International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Video Steganography Approach using Random Least Significant Bit Algorithm

Arijit Basu[1], Gaurav Kumar[2], Soumyajit Sarkar[3]

[1,2] Department of Information Technology, Heritage Institute of Technology, Kolkata, WB, India

[3]Department of Computer Science and Engineering's Thomas' College of Engineering and Technology, Kolkata, WB, India

Abstract: ***Steganography is the art of hidinginformation. It is derived from the Greek word ''Steganos'' which means covered writing, a science of secret communication. It is a tool for hiding information in a medium so that the information does not appear to exist. The idea of data hiding is not a novelty, it has been used for centuries all across the world under different regimes- but to date it is still unknown to most people. It is a tool for hiding information so that it does not even appear to exist. However Steganography operates at more complex level as detection is dependent on recognizing the underlying hidden data. The message to be hidden is known as the "embedded data", the medium for hiding is known as the "cover medium" and the encoded medium is known as the stego-object. In this paper we present a video steganographic process using the Random Least Significant Bit algorithm and hence perform a careful analysis of the same with the Sequential Least Significant Bit algorithm.***

Keyword: Steganography, Steganalysis,LSB, RLSB, RGB, PSNR, MSE

1. Introduction

The modern day video steganography presents the task of transferring the embedded information to the destination without being detected by the attacker. Many different file formats can be used but digital images are the most popular because of their frequency on the internet. . The safety of communication in organizations is a very important issue. It is about confidentiality, integrity and authentication during access or editing of confidential internal documents. A non-conventional means to increase security is the use of steganography to hide documents in digital videos, which makes possible to hide higher amounts of information and documents than steganography in images[7]. For hiding secret information in videos which is in fact an array of images, there exists a large variety of methods. Some of them are very and all of them have their strong and weak points.

A. Image Steganography

Image steganography, is one kind of steganographic system where the secret message is hidden in a digital image with some kind of hiding strategy. The conventional image steganographic algorithm is the Least Significant Bit (LSB) algorithm, the advantage of LSB is its simplicity to embed the bits of the message directly into the LSB plane of the cover image and many applications use this method. The storage of information bits in the least significant bits of the image does not affect the image in a greater scale and hence the change is not perceived by the Human Visual System (HVS). LSB embedding when applied to the pixels of an image sequentially make it easy for any intruder to uncover the information, hence the bits can be embedded in a random fashion to present a more secured way of information hiding [1].

B. Video Steganography

In Video steganography the medium of data hiding is an input video file. A video is nothing but a collection of frames. Using an efficient algorithm we can choose a key frame and then perform the RLSB and LSB algorithm on the pixels of that key frame/image. Then we need to put back that frame into its initial set of frames and merge them back into the video file. A video steganographic process can be considered more secured than image steganography or audio steganography. This is because whenever a sender hides some information inside a video file and sends it to the receiver, the intruder has a very low chance of understanding the presence of a message since the video frames move at a very high rate and makes it imperceptible for him to understand anything. Secondly even if he manages to get hold of the frames there are thousands or more frames to deal with because the sensitive information might be present in one frame only and each time the selection of frame will be different, hence previous knowledge won't suffice to perform this job. On the contrary it is possible for an image to get speckled and cause suspicion to the intruder or an unwanted noise in a source audio file can do the same in image and audio steganographic techniques respectively [3].

C. Approaches to Video Steganography

1) Hiding operations in a compressed domain
This approach of Video Steganography is based on the embedding of data within the macro blocks of Intracoded frames of a MP4 video with minimum scene change. A novel video steganographic approach called Tri Pixel Value Differencing is used for embedding the message [4].

2) Full Encryption
Encryption is done on the entire video bit stream for both compressed as well compressed videos. This approach particularly called the naïve approach uses a conventional cryptosystem for encryption. This approach provides lower computational complexity and faster performance.

3) Selective Encryption
Encryption is done on selective bits of the video, not the entire video. Bits are selected on the basis of spatial information and hence called spatial selective approach. In particular sections of a media file, image for example, only the face can be encrypted by using this approach.

4) Perceptual Analysis
Sometimes it is desirable to encrypt videos by taking an approach that preserves low quality perceptual information. By decrypting such video, one can get to the source video of original visual quality.

5) Encrypted bit stream compliance
Other approaches to this procedure are Format Compliant, Format Defiant, CODEC standard defiant approaches, CODEC standard compliant approaches. They are used in cases of non-perceivable encryption.

2. Proposed Work

In this work, we present a steganography technique using **MPEG-4** videos aiming to increase document secrecy. We propose a video based steganograhic approach using Least Significant Bit (LSB) techniques and Pseudo Random encoding to enhance the security of the communication. In ***LSB*** approach the basic idea is to replace every LSB bits of the cover image with the bits of the message without destroying the property of the cover medium significantly. The LSB based technique is the most challenging one as it is difficult to differentiate between the cover object and the ***stego object*** if few LSB bits are replaced. A key has been taken as input from the sender and it has been operated logically on the bits of the ***coverimage*** in a random fashion so that without the availability of the exact key at the receiver end, the message cannot be recovered. By using the key the chances of recovering the message becomes low.

3. Algorithms and Parameters

A) Algorithm 1.1 for frame selection
The frame with the highest amount of color information was selected as the Key frame. The following steps were followed:

Step1:
Read the image file

Step2:
Read the R, G, B values of every pixel for every frame.

Step 3:
Calculate the sum total of R, G, B values of every pixel for each frame.

Step 4:
Select the frame with the largest RGB sum as the key frame.

Algorithm 1.2 for frame selection
The video information was calculated and using the duration we implemented an algorithm where the middle frame was selected as one of the key frames. Further we applied the previous approach to select another key frame and then merged the two selected key frames to get one resultant key frame. The following steps were followed:

Step 1:
Calculate the total duration of the video.

Step 2:
Set the start time and seconds between frames.

Step 3:
Read the input video using IMediaReader and create BufferedImages in BGR 24bit color space.

Step 4:
Read out the contents of the media file and dispatch events to the attached listener. Calculate end time.

Step 5:
In attached listener if the selected video stream id is not yet set, select a video stream.

Step 6:
Set seconds between frames as equal to the half of the duration of the video.

Step 7:
Receive the resultant frame i.e the middle frame and the first frame in BufferedImages.

Step 8:
Merge both frames obtained in Step 7 to give a single frame i.e the key frame.

B) Least Significant Bit Embedding and Extraction

Fig 1 shows a generic embedding and extraction of data

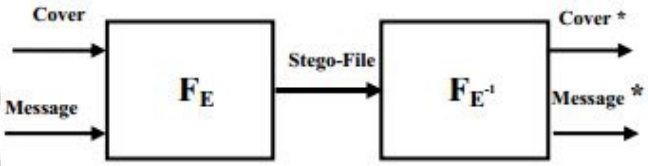


Fig 1

Embedding technique in the algorithm is based on replacing the LSB of the pixel (I (i, j)) with the message bits one by one. Hence if the message is equivalent to m-bits there are m-pixels to deal with, whose least significant bits will be replaced by the m-message bits. The embedding procedure can be described using the equation as follows [2]:

$$Is((i,j) = \begin{cases} I(i,j)-1 & LSB(I(i,j))=1 \text{ and } m=0 \\ I(i,j) & LSB(I(i,j))=m \\ I(i,j)+1 & LSB(I(i,j))\neq 0 \text{ and } m=1 \end{cases}$$

Algorithm 2.1 LSB Embedding:
Step 1: Read the cover image(key frame) and text message which is to be hidden in the cover image.
Step 2: Convert text message in binary.
Step 3: Calculate LSB of each pixels of cover image.
Step 4: Replace LSB of cover image with each bit of secret message one by one.
Step 5: Write stego image
Step 6: Calculate the Payload Capacity, Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.

Algorithm2.2 LSB Extraction
Step 1: Read the stego image.
Step 2: Calculate LSB of each pixels of stego image.
Step 3: Retrieve bits and convert each 8 bit into character

C) Random Least Significant Bit Embedding and Extraction

Algorithm 3.1 RLSB Embedding
Step 1: Read the cover image (key frame) and text message which is to be hidden in the cover image.
Step 2: Convert text message in binary.

Step 3: Generate a Pseudo Random Number
Step 4: Select pixels based on the random number generated
Step 5: Calculate the LSB of the randomly selected pixel and embed the random id into the image array.
Step 6:Replace LSB of cover image with each bit of secret message one by one.
Step 7: Write stego image.
Step 8: Calculate the Payload Capacity, Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image

Algorithm 3.2 RLSB Extraction:

Step 1: Read the stego image.
Step 2: Backtrack with the image array to find the positions of the randomly selected pixels.
Step 3: Calculate LSB of each pixels of stego image.
Step 4: Retrieve the bits and convert each 8 bit into a character

D) Parameters used for comparison

1) Peak Signal to noise ratio (PSNR)

PSNR is an engineering term between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR here refers to the ratio between the stego-image i.e. the image which has been embedded and the cover-image i.e. the original image [2].PSNR can be evaluated by using the following equation:

$$PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

2) Mean Square Error (MSE)

The Mean squared error of an estimator measures the average of the squares of the ‘’errors’’, i.e. the difference between the estimator and what is estimated. The difference occurs because of randomness or because the estimator does not account for information that could produce a more accurate estimate [2]. The MSE varies inversely with the PSNR. The M.S.E can be calculated from the following equation:

$$MSE = \frac{\sum_{M,N}[I1(m,n) - I2(M,N)]^2}{M * N}$$

Where **I1** (m, n) and **I2** (m, n) are the stego and cover images respectively and M, N are the dimensions of the image.

3) Security

When it comes to data hiding security is the major consideration. It evaluates the degree of safety and the degree of difficulty for the intruder to break through the algorithm and uncover the embedded information.

4) Text Retrieval

Text retrieval refers to the amount of text that can be obtained if the intruder manages to breach the security. It can be considered as a parameter because the intruder can sometimes manage to get some information bits and then apply a brute force method to retrieve the entire text pattern. It can be correlated to the confusion property in Cryptography which says that the cipher text should be obtained by utilizing every position of the plain text.

4. Experimental Results

We have implemented the entire process of Video Steganography using JAVA. We have used two Java media class libraries XUGGLER AND FFMPEG. The programming platform used is NetBeans IDE version 7.0.1. The project has been represented in an interactive platform using Java API also. Hence the encoded video can be transferred to any system having JDK and can be decoded out there since the application is a JAR file and can successfully run on any system having JDK. We have worked with an Avi video format considering the fact that MPEG-4 videos while splitted gives JPEG frames which has a lossy compression property and hence the Encoded video after getting decoded looses the information hidden. On the contrary we have obtained PNG frames which does not undergo lossy compression rather is associated with a lossless compression technique. The input video is output.avi and the encoded video obtained is test.avi. The workflow steps with their respective outputs follows:

Step 1: Reading an image file and displaying its header information:

Reading the pixel value is nothing but gathering the RGB information or the pixel information of the image.
Typically the header information includes image width, image height, number of components (1=Greyscale, 3=RGB), horizontal and vertical sampling factors for both components.

Step 2: Taking the input avi video file and splitting it into frames.

The video has been splitted using XUGGLER which is an open Java media class library.

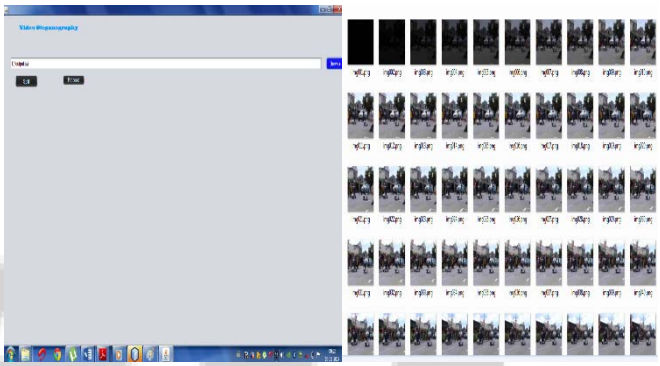


Figure 1.1: Input the video Fig 1.2 Array of PNG frames

Step 3: Selecting the Key frame:

The key frame has been selected using***Algorithm 1.1***and the text ’’Heritage Institute of Technology’’’ has been embedded using ***Algorithm 3.1*** first and then with ***Algorithm 2.1*** for a comparison analysis between the two and at the same time securing it with the aid of a key to prevent intrusion. The key is 6 bits long and is in a password protected format to prevent shoulder surfing. The key entered performs a logical operation (XOR) with the encoded information bits as is shown in Fig 2.2

Figure 2.1: Key frame (Cover Image)

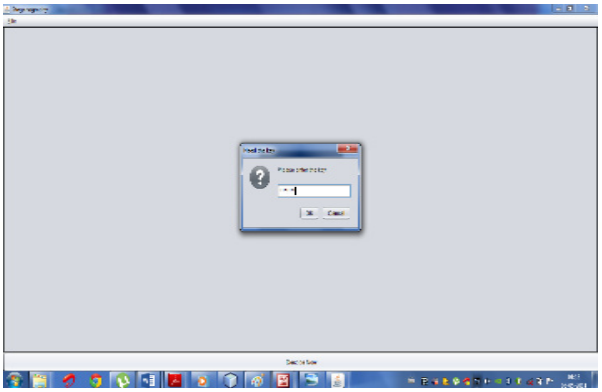


Figure 2.2: Embedded Text Fig 2.3 Securing with key

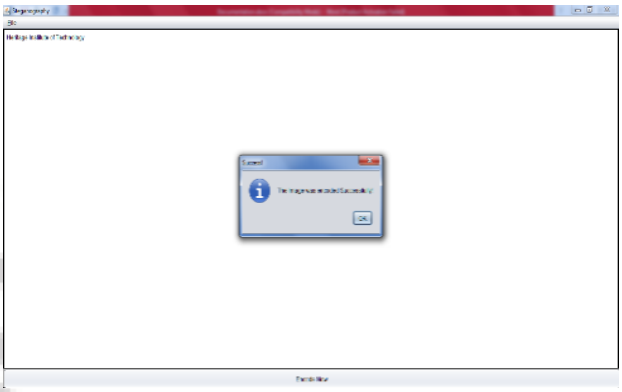


Figure 2.3: Successful Encoding

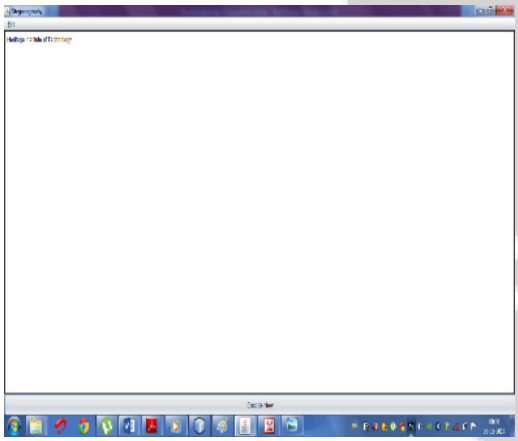
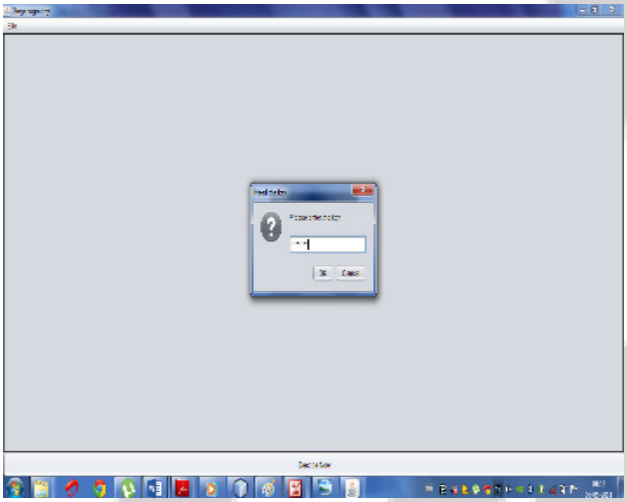
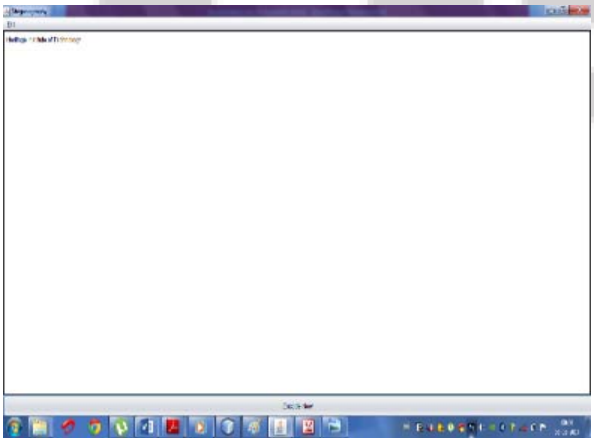


Figure 2.4: Encoded Frame





Step 4: Extracting the audio file from the Video
The audio file has been extracted from the input video file using FFMPEG media class library and has been recombined with the encoded video file sent to the receiver. The audio file retrieved is in MP3 format.

Step 5: Decoding the encoded Video at the receiver side
Following similar steps the encoded video is broken back into frames where the encoded frame is chosen and decoded but only after entering the exact key as was input at the sender side. The key serves as a very important role in securing this communication. The key if passed in wrong hands it becomes evident that the system can then be easily intruded an all sensitive information could be leaked.

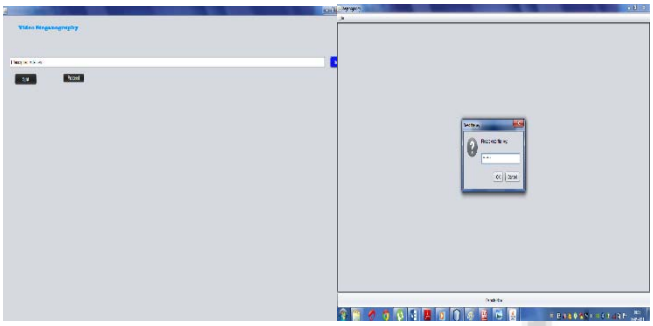


Figure 3.1: Encoded video input Fig 3.2 Entering the key

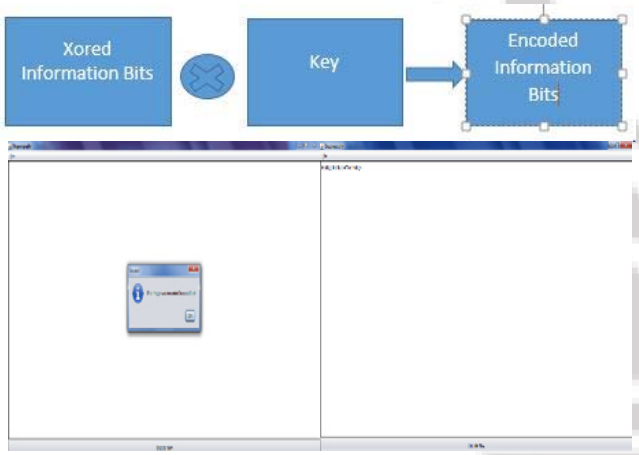


Figure 3.4: Successful Decoding Fig 3.5Text Retrieved

A. Comparing LSB vs Random LSB

1) Security

One variation would be random LSB, in which the secret data are spread out among the image data in a seemingly random manner. This can be achieved if both the sender and receiver share a secret key. They can use this key to authenticate whether the receiver is allowed to decode the video or not. The advantage of this method is that it incorporates some cryptography in that diffusion is applied to the secret message. However, it goes beyond just making it difficult for an attacker knows that there is a secret message to figure out the message. It also makes it harder todetermine that there was a secret message in the first place. The reason is because the randomness makes the embedded message seem more like noise statistically than in the sequential method. The steps followed in the algorithm we implemented ensures a better security. Hence the random LSB algorithm provides a better **security** than the regular sequential algorithm.

2) Text Retrieval

Another variation to regular LSB is to repeat the message multiple times across theimage data. This way, if the message is relatively small compared tothe coverimage,the message may survive any image manipulation, such as cropping. The intruder if on suspicion thinks that the algorithm that might have been used is the LSB algorithm he might not be able to uncover the data but he can perform an illegal act of cropping the keyframe because the information bits are likely to spread sequentially starting from the beginning of the image. Hence cropping might lead to loss of data. Whereas in RLSB the bits being randomly located even after cropping the image will not all the information bits. Hence the RLSB algorithm gives a **better chance** of text retrieval if the image gets cropped by the intruder.

3) PSNR

PSNR(Peak Signal to noise ratio) of Cover image to Stego image in case of Sequential LSB is lower in comparison to the same while using a Random LSB as are evident from their respective values calculated to be 16.79db for the former one and 19.1384db for the later one. This means that the stego image that is obtained using a regular LSB algorithm is more distorted than the stego image obtained using a Random LSB algorithm. Hence **PSNR** ratio in case of RLSB is more than that of Sequential LSB.

4) MSE

A high PSNR generates a low mean square error. Hence the **Mean square error** in case of RLSB is lower as compared to LSB.

B. A Statistical comparison between LSB, DCT and DWT based Steganography [6]

Table 1

Parameters	*LSB(Least Significant Bit)*	*DCT(Discrete Cosine Transform)*	*DWT(Discrete Wavelet Transform)*
Working	Works by replacing the least significant bit of each pixel with the information bits.	Embeds the information by altering the transformed DCT coefficients	Works by taking many wavelets to encode an image.
Visibility	Low	Medium	High
Payload	High	Medium	Low
PSNR	High	Medium	Low
MSE	Low	Medium	High

5. Conclusion

Video Steganography is a secured way of covert communication. Videos generally donot create too much temptation or suspicion in the eyes of an intruder to image or audio and difficulties incorporated even after breaching security as highlighted before must be taken into consideration. The soul and heart of this steganographic approach is the Random Least Significant bit algorithm. The RLSB algorithm is better than the LSB algorithm as evident from their brief comparison. Also LSB shows a better performance than DCT and DWT based techniques.The key plays a very important in embedding the message. Larger the key size, the more difficult to suspect the secrecy So the RLSB technique discussed is always a secured means of embedding, for steganographic processes. In conclusion it can be inferred that Video Steganography using Random Least Significant Algorithm serves as an efficient and effective means of communication in today's world of cyberspace vulnerable to security breaching.

6. Future Scope

The Random LSB algorithm serves as a good deal in terms of security, but the selection of bits of the cover medium can be improved if we concentrate on particular areas of the

image like the edges. We can use edge detection operators like Robert, Laplace, Prewitt, Sobel and Canny to detect the edges, mask it and then apply the RLSB algorithm, so that it can be good approach. Also, the message that has been hidden in the cover medium is a plain text. We can improve our algorithm to hide mp3, rar, flv and other extensions.

References

[1] Nitin Jain, SachinMeshram, ShikhaDubey, "Image Steganography using LSB and Edge Detection Technique",IJCSE,July 2012.
[2] StutiGoel, ArunRana, Manpreet Kaur, "Comparison of Image Steganography Techniques", IJCDS, Apr-May 2013, Vol. 3, Issue 1.
[3] Socek, H. Kalva, O. Marques, D. Culibrk, B. Furht: "New Approaches to encryption and steganography for digital videos", Springer-Verlag 2007.
[4] Blanca E. Carvajal-Gamez, Francisco J. Gallegos- Funes, Alberto J. Rosales Silva and Rene Santiago, Steganography in Different Colour Models Using an Adjustment Applying Wavelets,''Recent Advances in Steganography'',ISBN 978-953-51-0840-5,November 7, 2012
[5] Yingqi Lu, Cheng Lu, Miao Qi, A Effective video Steganographic method for biometric identification,proceedings of the 2010 international conference on Advances in computer science and information technology, Pages 469-479 Springer- Verlag Berlin, Heidelberg, June-23-2010
[6] ShashikalaChannalli, Ajay Jadhav, 'Steganography, an Art of Hiding Data'', IJCSE, Vol.1 (3), 2009, 137-141
[7] A.D. Ker, "Steganalysis of LSB Matching in Grayscale Images", IEEE signal processing letters, vol. 12, No 6, 2005.
[8] Raphael C.-W. Phan, H.-C. Ling, "Steganalysis of Random LSB Insertion using Discrete Logarithms proposed at CITA03".

Author Profile

Mr. Arijit Basuhas completed B.Tech in Information Technology from Heritage Institute of Technology, Kolkata, India and will be joining as a M.S. student at the University of Kansas, USA.

Mr. Gaurav Kumar has completed B. Tech in Information Technology from Heritage Institute of Technology, Kolkata, India.

Mr. Soumyajit Sarkarhas completed B.Tech in Computer Science from St. Thomas' College of Engineering &Technology, Kolkata, India and will be joining as a M.S. student at the University of Kansas, USA.