VISUAL CRYPTOGRAPHIC STEGANOGRPHY IN IMAGES

Neha Chhabra*

ABSTRACT:

In the multimedia steganocryptic system, the message will first be encrypted using public key encryption algorithm, and then this encrypted data will be hidden into an image file thus accomplishing both data encoding and hiding. The multimedia data will be used to provide the cover for the information. Visual steganography is one of the most secure forms of steganography available today. It is most commonly implemented in image files. However embedding data into image changes its color frequencies in a predictable way. To overcome this predictability, we propose the concept of multiple cryptography where the data will be encrypted into a cipher and the cipher will be hidden into a multimedia image file in encrypted format. We shall use traditional cryptographic techniques to achieve data encryption and visual steganography algorithms will be used to hide the encrypted data.

* Asst. Prof.(CSE Deptt,) GNI, Mullana.

1. INTRODUCTION:

In today's information age, information sharing and transfer has increased exponentially. The threat of an intruder accessing secret information has been an ever existing concern for the data communication experts. Cryptography and steganography are the most widely used techniques to overcome this threat. Cryptography involves converting a message text into an unreadable cipher. On the other hand, steganography embeds message into a cover media and hides its existence. Both these techniques provide some security of data neither of them alone is secure enough for sharing information over an unsecure communication channel and are vulnerable to intruder attacks. Although these techniques are often combined together to achieve higher levels of security but still there is a need of a highly secure system to transfer information over any communication media minimizing the threat of intrusion. In this paper we propose an advanced system of encrypting data that combines the features of cryptography, steganography along with multimedia data hiding. This system will be more secure than any other these techniques alone and also as compared to steganography and cryptography combined systems**.**

Steganography is the art of "secret communication". Its goal is to transmit a message (information) hidden inside another visible message. The typical visible message used in many steganographic systems is a digital image and the embedded message is usually hidden by working in the Fourier domain. The message is first coded by a sequence of small irregular images and then merged inside another image together with many other small images. Visual steganography is one of the most secure forms of steganography available today. It is most commonly implemented in image files. However embedding data into image changes its color frequencies in a predictable way. To overcome this predictability, we propose the concept of multiple cryptography where the data will be encrypted into a cipher and the cipher will be hidden into a multimedia image file in encrypted format. We shall use traditional cryptographic techniques to achieve data encryption and visual steganography algorithms will be used to hide the encrypted data.

1.1 BASIC OVERVIEW ON STEGANOGRAPHY

Steganography is the art of hiding the existence of the communication message before sending it to the receiver. It has been practiced since 440 B.C. in many ways like writing information on the back of cattle in a herd, invisible ink etc. Some relatively modern ways include hiding the information in newspaper articles and magazines etc. The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words “steganography means hiding one piece of data within another”. Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level. Hiding information into a media requires following elements

•The cover media(C) that will hold the hidden data

•The secret message (M), may be plain text, cipher text or any type of data

•The stego function (Fe) and its inverse (Fe-1)

•An optional stego-key (K) or password may be used to hide and unhide the message. The stego function operates over cover media and the message (to be hidden) along with a stego-key (optionally) to produce a stego media (S).

The schematic of steganographic operation is shown below.

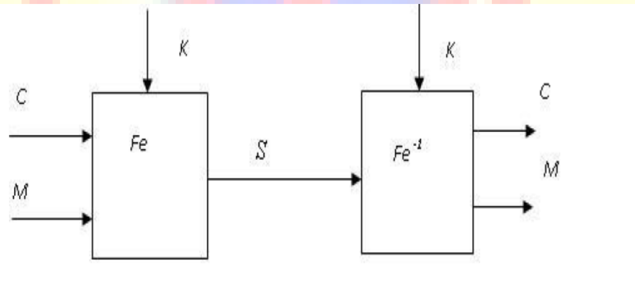

Figure1.1: The Steganographic operation

1.2 MULTIMEDIA STEGANOGRAPHY

Multimedia steganography is one of the most recent and secure forms of steganography. It started in 1985 with the advent of the personal computer applied to classical steganography problems. Visual steganography is the most widely practiced form of steganography and is usually done using image files. It started with concealing messages within the lowest bits of noisy images or sound files. Images in various formats like jpeg have wide color spectrum and hence do not reflect much distortion on embedding data into them.

We shall perform steganography on image files and we shall hide the encrypted message into image files in an encrypted format thus achieving a multiple cryptographic system. The most commonly used technique for image steganography is bit insertion where the LSB of a pixel can be modified. Ref [4] explains various other techniques involve spread spectrum, patch work, JPEG compression etc. Instead of traditional LSB encoding, we will use a modified bit encoding technique to achieve image steganography in which each pixel will store one byte of data.

1.3 MULTIMEDIA IMAGE FILES

Multimedia content basically comprises of images, videos and audio files. Images form the basis of visual multimedia. Videos are streams of images displayed in sequence at a certain speed. We shall focus on image files to achieve visual steganography.

Images are visual data stored in a picture frame. Images basically are made up of various regions consisting of pixels. These pixels in turn consist of three basic colors R (red), G (green) and B (blue). The pixel values (R, G, B values) can be manipulated to hide data in the images. A marginal deviation in these pixel values does not alter the images as a whole but a slight shade difference occurs in the altered region that is not visible in normal conditions. The image can hence serve as a cover for the information so as to achieve steganography. The edited image can be transmitted to the receiver along with the original image. The receiver then can decode the data from the image by pixel based image comparison [6]. The process involved in encoding and decoding uses a blend of media cryptography and asymmetric cryptographic algorithms. An image or a multimedia data has 5 + 1 properties which include the position of color pixel on the x-axis, the position of color pixel in the y-axis, the R component of color, the G component of color, the B component of color and the sixth is the image description properties like size, timestamp etc. These properties are stored in the first few lines of image property description. The number of bits per pixel is also a property that varies in different images. To achieve a more general bit encoding system we shall use 8-bits per pixel image.

1.4 VISUAL CRYPTOGRAPHY

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1994. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images and layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

When the random image contains truly random pixels it can be seen as a one-time pad system and will offer unbreakable encryption. In the overlay animation you can observe the two layers sliding over each other until they are correctly aligned and the hidden information appears. To try this yourself, you can copy the example layers 1 and 2, and print them onto a transparent sheet or thin paper. Always use a program that displays the black and white pixels correctly and set the printer so that all pixels are printed accurate (no diffusion or photo enhancing etc). You can also copy and past them on each other in a drawing program like paint and see the result immediately, but make sure to select transparent drawing and align both layers exactly over each other.

1.5 HOW VISUAL CRYPTOGRAPHY WORKS

Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks.

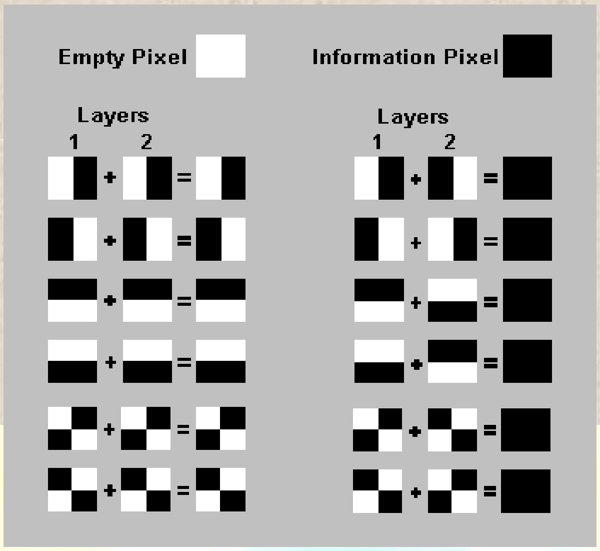

Figure1.2 Pixel Partition

In the fig above we can see that a pixel, divided into four parts, can have six different states. If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlaid pixel will be half black and half white. Such overlaid pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlaid version will be completely black. This is an information pixel.

We can now create the two layers. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlaid. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlaid, the areas with identical states will look gray, and the areas with opposite states will be black.

The system of pixel can be applied in different ways. In our example, each pixel is divided into four blocks. However, you can also use pixels, divided into two rectangle blocks, or even divided circles. Also, it doesn't matter if the pixel is divided horizontally or vertically. There are many different pixel systems, some with better contrast, higher resolution or even with color pixels.

If the pixel states of layer 1 are truly (crypto secure) random, both empty and information pixels of layer 2 will also have completely random states. One cannot know if a pixel in layer 2 is used to create a grey or black pixel, since we need the state of that pixel in layer 1 (which is random) to know the overlay result. If all requirements for true randomness are fulfilled, Visual Cryptography offers absolute secrecy according to the Information Theory.

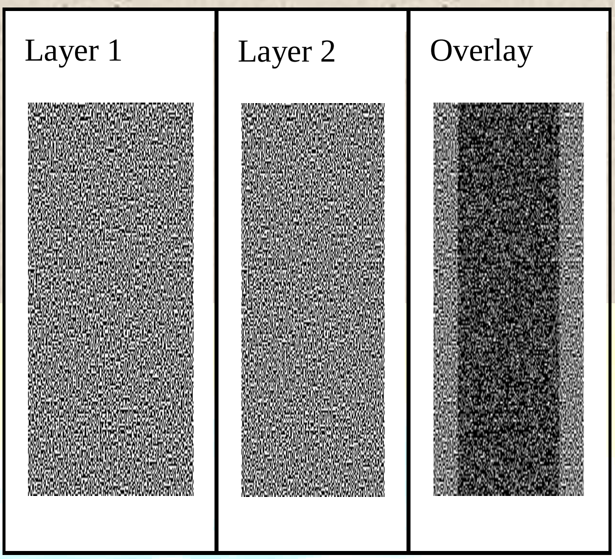

Figure1.3

If Visual Cryptography is used for secure communications, the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as both layers don't fall in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information.

2. IMPLEMENTATION:

In the multimedia steganocryptic system, the message will first be encrypted using public key encryption algorithm, and then this encrypted data will be hidden into an image file thus accomplishing both data encoding and hiding. The multimedia data will be used to provide the cover for the information. Each color in the multimedia data when considered as an element in an arrangement of 3D matrix with R, G and B as axis can be used to write a cipher (encoded message) on a 3D space. The method which we will use to map the data is a block or a grid cipher. This cipher will contain the data which will be mapped in a 3-D matrix form where the x-axis can be for R (red), y-axis can be for G (green) and z-axis can be for B (blue)

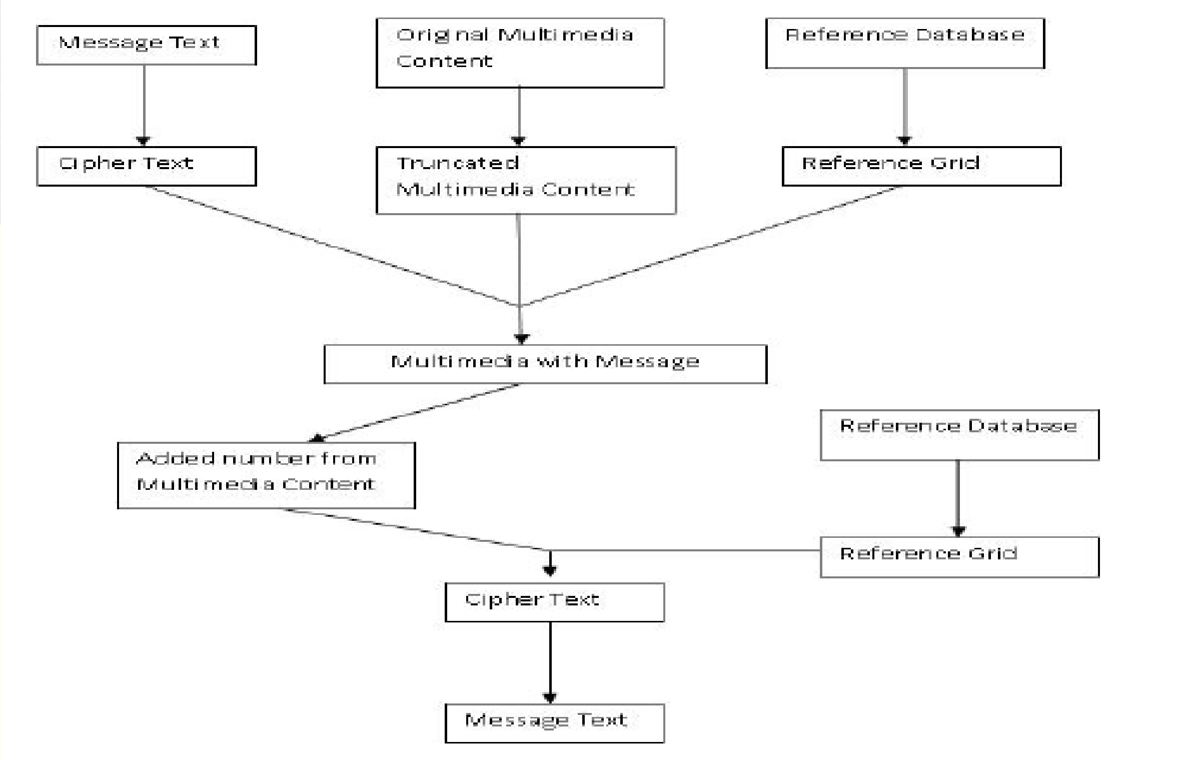

Fig 2.1 System Flow Chart

Embedding data into an image often changes the color frequencies in a predictable way and also gives redundancy in formats like bmp. To remove this predictability, we will embed the cipher in the image in an encrypted form using a reference database instead of direct bit variations. Also only jpeg image will be used as it reflects the least impact of steganography

3. PROPOSED METHOD:

Cryptographic algorithms generally need a reference table which aids the conversion of a small block of data into another block (may not be a block of data in the original content).

• In order to provide higher security levels the algorithm is designed to use a reference database as shown in Fig. 2. The reference database will consist of various reference grids. Each of these grids will have a 3-d representation of the encoding schema which will be used to represent the characters in terms of specific numbers. (The same number may or may not represent a different character in a different grid).

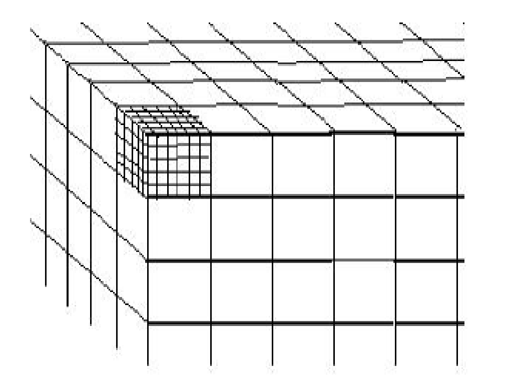

Fig. 3.1 Matrices in a Grid of the Reference database

3.1 Encryption Algorithm

• The message will first be encrypted using Asymmetric Key Cryptography technique. The data will be encrypted using basic DES algorithm [9]. This cipher will now be hidden into a multimedia file.

• The cipher will be saved in the image using a modified bit encoding technique by truncating the pixel values to the nearest zero digit (or a predefined digit) and then a specific number which defines the 3-D representation of the character in the cipher code sequence can be added to this number. For every character in the message a specific change will be made in the RGB values of a pixel. (This change should be less than 5 for each of R,G and B values) This deviation from the original value will be unique for each character of the message. This deviation also depends on the specific data block (grid) selected from the reference database. For each byte in the data one pixel will be edited. Thus one byte of data will be stored per pixel in the image.

• In this method the cipher sequence can be decoded without the original image and only the edited image will be transmitted to the receiver.

• In the first few lines of image properties, the attributes of the image will be encrypted and saved so as to provide us the information if the image is edited or modified or the image extension has been changed like jpg to gif. These properties can be used in the decoding (identifying the correct block of data from the data grid). So only the correct encrypted image in the correct format will produce the sent message.

• For decryption, the receiver must know which image to decode and in which format as changing the image format changes the color distribution of the image. Every image gives a random data on decryption that has no meaning. But only the correct Format decryption gives the original message.

• After hiding the data in the image, the image will be sent to the receiver. The receiver should have the decryption key (private key) which will be used to decode the data.

3.2. Decryption Algorithm

• The message can be decoded using an inverse function (as used in traditional techniques) using the receiver's private key. This key can be a part of the image or a text or any attribute of the image.

• The receiver's private key is used to identify the reference grid from the reference database.

• After selecting the correct grid, the x and y component of the image can define the block that has been used to encrypt the message and the RGB values can point to the data in the block identified by the x, y component as shown in Fig. 3.2

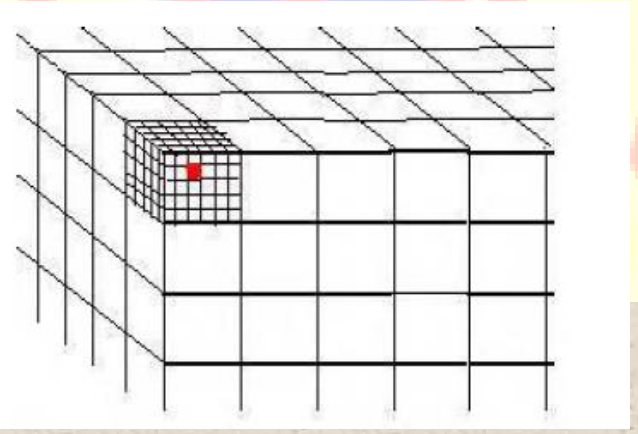

Fig.3.2 Matrix in a grid of Reference database

• The cipher is retrieved by obtaining the difference in the pixel value from the closest predefined value (zero truncation). These numbers will now define the saved bit and will form the cipher text.

• This cipher can now be decrypted using an inverse function of the DEA algorithm to get the message text.

4. EXPERIMRNTAL RESULTS:

The system was designed using an image of size 200x150(30000) pixels. Initially, the pixel values were incremented to the next higher multiple of 5. The message text was converted into cipher text using DEA algorithm. The secret key used was 'This is the Secret Key'. Maximum possible size (29 Kb) of message data was taken considering one byte per pixel. The cipher text was then embedded into the jpeg image by pixel variation (decrement) of the selected value that was between 0-3 for R, 0-4 for G and 0-4 for B values of the pixel. The reference database consisted of 3 data grids. The data grid was selected on the basis of the number of pixels of the image. If the pixels were less than 1, 00,000 pixels the data grid 1 was selected, if they were between 1, 00,000 and 10, 00,000 then the data grid 2 was selected else the data grid 3 was selected. Each data grid had 20 matrices which were selected on the basis of the height to width ratio. The image containing message data was found to have no visible distortion.

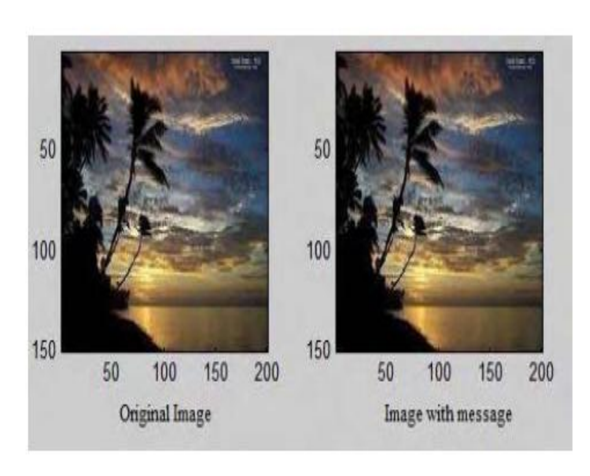

Fig. 4.1 Encryption result of the application.

For decryption the cipher was retrieved by checking the pixel variations and inverse DEA function was applied to retrieve the message. To retrieve the cipher from the image, the difference in the pixel value from the next higher multiple of 5 was calculated. The correct data grid from the reference database was selected on the basis of the number of pixels in the image. The correct matrix from the data grid was selected on the basis of the height to width ratio. After this the encrypted message was retrieved from the image. The inverse DEA function was applied to this encrypted message in order to retrieve the original message text.

The steganocryptic algorithm combines the features of cryptography and steganography and hence provides a higher level of security than either of the techniques alone. The algorithm also is more secure than a normal cryptographic system as the encrypted data is hidden into a multimedia file and then transmitted. It is also more secure than a Steganography system as the data to be hidden is in an encrypted format. The algorithm scores over traditional visual steganography systems like LSB encoding as it implements multiple encryptions.

The image bits are used not to store the message but a slight deviation which correspond to a unique character. This deviation is then retrieved from the image and used to decrypt the original message. The image used for encryption is jpeg as it has the least deviation of embedding data.

5. APPLICATIONS:

This method can be used to increase the security on web based applications. The user will be asked to provide the secret key and the password can be compared from image files using the key. It can be used as advancement over the existing option to input the security phrase in various web based applications.

Cryptography was used to assure only secrecy. Wax seals, signatures, and other physical mechanisms were typically used to assure integrity of the media and authenticity of the sender. With the advent of electronic funds transfer, the applications of cryptography for integrity began to surpass its use for secrecy. Electronic cash came into being from cryptography, and the electronic credit card and debit card sprung into widespread use. The advent of public key cryptography introduced the possibility of digital signatures, and other related concepts such as electronic credentials. In the information age, cryptography has become one of the major methods for protection in all applications

Steganography is applicable to the following areas:

1) Confidential communication and secret data storing

2) Protection of data alteration

3) Access control system for digital content distribution

4) Media Database systems

In the case of a secret message being transferred the information can be kept inside a multimedia data which will be the normal cipher which had to be transferred. This multimedia data can be transferred in the normal way. Video files and image streams can also be used to transmit data. In case of image streams part of message can be sent in each image. This will increase the security of the system, however the time consumption will increase in this case.

6. CONCLUSION:

The proposed system is aimed to simplify the complex and redundant process with the flexibility of a simple process. The proposed system is being developed as an attempt to overcome the difficulties of the existing system.

The following are the merits of the proposed system.

- It provides two levels of security to the information being transmitted. That is the intruders cannot easily break the system. Even if they realize the existence of a secret data they cannot easily recognize the data, since data is hidden in two ways.
- This system overcomes the demerits of using single level of hiding. That is either using cryptography or steganography. And one more thing to add is it requires only the computation time of single level hiding, because visual cryptography requires no computation to decrypt the information.
- This method can be used to increase the security on web based applications. The user will be asked to provide the secret key and the password can be compared from image files using the

key. It can be used as advancement over the existing option to input the security phrase in various web based applications.

- In the case of a secret message being transferred the information can be kept inside a multimedia data which will be the normal cipher which had to be transferred. This multimedia data can be transferred in the normal way. Video files and image streams can also be used to transmit data. In case of image streams part of message can be sent in each image. This will increase the security of the system, however the time consumption will increase in this case.

7. REFERENCES:

- Homes.esat.kuleuven.be/~fvercaut/talks/visual.pdf
- www.bioinfo.in/uploadfiles/13255803791_1_6_IJCI.pdf
- wscg.zcu.cz/wscg2002/papers_2002/a73.pdf
- www.ijest.info/docs/IJEST10-02-06-83.pdf
- www.cs.fsu.edu/~yasinsac/group/slides/burke2.pdf

8. AUTHOR'S PROFILE:

Neha Chhabra received the bachelor degree in Computer Science and Engineering from Haryana Engineering College, Jagadhri, India in 2010.Currently persuing Masters in CSE From Kurukshetra University. She has 2 year teaching experience. Presently she is working in Computer Science and Engineering Department of Guru Nanak Institutions Mullana.