RESEARCH ARTICLE OPEN ACCESS

Performance Evaluation of Secrete Image Steganography Techniques Using Least Significant Bit (LSB) Method

Anupriya Arya [1], Sarita Soni [2]

M-tech Scholar Student [1], Assistant Professor [2]

Department of Computer Science Engineering, BBAU Central University, Lucknow

UP – India

ABSTRACT

Steganography is an important area of research in recent years involving a number of applications. Its science of embedding information into cover image viz., text, video and image without causing statistically significant modification to cover image. In this paper author has proposed improved LSB substitution method for hiding secreted image data information image file into color image. Since only last bit each pixel of cover image gets changed, this method is capable of producing a secret-embedded image that is totally indistinguishable from the original image by the human eye. Many different carrier file formats can be used like bitmap, jpeg and PNG format to show that this technique is suitable for both formats. It is shown that the length of hidden messages embedded in the least significant bits of signal samples can be estimated with relatively high precision. In this paper intended performance evaluation of secrete image steganography techniques using LSB method for data and image security, its comparison on different size and image format (.bmp; .jpg; .png) and calculate its parameters like PSNR and MSE for its to analyze its hiding capacity with that of MATLAB implementation, which is a powerful method for data and image security.

Keywords:- Cover image Steganography, Data hiding Image; Histogram, LSB method, PSNR, MSB, Stego-image, MATLAB.

I. INTRODUCTION

In recent trends in the world, the communication is the basic necessity of every growing area. The growth of modern communication technologies imposes a special means of security mechanisms especially in case of data networks. Everyone wants the secrecy and safety of their communicating data. Information security is a major issue of concern while exchanging a data in an open network, as internet is not only a single network it is worldwide collection of loosely network. The network security is becoming more important as the volume of data being exchanged over the Internet increases day by day. The two important techniques for providing security are cryptography and steganography. Both are well known and widely used methods in information security. Steganography and Cryptography both plays a very important role in information security [1], [2]. Digital images stored in computer systems are composed of finite number of elements in the form of array; each element has its particular location and value, known as pixels. In case of 24 bit color image each pixel has three color components: Red, Green, and Blue (RGB). Each pixel is represented with three bytes to indicate the intensity of these three colors (RGB) [3].

The technique for steganography hiding secrete data into the least-significant bit (LSB) of each pixel in an image. Then based on the LSB technique, an algorithm for 8 and 24 bit color image is developed improves the stego-image quality of color image capable of producing a secret-embedded image that is totally indistinguishable from the original image by the human eye.

In steganography the process of hiding information content inside any multimedia content like image, audio, video is referred as a "Embedding". For increasing the confidentiality of communicating data both the techniques may be combined. So, steganography (hiding information) and cryptography (protecting information) are totally different from one another. Due to invisibility or hidden factor it is Difficult to recover information without known procedure in Steganography [4]. Detecting procedure of steganography known as Steganalysis. Good imperceptibility and sufficient data capacity (efficiency of hidden information) are two properties which should be possessed by all the steganography techniques. Some shared secret – key known as Stego-key is used in steganography algorithm. *Figure (1)* Shows Block Diagram of Steganography Moderate Significant Bit Replacement Technique:

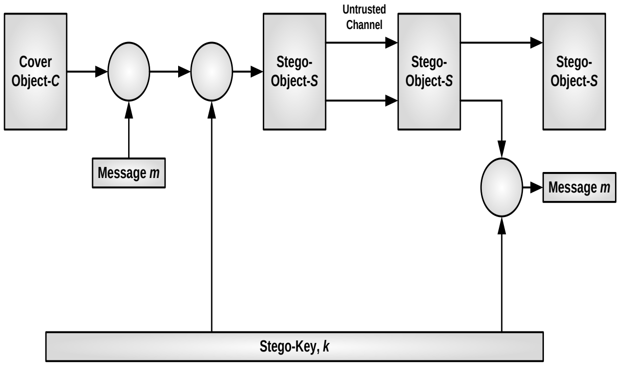


Fig. 1.1- Block Diagram of Steganography process

The moderate significant bits of each pixel in the cover image can be used to embed the secret message. This method improves sensitivity to modification, but it degrades the quality of stego-image [5].

This paper is organized as follows: Section II steganography overview Section III Least significant bit (LSB) method. Section IV

LSB Method for 8 & 24 Bit color images, Section V Simulation Results and Discussion, Section VI conclusion and future work of research work.

II. STEGANOGRAPHY OVERVIEW

Steganography is a Greek word which means concealed writing. The word “steganos” means “covered “ and “graphial “ means “writing”. The origin of steganography is the biological and physiological. The term “steganography” came into use in 1500’s after the emergence of Trithemius’ book on the subject “Steganographia”.. But today’s most of the people transmit the data in the form of text, images, video, and audio over the medium.

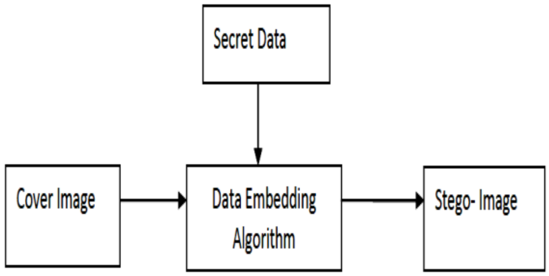


Fig. 2.1-Steganography Diagram

In order to safely transmission of confidential data, the multimedia object like audio, video, images are used as a cover sources to hide the data The overview of steganography field can be divided into three parts in given table –I [6].

Table-I

Past	Present	Future
It’s very older origins can be traced back to 440 BC.	The majority of today’s steganographic systems uses the multimedia objects like image; audio; video etc	Nowadays, “Hacking” is very famous term
In early times, messages were hidden on back of the wax writing tables, written on the stomachs of the rabbits, or the tattooed on the scalp of slaves	Its cover media because people often broadcast digital pictures over email and other Internet communication	It is nothing but an unauthorized access of data which can be collected at the time of the data transmission
Invisible ink has been in use for centuries—for fun by children and students and for serious espionage by spies and terrorists [7].	in present world of steganography various steganographic techniques have been proposed	Steg analysis is a process in which a steganalyzers cracks the cover object to get the hidden data
Cryptography became very common place in the middle periods	There are certain cases in which a combination of Cryptography and Steganography is used to achieve data privacy over secrecy	It is hoped that Steganography along with Cryptography may improve the privacy as well as secrecy.

III. LEAST SIGNIFICANT BIT (LSB) METHOD

The Least Significant Bit (LSB) is one of the most important techniques in spatial domain image steganography. LSB technique embeds the bits of secret message directly into the least significant bit (LSB) plane of the cover image. LSB Steganography can be classified by two methods LSB replacement and LSB matching. The terminology LSB replacement/ LSB matching was firstly discussed by T. Sharp [7]. First is LSB replacement which is simplest of the LSB.

In a gray-level image, every pixel consists of 8 bits. The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value. LSB is the most commonly used method to hide any secret information inside any medium as it leads to minimum distortion in cover medium. A method in [**8**] is an improvement to existing LSB method which resists histogram attack in LSB embedding by embedding some extra bits to make histogram look like the original one.

In this method, the overhead in previous method is removed by changing unused pixels such as to restore the frequency of bins. The methods have been implemented using MATLAB and experimental results proved them secure. From time to time, different methods have been used to increase the security and imperceptibility of the steganographic techniques.

IV. LSB METHOD FOR 8 & 24 BIT COLOR IMAGES

One of the most common techniques used in steganography today is called least significant bit (LSB) insertion. This method is exactly what it sounds like; the least significant bits of the cover-image are altered so that they form the embedded information. The Least Significant Bit insertion varies according to number of bits in an image. When converting an analog image to digital format, we usually choose between two different ways of representing colors

4.1 8-bit color

8-bit color graphics is a method of storing image information in a computer's memory or in an image file, such that each pixel is represented by one 8-bit byte. The maximum number of colors that can be displayed at any one time is 256. There are two forms of 8-bit color graphics. The most common uses a separate palette of 256 colors, where each of the 256 entries in the palette map is given red, green, and blue values. In most color maps, each color is usually chosen from a palette of 16,777, 216 colors (24 bits: 8 red, 8 green, 8 blue). But in the original VGA card's 320x200 mode, 256 on-screen colors could be chosen from a palette of 262,144 colors (18 bits: 6 red, 6 green, 6 blue). Some older cards prior to the VGA (like the Professional Graphics Controller) can only choose the 256-color palette from 4,096 colors (12 bits: 4 red, 4 green, 4 blue). The other form is where the 8 bits directly describe red, green, and blue values, typically with three bits for red, three bits for green and two bits for blue [9], [10]. This second form is often called 8-bit true color, as it does not use a palette at all, and is thus more similar to the 15-bit, 16-bit, and 24-bit true color modes.

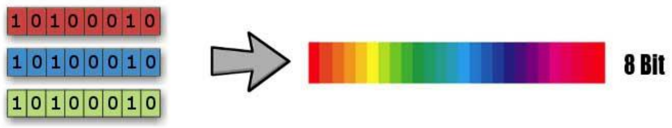


Fig. 4.1 8-bit color, with 3 bits of red, 3 bits of green, and 2 bits of blue

Consider an 8-bit color image *figure (4.1)* where each pixel is stored as a byte representing a grayscale value. Suppose the first three pixels of the original image have the following values:

4.2 24 Bit Color:

24 bits almost always uses 8 bits of each of R, G, B. As of 2018 24-bit color depth is used by virtually every computer and phone display and the vast majority of image storage formats. Almost all cases where there are 32 bits per pixel mean that 24 are used for the color, and the remaining 8 are the alpha channel or unused. The human eye can discriminate up to ten million colors and since the gamut of a display is smaller than the range of human vision, this means this should cover that range with more detail than can be perceived [9], [10]. However displays do not evenly distribute the colors in human perception space so humans can see the changes between some adjacent colors as color banding. Monochromatic images set all three channels to the same value, resulting in only 256 different colors and thus more visible banding. Some software attempts to dither the gray level into the color channels to increase this, although in modern software this is much more used for sub-pixel rendering to increase the space resolution on LCD screens where the colors have slightly different positions. Macintosh systems refer to 24-bit color as "millions of colors". The term "True color" is sometime used to mean what this article is calling "Direct color". It is also often used to refer to all color depths greater or equal to 24 [11].

4.3 Evaluation of Image Quality:

For comparing stego image with cover image results requires a measure of image quality, commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio [12] and histogram. The *Mean Square Error (MSE)* and the *Peak Signal to Noise Ratio (PSNR)* are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error [13], [14], [15].

4.3.1 Mean-Squared Error:

The Mean Square Error (MSE) represents the cumulative squared error between the compressed and the original image. The lower the value of MSE, the lower the error. The block calculates the mean-squared error using the following equation:

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M * N}$$

M and *N* are the number of rows and columns in the input images, respectively.

4.3.2 Peak Signal-to-Noise Ratio:

The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed, or reconstructed image.

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

R is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then *R* is 1. If it has an 8-bit unsigned integer data type, *R* is 255, etc.

4.3.3 Histogram:

Histograms are a type of bar plot for numeric data that group the data into bins. After you create a Histogram object, you can modify aspects of the histogram by changing its property values. This is particularly useful for quickly modifying the properties of the bins or changing the display.

V. SIMULATION RESULTS AND DISCUSSION

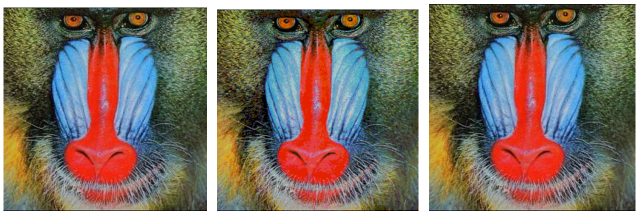
The proposed method, LSB technique and technique in [16] are simulated using MATLAB R2013a. in this section presents experiment results obtain for three cases –I, II and III, cover images, first image is “bitmap; jpeg; png” format *figure (5),* For experiments we have embedded variable amount of cipher in different standard color images of same and different dimensions to estimate the performance of the proposed technique [17]. The proposed technique is evaluated by 3 different perspectives; hiding the same amount of cipher in different images of the same dimensions; hiding variable amount of cipher in the same image of the same dimension and hiding same amount of cipher in the same image of different dimensions [18]. An 8-bit image of 256*256 is used as the cover image to form the stego image, concealing a 255*255 secret image. Both, the secret image and the cover image are in the .bmp‟ format.

There are three constant references along with different image format conditions are discussed for hiding image Steganography using LSB method which are as follows:

(a) (b) (c)

Fig. 5 Original Cover Image format (a) **.bmp** (b) **.jpg** and (c) **.png**

In our project we are using secret data as an image which is in .bmp; .jpg; & .png format and secret data is of size 255×255 as shown in figure (6).



(a) (b) (c)

Fig. 6 Secrete Image format (255 x 255) (a) **.bmp** (b) **.jpg** and (c) **.png**

This stego image is having of same size (i.e 255× 255) as that of cover image, in which we are hiding a secret image as shown in figure (7).

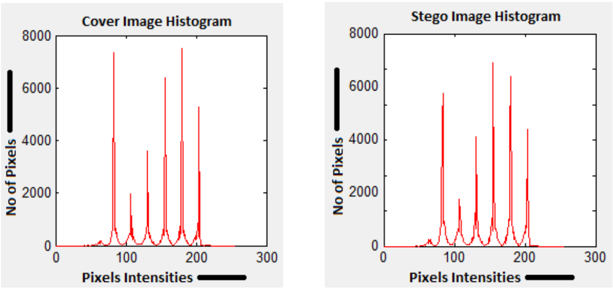
(a) (b) (c)

Fig. 7 Stego Image format (255 x 255) (a) **.bmp** (b) **.jpg** and (c) **.png**

Case-I Condition for .BMP Image format:

From figure – (6a) to (6d) shows the cover image Lena with its stego image *(.bmp) format* and *image size is 255x255, 191 KB*. The PSNR and MSE values have been shown between original Lena cover image and stego Lena image.

(a) (b)

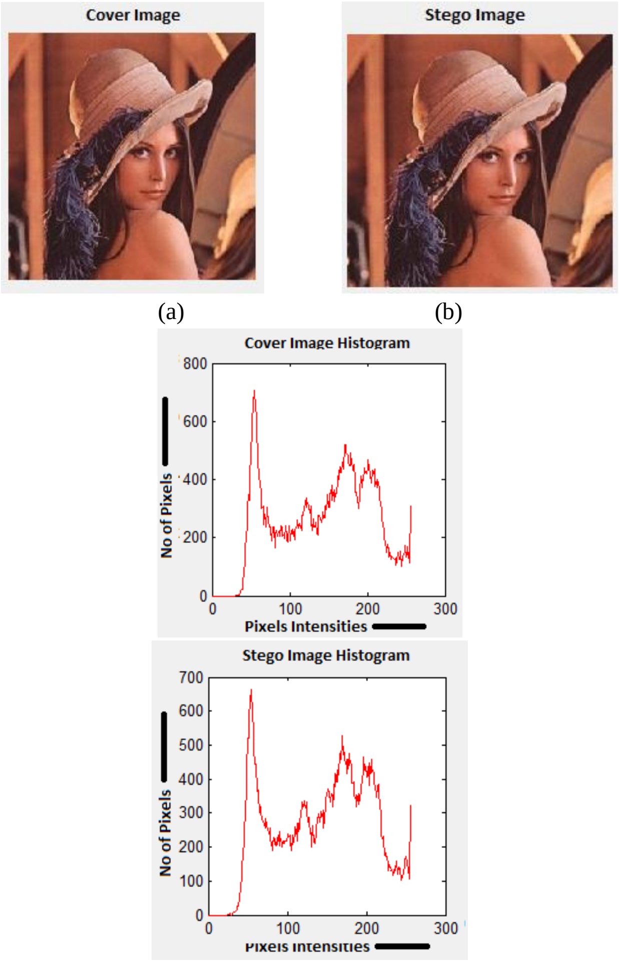


(c) (d)

Fig. 6: Lena cover and stego image (.bmp) format and their histograms

Case-II Condition for .JPG Image format

From figure (7a) to (7d) shows the cover image Lena with its stego image *(.jpg) format* and *image size is 255x255, 25.8 KB*. The PSNR and MSE values have been shown between original Lena cover image and stego Lena image.

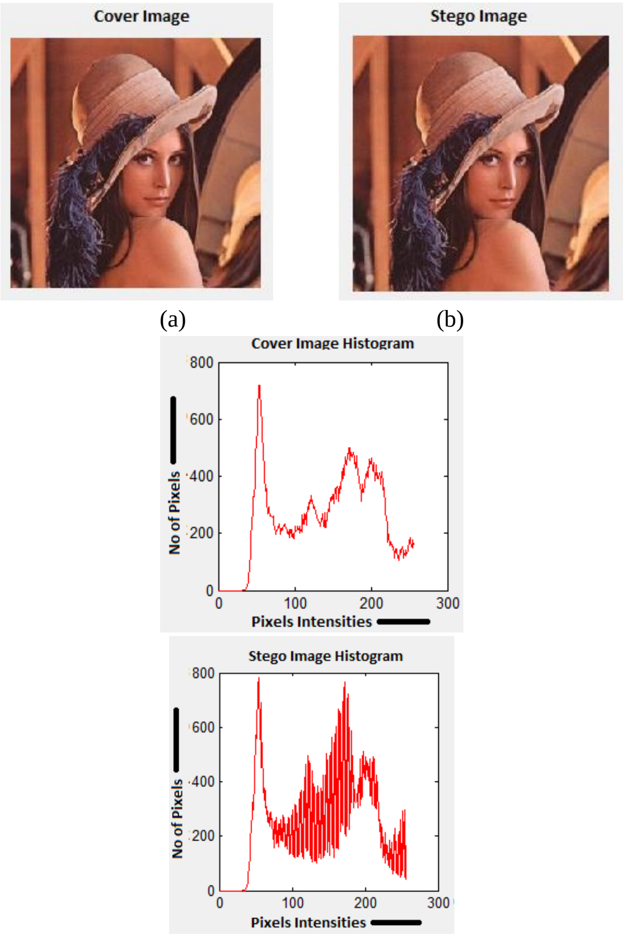


(c) (d)

Fig. 7: Lena cover and stego image (.jpg) format and their histograms

Case-II Condition for .PNG Image format

From figure (8a) to (8d) shows the cover image Lena with its stego image *(.png) format* and *image size is 255x255, 129 KB*. The PSNR and MSE values have been shown between original Lena cover image and stego-Lena image.



(a) (b)

(c) (d)

Fig. 8: Lena cover and stego image (.png) format and their histograms

Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are used to comparing the squared error between the original image and the reconstructed image. There is an inverse relationship between PSNR and MSE. So a higher PSNR value indicates the higher quality of the image (better). A comparison of BMP, JPG, and PNG image format with the using of LSB in each RGB channel as shown in table 1 and 2.

Table 1: PSNR Calculation Results of Image formats with LSB method in each R, G, B Channel

Cases	**Image Formats**	**PSNR-R**	**PSNR-G**	**PSNR-B**
I	Lena.bmp & Stego.bmp	53.20	56.19	56.95
II	Lena.jpg & Stego.jpg	37.68	38.73	37.43
III	Lena.png & Stego.png	53.07	52.80	52.36

Table 2: MSE Result of different Image formats with the use of LSB method in each R, G, B Channel

Cases	**Image Formats**	**MSE-R**	**MSE-G**	**MSE-B**
I	Lena.bmp & Stego.bmp	0.31	0.16	0.13
II	Lena.jpg & Stego.jpg	11.17	8.76	11.82
III	Lena.png & Stego.png	0.32	0.34	0.38

VI. CONCLUSION AND FUTURE WORK

In this paper proposed work for performance evaluation of secrete image Steganography techniques using LSB method for data and image security, its comparison on different size and image format (.bmp; .jpg; .png) and calculate its parameters like PSNR and MSE for its to analyze its hiding capacity with that of MATLAB implementation, which is a powerful method for data and image security. In this paper, we evaluate the performance of different cases of LSB Steganography with the help of MATLAB. Future work can be done in way to combining the concepts of cryptography and steganography, to provide more security to the secrete data message. Some more steganalytic techniques for text messages and to extend our model to mobile communication can be performed.

REFERENCES

[1] Sofyane Ladgham Chikouche and Noureddine Chikouche, "An improved approach for lsb-based image steganography using AES algorithm", *5th International Conference on Electrical Engineering - Boumerdes (ICEE-B), IEEE Xplore*, *14 December 2017.*

[2] Provos N. and Honeyman P, "Hide and Seek: An Introduction to Steganography", *IEEE Security and Privacy, vol. 01, issue 3, pp. 32-44,* May-June 2003.

[3] F. Piper, "Basic Principles of Cryptography", *IEEE Colloquium on Public uses of Cryptography, pp. 2/1-2/3, April* 1996.

[4] I.J. Cox, M.L. Bloom, J.A. Fridrich, and T. Kalkert, "Digital watermarking and Steganography", *USA: Morgan Kaufman Publishers, pp. 1-591*, 2008.

[5] Ashish T. Bhole and Rachna Patel, "Steganography over video File using Random Byte Hiding and LSB Technique", *IEEE international conference on computational intelligence and computing research*. 2012

[6] R.Nivedhitha and Dr.T.Meyyappan, "Image Security using Steganography and Cryptographic Techniques", *International Journal of Engineering Trends and Technology, Vol.7, pp. 366-371*, 2012.

[7] T. Sharp, "An implementation of key-based digital signal steganography," in Proc. Information Hiding Workshop, vol. 2137, Springer LNCS, 2001, pp. 13–26.

[8] Anjali A. Shejul, Prof. U. L. Kulkarni, "A DWT based Approach for Steganography using Biometric", *International Conference On Data Storage and Data Engineering, IEEE, pp. 39-43*, 2010.

[9] Wai Wai Zin, "Implementation and Analysis of Three Steganographic Approaches", *IEEE Xplore International Conference on Computer Research and Development, pp. 456-460*, March 2011.

[10] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das "A Tutorial Review on Steganography" *International conference on contemporary computing, volume 101*, 2008/8/7.

[11] Mehdi Hussain, Mureed Hussain, "A Survey of Image Steganography Technique", *International Journal of Advanced Science and Technology, Vol. 54, pp. 113-124*, 2013.

[12] C. Science and B. Bridgeport, "A Novel Video Steganography Algorithm in the Wavelet Domain Based on the KLT Tracking Algorithm and BCH Codes," (2015).

[13] Neil F. Johnson, Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", *IEEE, pp. 26-34*, Feb1998.

[14] Dr. R. Sridevi, Vijaya Lakshmi Paruchuri, K.S. Sadasiva Rao, "Image Steganography combined with Cryptography", *International Journal of Computers & Technology, Vol.9, pp. 976-984*, July 2013.

[15] Lokesh Kumar, "Novel Security Scheme for Image Steganography using Cryptography Technique", *International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, pp. 143-146*, April 2012.

[16] Ms. Hemlata Sharma,Ms. MithleshArya, Mr. Dinesh Goyal , "Secure Image Hiding Algorithm using Cryptography and Steganography", *IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 13(5), pp. 1-6*, August 2013.

[17] S.Ashwin, J.Ramesh, K.Gunavathi, "Novel and Secure Encoding and Hiding Techniques Using Image Steganography: A Survey", *IEEE Xplore International Conference on Emerging Trends in Electrical Engineering and Energy Management, pp. 171-177*, Dec 2012.

[18] Humanth Kumar, M.Shareef, R. P. Kumar, "Securing Information Using Steganography", *IEEE Xplore International Conference on Circuits, Power and Computing Technologies, pp. 1197-1200*, March 2013.

BIOGRAPHIES

Anupriya Arya was born in Kanpur, India. She received the degree in Bachelor of Computer Application (BCA) in 2011 from CSJM University, Kanpur, India and Master of Computer Application (MCA) from KNIT, Sultanpur, India 2014. She is currently a M.Tech Student in Computer Science & Engineering Department from BabaSahab Bhim Rao Ambedkar Central University, Lucknow, India. Her current research interests include image processing and cryptography.

Sarita Soni working as a Assistant Professor.She received the B.Tech degree in Computer Science & Engineering from AIET Lucknow which is affiliated by AKTU Lucknow, India in 2013. And M.Tech degree in Computer Science & Engineering From KNIT Sultanpur which is affiliated by AKTU lucknow India , in 2016. In August 2016, She joined the Department of Computer Science & Engineering from BabaSahab Bhim Rao Ambedkar (A Central University), Lucknow, India. Her current research area include QoS based Routing Protocol in MANET, Wireless Routing Protocol in VANET, QoS in Cloud Computing, & Network Security, Cryptography.