International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Steganography using Spatial Domain Techniques

Sumeet Kaur, R. K. Bansal, Savina Bansal

Abstract: ***In present world data transfer using the internet is growing. It is very easy and fast way to transfer information like confidential documents, economic transactions, business applications and other covert information over internet. With the advent and growth of internet, people are more concerned about security of information. Data Security is important while data is transferred over internet because any illegal user can access important and private data also make it worthless. Research in data security area will help government agencies, military organization and private companies to securely transmit their confidential data over internet. From past few years various steganography techniques have been developed to hide secret message using various multimedia objects having large amount of redundant data to support steganography. In this paper introduction about steganography, related concepts and implementation of commonly used spatial domain techniques like LSB(Least Significant Bit Technique) with modulus, PVD(Pixel Value Difference) with LSB replacement and adaptive data hiding over edges with LSB are considered. It is observed(while visual, statistical analysis and experiments were carried out) with benchmark cover and stego objects that embedding same amount of secret data in each pixel leads to more visible distortions in a stego image because all pixels do not bear same amount of changes and this effect is more observed in smooth area then edges. Improving stego image imperceptibility and adjusting hiding capacity adaptively are major related research challenges about spatial domain techniques.***

Keywords: Steganography, Secret Data, Spatial Domain, Redundant Data

I. INTRODUCTION

Internet is most extensively used for transmitting and exchanging information in present time. In current world data transfer using the internet is growing rapidly as it is a simple and rapid method to communicate personal, secret and other information. Security is a significant matter while data is transferred using public networks because any illegal user can use and/or damage data and also make it worthless or acquire information that is not supposed for him from the security point of view [1]. Steganography ensures privacy and validation for data delivered over public networks that no other security tool can provide.

Manuscript published on November 30, 2019.
* Correspondence Author
Sumeet Kaur*, Research Scholar, IKGPTU, Jalandhar. Email: purbasumeet@yahoo.com
Savina Bansal, GZS College of Engg. & Technology, Bathinda, India.
RK Bansal, GZS College of Engg. & Technology, Bathinda, India.

Steganography is a skill and science of embedding secret data into cover objects. Steganography can embed secret data within various cover objects like video, images and sound files. The key objectives of steganography methods are to increase the embedding capacity, reducing the visual distortion and change in image characteristics generated due to embedding the secret message in original cover objects [2].

Recently data embedding methods have received much attention from the industry and research community. In 1996, the very first conference was organized on data hiding subject, followed by several other seminars, workshops and conferences concentrating on data hiding. Continuous research publishing in journals, workshops, conferences and books on the subject are flourishing and highlighting the importance of information and securely transmitting it over the internet. Greek word 'Steganography' is meant 'secret or enclosed writing' [5]. It is used from ancient times and was used to shave the head of a messenger and tattooed some secret message on it and after his hair had grown then it is sent to the intended receiver to convey the secret message. Simmons acknowledged this in terms of communication in a Jail that is also usually known as 'Prison's Problem' [7]. In 1985, the concept of modern Steganography came with the development of personal computers whereas 'Digital Steganography' came into existence with the development of the internet. Steganalysis is the method of analyzing and finding out concealed secrets in the stego entity. Steganalysis has broadly two categories of analysis: Statistical and Visual Analysis. Visual investigation deals with revealing of hidden secret data with bare eyes. Statistical investigation deals with inspection of any alteration in statistical characteristics of stego object generated by steganography algorithm due to embedding [3].

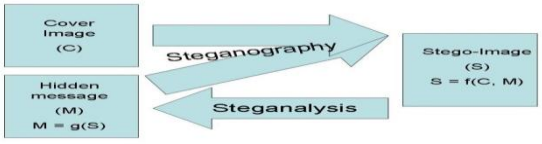

Fig: 1. Steganography and Steganalysis

II. COMMONLY USED DATA HIDING TECHNIQUES

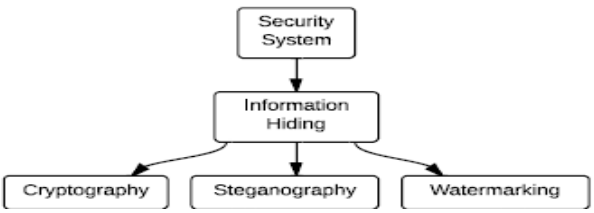

Fig: 2. Data Hiding Approaches

Data hiding techniques like cryptography, watermarking and steganography have different functions and applications. These techniques are together known as 'information hiding techniques'[4]. These methods are related but based on different concepts and have different purposes.

A. Cryptography

Also known as encryption is the science of scripting in covert codes and also consider all of the basics factors for secure communication over an insecure and public networks like authentication, confidentiality, and non-repudiation etc. Cryptography does not ensure secure communication for all time. A difficulty with cryptography is that it does not conceal the existence of confidential data and making it easier for eavesdropper to attack whereas steganography conceals the presence of covert message.

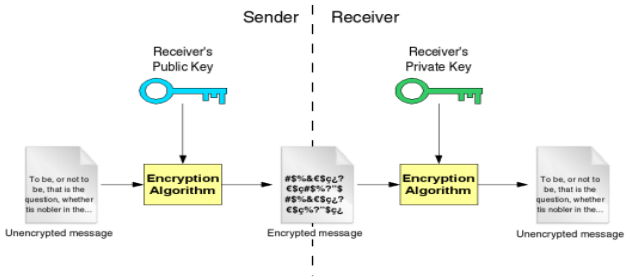

Fig: 3. Cryptography as a data Hiding Technique

B. Steganography and Watermarking

Steganography and watermarking are related to each other but differ in functions and applications. Steganography has key objective of concealing the presence of secret data into cover object with large hiding capacity, but on other hand watermarking mostly focuses on the robustness and strength of embedding instead of capacity of hidden secret message. Achieving robustness and high capacity at the same time is not possible because both are conflicting parameters. Watermarking can also be used for investigating genuine use of a particular media or software, copyright protection and also make sure a way of the ownership of such digital materials [5][6].

III. General Model for Steganography

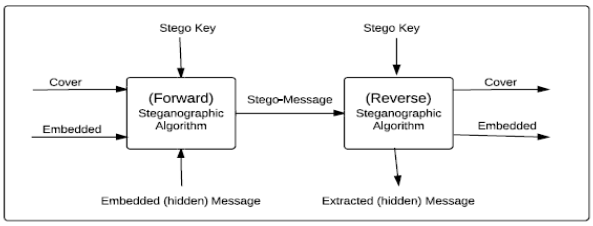

Fig: 4. General Model for Steganography

Secret message is embedded in a suitable cover object and transmitted over internet. To enhance further security, steganography algorithm can be used with an additional secret key that makes it hard to identify the existence of confidential data. After embedding the cover object is done with covert data, then it is recognized as 'stego object' [1]. Extraction process is used to extract secret message from stego object by use of reverse embedding algorithm and stego key [8][9].

IV. COVER OBJECTS FOR STEGANOGRAPHY

Different type of cover objects can be used to hide confidential message. Digital images are extensively used medium for steganography. Many steganography algorithms are there which use certain embedding logics to hide image as well text. Most widely used image formats are Bitmap format, Graphic Interchange Format, Portable Network Graphics, Joint Photographic Expert Group [6].

V. NECESSITIES AND FEATURES FOR A STEGANOGRAPHY ALGORITHM

The key requirements for any steganography algorithm are embedding capacity, visual quality and robustness. Even though it is not easy for any steganography algorithm to simultaneously achieve all the parameters because there is normally trade-off between these conflicting parameters [2].

Capacity: The quantity of hidden data to be embedded in cover object and later on that can be extracted effectively without considerably altering the cover object.

Visual Quality: There should be no visual distortion and difference between cover and stego objects when inspected with naked eyes.

Robustness: A steganography algorithm is said to be robust if stego object generated by it can tolerate any attack even if it undergoes various transformations and operations like lossy compression, rotation, scaling, filtering etc.

VI. APPLICATIONS OF STEGANOGRAPHY

Steganography has applications in various fields. Though its use is not limited, the following examples highlight some of the applications of steganography. Steganography can be used in defense organizations, military, and other intelligence agencies for safe circulation of secret data.

- To make online voting systems more secure and robust against various fraudulent activities.
- Steganography can be used to enforce access control on a digital medium such as music files when an unauthorized user plays the file, the access control information can be extracted and verified against the permission for that file. It can also be used to enforce digital right management (DRM) policies.
- Business needs to protect its intellectual property and information like trade secrets etc. can be protected by using watermarking which is another form of steganography.
- In the medical imaging system, a patient's personal information needs to be embedded to maintain its privacy and also to reduce transmission cost and time.
- In Smart cards, personal data information can be embedded for copyright control and protection purposes.

- In countries, where cryptography is prohibited, steganography can be used for safe online banking and handling of other secret transactions.

VII. COMMONLY USED EXISTING SPATIAL DOMAIN TECHNIQUES

A. Least Significant BitTechniques

Image steganography generally use 8-bit grayscale images and 24-bit color images. More information can be embedded with large size images. However, larger images may require compression to avoid detection. LSB replaces the least significant bits with the message to be encoded and are most popular techniques when dealing with images. These techniques are simple but susceptible to lossy compression and image manipulation. LSB techniques are quite strong for passive warden attacks as there is no perceptible difference in cover and stego image but sensitive towards active warden. These techniques are commonly used steganography techniques but they are very little robust and vulnerable to various attacks and transformations to image [13][14][15]. About LSB techniques certain important findings are considered here:

Any kind of geometrical transformation can destroy a secret message that is embedded through LSB and other kind of image processing operations like blurring, compression, also wipe out embedded message.

Generally LSBs approaches are based on the assumption that bits are not significant and random hence LSB bits are selected and are used for data hiding based on some PRNG but such statements are not always true particularly for cover image with a variety of flat regions.

If the length of a secret message is less than cover then after embedding certain elements of cover used for embedding will have different statistical properties than others that are not used for embedding and these lead to change in statistical properties are easily detected by various steganalysis methods. Embedding methods based on simple LSB are less secure and can be easily detected by various steganalysis methods like RS steganalysis.

Embedding in least significant four bits generally gives no distortion; beyond that there is clear visual distortions can be examined visually or other statistical check can be performed like peak signal to noise ratio etc.

LSB techniques are not suitable for watermarking where robustness is a major concern and watermarked image has to go for various transformations.

B. Pixel Value Differencing Techniques (PVD)

Various steganography methods based on PVD concepts have been developed and used. Using PVD techniques a grayscale image is divided into non-overlapping blocks consisting of successive pixels. From each block, a difference value can be calculated by subtracting considered successive pixels. With PVD techniques data hiding is performed by considering a different number of adjacent pixels in a block and difference between their intensity values, further random traversing can be done over chosen blocks of pixels. Block with large intensity difference is considered as corners, contours and sharp edges. Block with low difference values are situated in low intensity and smooth areas. Different spatial domain techniques concepts like LSB, OPAP, Modulus function, and adaptive methods are also combined with PVDs to improve existing PVD data hiding techniques. The PVD process recommended by Wu and Tsai can provide both high embedding capacity and visual imperceptibility for the stego-images. Original PVD schemes were not strong and suffer from various attacks like histogram analysis [11][16][17][18][19][20].

PVD methods offer more visual quality as compared to LSB methods with comparable level of data hiding capacity, but these techniques do not defend against change in statistical characteristics even at very low data hiding capacity [21]. Adaptive PVDs are the robust and superior version of common and non-adaptive PVD embedding methods. Adaptive techniques give not only high embedding capacity but also good imperceptibility for the stego-images. Certain Pixel value difference methods use characteristics of human visual systems like high-intensity regions such as sharper and edge regions can be used to provide enhanced embedding capacity and robustness.

C. Edge Based Techniques

A further improvement to the PVD methods was the use of the edge pixels to embed secret message bits into a cover object. The use of edge blocks for embedding is based on the human visual perception system since eyes are more receptive to changes in smooth areas rather than sharp and edge regions. The intensity of edge pixels is generally either higher than their neighboring pixels, thus causing a sharp change in the image. Hence edge blocks are most appropriate to hide secret information in an image. Several edge detection techniques have been proposed and designed over the years. Canny designed an approach to edge detections which involved a few localization conditions, on different types of edges in 1986. Li et al. used the Sobel operator to create edges for an image in 2009. Using Edges for data hiding, first edge recognition is carried out over all the image planes then corresponding to all edges, LSBs of each pixel are used to embed data. Finally, the stego planes were united to obtain the stego image. This method did not make sure high embedding capacity. Chen et al. designed a hybrid edge detector by combining the canny edge detector and fuzzy edge detection methods in 2010; this method leads to a good visual quality stego image. PVD embedding with edges and LSB are used to increase image quality and imperceptibility. These techniques are used to hide secret data into color and grayscale images [12][22][23][24][25].

VIII. Performance Analysis of Commonly used Spatial Domain Techniques

To analysis performance of commonly used spatial domain techniques here LSB with modulus function, PVD based techniques, Edge based techniques are implemented using benchmark images. Commonly used techniques are checked by experimentally calculating different parameters like capacity of embedded data and PSNR, etc. Experimental results are shown in tabular form and performance of these techniques are compared and represented graphically.

A. Data embedding Using Modulus Function [10]

This technique provides good capacity, imperceptibility, uses secret keys and also has low embedding and extracting cost. It makes use of modulus function, and also generates set of functions based on set of input secret keys. Each pixel of cover image generates pixel group with adjacent pixel using modulus function for embedding secret message bits

Table: 1. Capacity and PSNR Data embedding using Modulus Function [10]

Capacity=786432 bits, bpp=3	
Image	PSNR
Lena	37.91
Baboon	37.91
Peppers	37.92
Barbra	37.94
Jet	37.92
Boat	37.93
Tiffany	37.93

B. PVD and LSB Replacement Based On [11]

In this paper hybrid technique is used based on concepts of PVD, LSB and edge to achieve high imperceptible quality and hidden capacity for secret message. Image is divided into blocks of consecutive pixels and difference in intensity values is computed. Difference value is used to decide smooth (low intensity) and edge(high intensity)areas. Smooth areas are embedded with secret bits using LSB methodology while with edge area embedding is done using PVD technology.

Table: 2. Capacity and PSNR for PVD and LSB replacement based on [11]

Image	Capacity (bits)	PSNR
Lena	766942	37.62
Baboon	720200	35.94
Peppers	774342	37.67
Barbra	744381	34.45
Jet	769649	37.49
Boat	759719	36.97
Tiffany	771189	37.63

C. Adaptive Data Hiding In Edge Area

This approach has high capacity and visual quality. Here image is divided into blocks, difference value of adjacent pixels is used to find out no of secrets bits to be embedded. Pixels belonging to edge areas are used to embed k larger bits of secret bits as compared to smoother areas using LSB method.

Table3: Capacity and PSNR for Adaptive Data Hiding in Edge Areas with LSB [12]

Image	Capacity (bits)	PSNR
Lena	809966	37.63
Baboon	886516	36.29
Peppers	802228	37.97
Barbra	892917	36.12
Jet	809262	37.53
Boat	821774	37.29
Tiffany	806847	37.79

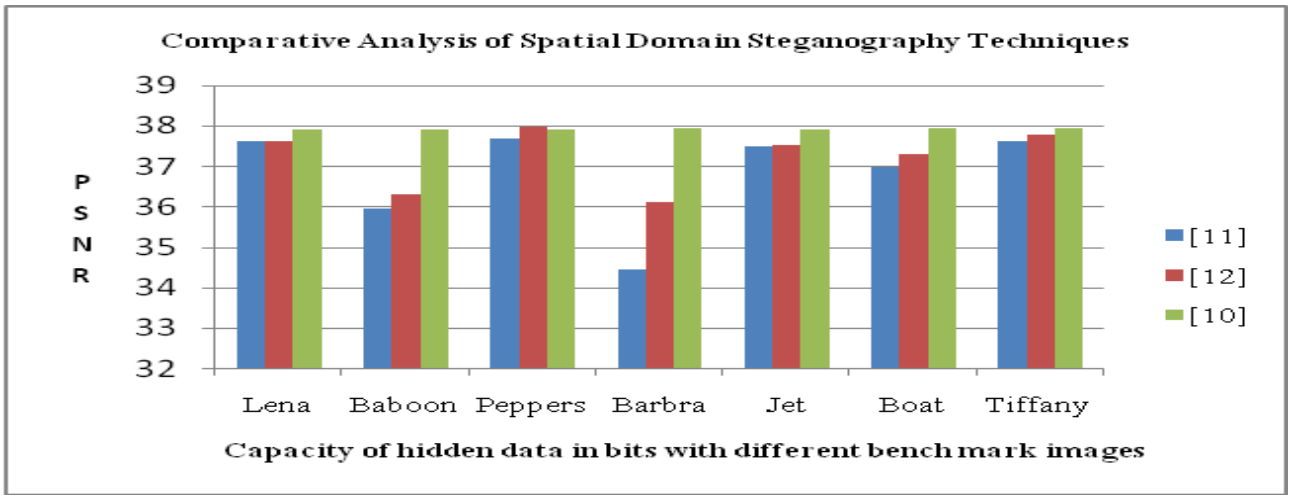

Fig 5: Analysis of Spatial domain Techniques

From experiments conducted over different benchmark images it was observed that embedding fixed-length secret data in each pixel leads to more visible distortions in a stego image because all pixels do not tolerate same amount of changes and effect is more in smooth area then edges thus adjusting embedding capacity and image quality adaptively are major related research area about LSB and PVD techniques.

Lossless compression of images with a large variety of colors is good for embedding when used as cover. It is best to use a grayscale palette with different shades of colors or image with noisy areas can be used for embedding. The type of cover object also plays an important role for an efficient steganography algorithm. The most common requirement for efficient steganography is that cover objects should support a large variety of colors.

IX. CONCLUSION

Steganography is used to embed a confidential message in a cover image such that no one other than the authorized receiver can know even about the existence of hidden data. Cryptography can be used with steganography in combination so that the additional layer of security can be provided. Steganography is an ongoing research area and used in different areas such as band captioning, combination of several media for reliable and suitable storage management, secret communication like in medical and military fields, video surveillance, error correction, and version upgrading, embedding executables for function control, etc.

In this paper commonly used steganography algorithms like LSB, PVD and edge based techniques are discussed and analyzed experimentally. It was observed that embedding capacity and imperceptible quality are conflicting parameters. LSB techniques are simple and provide high embedding capacity. PVD and edge based techniques provide high imperceptibility. Latest spatial domain techniques are based on hybrid approaches combining concepts like PVD, edge based and LSB embedding

The strength of a particular steganography algorithm depends upon various parameters type of cover object, compression methods used, texture and shades of color available etc. Different applications have different requirements for embedding capacity and visual quality. There is a need to decide which algorithm is to be used depending upon requirements of application.

Steganography can also be used for illegal purposes and there is a need to be familiar with and researchers need to work in tandem protect such threats. It is required to spread awareness about steganography.

REFERENCES

1. Ross J. Anderson, Fabien A.P. Petitcolas , "On the Limits of Steganography" , IEEE Journal of Selected areas in communications, 16(4): 474-481, May 1998, ISSN 0733-8716.
2. M. Kharrazi, H.T. Sencar and N. Memon , "Cover Selection for Steganographic Embedding", IEEE International Conference on Image processing, 8-11 Oct 2006, Atlanta USA, pp 117-120
3. Neil Provos and Peter Honeyman, "Hide and Seek –An Introduction to Steganography", IEEE Security and Privacy, May/June 2003 pp 32-44.
4. Rajarathnam Chandramouli, Mehdi Kharrazi, and Nasir Memon, "Image Steganography and Steganalysis: Concepts and Practice", T. Kalker et al. (Eds.): IWDW 2003, LNCS 2939, Springer-Verlag Berlin Heidelberg, 2004, pp. 35–49.
5. P. Salee, "Model–based Steganography", in: proceeding of the 2nd International workshop on digital water marking, Seoul , Korea, October 20-22 2003 , LNCS , vol.2939, pp. 254-260.
6. Abbas Chedad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods", Signal Processing, Vol 90, Issue 3, March 2010, page 727-752.
7. G.J. Simmons, "The Prisoner's Problem and the Subliminal Channel", In: Proceedings of CRYPTO '83. 1984, pp 51-67.
8. Fridrich, J. and Goljan, M, "Practical steganalysis of digital images: State of the art.", in: Proceedings of the SPIE Security and Watermarking of Multimedia Contents IV, vol. 4675. International Society for Optical Engineering, San Jose, California, January 21-24, 2002, pp. 1-13.
9. P. Amat, W. Puech, S. Druon, J.P. Pedeboy, "Lossless 3D Steganography based on MST and Connectivity modification", Signal Processing: Image communication 25, 2010 Elsevier, pp 400-412.
10. Lee, C.-F., Chen, H.-L.: 'A novel data hiding scheme based on modulus function', J. Syst. Softw., 2010, 83, (5), pp. 832–843
11. Wu, H.-C., Wu, N.-I., Tsai, C.-S., Hwang, M.-S.: 'Image steganographic scheme based on pixel-value differencing and LSB replacement methods', Proc. Inst. Electr. Eng., Vis. Image Signal Process., 2005,152, (5), pp. 611–615
12. Yang, C.-H., Weng, C.-Y., Wang, S.-J., Sun, H.-M.: 'Adaptive data hiding in edge areas of images with spatial LSB domain systems', IEEE Trans. Inf. Forensics Sec., 2008, 3, (3), pp. 488–497
13. W.N Lie, L.C Chang, " Data hiding in images with adaptive number of least significant bits used on human visual system, pattern recognition , IEEE International Conference on Image Processing, vol 1, issue 7, pp. 286-290, 1999
14. C.K. Chan, L.M. Chang, "Hiding data in images by simple LSB substitution" Pattern Recognition Letters, Vol. 7, issue 3, pp. 469-474, 2004
15. R.Chandramouli and Nasir Memon, "Analysis of LSB based image steganography Techniques" 2001 IEEE, pg 1019-1022
16. D.C. Wu and L.C Tsai, "A Steganography methods for images by pixel value Differencing", Pattern Recognition Letters, Vol. 24, pp. 1613-1626, 2003
17. Ko-Chin Chang, C-P. Chien-Ping Chang Ping S. Huang and Te-Ming Tu, " A Novel image Steganographic Method Using Tri- way Pixel value Differencing", Journal of Multimedia, Vol.3, No. 2, pp 37-44, June 2008
18. Han-ling ZHANG, Guang-zhi GENG, Cai-qiong Xing, 2009."Image Steganography using Pixel-Value Differencing", IEEE DOI 10.1109/ISECS.2009.139), 109–112.
19. Dr H.B Kekre, Ms Pallavi Halarnkar, Kahkashan Ansari, Parakh Jindal, Yash Chaturvedi," Information hiding with increased capacity using KMLA+PVD approach", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 2, No.2, April 2012
20. J. K. Mandal and Debashis Das, "Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain", International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012, 83-93
21. Weiqi Luo, Fangjun Huang and Jiwu Huang, "A more Secure Steganography based on Adaptive pixel-value Differencing Scheme", Multimedia Tools and Applications Vol. 52, No. 2-3, pp. 407-430, (2011
22. Canny J (1986), A computational approaches to edge detection. IEEE Trans Pattern Anal Mach Intell 8(6):679–698
23. Li L, Luo B, Li Q, Fang X (2009) A color Images steganography method by multiple embedding strategy based on Sobel operator. In: 2009 International Conference on Multimedia Information Networking and Security (Vol. 2, pp 118- 121). IEEE
24. Chen WJ, Chang CC, Le TH (2010) High payload steganography mechanism using hybrid edge detector. Expert Syst Appl 37(4):3292–3301
25. Modi, Islam, Gupta, M.R. Modi, S. Islam, P. Gupta (2013) Edge based steganography on colored images, Intelligent com- puting theories pp 593–600.

AUTHORS PROFILE

Sumeet Kaur is pursuing her Ph.D. from IKG- PTU, Kapurthala. Her area of research is image processing and steganography. She has around 70 publications in various international, national journals and conferences.

Dr. Savina Bansal, area of research is High Performance, Energy efficient and Fault-tolerant Computing, WSNs, Wireless Communications. She has 30 years of teaching experience and presented more than 100 research papers in various international and national journals & conferences. She had guided 04 Ph.D.s and 50 M.Tech. students for dissertation work.

Dr. R.K. Bansal area of research is real time Computing, Wireless Sensor Networks. He has more than 32 years of teaching experience and presented 80 research papers in international and national journals and conferences. He had guided 01 Ph.D. and 25 M.Tech. students for dissertation work.