International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

RS and OFDM Methods Over Encrypted and Data Embedded Video Streams

Jithya J. Prakash[1], Hemand E. P.[2]

[1, 2]Department of Computer Science and Engineering, KMCT College of Engineering, Calicut, India

Abstract: ***Data hiding techniques are usually used in image processing. It is used to embed a secret message into a image for ensuring privacy. Data hiding can also be applied to videos. So the confidentiality of the image, video and embedded data is maintained. Sometimes digital video needs to be processed in an encrypted format to maintain security and privacy. For the purpose of content notation and/or tampering detection it is necessary to perform data hiding in these encrypted videos. There exist different techniques for hiding private data in videos. Several data hiding techniques in videos have been proposed. The data is embedded by using data hiding algorithm. This method preserves the exact data and video quality. There are some challenges while transmitting an encrypted video with hidden data from a sender to a receiver. At the time of transmission there is a chance of occurrence of errors in the content of video due to the presence of noise and by some other factors. Hence introduced a Reed Soloman error detection and correction method, which detect and correct the error. To improve the data rate through the channel an OFDM (Orthogonal Frequency Division Multiplexing) method is also proposed. These methods provide better efficiency, accuracy and performance.***

Keywords: Data Hiding, Reed Soloman Method, OFDM, Chien search Algorithm

1. Introduction

Image Processing is the Processing of images using mathematical operations by using any form of signal processing. An image is an array, or a matrix, of square pixels arranged in columns and rows. A pixel is the smallest unit of an image. The information like video, audio, images, and other multimedia, are being transmitted through the network. But there may occur privacy problems in the network. So data hiding techniques are usually used in image processing. Data Hiding is the process of secretly embedding information inside a data source without changing its perceptual quality. Data hiding can be done through different methods. Encryption is also an important part that provides security to confidential data. So, stegenography and cryptography are major areas which provide secure data transmission over internet. Stegenography provide more security compared to cryptography. Cryptography provide security only when the data transmitting. In the time of decryption there is no more protection left.

Cloud computing has become a popular technology, which can provide highly potent computation and huge storage solution for video data. The capability of performing data hiding is done in encrypted H.264/AVC video bitstreams [1] which would avoid the leakage of video information also can help to maintain security and privacy concerns with cloud computing.H.264/AVC video streams would avoid leakage of video content which can help address the security and privacy concerns with cloud computing.

The increasing demands of video data security and privacy protection, data hiding in encrypted videos will become popular. The video stream consist mainly three sensitive parts. The content owner encrypts the original video stream using advanced encryption standard algorithm. Then, the data hider (e.g., a cloud server) can embed the additional data into the encrypted video stream by using data hiding algorithm, without knowing the original video content. Hidden data can be extracted at the receiver end. The hidden data is extracted first and then decrypt the video. This encryption scheme provide security, efficiency, and format compliance. It encrypt the codeword of IPMs, the codeword of MVDs, and the codeword of residual coefficients [2] for the encryption of video. The method ensures the strict preservation of the exact data and video quality

There are some challenge while transmitting an encrypted video with hidden data from a sender to a receiver. At the time of transmission there is a chance of occuring errors in the content of video due to the presence of noise and by some other factors. So there is a great need of a error detection and correction method. Hence introduced a Reed Soloman error detection and correction method here. The data is sending through a single channel, the data rate is less. Low data rate makes some problems in receiver. So OFDM (Orthogonal Frequency Division Multiplexing) is used. OFDM is a special case of frequency division multiplexing. It is multi carrier system where data bits are encoded to multiple sub carriers, while being send simultaneously. There is an optimal usage of bandwidth. The primary advantage of OFDM over single-carrier schemes is its ability to cope with severe conditions.

2. Related Works

Many researches have been done in the area of data hiding and video encryption. In last few years various efficient methods have been proposed. Some of them are summarized here:

KokSheik Wong [3] proposes a novel data hiding method in the compressed video domain that safeguards the quality of the image of the host video whereas inlaying information into it. Mquant and quantized discrete cosine transform coefficients are the significant parts of MPEG and H.26x based compression standards and then information is embedded into a compressed video by simultaneously wielding Mquant and quantized discrete cosine transform

coefficients. This is a reversible method, where the original video is obtained by omitting the embedded information. Reverse Zerorun Length (RZL) is a new data representation scheme. It is proposed to exploit the statistics of macroblock in order to attain high embedding efficiency. Two independent solutions are proposed to suppress the bitstream size increment which is a problem caused by data embedding. An average increase of four bits in the video bitstream size is observed for every message bit embedded.

Here data hiding in compressed video domain mainly focuses on complete image quality preservation, reversibility, and efficient data representation scheme. Generally data hiding methods produce image/video of high quality but even then the image quality of the modified video is always lower than that of the original video. To solve this major drawback, novel data hiding method in the compressed video domain is proposed and it preserves the image quality. Video annotation is an important application of this method where high image quality and reversibility are greatly desired. Along with high quality video, advanced special functions for searching, playback control, and/or hyper linking with other media are provided.

Xinpeng Zhang [4] proposed schemes which focus on reversible data hiding technique in encrypted image**.** This include the following phases. Image encryption data embedding and data extraction/image recovery. the original image is encrypted by the content owner using an encryption key, and by using a data hiding key a data hider embeds additional data into the encrypted image, yet he does not know the original content. This is send to the receiver. It provide security to the image content. Receiver receives an encrypted image containing additional data, and may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data hiding key, with the aid of spatial correlation in natural image. The data hider segments the encrypted image into a number of non overlapping blocks and each block will be used to carry one additional bit. The least significant bits are used to carry the embedded data. The receiver may segment the decrypted image into blocks and divide the pixels in each block into two sets in a same way.

In this method even someone known the encryption key and can obtain a decrypted image and also detect the presence of hidden data, it is impossible to extract the additional data. That is this activity of data extraction is not separable from the activity of content decryption.

Shiguo Lian present [5] a video encryption and watermarking scheme based on H.264/AVC codec, it gives a remedy to the commutation of encryption and watermarking. This method embeds the watermark without exposing video content's confidentiality, Here the encryption and watermarking operations are commutative, there for the watermark can be extracted from the encrypted videos, and the encrypted videos can be re watermarked**.** In this scheme, whereas the amplitude of dc or ac is watermarked, the parameters like IPM, MVD and residue coefficient's sign are encrypted. the selected parameters are encrypted partially for reducing the computational cost. Here traditional watermark embedding method is modified. So the sign encryption and amplitude watermarking independent

This method has several components. They are the compression component, it includes intra prediction, inter prediction, variable length coding (VLC), etc. the encryption component includes IPM encryption, MVD encryption and residue encryption, and the watermarking component refers to residue watermarking. The independent keys are used to control the encryption process and watermarking process. The coefficients are selected carefully according to macro block type to provide robustness and imperceptibility. This method provides a secure video transmission or distribution between sender and receiver.

Xianfeng Zhao [6] proposed a method in which it reserving room before encryption with a traditional RDH algorithm. This helps the data hider to reversibly embed data in the encrypted image. The method provides real reversibility. This make data extraction and image recovery are free from error. The existing RDH techniques do not give real reversibility. In reversible data hiding method, the original content can be losslessly recovered after the embedded message is extracted. We can increase the rate of data to be hidden. This is useful in the way that these methods recovers the image with its original quality with improved PSNR ratio. Some of the previous methods may subject to some errors in data extraction and image recovery. And also the hackers can recover the embedded data from the original image easily because data is placed in particular bit position after image encryption. But the proposed RDH technique can take the advantage of all the traditional techniques.

Here the content owner first reserves sufficient space on original image and then by using the encryption key converts the image into its encrypted form. Now, the data embedding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previous emptied out. It separates data extraction from image decryption The data extraction and image recovery are identical to that of Framework VRAE. These techniques can only achieve small payloads or generate marked image with poor quality for large payload. To separate the data extraction from image decryption, he emptied out space for data embedding by compressing encrypted images. This technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed.

Wei Liu [7] propose an efficient way to compress encrypted images through resolution progressive compression (RPC). Which compresses an encrypted image progressively in resolution. This enables the decoder to observe a low resolution version of the image, study local statistics based on it, and use the statistics to decode the next resolution level. With the help of progressive decomposition and rate compatible punctured turbo codes, this technique provide a lossless compression method for encrypted gray image, which is achieved through Slepian Wolf coding. Resolution

progressive compression shows better coding efficiency and less computational complexity than existing techniques. At first encoder send a down sampled version of the ciphertext. The corresponding low resolution image is decoded and decrypted at the decoder and a higher resolution image is obtained by intraframe prediction. To decode the next resolution level the predicted image and the secret encryption key, is used as the side information (SI).This process is repeated until the whole image is decoded. The task of de correlating the pixels is not possible for the encoder, So by doing so it is shifted to the decoder side.

Wenjun Lu [8] proposed schemes which focus on the challenges in secure video processing. Video is different from text due to its large data volume and rich content diversity. A sequence of images possibly accompanied by audio information is generally considered as a video. The rich information contained in video and its temporal nature bring unique challenges in secure video processing This paper include video search, classification, and summarization User need to search his/her private database using video queries by keeping the query and database content secret from the server. To encrypt visual features or search indexes from images in a distance preserving fashion. It allows the server to compare the similarity between encrypted images and encrypted database without additional communication with the user. This can be effectively applied for video retrieval.

Based on literature survey, it has been found that most of the paper discus about the images. Providing security and data hiding technique in video are very rare. This project focuses on data hiding and security of videos. For finding the error in transmission channel due to noise interference is avoid by using a Reed Soloman error correction method. Also the transmission rate is increased by using an Orthogonal Frequency Division Multiplexing. The proposed project encryption and data embedding scheme also provide strict preservation of file-size, whereas the degradation in video quality caused by data hiding is quite small.

3. RS & OFDM for Data Hiding

The Proposed system deals with the secure and high data rate transmission of an encrypted video with hidden data. First step is to select a video to be transmit and encrypt its sensitive parts. That is only a fraction of video data is encrypted to improve the efficiency while still achieving adequate security. Encrypt both spatial information (IPM and residual data) and motion information (MVD) during encoding. In Intra Prediction mode and Motion Vector Difference the encryption is done by using advanced encryption standard algorithm. An encryption key is used there. Then data is embedded using data hiding algorithm and it also use a data hiding key.

The encrypted video with hidden data is transmitted from sender to receiver. Here data is send in binary format. Due to the interference of noise in the channel lead to error in the video content. A Reed Soloman error detection and correction method is used to detect and correct the errors. It is very powerful in correcting random error and bursty error

and ensures the error correction in digital communication systems. For increasing the data rate through the channel an orthogonal Frequency Division Multiplexing is used.

At the receiver side the hidden data can be extracted either in encrypted or decrypted domain. Data extraction process is fast and simple. In the encrypted domain the hidden data is extracted first and then decrypt the video stream. In the decrypted domain, first the video stream is decrypted and then from that the hidden data is extracted.

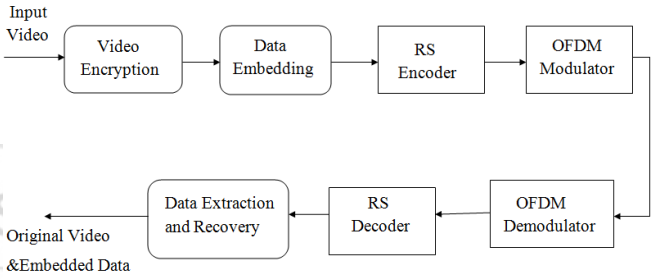


Figure 1: The Framework

The proposed scheme is the integration of video encryption and decryption, data embedding, Reed Soloman error correction technique and Orthogonal Frequency Division Multiplexing method. The content owner encrypts the video by encrypting its sensitive parts and data hider embeds a data on that. For avoiding the error due to interference of noise, an error detection and correction method is proposed. The introduced method is Reed Soloman error correction method. This RS method has a syndrom calculation block, a key equation solver block and a Chien search and error evaluation (CSEE) block. One more method is proposed to improve the data transmission rate through the channel. For that an Orthogonal Frequency Division Multiplexing is used.

3.1 Video Encryption

Advanced Encryption Standard (AES) is used for video encryption. Only a fraction of video data is encrypted to improve the efficiency. The spatial information (IPM and residual data) and motion information (MVD) are encrypted here. In AES, 128 bit is the input of each round. It is converted into 4x4 matrix by using S box method. Next step is shifting rows. There is no change in first row. In second row one step shift to left and the extra bit is placed to right. In third and fourth row shift two and three steps left respectively and extra bit is placed to right. After that by using mathematical functions change the column values and is not done in last round and in each round add the round key. Finally obtained the encrypted video.AES algorithm provides better security than other methods.

3.2 Data Embedding

Text data can embed on the encrypted video. The size of the embedded data depends on the size of input video. Here a data embedding algorithm is used. Initially select first

frame's first pixel and consider its RGB values and select one then clear its LSB bit and replace it with LSB bit of data these steps repeat until whole data is embedded, and rest of pixels are embedded with 0

3.3 Reed Solomon Encoder

Reed solomon error detection and correction method [9] ensures the error correction in digital communication system. When the encoder receives an information sequence, it creates encoded blocks consisting of $N = 2^m - 1$ symbols each. The encoder divides the information sequence into message blocks of $K = N-2T$ symbols. Each message block is equivalent to a message polynomial of degree $K-1$, denoted as $m(x)$.There is a parity generator and it generate a parity bit and add it with data. If the data is r (s), Then after added parity bit it will become r (s)+p (s).

3.4 OFDM Modulator

Orthogonal frequency-division multiplexing (OFDM) [10] is a method of digital modulation in which a signal is split into several narrowband channels at different frequencies. OFDM modulator receives the data with parity. At this level first a constellation mapping is applied on the input data to eliminate the phase error. This phase error is due to the transmission through different channels. The data is not transmitted at frequency domain. It is possible only in time domain. So for the conversion of frequency domain into time domain here an inverse fast Fourier transform is used. Then it is transferred to OFDM demodulator.

3.5 OFDM Demodulator

Here the reverse operation of OFDM modulator is takes place. First take the output received from OFDM modulator and then a fourier transform is applied on that wave for the conversion of time domain to frequency domain. After that Perform deconstellation mapping. While using OFDM the data transmission rate is improved and accurate result is obtained.

3.6 Reed Solomon Decoder

RS decoder consists a syndrom calculation block [11], a key equation solver block and a Chien search and error evaluation (CSEE) block. The syndrome calculation is the first step in the Reed-Solomon decoding process. This is done to detect if there are any errors in the received code word.

$$S_i = R(\alpha^i)$$
$$= R_{n-1}(\alpha^i)^{n-1} + R_{n-2}(\alpha^i)^{n-2} + \ldots + R_1\alpha^i + R_0$$

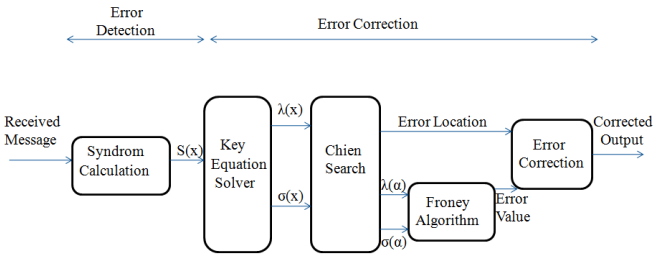


Figure 2: Reed Solomon Decoder

where the coefficients $R_{n-1}.... R_0$ are the symbols of the received code word. Since the code word is generated by multiplying with the generator polynomial, if the received code word is error free then its modulus with respect to the generator polynomial should evaluate to zero. Then the KES Block find error locator λ (x) and error evaluator polynomial σ (x), and it is fed into Chien search block and Forney algorithm block respectively. The Chien search block calculates the roots of the error locator polynomial. The Forney algorithm block calculates the magnitude of the error symbol at each error location.

$$\lambda(x) = x^t + \lambda_{t-1}x^{t-1} + \ldots + \lambda_0$$

$$\sigma(x) = S(x).\lambda(x) \bmod x^{2t}$$

$$y_i = x^{2t}\sigma(x) / x\,\lambda'(x)$$

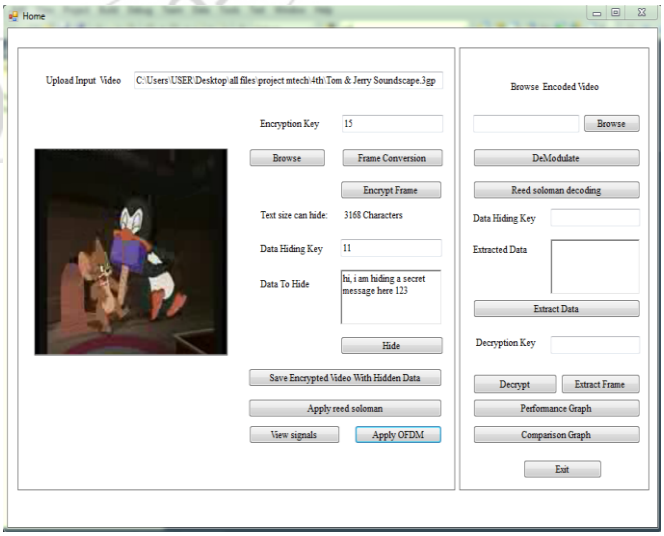
Then the error correction performed and an error free data is obtained.

3.7 Video Extraction and Recovery

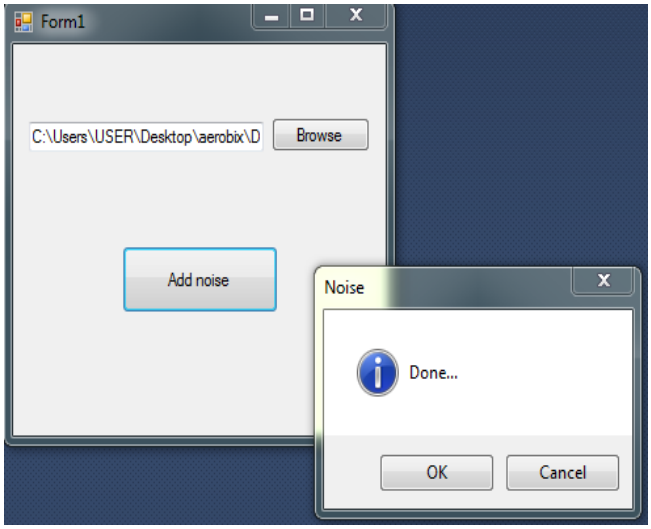
This is the final step. Here the video is decrypted by using a decryption key and after that the embedded data is extracted using data hiding key. Accurate data and video is obtained by using this system and it is a secure and efficient method.

4. Implementation and Analysis

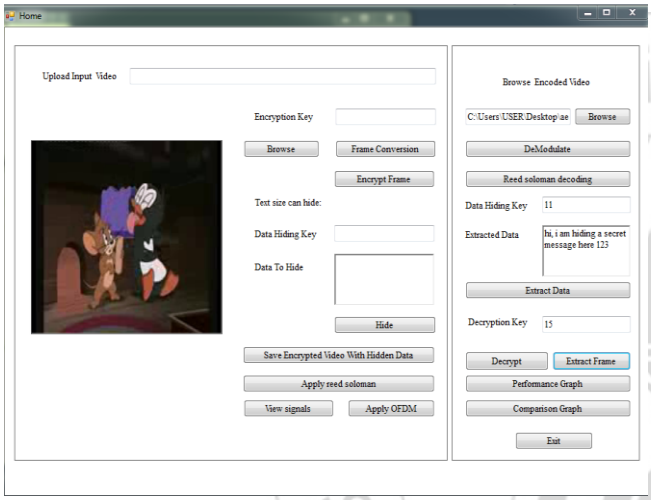
RS and OFDM with Data Hiding is implemented using ASP.Net. The proposed method is appropriate for all videos. Length of the video is very large it will take extra time, otherwise it is very fast and efficient method. The size of the embedded data is depending upon the size of input video. It will be shown in the screen before embedding data. This system support all video formats like 3gp, MP4, MP3 etc. The noise is added for showing the error detection and correction.



(a)



(b)



(c)

Figure 3: (a) Sender Side, (b) Adding Noise (c) Receiver Side

By comparing with the existing similar methodologies, the proposed system performs more efficiently. It results in good accuracy and has high performance.

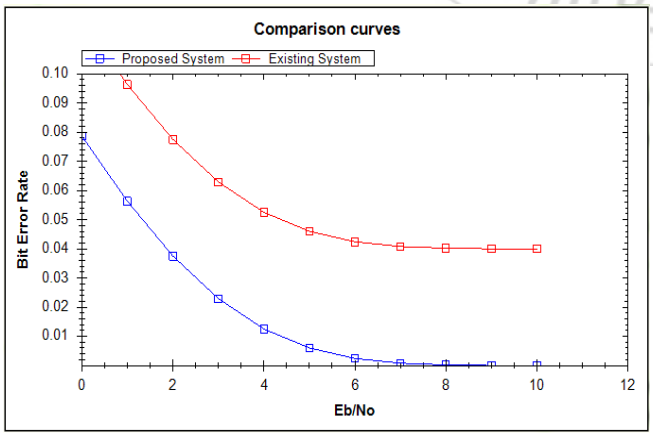


Figure 4: Comparison Graph

A comparison graph is plotted with Bit Error Rate against Signal to Noise Ratio. The proposed system is compared with other existing system. Finally the proposed method outperforms well. It has a reduced error rate compared with the other systems.

5. Conclusion

The paper proposes a novel data hiding scheme for encrypted video. This consist of video encryption, data embedding, video extraction and recovery, Reed Soloman error correction and OFDM methods. The video is encrypted by using advanced encryption standard and the data is embedded using a data hiding method. The Reed Soloman methods detect and correct all the errors, which are occurring at the transmission time. These errors are occurred due to the interference of noise. The OFDM method provide high data rate. All these provide a good transmission of videos with better efficiency and accuracy.

References

[1] Dawen Xu, Rangding Wang, and Yun Q. Shi, Fellow, IEEE "Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution", Vol. 9, No. 4, April 2014.
[2] S. G. Lian, Z. X. Liu, Z. Ren, and H. L. Wang, "Secure advanced video coding based on selective encryption algorithms, " IEEE Trans. Consumer electron., vol. 52, no. 2, pp. 621–629, May 2006.
[3] KokSheik Wong, Kiyoshi Tanaka, Koichi Takagi, and Yasuyuki Nakajima, "Complete Video Quality-Preserving Data Hiding, IEEE Ttanscations on circuits and system for video technology, Vol. 19, NO. 10, October 2009
[4] X. Zhang, "Reversible data hiding in encrypted images, " IEEE Signal Process. Lett., vol. 18 Apr. 2011.
[5] S. G. Lian, Z. X. Liu, and Z. Ren, "Commutative encryption and watermarking in video compression, " IEEE Trans. Circuits Syst. Video Technol., Jun. 2007
[6] Kede Ma, Wei. Zhang, Xianfeng Zhao, "Reversible data Hiding in Encrypted Images by reserving Room before encryption", IEEE trans.
[7] On information forensics and security, vol, 8 No.3, march 2013.
[8] Wei Liu, , Wenjun Zeng, Lina Dong, and Qiuming Yao, "Efficient Compression of Encrypted Grayscale Images", IEEE Ttanscations on image processing, Vol. 19, NO. 4, APRIL 2010
[9] W. J. Lu, A. Varna, and M. Wu, "Secure video processing: Problems and challenges, " in Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing, Prague, Czech Republic, May 2011, pp. 5856–5859.
[10] Sarwate, D.V., and Shanbhag, N.R.: 'High-speed architectures for Reed-Solomon decoders', IEEE Trans. Very Large Scale Integr. (VLSI) Syst., 2001, 9, (5), pp. 641–655
[11] Jinyong Lee, Jonghwa Lee, "Low-Complexity ICI Reduction Method for OFDM Systems With Large Subcarrier Numbers", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 64, NO. 8, AUGUST 2015
[12] Samir D.Mhaske, Dr.G.G.Sarate, "Design Of Area Efficient Reed Solomon Decoder", 2014 2nd International Conference on Devices, Circuits and

Systems (ICDCS)

Author Profile

Jithya J. Prakash is pursuing her M.Tech degree in Computer Science and Engineering from KMCT College of Engineering, Calicut University. She completed her B.Tech Degree in Information Technology from Cochin University College of Engineering, Kuttanad, in 2014

Hemand E.P is Assistant Professor, Department of Computer Science and Engineering, KMCT College of Engineering, Calicut University. He. Completed his B.Tech degree in Computer Science & Engineering from Government College of Engineering, Kannur in 2008..he obtained his M.Tech degree in Computer Network Engineering from RV College of Engineering, Bangalore in 2012.