International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol. 9, Issue.7, July 2021 E-ISSN: 2347-2693

Literature Review on Improving Data Security using DES and DCT

Vikas Singhal[1*], Devendra Singh[2], Sanjai Gupta[3]

[1]Research Scholar, IFTM University, Moradabad, India
[2]Department of Computer Science and Engineering, IFTM University, Moradabad, India
[3]Department of Computer Science and Engineering, BIET, Jhansi, India

[*]*Corresponding Author: vikassinghal75@gmail.com, Tel.: 9818088860*

DOI: https://doi.org/10.26438/ijcse/v9i7.7883 | Available online at: www.ijcseonline.org

Received: 12/Jul/2021, Accepted: 19/Jul/2021, Published: 31/Jul/2021

***Abstract*—** Steganography is the art and science for hiding information by embedding data into cover media. Image processing in steganography is done mainly by using spatial domain and frequency domain. In this review literature, hiding spatial domain using LSB technique and hiding frequency domain using DCT technique is studied and compared. BMP cover images with 256x256 and 512x512 resolutions for LSB and DCT techniques are used for experimental study. For DCT technique, various BMP image is converted to JPEG image. The DCT technique is used to hide the data into the JPEG cover image. The resultant stego image obtained in JPEG is converted to BMP stego image. Thereafter, the comparison tool PSNR is used to compare the BMP images obtained from LSB and DCT. The data security and privacy play an important role for data transmission for exchanging information over internet. The two techniques like; cryptography and steganography both are pillars to be utilized for securing digital data by using different methods specifically DES (Data Encryption Standard) and DCT (Discrete Cosine Transform). The mixture of DES and DCT improves the digital data security with multiple level of security for encryption process which shows better results. In this research, we analyze the combination of cryptographic method with DES technique and stenographic method with DCT technique to develop a framework for digital data security environment. This paper also presents a proposed least significant bit (LSB) based framework for DES and DCT to secure digital data with better compression approach**.**

***Keywords*—** LSB, DCT, DES, Stego Image

I. INTRODUCTION

Steganography is the art and science of communicating in a way that the presence of a secret message apart from the identity of the sender and intended recipient cannot be detected by unauthorized users. Steganography is a technique which is used to hide a secret message within a cover media in such a way that others cannot detect the presence of the hidden message. Steganography is made from the Greek words *steganos* meaning "covered or protected" and *graphei* meaning "writing". While classical cryptography is about concealing the content of messages, steganography is about concealing their existence.

Steganography goes back to ancient times and used by different cultures such as: Greeks, Chinese, and medieval Europe. A famous case which dates back to 1586, when Mary Queen of Scots was conspiring to have Queen Elizabeth of England assassinated, with a view to taking over the English throne [1]. Also during the 1980's, Margaret Thatcher became so irritated at press leaks of cabinet documents that she had the word processors programmed to encode their identity in the word spacing, so that disloyal ministers could be traced [2]. Similar techniques are now undergoing trials in an electronic publishing project, with a view to hiding copyright messages and serial numbers in documents. In some applications, it is enough to hide the identity of either the sender or the recipient of the message, rather than its very existence [3]. Modern steganography entered the world in 1985 with the advent of the personal computer being applied to classical steganography problems. Also in modern Steganography practice the larger the cover message is relative to the hidden message, the easier it is to hide the latter [4].

II. BASIC FRAMEWORK OF STEGANOGRAPHY

An Example of steganography can be given in terms of communication between two people, Alice and Bob, where Alice and Bob are two inmates who wish to communicate in order to exchange some secret information. However, all communication between them is examined by the eavesdropper, Wendy, the third party who will try hardly to disclose, alter and/or destruct their secret message. Specifically, in the general model for steganography, illustrated in Figure 1.1, Alice wishes to send a secret message *m* to Bob. In order to do so, she "embeds" *m* into a *cover-object c*, and obtains a *stego-object s*. The stego-object *s* is then sent through the public channel. Thus we have the following definitions:

Cover-object: is the object used as the carrier to embed messages into many different objects have been employed

to embed messages into for example images, audio, and video as well as file structures, and html pages to name a few.

Stego-key: is the code that the sender of the secret message is going to use to embed the message into the cover-object. This same stego-key will be used by the recipient to extract the secret message.

Stego-object: is the combination of the cover object, the stego-key and the secret message

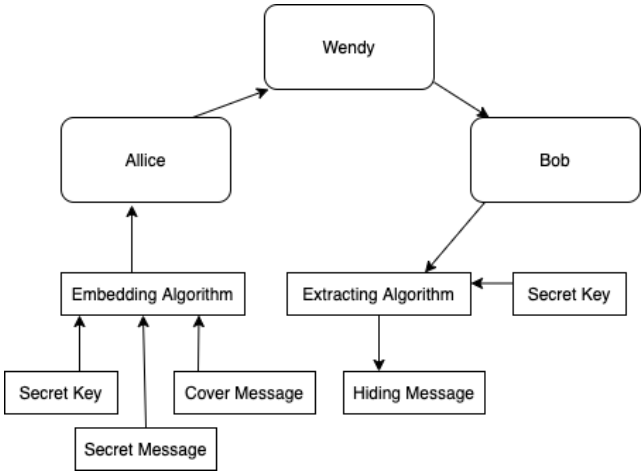

Figure 1: General model of Steganography [5]

III. TYPES OF STEGANOGRAPHY

The four main types of Steganography are digital image steganography, audio steganography, text steganography and video steganography. Figure 1.2 shows the overall structure of System Security which basically consists of Cryptography and Information Hiding which has been divided also into another two categories which are Watermarking and Steganography. This study will focus on information hiding using digital image steganography.

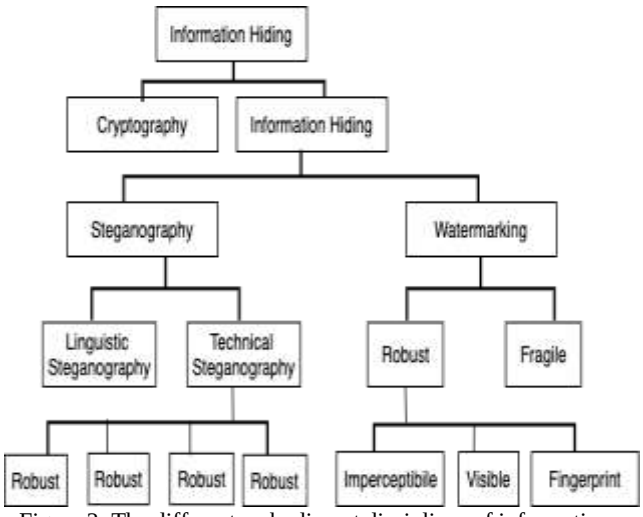

Figure 2: The different embodiment disciplines of information hiding [6]

A cover object is the object designated to carry the embedded bits or secret information. The cover objects can be a text file, image file, audio file or video file.

A. TEXT STEGANOGRAPHY

Historically hiding information in the text was a simple and the most important method of steganography but due to the beginning of the Internet and due to the different type of digital file formats it has decreased in importance. Text steganography using digital files is not used very often because the text files have a very small amount of redundant data [8].

B. AUDIO STEGANOGRAPHY

Audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. An audible, sound becomes inaudible in the presence of another louder audible sound. This property allows the selection of the channel in which the information will be hidden. Although it is similar to images in steganographic potential, the larger size of meaningful audio files makes them less likely to use than images [8].

C. IMAGE STEGANOGRAPHY

Image Steganography will be used as cover object or host image for this project because Images are considered as the most popular file formats used in steganography. They are known for constituting a non-causal medium, due to the possibility to access any pixel of the image at random. In addition, the hidden information could remain invisible to the eye. However, the image steganography techniques will exploit "holes" in the Human Visual System (HVS) [8] [9].

i. Image Format

This research focuses on some specific image formats. The followings are the formats that this research focuses on.

- **TIFF File:** Tagged Image Format File (TIFF) is an image format file for high quality graphics. TIFF files were created in the 1986 as a file format for scanned imaged in an attempt to get all companies to use one standard file format instead of multiple. Though TIF files originally only supported black and white, the update in 1988 added a color palette [10].

- **GIF File:** Graphics Interchange Format is used for the purpose of storing multiple bitmap images in a single file for exchange between platforms and images. It is often used for storing multibit graphics and image data. GIF is not associated with a particular software application but was designed “to allow the easy interchange and viewing of image data stored on local or remote computer systems” [10] [11].

- **BMP File:** The letters “BMP” stand for “bitmap”, Bitmap images were introduced by Microsoft to be a standard image file format between users of their Windows operating system. The file format is now supported across multiple file systems and operating

systems, but is being used less and less often. A key reason for this is the large file size, resulting from poor compression and verbose file format. This is, however, an advantage for hiding data without raising suspicion. To understand how bitmap images can be used to conceal data, the file format must first be explained. A bitmap file can be broken into two main blocks, the header and the data. The header, which consists of 54 bytes, can be broken into two sub-blocks. These are identified as the Bitmap Header, and the Bitmap information. Images which are less than 16 bit have an additional sub-block within the header labeled the Color Palette [12] [13].

- **JPEG File:** Joint Photographic Experts Group (JPEG) format is one of the Transform Domain Techniques which has an advantage over LSB techniques because they hide information in areas of the image that are less exposed to compression, cropping, and image processing [9]. Also JPEG is most common image file format on the internet owing to the small size of resultant images obtained by using it, and it is efficient for appearing the stage image to something similar to the original image [14].

ii. Image Compression

When working with larger images of greater bit depth, the images tend to become too large to be transmitted over a standard Internet connection. In order to display an image in a reasonable amount of time, techniques must be incorporated to reduce the image's file size. These techniques make use of mathematical formulas to analyze and condense image data, resulting in smaller file sizes. This process is called compression. In images there are two types of compression: lossy and lossless [9].

- **Lossless compression:** It is known for being preferable when the original data should stay in its entirety. In this manner, the original image information will never be removed, and this makes it possible the reconstruction of the original data from the compressed data. This is typical of images in GIF and BMP.

- **Lossy compression:** It saves storage space by discarding the points the human eyes find difficult to identify. In this case the resulting image is expected to be something similar to the original image, but not the same as the original. **JPEG compression** uses this technique.

a) **JPEG Compression:** The process of embedding information during JPEG compression results in a stego image with a high level of invisibility, since the embedding takes place in the transform domain. Originally it was thought that steganography would not be possible to use with JPEG images, since they use lossy compression which results in parts of the image data being altered. JPEG images are the products of digital cameras, scanners, and other photographic image capture devices. This is simply why concealing secret information in JPEG images might provide a better disguise [9] [15].

For JPEG, the Discrete Cosine Transform (DCT) is used. It is important to recognize that the JPEG compression algorithm is actually divided into lossy and lossless stages. The DCT and the quantization phase form part of the lossy stage, while the Huffman encoding used to further compress the data is lossless. Steganography can take place between these two stages. Using the same principles of LSB insertion, the message can be embedded into the least significant bits of the coefficients before applying the Huffman encoding. By embedding the information at this stage, in the transform domain, it is extremely difficult to detect, since it is not in the visual domain [16].

IV. STEGANOGRAPHY DOMAINS AND TECHNIQUES

Over the past years, many literatures discussed the technique of information hiding. Up until now, there are two techniques developed in information hiding, spatial-domain manner and frequency-domain manner. Owing to the fact that the media considered in these literatures are image illustrations, we therefore will include images in our discussions. The so-called spatial-domain refers to the fact that the secret is mixed into the distributed pixels (regions) directly. While in the frequency-domain, it is necessary to transform the host-image first using a frequency-oriented mechanism, such as a discrete cosine transformation based (DCT-based), wavelet-based, etc., after which the secret is then combined with the relative coefficients in the frequency-form image. Let us take another look at the spatial-domain manner. Generally speaking, it is simpler to achieve the goal of information hiding in the course of secret embedding. The least significant bit (LSB for short) secret embedding or LSB-like embedding is the most commonly used method in the spatial-domain approach [17].

A. SPATIAL DOMAIN

These techniques use the pixel gray levels and their color values directly for encoding the message bits. These techniques are some of the simplest schemes in terms of embedding and extraction complexity. The major drawback of these methods is amount of additive noise that creeps in the image which directly affects the Peak Signal to Noise Ratio and the statistical properties of the image. Moreover these embedding algorithms are applicable mainly to lossless image-compression schemes like TIFF images. For lossy compression schemes like JPEG, some of the message bits get lost during the compression step. The most common algorithm belonging to this class of techniques is the Least Significant Bit (LSB) replacement technique.

- **Least Significant Bit Technique:** Popular stenographic tools based on LSB embedding vary on the existing approaches for hiding information. Some algorithms change LSB of the pixels visited in a

random walk, others modify pixels in certain areas of images, or instead of just changing the last bit they increment or decrement the pixel value. The concept of least significant bit (LSB) Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by the standard of human vision. Therefore, an altered image with slight variations in its colors will be indistinguishable from the original by a human being, just by looking at it. When using the least significant bit of the pixels' color data to store the hidden message, the image itself is seemed unaltered. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small. To hide a secret message inside an image, a proper cover image is needed. It is necessary to use a lossless compression format, because this method uses bits of each pixel in the image, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel. For example, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

When the character A, which binary value equals 10000001, is inserted, the following grid results:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

In this case, only three bits are needed to be changed to insert the character successfully. On average, only half of the bits in an image will be needed to be insider modified to hide a secret message using the maximal cover size. The result changes that are made to the least significant bit are too small to be recognized by the human visual system (HVS), so the message is effectively hidden [18]. The least significant bit of the third color remains without any changes. It can be used for checking the correctness of 8 bits which are embedded in these 3 pixels.

- **LSB Algorithm Steps**

a) Select a cover image of size M*N as an input.
b) The message to be hidden is embedded in RGB component only of an image.
c) Use a pixel selection filter to obtain the best areas to hide information in the cover image to obtain a better rate. The filter is applied to Least Significant Bit (LSB) of every pixel to hide information, leaving most significant bits (MSB).
d) After that Message is hidden using Bit Replacement method.

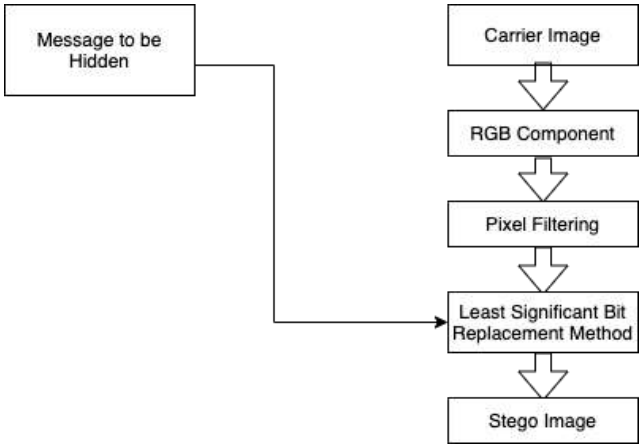

Figure 3: Algorithm of Least Significant Bit [19].

B. FREQUENCY DOMAIN

These techniques are applied in encoding message bits in the transform domain coefficients of the image. Data embedding performed in the transform domain is widely used for robust watermarking. Similar techniques can also realize large capacity embedding for steganography. Candidate transforms include Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT). By being embedded in the transform domain, the hidden data resides in more robust areas, spread across the entire image, and provides better resistance against signal processing. For example, we can perform a block DCT and, depending on payload and robustness requirements, choose one or more components in each block to form a new data group that, in turn, is pseudo randomly scrambled and undergoes a second-layer transformation. Modification is then carried out on the double transform domain coefficients using various schemes. These techniques have high embedding and extraction complexity. Because of the robustness properties of transform domain embedding, these techniques are generally more applicable to the "Watermarking" aspect of data hiding. Many stenographic techniques in these domain have been inspired from their watermarking counterparts [20] [21].

i. **Discrete Cosine Transform Technique:** DCT is a method of hiding information in transforms domain images. This method hides messages in significant areas of the cover image. The DCT transforms a signal from an image representation into a frequency representation, by grouping the pixels into 8 × 8 pixel blocks and transforming the pixel blocks into 64 DCT coefficients each A modification of a single DCT coefficient will affect all 64 image pixels in that block. The next step is the quantization phase of the compression. Here another biological property of the human eye is exploited: The human eye is fairly good at spotting small differences in brightness over a relatively large area, but not as good as to distinguish between different strengths in high frequency brightness. This means that the strength of higher frequencies can be diminished, without changing the appearance of the image. [15].

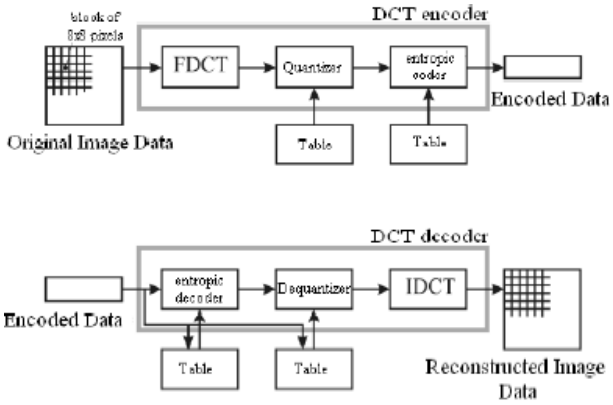

Figure 4: Block diagram of JPEG encoder and decoder [15].

- **DCT Algorithm**

a) The One-Dimensional DCT [22]

$$G_f = \frac{1}{2} C_f \sum_{t=0}^{n-1} p_t \cos\left(\frac{\pi(2t+1)f}{2N}\right)$$

$$C(f) = \begin{cases} \frac{1}{2}, & f = 0 \\ 1, & f > 0 \end{cases}$$

N=size, p=pixel, G=coefficients

b) The Two-Dimensional DCT [22]

$$G_f = \frac{1}{\sqrt{2n}} C_i C_f \sum_{x=0y=0}^{n-1n-1} p_{xy} \cos\left(\frac{\pi(2y+1)j}{2n}\right) . \cos\left(\frac{\pi(2x+1)i}{2n}\right)$$

N=size, p=pixel, G=coefficients

- **Discrete Wavelet Transform**

Wavelets are special functions which (in a form analogous to sins and cosines in Fourier analysis) are used as basal functions for representing signals. The simplest DWT is Haar. In Haar-DWT the low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. A signal is passed through a series of filters to calculate DWT [22].

I.

- **Peak Signal to Noise Ratio (PSNR)**

The Peak Signal to Noise Ratio (PSNR) is an engineering term for the well-known objective image quality metrics that uses for image measuring. Where PSNR formula is: [7] [22]

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

$$PSNR = 20.log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

$$PSNR = 20.log_{10}(MAX_I) - 10.log_{10}(MSE)$$

Where MAX_I is the maximum possible pixel value of the image and MSE is Mean Square Error.

The high PSNR value indicates high security because it indicates the minimum difference between the original and stego values. So no one can suspect the hidden information.

a) **Capacity:** The amount of information that can be hidden relative to the size of the cover object without deteriorating the quality of the cover object.

b) **Robustness:** It is the ability of the stego to withstand manipulations such as filtering, cropping, rotation and compression.

V. CONCLUSIONS

This research basically reviews a frame work of steganography, the purpose of steganography, types of steganography and different file formats of image steganography. It also discusses in detail the steganography techniques, Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) and The Peak Signal to Noise Ratio (PSNR) as a well-known objective image quality metrics that uses for image measuring.

REFERENCES

[1] Anderson, R. J., & Petitcolas, F. A., On the limits of steganography.*Selected Areas in Communications, IEEE Journal on*, **16(4), 474- 481, 1998.**

[2] Anderson, R., Stretching the limits of steganography. In *Information Hiding*. Springer Berlin Heidelberg, **pp. 39-48, 1996, January.**

[3] Amin, M. M., Salleh, M., Ibrahim, S., Katmin, M. R., & Shamsuddin, M. Z. I. Information hiding using steganography. In*Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on*, **pp. 21- 25, 2003, January**. IEEE.

[4] Saraswat, P. K., & Gupta, D. R., A Review of Digital Image Steganography. *Journal of Pure and Applied Science & Technology Copyright*, **2(1), 98-106, 2011.**

[5] General model of today's Steganography. Retrieved on **December 8, 2013** from: http://www.datahide.com

[6] Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P., Digital image steganography: Survey and analysis of current methods. *Signal processing*, **90(3), 727-752, 2010.**

[7] Hemalatha, S., Acharya, U. D., Renuka, A., & Kamath, P. R., A secure and high capacity image steganography technique. *Signal & Image Processing: An International Journal (SIPIJ)* ***Vol, 4,*** **83-89, 2013.**

[8] Kaur, R., & Singh, B., Survey and Analysis of Various Steganography Techniques. *International Journal of Computer Science and Advanced Technology*, **6(3), 561 – 566, 2012.**

[9] Hamid, N., Yahya, A., Ahmad, R. B., & Al-Qershi, O. M., Image steganography techniques: an overview. *International Journal of Computer Science and Security (IJCSS)*, **6(3), 168-187, 2012.**

[10] Rouse, M. (2010). Retrieved on **December 19, 2013,** from: http://whatis.techtarget.com

[11] Tiwari, N., & Shandilya, D. M., Evaluation of Various LSB based Methods of Image Steganography on GIF File Format. *International Journal of Computer Applications*, **0975–8887, 2010.**

[12] Grantham, B., "Bitmap Steganography: An Introduction", 2007.

[13] Fridrich, J., Goljan, M., & Hogea, D., Steganalysis of JPEG images: Breaking the F5 algorithm. In *Information Hiding*, Springer Berlin Heidelberg. **pp.310-323, 2003, January.**

[14] Provos, N., & Honeyman, P., Hide and seek: An introduction to steganography. *Security & Privacy, IEEE*, **1(3), 32-44, 2003.**
[15] Jókay, M., & Moravćík, T, Image-based JPEG steganography. *Tatra Mountains Mathematical Publications*, **45(1), 65-74, 2010.**
[16] Morkel, T., Eloff, J. H., & Olivier, M.S., An overview of image steganography. In *ISSA***, pp. 1-11, 2005, June.**
[17] Wang, S.J., Steganography of capacity required using modulo operator for embedding secret image. *Applied Mathematics and Computation*, **164(1), 99-116, 2005.**
[18] Hariri, M., Karimi, R., & Nosrati, M., An introduction to steganography methods. *World Applied Programming*, **1(3),191-195, 2011.**
[19] Joshi, R., Gagnani, L., & Pandey, S., Image Steganography With LSB.*International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, **2(1), pp-228, 2013.**
[20] Sutaone, M. S., & Khandare, M.V., Image based steganography using LSB insertion technique. In *Wireless, Mobile and Multimedia Networks, 2008. IET International Conference on*, **pp. 146-151, 2008 January.** IET.
[21] Sravanthi, M. G., Devi, M. B. S., Riyazoddin, S. M., & Reddy, M.J., A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method. *Global Journal of Computer Science and Technology Graphics & Vision*, **12 (15), 2012.**
[22] Gupta, M., & Garg, A.K., Analysis of Image Compression Algorithm Using DCT. *International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622* **Vol. 2, 515-521, 2012.**

Authors Profile

Mr. Vikas Singhal is a research scholar from IFTM University, Moradabad, India. He has completed his Masters in Technology in Information Technology from GGSP Indraprastha University Delhi. He has 20 years of teaching experience and 3 years of Research Experience.

Dr. Devendra Singh is currently working as Associate Professor at the Department of Computer Science & Engineering, IFTM University, Moradabad, India. He does research in Computer Communications (Networks), Computer Security and Reliability and Operating Systems.

Dr. Sanjai Kumar Gupta is currently working in the Department of Computer Science and Engineering at Bundelkhand Institute of Engineering and Technology, Jhansi, India.

