ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Data Hiding in Image Using Tree Based Parity Check with LSB Matching Revisited Algorithm

R.Shanthakumari [1], Dr. S.Malliga [2]

Assistant Professor(SLG), Department of IT, Kongu Engineering College, Perundurai, Tamilnadu, India[1]

Professor, Department of CSE, Kongu Engineering College, Perundurai, Tamilnadu, India[2]

ABSTRACT: Image steganography is a technique for embedding the data inside a cover image. It is a technique in which a stego image is sent to the intended recipient in such a way that no third party can detect the existence of the secret data. Most of the existing methods hide data inside the randomly selected pixels without considering the nearby pixel values. Therefore chances for hiding data inside the smooth regions of the image are high. In this paper, data is hidden inside the edge boundaries of an image by an edge adaptive scheme to improve the symmetry between cover image and stego image. Tree Based Parity Check (TBPC) with Least Significant Bit Matching Revisited (LSBMR) algorithm is used to embed data inside the cover image in a secured manner. The proposed system is evaluated using the quality metrics like Mean Squared Error, PSNR and Embedding Capacity.

KEYWORDS: Data Hiding ; Edge Adaptive Scheme; LSBMR; Steganography; Tree Based Parity Check;

I. INTRODUCTION

Steganography is a technique for information hiding. This scheme hides secret message in the communication between the sender and receiver such that no other parties can detect the existence of the secret message**.** It aims to hide the secret data inside a cover media like digital audio, image and video. A Steganography method consists of embedding and extraction algorithms. Embedding algorithm describes how to hide secret data into the cover media and the extraction algorithm illustrates how to extract the message from the stego media. Cover media has to sacrifice its originality due to hidden secret data. It means that for embedding the message, cover media has to slightly modify into stego media. Reducing distortion between cover and stego media is taken as a crucial issue for steganography methods. This paper proposes an efficient image steganography embedding and extracting algorithm that uses least number of changes over cover image to produce stego image after data embedding process. In general, image steganography is the method of data hiding into cover image and generates a stego image which can be sent to the other party by known medium, where the third party does not know that this stego image has a hidden message. At the receiver end, hidden message can be simply extracted from stego image with or without using a stego key [1].

II. RELATED WORK

The most popular steganography method is LSB Replacement (LSB-R), where LSBs of the pixels are used for hiding the message bits according to the Pseudo Random Number Generator (PRNG) which arises the asymmetry between cover image and stego image [2]. LSB Matching (LSBM) is another well-known method of steganography in which a slight modification is employed to the previous method. It helps to avoid asymmetry artifact introduced by LSB-R method. Some standard steganalytic algorithms such as [3], [4], and [5] can be used for exposing the stego images generated by LSBM with high detection accuracy. Wu et al [6] took the difference of adjacent pixels of image for computing the size of the hidden data bits. Histogram analysis method [7] was based on the [6] Pixel Value Differencing (PVD) method. Motameni [8] has introduced a data hiding technique which finds out the dark region of the image and used LSB to embed secret data. Crandall [9] introduced the idea of matrix embedding for data hiding to improve embedding efficiency. Matrix embedding uses linear codes called as syndrome coding. It embeds and extracts a message by using the parity check matrix of a linear code. Zhang [12] proposed a novel reversible data hiding scheme

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

for an encrypted image, the receiver with the knowledge of encryption key can obtain a decrypted image and detect the presence of hidden data using LSB steganalytic methods. Also with the data hiding key, it is possible to extract the additional data and recover the original image. C.Tsai et al [10] proposed a scheme called Tree Based Parity Check (TBPC) with majority vote strategy to reduce distortion on a cover object based on a tree structure model. Tan [11] proposed LSBMR algorithm with edge adaptive scheme in which the histogram of the absolute difference of the pixel pairs is taken, and a pulse distortion to the long exponential tail is applied. From the above papers it is observed that the nearby pixels are not considered for data embedding, thus resulting in the distortion of the image. Here we proposed a data hiding scheme, Tree Based Parity Check with LSBMR algorithm which overcomes the above problem. The rest of the paper is organized as follows. In section 2, the proposed scheme is discussed. Experimental results is described in section 3, section 4 concludes the paper.

III. PROPOSED ALGORITHM

Reducing distortion between the cover image and the stego image is an important issue in steganography. Most of the steganography methods generally use randomly selected pixels for data embedding. These pixels are selected without considering adjacent pixel. In such cases the probability of embedding in the smooth regions will be high. In general, the sharper regions have more complicated statistical features and random characteristics than the smoother ones. It is expected that detectable and visual artifact would be left very low in the sharper regions after data embedding. It makes the detection is more difficult. In this paper, analysis is done when data is embedded in the edge boundaries using Tree Based Parity Check (TBPC) with LSBMR algorithm. The details of data embedding and data extraction algorithms are as follows.

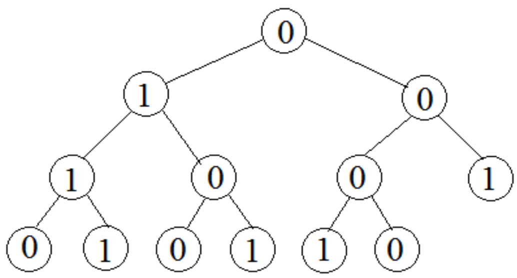
III.1 Data Embedding Algorithm

Step 1: Location Finding Method: Hiding Secret data in edge regions of an image is more secure hence edge regions are preferred. The Edge Region(ER) consists of a pair of pixels as an embedding unit (x_i, x_{i+1}), in which difference between those two pixels will be greater than or equal to threshold (T) value known by the sender and receiver. The non-overlapping consecutive pixel pair in each embedding unit is found by traversing each row in the matrix representation of the cover image from left to right. Depending on number of nodes in the master tree, number of pixel pairs is determined. ER (T) = {(x_i, x_{i+1}) || where | (x_i, x_{i+1})|>=T, (xi, x_{i+1}) € I}

Step 2: Tree Based Parity Check (TBPC) Method: The TBPC method is a least significant bit steganography method. This method is used for generating stego code using the LSB of selected pixels which consist of following three steps.

Step 2.1: Construction of master tree and create master string and toggle string: The method constructs a complete binary tree called the master tree. The number of leaf nodes of the tree is equivalent to the message length (l) .The nodes in the master tree is filled with the LSBs of the selected pixels level by level, from top to bottom and left to right. The master string is created by performing even parity check on the master tree from the root to leaves. Exclusive-OR bit wise (XOR) operation is performed between message and master string to get a toggle string. For example message to hide is h(1 1 0 1 0 0 0).The following are the selected pixels 156,159,154, 165,160,162,165,160,161,162,165,171,166.Use the LSB of each pixel for creating the master tree. The figure 1 represents the creation of Master Tree.

Fig.1 Master Tree



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Performing the parity check from root to leaf node is called the Master String. Master String: 0 1 1 0 1 0 1 Message String:1 1 0 1 0 0 0. Toggle string(1 0 1 1 1 0 1) is obtained by performing exclusive-OR operation between the Message and the Master String. The Toggle string is shown in figure 2.

Step 2.2: Creation of toggle tree: Toggle tree is created by filling the leaf nodes with the toggle string and all the other non-leaf nodes with 0. Then, traverse through each level, from the bottom to the root, the non-leaf node and their corresponding leaf nodes are flipped if both of its children have bits as one. The Toggle tree is shown in figure 3.
Step 2.3: Construction of stego tree: The embedding algorithm obtains the stego tree by performing XOR between the master tree and the toggle tree. The stego code is obtained from the stego tree. The construction of the stego tree is shown in figure 4.The stego code (0 1 0 1 1 0 0 1 1 0 1 0 0) is embedded inside an image using LSBMR algorithm. The resultant stego image hides secret bits in a highly secure manner.

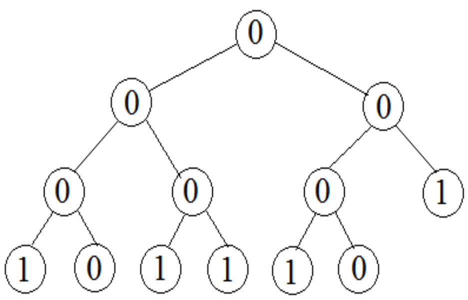


Fig. 2 Toggle String

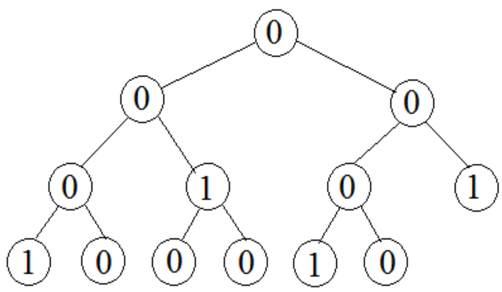


Fig. 3 Toggle Tree

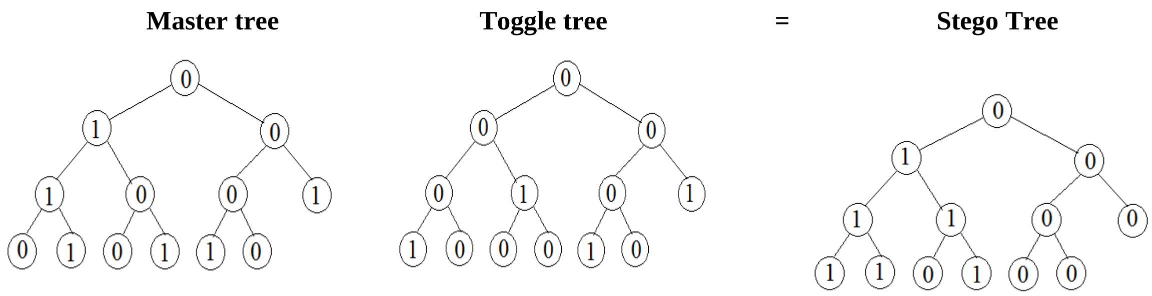


Fig. 4 Construction of stego tree

Step 3: LSBMR Algorithm: LSBMR algorithm is applied to the stego code. For each embedding region (x_i,x_{i+1}), consecutive two bits of the stego code is embedded according to the following 4 cases.
Case 1: LSB (x_i) = m_i & LSB (f (x_i, x_{i+1})) = m_{i+1} then (x_i', x_{i+1}') = (x_i, x_{i+1})
Case 2: LSB (x_i) = m_i & LSB (f (x_i, x_{i+1}))! = m_{i+1} then (x_i', x_{i+1}') = (x_i, x_{i+1}+1)
Case 3: LSB (xi)! = m_i & LSB (f (x_i -1, x_{i+1})) = mi_{+1} then (x_i', x_{i+1}') = (x_i -1, x_{i+1})
Case 4: LSB (xi)! = m_i & LSB (f (x_i -1, x_{i+1}))! = mi_{+1} then (x_i', x_{i+1}') = (x_i+1, x_{i+1})
Where m_i and m_i +1 denote i^{th} and $i+1^{th}$ position stego code bits to be embedded. The function 'f' is defined as f (a, b) = (a/2) +b. (x_i', x_{i+1}') denotes the resultant pixel pair after data hiding. Finally, the stego image is obtained.

III.2 Data Extraction Algorithm
Step 1: Location Finding Method : Identify the pixel pairs (x_i',x_{i+1}') in the stego image where data are embedded by following location finding method in step 1 of the data embedding algorithm.
Step 2: Stego Code Extraction: For each qualified pixel pairs, extract the two stego code bits m_i and m_i +1 as follows: mi = LSB (x_i') & mi+1 = LSB ((x_i'/2)+ x_{i+1}')

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Step 3: Creation of stego Tree: Construct the complete binary tree by filling its nodes by the stego code. Original message can be extracted by performing parity check.

IV. EXPERIMENTAL RESULTS

The proposed algorithm has been implemented using MATLAB 7.11. Performance of the algorithm has been evaluated in terms of Mean Squared Error, Peak Signal to Noise Ratio, Embedding Capacity and Elapsed Time. Figure 5 (a) –(d) shows the original cover(carrier) images for Cameraman, Lena, Nature and Girl , Figure 6(a) –(d) shows the stego images. Some of the images (Grayscale and RGB) from Image database and from internet were used to test the performance of the proposed algorithm. The above measures are calculated for the test images by varying the number of characters embedded. Here the results of PSNR, MSE, CAP and ET are shown in Table 1 for grayscale images and the results of RGB images are shown in Table 2.

(a) Cameraman (512 x 512) (b) Lena (256 x 256) (c) Nature (512 x 640) (d) Girl (400 x 267)

Figure 5 (a) – (d) original cover (carrier) images.

(a) Cameraman (512 x 512) (b) Lena (256 x 256) c) Nature (512 x 640) (d) Girl (400 x 267)

Figure 6(a) – (d) stego images.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Table 1 PSNR, MSE, CAP and ET for Grayscale Images

Grayscale Images		Cameraman (256 x 256)					Lena (512 x 512)				
No. of Characters Embedded		50	100	150	200	250	50	100	150	200	250
PSNR (db)	TBPC with LSBR	65.503	62.247	60.566	59.203	58.912	71.347	68.336	66.439	65.231	64.200
	Proposed System	71.778	68.631	66.956	65.688	65.669	77.291	74.436	72.539	71.340	70.329
MSE	TBPC with LSBR	0.018	0.038	0.057	0.078	0.091	0.004	0.009	0.014	0.019	0.024
	Proposed System	0.004	0.008	0.013	0.017	0.022	0.001	0.002	0.004	0.005	0.006
CAP	TBPC with LSBR	0.010	0.021	0.032	0.042	0.053	0.002	0.005	0.008	0.010	0.013
	Proposed System	0.010	0.021	0.032	0.042	0.053	0.002	0.005	0.008	0.010	0.013
ET (Sec)	TBPC with LSBR	2.947	17.336	52.031	119.298	225.740	2.603	17.001	53.561	120.241	224.998
	Proposed System	2.967	17.720	53.680	120.376	226.012	3.012	17.576	55.834	121.530	225.773

Table 1 shows the result of the MSE value calculated for Grayscale images. From the experimental results in Table 1, it is either 0 or 0.03 which means there is no significant difference between the cover image and stego-image even after embedding. From the Table 1 it is observed that all our PSNR values are greater than 65 dB. The embedding capacity is exactly same in TBPC with LSBR and TBPC with LSBMR.

RGB Images		Nature (512 x 640)					Girl (400 x 267)				
No. of Characters Embedded		50	100	150	200	250	50	100	150	200	250
PSNR (db)	TBPC with LSBR	77.122	74	72.398	71.110	70.042	72.505	69.004	67.450	66.294	65.208
	Proposed System	78.587	75.403	73.652	72.432	71.496	73.898	70.842	69.137	67.712	66.693
MSE	TBPC with LSBR	0.001	0.002	0.004	0.005	0.006	0.003	0.008	0.011	0.015	0.019
	Proposed System	0.0009	0.001	0.003	0.004	0.005	0.002	0.005	0.007	0.011	0.013
CAP	TBPC with LSBR	0.002	0.004	0.006	0.009	0.010	0.007	0.013	0.019	0.026	0.038
	Proposed System	0.002	0.004	0.006	0.009	0.010	0.007	0.013	0.019	0.026	0.038
ET (Sec)	TBPC with LSBR	2.513	15.917	54.187	119.547	230.208	3.254	17.299	54.511	119.449	227.043
	Proposed System	2.703	16.859	56.187	120.532	232.590	3.300	18.182	54.551	120.885	230.512

Table 2 PSNR, MSE, CAP and ET for RGB Images

Table 2 shows the result of the MSE value calculated for RGB images. From the experimental results in Table 1, it is either 0 or 0.01 which means there is no significant difference between the cover image and stego-image even after embedding. From the Table 1 it is observed that all our PSNR values are greater than 65 dB. The embedding capacity is exactly same in TBPC with LSBR and TBPC with LSBMR.

IV.1 Mean Squared Error (MSE)

MSE is the cumulative squared error between the stego image and the original image. Mean Squared Error can be computed using the formula

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (I - I')^2 \;\; ....(1)$$

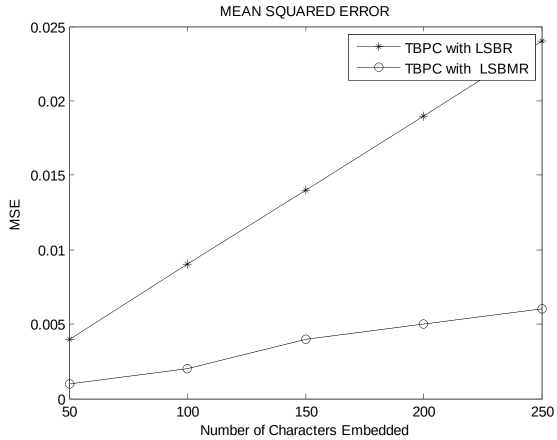


Fig.7 MSE of Lena

MSE of Lena image for different number of characters embedded is shown in Figure 7.Here distortion is reduced by 1 to 5 % compared to TBPC with LSBR.

IV.2 Peak Signal to Noise Ratio (PSNR)

The PSNR is used to measure the quality of stego image. Usually if PSNR values are greater than 30 dB then the stego image is of good quality. Peak Signal to Noise Ratio can be computed using the formula

$$\mathbf{PSNR = 10 * \log 10 (255^2 / MSE) \ldots\ldots. \quad (2)}$$

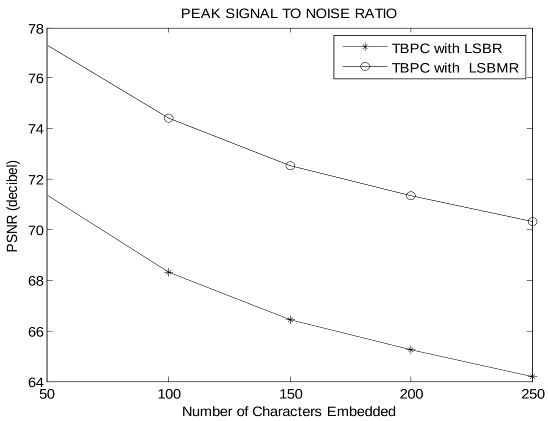


Fig.8 PSNR of Lena

The PSNR of Lena image for different number of characters embedded is shown in Figure 8. Here PSNR is improved by 1 to 5 % compared to TBPC with LSBR.

IV.3 Embedding Capacity

The CAP is the ratio between number of bits embedded in cover image and total number of pixels in the cover image.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Here the embedding capacity is used to measure the capacity of image and it is usually expressed as bits per pixels.

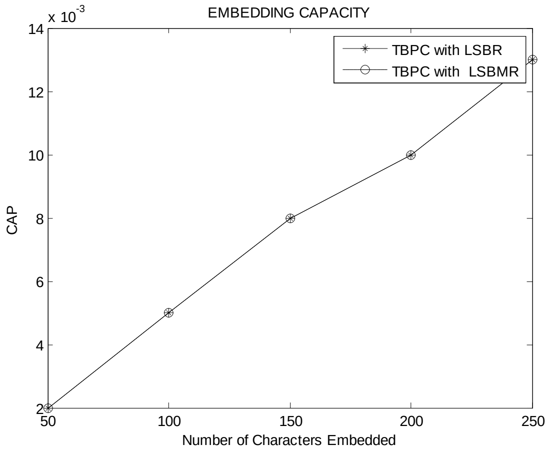


Fig.9 Embedding Capacity of Lena

The CAP of Lena image for different number of characters embedded is shown in Figure 9.The embedding capacity is exactly same in TBPC with LSBR and TBPC with LSBMR.

IV.4 Elapsed Time

The time duration that extends while some event is occurring is Elapsed Time which means time taken between starting and ending of the program. It is usually expressed in seconds. Elapsed time is slightly increased by 0.020 - 3 seconds in the proposed scheme.

V. CONCLUSION AND FUTURE WORK

By introducing tree based parity check with LSBMR algorithm using adaptive scheme, the stego image is constructed effectively under the tree structure model with minimum distortion rate. The LSBMR algorithm is used for embedding the secret data. Therefore, by this method, the problem of asymmetry between cover image and stego image is solved. In order to reduce the distortion between the cover image and the stego image, data is embedded in the edge regions and LSBMR algorithm is used for embedding stego code inside the image which helps to increase the security level. This scheme can be applied to other covers like audio and video which can be taken as the future work. Embedding capacity can also be improved by creating tree with more than two child nodes and novel steganography scheme based on multi-pixels differencing.

REFERENCES

1. N. Johnson and S. Jajodia 1998, Exploring steganography: seeing the unseen, *IEEE Computer*, pp. 26-34.
2. M. Hussain 2011, Embedding Data in Edge Boundaries with High PSNR , *IEEE Transactions*, Volume 11,978-1-4577-0768-1
3. Y. Q. Shi et al. 2005, Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network *in Proc. IEEE Int. Conf. Multimedia and Expo*, Jul. 6–8, pp. 269–272.
4. Li, J. Huang, and Y. Q. Shi. 2008 , Textural features based universal steganalysis, *Proc. SPIE on Security, Forensics, Steganography and Watermarking of Multimedia*, vol. 6819, p. 681912.
5. M. Goljan, J. Fridrich, and T. Holotyak . 2006, New blind steganalysis and its implications, Proc. SPIE on Security, Forensics, Steganography and Watermarking of Multimedia, vol. 6072, pp. 1–13
6. C. Wu and W. H. Tsai 2003, A steganography method for images by pixel-value differencing, *Pattern Recognition Letters*, vol. 24, no. 9-10, pp. 1613-1626.
7. H.C.Wu, N.I Wu, C.S. Tsai and M.S. Hwang 2005, Image Steganography scheme based on pixel-value differencing and LSB replacement methods, *VISP (152)*, No. 5.
8. H.Motameni, M.Norouzi, M.Jahandar and A.Hatami 2007, Labelling Method in Steganography, *World Academy of Science, Engineering and Technology*, France

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

9. R. Crandall 1998, Some Notes on Steganography, Posted on Steganography Mailing List,[Online].Available: http://os.inf.tudresden.de/westeld/crandall.pdf.
10. C. Hou, C. Lu, C. Tsai and W. Tzeng 2011, An Optimal Data Hiding Scheme With Tree-Based Parity Check, *IEEE Transaction on Image Processing*, vol. 20, no.3,pp.880-886
11. S. Tan 2012, Targeted Steganalysis of Edge Adaptive Image Steganography Based on LSB Matching Revisited Using B-Spline Fitting *IEEE Signal Processing Letters*, Vol.19,No. 6.
12. Zhang (2010), Reversible Data hiding in Encrypted Image, *IEEE Signal Processing Letters*, Vol.18, No.4, pp.255-258.

BIOGRAPHY

R.Shanthakumari presently working as an Assistant Professor (Selection Grade) in the Department of Information Technology, Kongu Engineering College, Tamilnadu, India. She received her B.E., in Computer Science and Engineering in 1997 at Bharathiar University, Coimbatore. M.E. in Computer Science and Engineering in 2007 at Anna University, Chennai. Her area of interest includes Networks, Network Security and Digital Image Processing.

Dr.S.Malliga is working as a Professor in the Department of Computer Science and Engineering, Kongu Engineering College, Tamil Nadu, India. She has completed PhD in the year 2010 from Anna University, Chennai. Her main research area is Network and Information Security. She has done consultancy project for BPL and offered several courses on latest technology. Currently she is guiding three research scholars. She has also guided many UG and PG projects. She has published 12 articles in international journals and presented more than 25 papers in national and international conferences in her research and other technical areas.. She is also interested in cloud and virtualization technologies.