A Secure Image Steganography based on RSA Algorithm and Hash-LSB Technique

Ms.ShrideviShetti
IV SemM. Tech Digital communication Networking
T. John Institute of Technology
Bengaluru, India

Mrs.Anuja S
Assistant professor, Dept. of ECE
T. John Institute of Technology
Bengaluru, India

***Abstract* — Steganography is a method of hiding secret messages in a cover object while communication takes place between sender and receiver. Security of confidential information has always been a major issue from the past times to the present time. It has always been the interested topic for researchers to develop secure techniques to send data without revealing it to anyone other than the receiver. Therefore from time to time researchers have developed many techniques to fulfill secure transfer of data and steganography is one of them. In this paper we have proposed a new technique of image steganography i.e. Hash-LSB with RSA algorithm for providing more security to data as well as our data hiding method. The proposed technique uses a hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of the cover image. This technique makes sure that the message has been encrypted before hiding it into a cover image. If in any case the cipher text got revealed from the cover image, the intermediate person other than receiver can't access the message as it is in encrypted form.**

Keywords* — *Cryptography, Steganography, LSB, Hash-LSB, RSA Encryption –Decryption.

I. INTRODUCTION

The basic need of every growing area in today's world is communication. Everyone wants to keep the inside information of work to be secret and safe. We use many insecure pathways in our daily life for transferring and sharing information using internet or telephonically, but at a certain level it's not safe. Steganography and Cryptography are two methods which could be used to share information in a concealed manner. Cryptography includes modification of a message in a way which could be in digesting or encrypted form guarded by an encryption key which is known by sender and receiver only and without using encryption key the message couldn't be accessed. But in cryptography it's always clear to intermediate person that the message is in encrypted form, whereas in steganography the secret message is made to hide in cover image so that it couldn't be clearer to any intermediate person that whether there is any message hidden in the information being shared. The cover image containing the secret message is process and secret key provided by the sender.

A. Cryptography

The field of cryptography has a rich and important history, ranging from pen and paper methods, to specially built machines, to the mathematical functions that are used today. In this paper only brief discussion that is essential for knowledge transfer has been presented. Cryptology is the science of coding and decoding secret messages. (Cryptology is the Greek root for secret or hidden) [27]. It is usually divided into cryptography, which concerns designing cryptosystems for coding and decoding messages. It states that the term cryptography generally refers to the collection of cryptographic mechanisms that include:

- Encryption and decryption algorithms
- Integrity check functions
- Digital signature schemes

B. Steganography

Steganography is a technique used to transmit a secret message from a sender to a receiver in a way such that a potential intruder does not suspect the existence of the message. Generally this can be done by embedding the secret message within another digital medium such as text, image, audio or video. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphie meaning "writing" [2]. The first recorded use of the term was in 1499 by Johannes Trithemius in his Stegano-graphia, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other "cover-text" and, classically, the hidden message may be in invisible ink between the visible lines of a private letter. It is a high security technique for long data transmission. There are various methods of steganography:

- Least significant bit (LSB) method
- Transform domain techniques
- Statistical methods
- Distortion

II. PROBLEM STATEMENT

The problem statement consists of embedding the secret message in the LSB of each RGB pixels value of the cover image. Before embedding the secret message have to be converted to cipher text using RSA algorithm to enhance the secrecy of the message. In this approach we implemented a technique called Hash-LSB derived from LSB insertion on images. In this Hash-LSB, we are using a hash function to evaluate the positions where to hide the data bits or to be embedded. It is a challenging process which will lead us to combine the two technologies, one of them is RSA algorithm from cryptography and other is Hash-LSB from steganography. Our research has focused on providing a solution for transferring and sharing important data without any compromise in security. All the reputed organizations while sending business documents over the internet always use encryption of the data to protect leakage of information about their organization from their rivals or intruders. We have used Hash-LSB and RSA algorithm to create a secure steganography algorithm which is far more secure than many systems being used for the purpose of secretly sending the data.

A. Cover Image and Secret Message

In our proposed system, first of all we select a true color image of size 512 x 512 for to it as a cover image and a secret message which will be embedded in the cover image.

B. Related Work

Researchers have proposed various techniques to hide information in an image.

DeepeshRawat[1], has purposed improved LSB substitution method for hiding text information written in text file into color image. In this method each character of secret message including special character such as space, enter, <,?, $etc. is converted in ASCII code then each value is converted in 8 bit binary number. Each bit of each character is embedded in last LSB of each pixel of cover image. Since only last bit each pixel of cover image get changed, this method is capable of producing a secret-embedded image that is totally indistinguishable from the original image by the human eye.
M.Rajkamal[2],B.S.E. Zoraida[3], From day to day researchers have developed many other Techniques, such as The spatial domain based steganography technique use either the LSB or Bit Plane Complexity Segmentation (BPCS) algorithm The most widely used technique to hide data is the usage of the LSB . The existing techniques are mainly based on LSB (Least Significant Bit) where LSBs of the cover file are directly changed with message bits. A significant number of methods have been proposed for LSB steganography. Masud et al. has proposed a LSB technique for RGB true color image by enhancing the existing LSB substitution techniques to improve the security level of hidden information.

III. THE PROPOSED ALGORITHM

A. Hash-LSB (Least Significant Bit) Process

The Hash based Least Significant Bit (H-LSB) technique for steganography in which position of LSB for hiding the secret data is determined using hash function. Hash function finds the positions of least significant bit of each RGB pixel's and then message bits are embedded into these RGB pixel's independently. Then hash function returns hash values according to the least significant bits present in RGB pixel values. The cover image will be broken down or fragmented into RGB format. Then the Hash LSB technique will uses the values given by hash function to embed or conceal the data. In this technique the secret message is converted into binary form as binary bits; each 8 bits at a time are embedded in least significant bits of RGB pixel values of cover image in the order of 3, 3, and 2 respectively. According to this method 3 bits are embedded in red pixel LSB, 3 bits are embedded in green pixel LSB and 2 bits are embedded in blue pixel LSB as illustrated in Fig. 1. These 8 bits are inserted in this order because the chromatic influence of blue color to the human eye is more than red and green colors. Therefore the distribution pattern chooses the 2 bits to be hidden in blue pixel. Thus the quality of the image will be not sacrificed. Following formula is used to detect positions to hide data in LSB of each RGB pixels of the cover image [2].

$k = p \% n$ ……..…… (1) where, k is the LSB bit position within the pixel; p represents the position of each hidden image pixel and n is the number of bits of LSB which is 4 for the present case. After embedding the data in cover image, a stego image will be produced. The recipient of this image has to use the hash function again to extract the positions where the data has been stored. The extracted information will be in cipher text. After decryption of it, combining of bits into information will produce the secret message as required by the receiver.

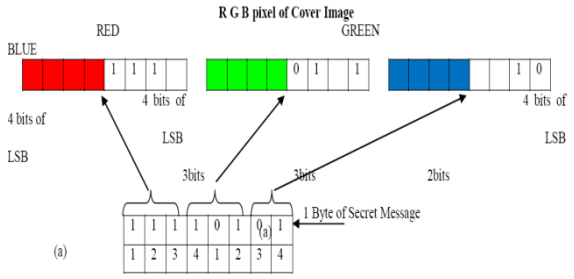


Fig 1.RGB pixel of cover image.

B. RSA Encryption and Hash-LSBEncoding

This approach of image steganography is using RSA encryption technique to encrypt the secret data. Encryption includes a message or a file encryption for converting it into the cipher text. Encryption process will use recipient public key to encrypt secret data. It provides security by converting secret data into a cipher text, which will be difficult for any intruder to decrypt it without the recipient private key. At the start of this process we take cipher text encrypted from the secret message to be embedded in the cover image. In this process first we converted cipher text into binary form to convert it into bits. Then by using hash function it will select the positions and then 8 bits of message at a time will be embedded in the order of 3, 3, and 2 in red, green and blue channel respectively. The process is continued till entire message of bits will got embedded into the cover image [2].

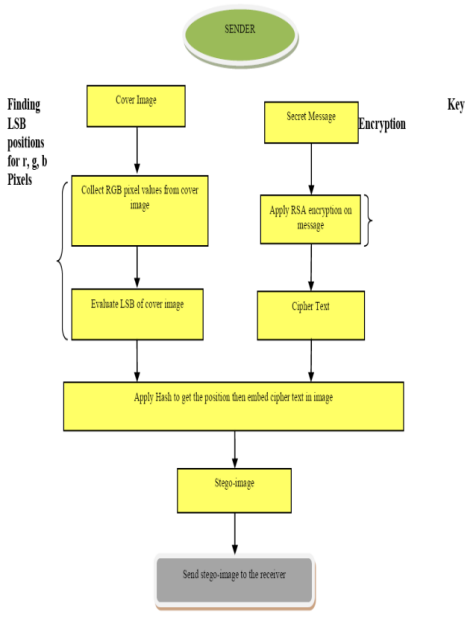


Fig 2.Encryption Flow Chart

Bedding Algorithm*:*

Step 1: Choose the cover image & secret message.

Step 2: Encrypt the message using RSA algorithm.

Step 3: Find 4 least significant bits of each RGB pixels from cover image.

Step 4: Apply a hash function on LSB of cover image to get the position.

Step 5: Embed eight bits of the encrypted message into 4 bits of LSB of RGB pixels of cover image in the order of 3, 3 and 2 respectively using the position obtained from hash function given in equation 1.

Step 6: Send stego image to receiver.

C. Hash-LSB Decoding and RSA Decryption

In the decoding process we have again used the hash function to detect the positions of the LSB's where the data bits had been embedded. When the position of the bits had been specified, the bits are then extracted from the position in the same order as they were embedded. At the end of this process we will get the message in binary form which again converted into decimal form, and with same process we got the cipher text message. After retrieving the positions of LSB's that contain secret data, the receiver will decrypt secret data using RSA algorithm. To apply RSA algorithm receiver will use his/her private key because the secret data have been encrypted by recipient public key. Using receiver private key cipher text will be converted into original message which is in readable form.

Retrieval Algorithm*:*

Step 1: Receive a stego image.

Step 2: Find 4 LSB bits of each RGB pixels from stego image.

Step 3: Apply hash function to get the position of LSB's

Step 4: Retrieve the bits using these positions in order of 3, 3, and 2 respectively.

Step 5: Apply RSA algorithm to decrypt the retrieved data.

Step 6: Finally read the secret message.

with hidden data.

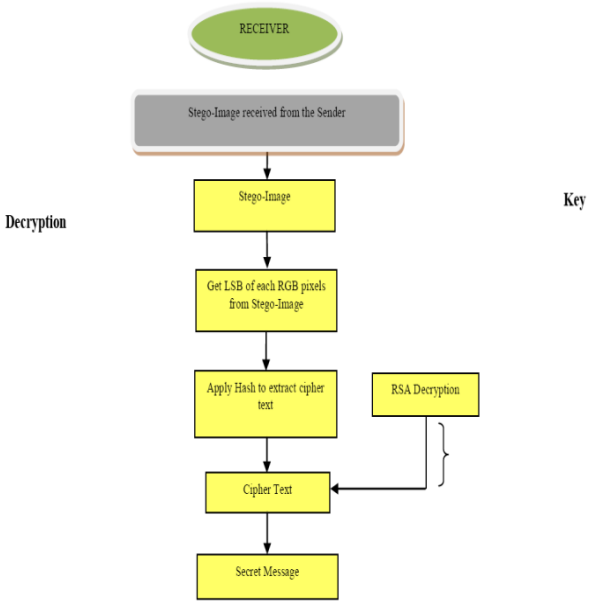


Fig 3.Decryption Flow Chart

IV. EXPERIMENTAL ANALYSIS

The objective of the work have been implemented an image steganography technique using Hash-LSB (Least Significant Bit) method with RSA algorithm to improve the security of the data hiding technique. The performance of the Hash-LSB technique has been evaluated and graphically represented on the basis of two measures are – Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) and obtained values are much better than existing techniques. The technique called "A Secure Steganography Based on RSA Algorithm and Hash-LSB Technique" has been implemented on MATLAB tool by analyzing four color images of size 512 x 512 tiff format as selected to hide a fixed size of secret data. In this process stego-image is generated using Hash-LSB and RSA encryption which carried out to enhance the security of hidden data. For the performance analysis of the Hash-LSB technique to be implemented on four cover images Barbara, Tulips, Lenna, and Baboon are considered.

The results for all stego images using Hash-LSB with RSA technique have been compared to simple LSB substitution with RSA technique which gives very lesser MSE values and higher PSNR values. The Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) [2] between the stego image and its corresponding cover image have been studied and given below as eq. 2 and 3.

$MSE=1H*WPi, -Si, Hi=12$ …….. (2) Where, MSE is Mean Square Error, H and W are height, width and P (i, j) which represents the cover image and S (i, j) represents its corresponding stego image.

(a) Barbara

(b) Tulips

(c) Lenna

(d) Baboon

Fig. (a)-(d) four cover images

$PSNR=10log\ 10\ L2MSE$ …….. (3) Where, PSNR is peak signal to noise ratio, L is peak signal level for a color image have been taken as 255. In this technique of image steganography eight bits of data are embedded in 3 pixels of the cover image. The mean square error (MSE) and the peak signal to noise ratio (PSNR) for different stego images are shown in the Table I. By comparing the PSNR values of all the stego images, it has been analyzed that only Lenna as a cover image have given the best PSNR value. The same is true in the case for the MSE values while comparing with different stego images, Lenna as a cover image have given the least MSE value.

The results for all stego images using Hash-LSB with RSA technique have been compared to simple LSB substitution with RSA technique which gives very lesser MSE values and higher PSNR values. The Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) [2] between the stego image and its corresponding cover image have been studied and given below as eq. 2 and 3.

$MSE=1H*WPi, -Si, Hi=12$ …….. (2)

Where, MSE is Mean Square Error, H and W are height, width and P (i, j) which represents the cover image and S (i, j) represents its corresponding stego image.

$PSNR=10log\ 10\ L2MSE$ …….. (3) Where, PSNR is peak signal to noise ratio, L is peak signal level for a color image have been taken as 255. In this technique of image steganography eight bits of data are embedded in 3 pixels of the cover image. The mean square error (MSE) and the peak signal to noise ratio (PSNR) for different stego images are shown in the Table I. By comparing the

PSNR values of all the stego images, it has been analyzed that only Lenna as a cover image have given the best PSNR value. The same is true in the case for the MSE values

while comparing with different stego images, Lenna as a cover image have given the least MSE value.

Table I: Results obtained from LSB withRSA and H-LSB with RSA Technique.

RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key. RSA algorithm itself is very secure that's why we used in this technique to increase the security of the secret message. A specified embedding technique uses hash function and also provide encryption of data uses RSA algorithm; makes our technique a very much usable and trustworthy to send information over any unsecure channel or internet. The H-LSB technique have been applied to .tiff images; however it can work with any other formats with minor procedural modification like for compressed images. Performance analysis of the developed technique have been evaluated by comparing it with simple LSB technique, which have resulted a very good MSE and PSNR values for the stego images. The future scope for the proposed method might be the development of an enhanced steganography that can have the authentication module along with encryption and decryption. Meanwhile the work can be enhanced for other data files like video, audio, text. Similarly the steganography technique can be developed for 3D images. The further work may contain combination of this method to message digesting algorithms.

Image 1: - cover image

Image 2: - stego-image

Image 1: - cover image
Image 2: - stego-image

PSNR between Image (1) and Image (2) = 76.5444
MSE between Image (1) and Image (2) = 0.0027

Name of the image file	Resultsobtained using LSB with RSA		Results obtained using Hash-LSB with RSA	
	PSNR(db)	MSE	PSNR(db)	MSE
Barbara	51.1655	0.4972	76.5444	0.0027
Lenna	51.0728	0.5097	75.0189	0.0024
Tulips	51.3453	0.4770	74.4220	0.0021
Baboon	51.1490	0.4991	73.9528	0.0021

Image 3: - cover image

Image 4: - stego-image

Image 3: - cover image
Image 4: - stego-image

PSNR between Image (3) and Image (4) = 75.0189
MSE between Image (3) and Image (4) = 0.0024

Image 5: - cover image

Image 6: - stego-image

Image 5: - cover image
Image 6: - stego-image

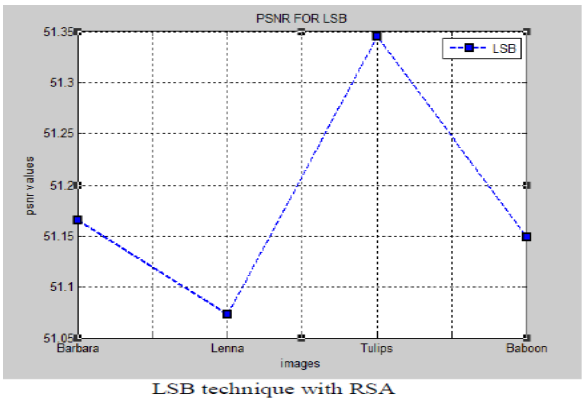
PSNR between Image (5) and Image (6) = 74.4220
MSE between Image (5) and Image (6) = 0.0021

Image 7: - cover image

Image 8: - stego-image

Image 7: - cover image
Image 8: - stego-image

PSNR between Image (7) and Image (8) = 73.9528
MSE between Image (7) and Image (8) = 0.0021



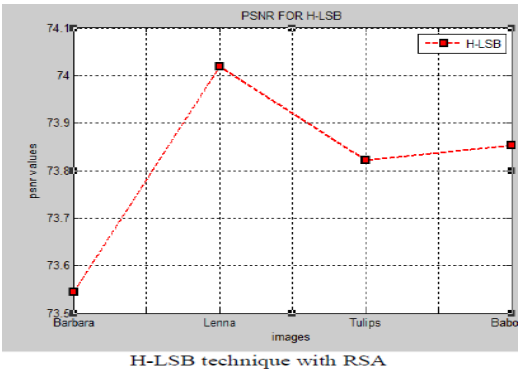
LSB technique with RSA

Fig.4(a) PSNR for LSB

In Fig. 4(a), the graphical representation of PSNR values of different stego images. The horizontal axis shows the stego images and vertical shows the range of PSNR value in decibel.

The Fig. 4 (a) the blue line shows the PSNR values of LSB with RSA technique and the Fig. 4(b) the red line shows the PSNR values of H-LSB with RSA. The PSNR values for LSB with RSA are lesser than the PSNR values of H-LSB with RSA as compared in both figures.

Fig. 4 (a) - (b) The graphical representation of PSNR values The MSE values for LSB with RSA are higher than the MSE values of H-LSB with RSA as compared in both figures.

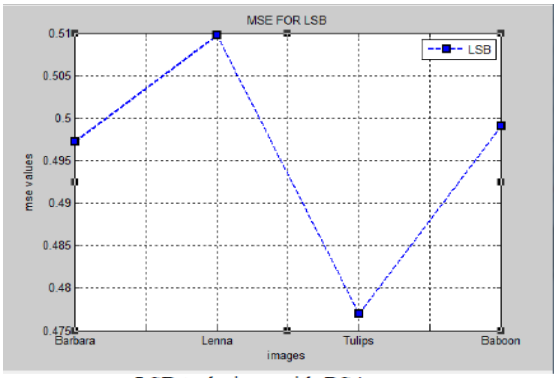


H-LSB technique with RSA

(b)

Fig 4(b). PSNR FOR H-LSB

In Fig. 5(), the graphical representation of MSE values of different stego images. The horizontal axis shows the stego images and vertical shows the range of MSE value. The Fig. 5 (a) the blue line shows the MSE values of LSB with RSA technique and the Fig. 5 (b) the red line shows the MSE values of H-LSB with RSA technique.



LSB technique with RSA

(a)

Fig.5(a) MSE for LSB

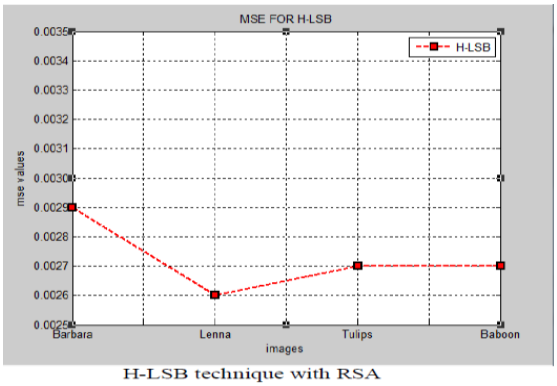


Fig.5(b) MSE for H-LSB

V. CONCLUSION

A secured Hash based LSB technique for image steganography has been implemented. A secured Hash based LSB technique for image steganography has been implemented. An efficient steganographic method for embedding secret messages into cover images without producing any major changes has been accomplished through Hash-LSB method.There is less chance for degradation of the original image. More information can be stored in an image.The future scope for the proposed method might be the development of an enhanced steganography that can have the authentication module along with encryption and decryption. Meanwhile the work can be enhanced for other data files like video, audio, text. Similarly the steganography technique can be developed for 3D images. The further work may contain combination of this method to message digesting algorithms.

ACKNOWLEDGMENT

The author would like to thank the staff and students of the Electronics and Communication Department, T. John Institute of Technology for their guidance and support during the course work.

REFERENCES

1. S. M. MasudKarim, Md. SaifurRahman, Md.Ismail Hossain "*A New Approach for LSB Based Image Steganography using Secret Key*", International Conference on Computer and Information Technology (ICCIT), Pages No. 286 – 291, 22-24 Dec., 2011.
2. DeepeshRawat, VijayaBhandari, "*A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image*", International Journal of Computer Applications, Vol. 64, Issue No. 20, Feb., 2013.
3. Swati Tiwari, R. P. Mahajan, "*A Secure Image Based Steganographic Model Using RSA Algorithm and LSB Insertion*", International Journal of Electronics Communication and Computer Engineering (IJECCE), Vol. 3, Issue No. 1, 2012.
4. N. F. Johnson, S. Jajodia, "*Steganography: seeing the unseen*", IEEE Computer, Vol. 31, Issue No. 2, Pages No. 26 - 34, Feb., 1998.
5. WeiqiLuo, Fangjun Huang, Jiwu Huang, "*Edge Adaptive Image Steganography Based on LSB Matching Revisited*", IEEE Transactions on Information Forensics and Security, Vol. 5, Issue No. 2, Pages No. 201 – 214, June, 2010.
6. Ross J. Anderson, Fabien A. P. Petitcolas, "*On the Limits of Steganography*", IEEE Journal on Selected Areas in Communications, Vol. 16, Issue No. 4, Pages No. 474 – 481, May, 1998.
7. Min-Wen Chao, Chao-hung Lin, Cheng-Wei Yu, Tong-Yee Lee, "*A High Capacity 3D Steganography Algorithm*", IEEE Transactions on Visualization and Computer Graphics,Vol. 15, Issue No. 2, Pages No. 274 – 284, March-April, 2009.
8. Nicholas Hopper, Luis von Ahn, John Langford, "*Provably Secure Steganography*", IEEE Transactions onComputers, Vol. 58, Issue No. 5, Pages No. 662 – 676, May, 2009.
9. Mohammad TanvirParvez, Adnan Abdul-Aziz Gutub, "*RGB Intensity BasedVariable-Bits Image Steganography*", Asia-Pacific ServicesComputing Conference, IEEE, Pages No. 1322 – 1327, 9-12 Dec., 2008.
10. Jing-Ming Guo, Thanh-Nam Le, "*Secret Communication Using JPEG Double Compression*", Signal Processing Letters, IEEE, Vol. 17, Issue No. 10, Pages No. 879 – 882, Oct., 2010.
11. KousikDasgupta, J. K. Mandal, ParamarthaDutta, "*Hash Based Least Significant Bit Technique for Video Steganography (HLSB)*", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, Issue No. 2, April, 2012.
12. AnkitChaudhary, J. Vasavada, J. L. Raheja, S. Kumar, M. Sharma, "*A Hash based Approach for Secure Keyless Steganography in Lossless RGB Images*", 22nd International Conference on Computer Graphics and Vision, 2012.

AUTHOR PROFILE

Ms.Shreedevi Sis pursuing M.Tech degree in Digital Communication & Networking in T. John Institute of Technology, Bengaluru from Visvesvaraya Technological University. Her research interests include Communication and networking, Information security and Network Security.

Mrs.Anuja Sis currently working as an Assistant Prof. at T. John Institute of Technology, Bengaluru. Her research interest includes Network security, Digital signal processing.