International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 4 | May-Jun 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

Video Steganography Using Discrete Wavelet Transform and Artificial Intelligence

Shivani Gupta[1], Gargi Kalia[2], Preeti Sondhi[2]

[1]M.Tech Student, [2]Faculty
[1,2]Computer Science and Engineering, Universal Institution of Engineering & Technology, Lalru, Punjab, India

How to cite this paper: Shivani Gupta | Gargi Kalia | Preeti Sondhi "Video Steganography Using Discrete Wavelet Transform and Artificial Intelligence " Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.1210-1215, URL: https://www.ijtsrd.com/papers/ijtsrd25067.pdf

IJTSRD25067

ABSTRACT

Several developments in the transfer of data through the internet make it easier to transfer the data faster and accurately to the destination. But in this, anyone can misuse and modify the critical information through hacking. Video steganography is a technique which is used to hide the message and to transfer the message inside a video. Video is an application of many frames of audio, text, and images. The segmentation is known as the advanced technology that provides rich information of an image. The purpose of this paper is to propose a new technique to hide the data using video steganography with the help of artificial intelligence and DWT. This paper focuses on analyzing the various video steganography techniques which were proposed for securing the data transmission. In this paper, artificial intelligence is applied in order to improve the integrity and security of data transfer. The performance of the proposed method is evaluated on the basis of Bit error, mean square error, and PSNR metrics.

Keywords: *Video Steganography, Artificial Intelligence, DWT, Embedding Capacity, Steganography, Cryptography, Cover image*

1. INTRODUCTION

Steganography is referred to as a technique of hiding secret data. It is an encryption technique which is used along with cryptography in order to protect data. It can be applied to a video file, images and audio file. It is written in characters which include hash marketing.

This method protects pirating aiding and copyrighted materials in unauthorized viewing. This type of technique is used when encryption is not used. It is used as a supplement of encryption. Using steganography, an encrypted file hides information. The messages in steganography will appear ordinary such as a grocery list, image of a cat, etc. The hidden things in these ordinary objects or writing are hidden messages. The message is hidden in plain sight in stenographic communication. In this process, the message in a cover file initially encrypted with the help of a key and it is forwarded to the recipient. The recipient also uses the same key as on receiving the message in order to read the encoded message. One use of the steganography is watermarking that hides the copyright information by overlaying files within a watermark which cannot be detected easily by the naked eye. It also prevents fraudulent actions and also provides copyright protected from media extra protection [1].

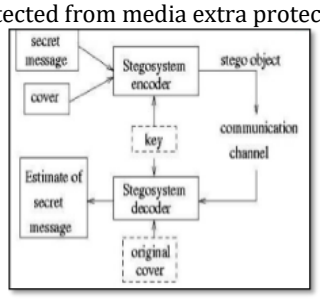

Fig. 1: Steganography Model

Steganography process is being applied in different fields such as industrial and military applications. The lossless steganography techniques are used for the successful and secure transmission of me information from the sender to receiver. Following are some main components of the steganography: [2]

1. Stego Key: It is mainly used for hiding the secret messages.
2. Embedded payload: It is the amount of data which is hidden in the cover
3. Cover Medium: This medium use video or image as a cover.
4. Embedding Efficiency: It describes the capacity in order to hide the data without any distortion.

1.1 Types of Steganography

There are many types of steganography. It depends on the type cover object that is followed to obtain the security[1].

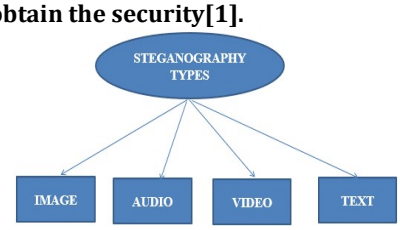

Fig. 2: Types of Steganography

1.1.1 Image Steganography

Image steganography is referred to as hiding the information inside images. An image having a secret message that can easily spread in a newsgroup or the World Wide Web. When the cover object is used as an image in steganography then it is known as image steganography. In this type of technique, pixel intensities are used in order to hide the information. In image steganography, 24-bit and 8-bit images are common. The size of the image should be large in order to hide more information in it. The larger images need compression in order to avoid the detection. The techniques that are used in image steganography are Masking and filtering and LSB insertion. These types of techniques can be used with vary degrees of success on various types of image files.

1.1.2 Audio Steganography

The audio steganography is referred to as a secret message that is embedded into a digitized audio signal. It results in the slight altering of the binary sequence which corresponds to the audio file. It is a type of technique which is used for transmitting the hidden information through modifying the audio signal in an imperceptible manner. Audio steganography is the science of hiding the secret audio or text information in a host message. The stego message after steganography and host message before steganography has the same characteristics. It is taking audio as a carrier in order to hide the information. It is known as an important medium. It is used for digital formats like MIDI, WAVE, AVI, and MPEG for the steganography. The method is echo hiding, LSB coding, parity coding, etc.

1.1.3 Text Steganography

Text steganography can be obtained by altering the certain characteristics of the textual elements and text formatting. The aim of the coding methods of design is to develop the alteration which is decodable reliably and invisible to the reader. These reliable decoding criteria and minimum visible change is the main challenge found in the designing document marking techniques. The document format file is mainly referred to as a computer file that presents the page layout and document content by using the standard format description languages like TeX, PostScript2, @off, etc. The various techniques that are used in the text are white spaces, a number of tabs, capital letters. In text steganography, Morse code is used to hide the information.

1.1.4 Video Steganography

Video steganography is referred to as a technique that is used to hide any type of information or files into digital video type. It is the combination of pictures which is used to carry hidden information. DCT (Discrete Cosine Transform) changes the values to 9 from 8.667. It is used to hide the information of all the images in the video that are not justified for the human eye. It is used as AVI, MPEG, Mp4, H.264 or other video formats.

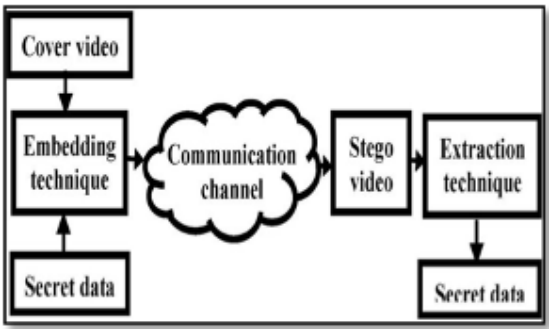

Fig.3: Block Diagram of Video Steganography

The video steganography is one of best technique which is used for data hiding. Basically, it is the extension of the image steganography. In this type of process, the video files view as a series of various images. It produces the video data which is the same as image data hiding. It is the system of whipping clandestine message inside a video. The video dependent steganography is suitable as compared to some other multimedia files due to memory and size necessities. It hides only some particular type of files in the video file.

There are several differences between image steganography and video steganography. The video content is dynamic because the hidden data detection is less likely in the video as compared to images. During the video processing, there are several attacks on video like frame rate changes, lossy compression, frame addition or deletion and format switching. The video provides new dimensions for hiding of data like hiding the message in motion components. The various components of audio or video files can use for data hiding.

Some advantages of video steganography are that videos that contain a large amount of data can easily hide in the videos. So, small distortions go by unobserved by humans due to the continuous flow of information. This type of technique is important in various application areas. The audio, digital video, and images are embedded with an imperceptible mark. It helps in preventing the unauthorized copy. It is also used in commercial and financial applications.

2. RELATED WORK

A. Arya and S. Soni (2018) presented a literature review on different techniques of Steganography that provides security and hides the message behind any image. Data is generally presented in the form of audio, text, image, and video. The image steganography can apply to video, text and audio file. Image steganography is known as hiding the information in image and video steganography is hiding the information in the video file. This paper demonstrated the various steganography techniques such as vector embedding and statistical technique, spatial domain transfers, distortion technique, masking, and filtering techniques. The future work that can be done in this research area is combining the various concepts of steganography and cryptography in order to provide security to secret message [1].

S. Pal and S. Bandyopadhyay (2016) described various methods of video steganography. From some time, security becomes one of the greatest challenges in the transmission medium because of the development of multimedia contents such as image, video, audio, etc and Internet. Security issue should be considered for transmitting secret images because hackers prefer to use the weak links over the communication network in order to steal the information which they want. Basically, video steganography is referred to as the process of hiding the secret information in the video file. The information contained in the video is not predictable and recognized by the human eye because the change of pixel color is negligible. This paper demonstrated about Neural Network method for the improvement of computer which is growing on basis of artificial intelligence. In this paper, the authors reviewed the visual cryptography schemes of secret sharing methods and its performance is determined on four criteria such as image format, pixel expansion, a number of secret images and type of share generated [2].

G. Nikam et al.(2017) presented a survey of various video steganography techniques. With the help of the Internet, data can be transferred from one place to another with high speed. It is very risky to transfer the data over the internet for security purpose. The various steganography techniques are used to prevent and maintain the information from an unauthorized person from extracting the critical information. Steganography technique mainly used for hiding the secret data including image, text, video, and audio. This type of secret information will be hidden in audio, image, text and video files. Video steganography is referred to as hiding secret information in the video file. This paper conducted the research on video steganography using various methods such as Modified Least Significant Bit, Least Significant Bit (LSB), Hash-Based Least Significant Bit (HLSB) and Discrete Cosine Transform (DCT). A vector embedding method is used in this research for compressed video. The results indicated that the vector embedding approach is efficient for hiding the information and efficient in transmission of the text message and secret data using the Internet [3].

M. Kasapbas and W. Elmasry (2018) presented LSB-based color image steganography method in order to increase the efficiency in security, payload capacity, and integrity check. The steganography is a technique that is used to hide information within a carried file and prevent the data from unauthorized parties. This paper combines several techniques in order to collect a new method that can be used for color image steganography. It helps in obtaining the increased payload capacity, enhanced efficiency, security with cryptography and possess integrity check. The code word is used in the proposed method with CRC-32 checksum and secret data. After that Gzip is used to compress by code word before encryption by AES. At last, it is added to the encryption header information for further process and then embedded into the cover image. The header information process and encrypted data use the Fisher-Yates Shuffle algorithm for selecting the location of the next pixel location. Different least significant bits are used to hide one byte of all color channels of the selected pixel. The comparative performance tests carried various spatial image steganography techniques by using well-known image quality metrics. The enhanced histogram Chi-square analyses and LSB analyses are used for security analysis. The results show that the proposed method efficiently improve security, payload capacity and integrity check for the LSB method. It also enhances the visual quality of the stego image [4].

M. Shanthi Rani et al. (2017) demonstrated video steganography with the help of mid-prime and discrete wavelet techniques. The steganography technique is used for hiding the secret information in cover media. The type of cover media is audio, text, video and digital images. Previous researches were conducted on image and text steganography. This paper also presented the method of concealing of an image on different frames of video with the help of DWT algorithm [5].

S. S. Ziabari (2018) described video steganography in the compressed area. Steganography concealed a file within some another file. These types of files are suitable for the encryption due to high redundancy and large size of the video file. In this paper, the authors implement a new algorithm mainly for encrypted the data for video files by using encryption techniques. The proposed algorithm divides and encrypts the secret data using motion vectors and to check the data changes in each vector [6].

K. Kaur and B. Kaur (2018) presented a DWT-LSB Approach for video steganography with the help of an artificial neural network. In this paper, the authors concentrated on providing security to data by using a combination of the decomposition technique. It uses the machine learning methods for increasing the security in realistic applications. There are several parameters such as MSE, PSNR and entropy are used to check the results that are obtained from simulation work [7].

S. Sharma and D. Somwanshi (2016) presented a DWT based attack on video steganography for protection of data. This paper described two methods i.e. steganography and cryptography for the reliable and secure transmission of the data. These techniques include multilevel data hiding methodology. Cryptography is used for transferring of data in an unreadable format. On the other hand, steganography is used to hide data behind cover. Three level DWT is efficient in enhancing the security of data. the results indicated that data is extracted securely after performing several attacks because of attack resistant based video steganography method [8].

3. PROBLEM FORMULATION

Steganography has changed the digital media completely in such a way in which intended recipient and sender is able to detect the message which is sent through it. Previously, there are numerous video steganography techniques have been proposed. The previously introduced video steganography techniques were not so much secure. They can tamper temporarily with an intention that the task was not fulfilled. At that time, when the message is encoded before sending the message to prevent the critical information then the hacker decoded the message easily by using some specific algorithm. Video steganography also could not lead in better and efficient results because the technique which is used for video steganography with LSB was not so much efficient. The previous PSNR results were unsatisfactory and poor. Most of the problems already exist in the already proposed algorithm. This thesis work designed a new artificial intelligence which is based on the algorithm used to overcome the problem and for data security. Its comparison is also presented with wavelets on the basis of bit error and PSNR.

4. PROPOSED METHODOLOGIES

DWT and artificial intelligence method are used in this research for improving the security of transferred data through video files. The proposed method involved two methods i.e. encoding and decoding. The proposed methodologies help in analyzing various steganography techniques proposed for securing the transmission of data. It also helps in achieving minimum distortion. These techniques help in conducting performance evaluation on the basis of Bit error rate and PSNR.

Encoding: For the Encoding, the LSB algorithm is used and the below steps are used to perform it:

A. Enter the Video file in which the data need to hide and a text file which consist of the secret data.
B. An object is created to create Stegano Video from the frames.
C. Check the size of the message and video, if the size of the message is greater than the size of the video, stops the execution.

Fig.4: Flow Diagram of Video Steganography Encoding

Now, the data is hidden inside the frames using the data hiding mechanism. The LSB algorithm is performed on each frame by extracting the R, G, B channel of the Frame

D. and Bitwise AND and OR operation is used until the data is hidden completely.

After that, the Key file which will be used during Decoding and a Stegano video is created with encoded frames.

Decoding: For the Decoding, the same algorithm is used and the below steps are used to perform it:

A. Enter the Stegano video obtained from encoding and Key file which consist of some binary data which helps to decode the message.
B. After that, the frames are extracted from the video and the key data is also extracted from the file to decode the message.
C. Then from each frame, R, G, B channel are extracted.
D. Perform the Bitwise AND and OR operation on each channel of the frames and data is extracted from the frame.
E. The extracted data is Stored in Extracted.txt file.

Fig.5: Flow Diagram of Video Steganography Decoding

For measuring the performance, before performance metrics will be used.

Peak Signal to Noise Ratio (PSNR): It is referred to as the ratio between the power of corrupting noise and the maximum possible power of a signal. It affects the fidelity of its representation. PSNR is presented in terms of the logarithmic decibel scale and used to evaluate the quality of the reconstructed image. The higher value of PSNR shows that the reconstruction is of higher quality.

Bit Error: Bit error is referred to as the actual number of bit position and this position is changed in the stego image than cover image. Signal strength should be greater and Bit error should be less.

5. FINAL RESULTS

Encoding GUI

In the below figure of video steganography, we can input video and input text file in order to encode it to transfer information from one place to another and protect it from unauthorized access or hackers to view the data which is sent through video.

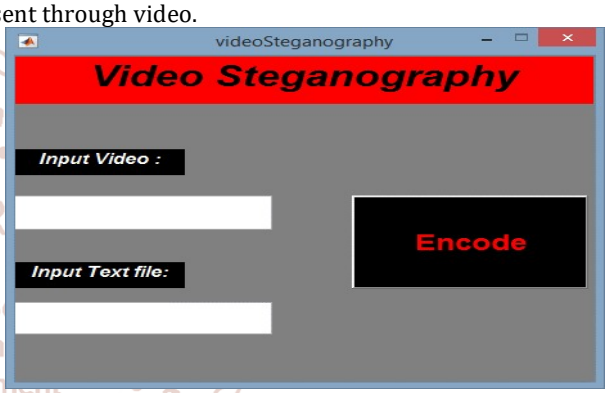

Fig.6: Encoding GUI

Input Secret Text File

The below figure shows the input secret text file that we want to transfer from one place to another without any unauthorized access.

Fig. 7: Input Secret Text File

Input Video File

The below figure shows the input secret video file that we want to transfer from one place to another without any unauthorized access.

Fig. 8: Input Video1 File

Output Key file

The below figure shows the output key file which is found to another person who does not have access to view the encrypted file.

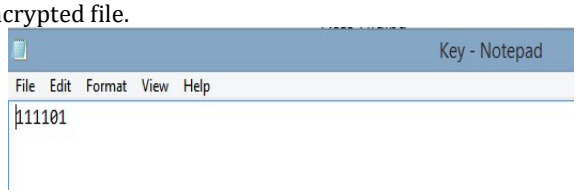

Fig.8: Output Key file

Decoding GUI

The below figure shows the image where we can decode the contents which are sent through video with security. In this, we enter stego video and enter key to get the original data.

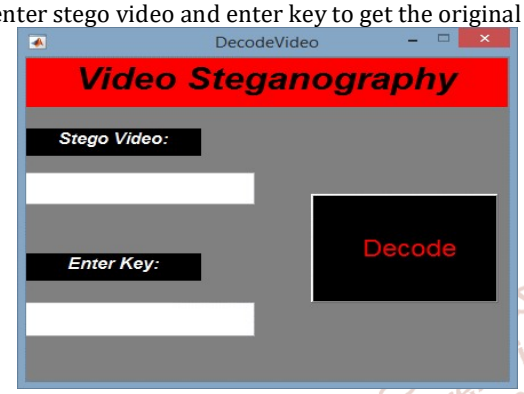

Fig.9: Decoding GUI

Extracted Data File

After entering the stego video and enter key, the original data file is extracted which shows in the below figure.

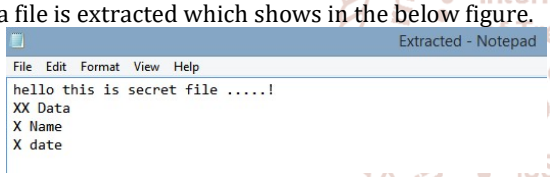

Fig.10: Extracted Data File

Fig. 12: Input Video2 File

Fig. 13: Input Video3 File

Three videos were used to test the new algorithm and its efficiency. The results comparison of all three videos is shown in the below graphs in term of PSNR, MSE, and BER.

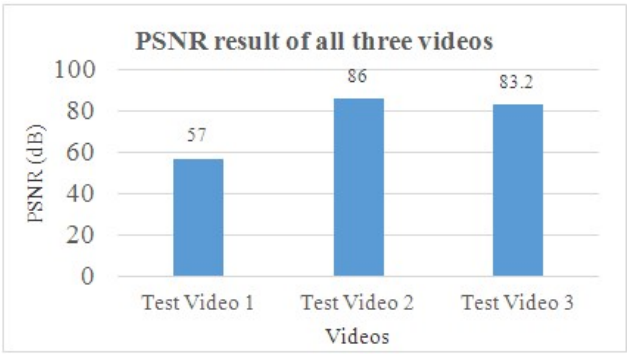

Fig. 14: Result of PSNR

Figure 14 shows the result of PSNR achieved after the steganography technique. It can be seen that all the three videos achieved a high value of PSNR that shows the efficient working of the proposed algorithm.

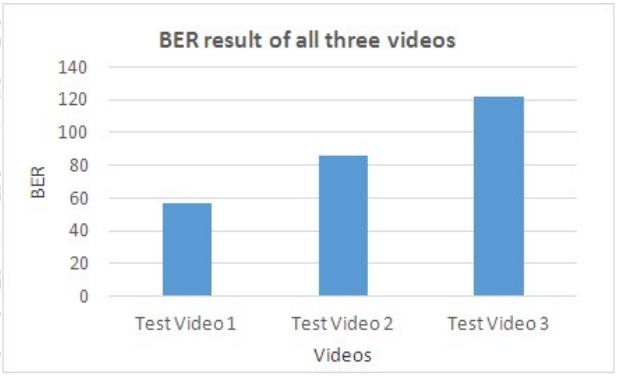

Fig. 15: Result of bit error rate

The bit error rate is also less as compared to the total number of pixels in the video. As there were errors in a few bits only.

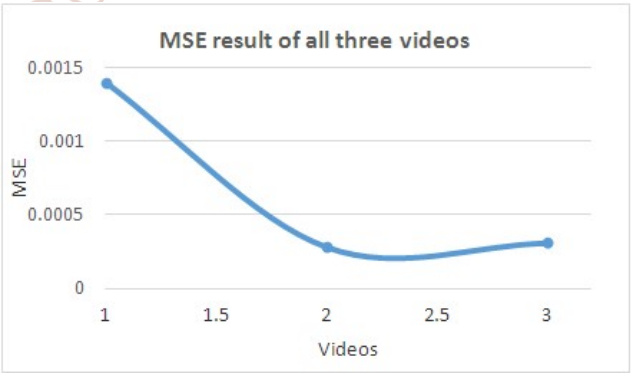

Fig. 16: Result of MSE

The result of MSE are also efficient as there is less error while encoding the data in the video that results in the high value of PSNR.

Table 1: Matlab output of Test video1

Test video1 (360X640)	
PSNR	57.000
BER	58.765
MSE	0.0014

Table 2: Matlab output of Test video2

Test video2 (674X1280)	
PSNR	86.000
BER	83.650
MSE	0.000283

Table 3: Matlab output of Test video1

Test video3 (720X1280)	
PSNR	83.247
BER	122.000
MSE	0.000310

6. CONCLUSION

Video steganography is a method used for hiding the secret messages into cover media so that intruder would not able to see the secret messages. There are several techniques used for video Steganography which exist with a degraded quality of extracted messages. So, the proposed video Steganography has used with artificial intelligence and DWT in order to determine the best bits from cover video to insert secret data. This research mainly focuses on security with the combination of two techniques to enhance the rate of security in the realistic applications.

7. FUTURE SCOPE

In the proposed methodology, artificial intelligence and DNN is used for the enhancement in the hiding process in video which can be further improved to get more better results with enhanced security and resolution. In the future, artificial intelligence and DNN could be more optimized that can help in increasing the quality of the secret data.

8. ACKNOWLEDGMENT

Completing a research and coming up with a conclusion cannot be accomplished without proper guidance. Having a perfect guide to assist is a blessing. Here I heartedly acknowledge to all those who guide me throughout my entire research especially Gargi Kalia.

9. REFRENCES

[1] A. Arya and S. Soni, "A Literature Review on Various Recent Steganography Techniques", International Journal on Future Revolution in Computer Science & Communication Engineering, vol. 4, no. 1, pp. 143-149, 2018.

[2] S. Pal and S. Kumar Bandyopadhyay, "VARIOUS METHODS OF VIDEO STEGANOGRAPHY", International Journal of Information Research and Review, vol. 3, no. 6, pp. 2569-2573, 2016.

[3] G. Nikam, A. Gupta, V. Kalal, and P. Waghmare, "A Survey of Video Steganography Techniques", Journal of Network Communications and Emerging Technologies, vol. 7, no. 5, pp. 33-35, 2017.

[4] M. Cem kasapbaşi and W. Elmasry, "New LSB-based color image steganography method to enhance the efficiency in payload capacity, security and integrity check", Sādhanā, vol. 43, no. 5, pp. 1-14, 2018. Available: 10.1007/s12046-018-0848-4.

[5] M. Shanthi Rani, S. Lakshmanan and P. Saranya, "VIDEO STEGANOGRAPHY USING MID-PRIME AND DISCRETE WAVELET TECHNIQUE", International Journal of Computer Engineering and Applications, vol., no., pp. 180-190, 2017.

[6] S. Mohammadi Ziabari, "Video-Steganography in the compressed area", Research Gate, pp. 1-17, 2017.

[7] K. Kaur and B. Kaur, "DWT-LSB Approach for Video Steganography using Artificial Neural Network", International Advanced Research Journal in Science, vol. 5, no. 7, pp. 20-25, 2018.

[8] S. Sharma and D. Somwanshi, "A DWT based Attack Resistant Video Steganography", International Conference on Computational Intelligence and Communication Networks, pp. 1-5, 2016

[9] H. Goyal and P. Bansal, "VIDEO STEGANOGRAPHY USING NEURAL NETWORK AND GENETIC ALGORITHM", International Journal of Emerging Technology and Innovative Engineering, vol. 1, no. 9, pp. 7-14, 2015.

[10] M. Zamani, H. Taherdoost, A. Manaf, R. Ahmad and A. Zek, "An Artificial-Intelligence-Based Approach for Audio Steganography", Journal of Open Problems in Science and Engineering, vol. 1, no. 1, pp. 64-68, 2009.

AUTHORS PROFILE

Shivani Gupta has done B.Tech and recently pursuing M. Tech in Computer Science and Engineering from Universal Institute of engineering and Technology(UIET) Lalru.

Gargi Kalia has done B.Tech from Punjab Technical University and M.Tech from Rayat anad Bahra University. She is currently working in Universal Institute of Engineering and Technology(UIET) ,Lalru.

Preeti Sondhi has done B.Tech from Ganpati Institute of Engineering and Technology and M.Tech from Sidivinayk Group of Institutions. She is currently working in Universal Institute of Engineering and Technology (UIET) ,Lalru.