.

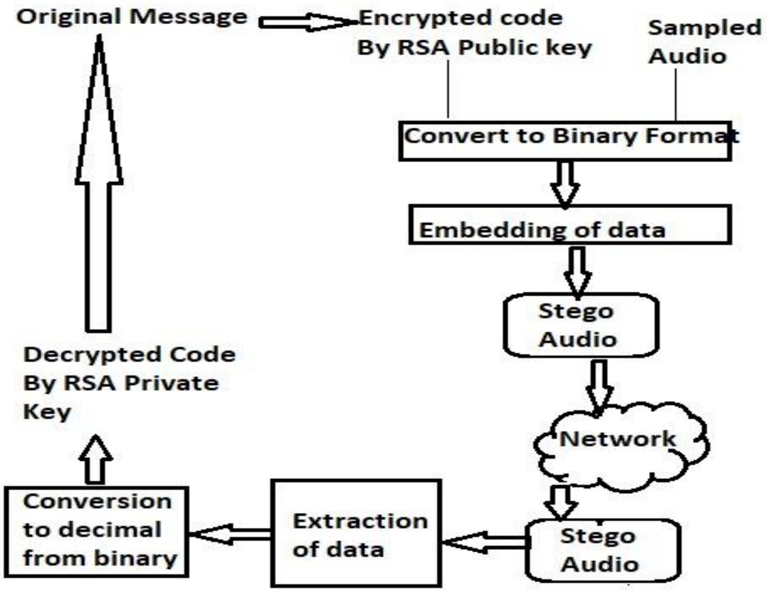


Figure. 5 Work Flow of the system

1) First take an audio file and then perform sampling on the file in eight bits per frame.

2) Give an input which we want to transmit as message file. Then applied encryption by using public key and RSA algorithm.

3) Then encrypted data will be covered in the audio file with the help of LSB algorithm for embedding. The above operations will be performed at the sender side.

4)After that,Stego audio is transferred to receiver.

5) For the extraction from the LSB algorithm, receiver will extract the encrypted data above steps are useful.

6) Then receiver will decryption the message with the help of private key.

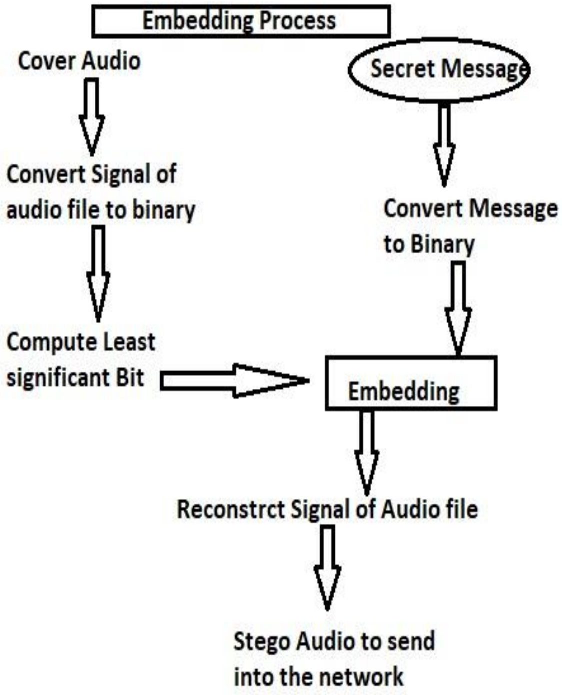

Embedding Process
Cover Audio
Secret Message
Convert Signal of audio file to binary
Convert Message to Binary
Compute Least significant Bit
Embedding
Reconstrct Signal of Audio file
Stego Audio to send into the network

Figure. 6 Steps in Data Embedding

Steps for Data Embedding as shown in figure 6.

1) Read the cover audio signal.

2) Convert audio signals into binary.

3) Use RSA algorithm to generate public and private key.

4) Then encrypt plaintext to produce cipher text by using public key

5) After that calculated LSB.

6) Convert message into a sequence of binary bits

7) Finally embed the message by using LSB algorithm.

8) Then reconstruct the audio signal known as Stego audio (Stego object)

Received 25 April 2021; Accepted 08 May 2021.

Steps for Data Extraction

1) Read the stego object (Audio File)

2) Convert audio signals into binary

3) Then calculated LSB.

4) Extract the cipher text from stego audio (Stego object).

5) Finally apply RSA algorithm for decryption by using private key to recover plaintext

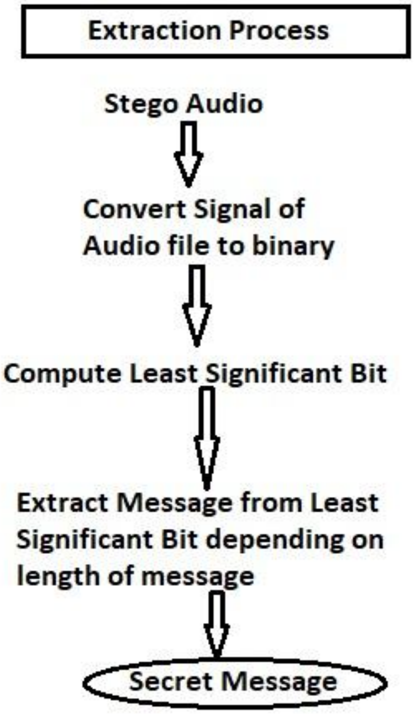

Extraction Process
Stego Audio
Convert Signal of Audio file to binary
Compute Least Significant Bit
Extract Message from Least Significant Bit depending on length of message
Secret Message

Figure. 7 Steps in Data Extraction

Audio Steganography Methods

Echo Hiding

Data is embedded into audio signal by adding a small echo to the hosting signal,

Phase Coding

In this sound phase components are not as detectable to the ear. It encodes the message bits, phase spectrum of a digital signal as phase shifts.

Parity Bit Coding

In this method it break a signal into different parts of samples and then encode the hidden message of each bit into a sample parts parity bit.

Spread Spectrum

This method is used to spread message bits over entire audio file.

Tone Insertion

In this techniques inaudibility of lower power tones in the existences of significantly higher ones.

4. VIDEO STEGANOGRAPHY

In Video Steganography secret message is hidden in a video file. It is more secure and capable in contrast to that of image steganography and main purpose is to enclosed large amount of data, and are filtering, cropping, rotation and compression. Video frames are in the form of images so image steganography is utilized on video frames. When audio is extracted from video files, it is similar to an audio file so audio steganography is utilized on audio files. The secret information cannot be detected by third party, hence the system is secure. Data security using video steganography which prohibit from any kind of hacking data. In AES algorithm,for encryption and decryption same key is used as shown in below figure 8.

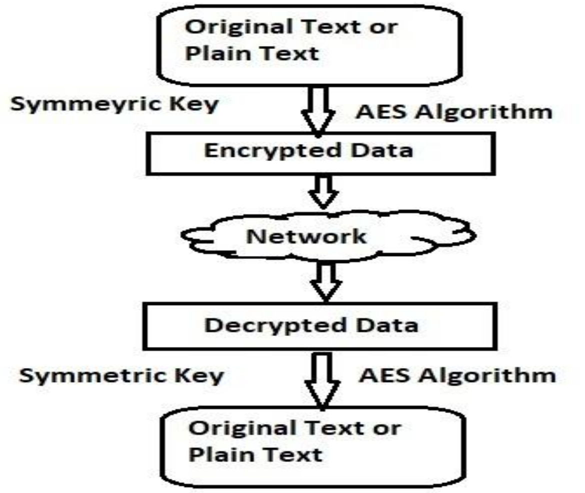


Figure. 8 AES algorithm

It is consist of two phases, one is extraction of video files and other is embedding of secret message as shown in figure 9.

Received 25 April 2021; Accepted 08 May 2021.

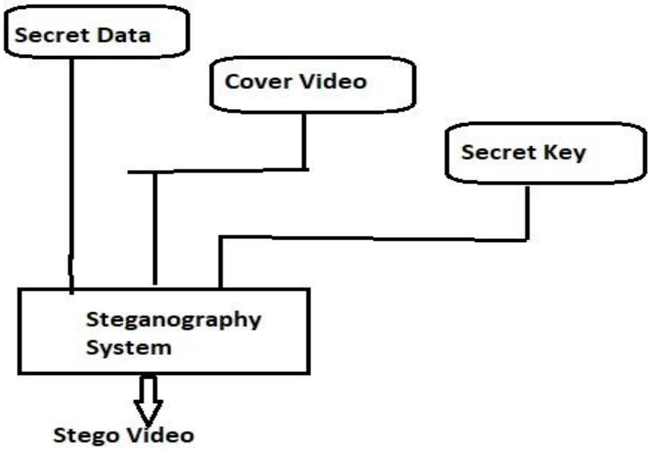


Figure. 9 Embedding Algorithm

Extraction

The taking out of video files is results in frames. Videos is consists of images and audio. So from videos file audio and images extracted.

5. CONCLUSION

Steganography is a method used to hiding the secret information, data can be covered in different forms like text, image, audio, video etc. Data hiding is very important for securing confidential data. This paper gives brief overview on types of steganography methods.

6. REFERENCES

1. Priya Pareek, N. Monica,"An Overview of Steganography: Data Hiding Technique", International Research Journal of Engineering and Technology (IRJET),ISSN: 2395-0056,Volume: 07 Issue: 01 | Jan 2020.

2. Namrata Singh, "Survey Paper on Steganography" ,International Refereed Journal of Engineering and Science (IRJES),ISSN 2319-183X,Volume 6, Issue 1 (January 2017), PP.68-71.

3. Fitra Chairil Akbar, Tito Waluyo Purboyo and Roswan Latuconsina, "A Study of Text Steganography Methods", Journal of Engineering and Applied Sciences 15 (2): 369-372, 2020, ISSN: 1816-949X,Medwell Journals, 2020.

4. Shivani Sharma, Dr. Avadhesh Gupta, Munesh Chandra Trivedi, Virendra Kumar Yadav, "Analysis of Different Text Steganography Techniques: A Survey", 2016 Second International Conference on Computational Intelligence & Communication Technology.

5. Bhinal Chauhan, Shubhangi Borikar, Shamali Aote, Prof. Veena Katankar,"A Survey on Image Cryptography Using Lightweight Encryption Algorithm".2018 IJSRSET | Volume 4 | Issue 4 | Online ISSN: 2394-4099. Themed Section: Engineering and Technology.

6.Deepali V. Patil, Mr. Shatendra Dubey,"REVIEW PAPER ON IMAGE STEGANOGRAPHY", International Journal Of Research In Computer Applications And Robotics,ISSN 2320-7345,Vol. 2, Issue 6,Pg:35-40 June 2014.

7.Mohammed A. Saleh," Image Steganography Techniques - A Review Paper", International Journal of Advanced Research in Computer and Communication Engineering , ISSN 2278-1021 ,Vol. 7, Issue 9, September 2018.

8. Rejoy Chakraborty and Arpan Roy,"Audio Steganography- A Review, International Journal of Trend in Research and Development, Volume 6(3), ISSN: 2394-9333.

9. Arfan Shaikh, Kirankumar Solanki, Vishal Uttekar, Neeraj Vishwakarma,"Audio Steganography and Security Using Cryptography", International Journal of Emerging

Technology and Advanced Engineering,ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 2, February 2014, 30014Vol.2 Issue.6, Pg.: 35-40

10. Ms. Pratidnya Sapate, Ms. Varsha Patil, Ms. Mayuri Pardeshi, Prof. Arjun Nichal, “A Review Paper on Video Steganography”, International Advanced Research Journal in Science, Engineering and Technology, ISSN 2394-1588,ISO 3297:2007 Certified Vol. 3, Issue 12, December 2016.

11. C. Ezhilarasi, R.Anitha,”Video Steganography and Security Cryptography”, International Journal of Linguistics and Computational Applications (IJLCA), ISSN 2394-6393 , Volume 4, Issue 4, October – December 2017.

7. AUTHORS

[1] Ms. FARHANA BEGUM, working as an Assistant professor in the Department of Information Technology at Vardhaman College of Engineering, Hyderabad. She worked as an Assistant Professor for 4years in Aurora’s Technological and Research Institute affiliated to Jawaharlal Nehru Technological University, Hyderabad. At present she is working in her area of research i.e., Cryptography and network security and also in Cyber security.

[2] Ms. GIRIJA RANI SUTHOJU pursuing Ph.D in the Department of Computer Science and Engineering at JNTU Hyderabad. She received Masters degree (M.Tech) in the Department of CSE at Aurora’s Technological and Research Institute belongs to JNTU, Hyderabad in 2014 and Bachelors degree (B.Tech) in the Department of Computer Science and Engineering from the same University in 2012. She worked as an Assistant Professor for 5years in Aurora’s Technological and Research Institute affiliated to Jawaharlal Nehru Technological University, Hyderabad. At present she is working in KLEF (K L deemed to be University) Hyderabad. Ms. Girija Rani Suthoju received Teaching Excellence award for best teaching thrice from 2016 to 2018. At present she is working in her area of research i.e., Cryptography and network security.