Edge Adaptive Steganography Using DWT

Ajinkya S. Jamdar, Atul V. Shah, D. D. Gavali, S. L. Kurkute

Abstract-The least-significant-bit (LSB)-based approach is a popular type of Steganography algorithms in the spatial domain. The least-significant-bit (LSB)-based approach is a popular type of steganographic algorithms in the spatial domain. However, we find that in most existing approaches, the choice of embedding positions within a cover image mainly depends on a pseudorandom number generator without considering the relationship between the image content itself and the size of the secret message. Thus the smooth/flat regions in the cover images will inevitably be contaminated after data hiding even at a low embedding rate, and this will lead to poor visual quality and low security based on our analysis and extensive experiments, especially for those images with many smooth regions. In this paper, we expand the LSB matching revisited image steganography and propose an edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. For lower embedding rates, only sharper edge regions are used while keeping the other smoother regions as they are. When the embedding rate increases, more edge regions can be released adaptively for data hiding by adjusting just a few parameters. The experimental results evaluated on 6000 natural images with three specific and four universal steganalysis algorithms show that the new scheme can enhance the security significantly compared with typical LSB-based approaches as well as their edge adaptive ones, such as pixel-value-differencing-based approaches, while preserving higher visual quality of stego images at the same time.

Index Terms- LSB, DWT, Secret Message, Pixel.

I. INTRODUCTION

The Least Significant Bit (LSB) substitution is an example of spatial domain techniques. The basic idea in LSB is the direct replacement of LSBs of noisy or unused bits of the cover image with the secret message bits. Till now LSB is the most preferred technique used for data hiding because it is simple to implement offers high hiding capacity, and provides a very easy way to control stego-image quality but it has low robustness to modifications made to the stego-image such as low pass filtering and compression and also low imperceptibility[1].

Manuscript received on April, 2013.

Mr. Ajinkya S. Jamdar, faculty at Navsahyadri Group of Institution's Faculty of Engineering, Naigaon, Pune, India.

Prof. Atul V. Shah, Assistant Professor at the Department of Electronics & Telecommunication Engineering at D.K.T.E.S. Textile & Engineering Institute, Ichalkarnji, Maharashtra, India.

Prof. Dhananjay D. Gavali, Assistant Professor & Head of the Department of Electrical Engineering at Navsahyadri Group of Institution's Faculty of Engineering, Naigaon, Pune

Prof.Sanjay L. Kurkute, Associate Professor in the Department of Electronics & Telecommunication Engineering at Navsahyadri Group of Institutions, Faculty of Engineering, Pune, India.

The other type of hiding method is the transform domain techniques which appeared to overcome the robustness and imperceptibility problems found in the LSB substitution techniques.

There are many transforms that can be used in data hiding, the most widely used transforms are; the discrete cosine transform (DCT) which is used in the common image compression format JPEG and MPEG, the discrete wavelet transform (DWT) and the discrete Fourier transform (DFT)[3].

Unfortunately, replacing the redundant information with structured message data often results in the stego-object being an augmented version of the cover "marked" by the hidden data – and this makes it easy to suspect the presence of steganography. Most of these marks can be attributed to the hiding algorithm's lack of concern for the cover's content. If the cover's original content were taken into account then the message could be concealed in areas of the cover where it would be less likely to leave marks. Previous attempts at achieving this goal have required the user to provide the original cover as well as the stego-object. The best areas to hide are first identified in the original cover, then these areas are mapped across to the stego-object and the hidden information is retrieved. The original cover must be provided because the information overwritten in the message hiding process may have been used to identify the best hiding areas. However, to provide the original object is not secure, because taking the differences between the two objects would be enough to suspect the existence of (and in some cases, recover) the hidden information.

II. METHODOLOGY

1. Selection of image

We will select the grayscale image of any size (more than or equal to 256×256) for hiding any secret message in it. If we are going to use any color image then after hiding the secret message into it then the quality of RGB can be decreases as compared to grayscale image. Grayscale PNG format image is more preferable for hiding the message into the edges of the image. Also we can convert the multi color image into grayscale image for hiding the message.

2. Image Compression

Digital Image compression addresses the problem of reducing the amount of data required to represent a digital image. The underlying basis of the reduction process is removal of redundant data. From the mathematical viewpoint, this amounts to transforming a 2D pixel array into a statically uncorrelated data set. The data redundancy is not an abstract concept but a mathematically quantifiable entity. If n1 and n2 denote the number of information-carrying units in two data sets that represent the same information, the relative data redundancy R_D [2] of the first data set (the one characterized by n1) can be defined as,

$$R_D = 1 - \frac{1}{C_R}$$

Where C_R called as compression ratio [2]. It is defined as

$$C_R = \frac{n1}{n2}$$

In image compression, three basic data redundancies can be identified and exploited: Coding redundancy, interpixel redundancy, and phychovisal redundancy. Image compression is achieved when one or more of these redundancies are reduced or eliminated.

The image compression is mainly used for image transmission and storage. Image transmission applications are in broadcast television, remote sensing via satellite, air-craft, radar, or sonar, teleconferencing, computer communications& facsimile transmission. Image storage is required most commonly for educational and business documents, medical images that arise in computer tomography (CT), magnetic resonance imaging (MRI) and digital radiology, motion pictures, satellite images, weather maps, geological surveys, and so on.

III. WAVELET DECOMPOSITION OF IMAGES

In wavelet decomposing of an image, the decomposition is done row by row and then column by column. For instance, here is the procedure for an N x M image. You filter each row and then down-sample to obtain two N x (M/2) images. Then filter each column and subsample the filter output to obtain four (N/2) x (M/2) images.

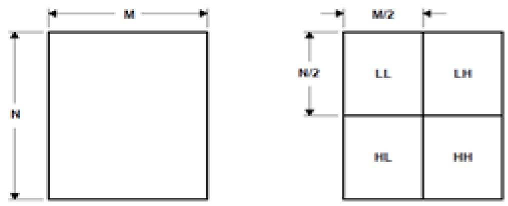


Fig.3.1 One level 2-D Decomposition

The four subimages obtained as seen in Figure 3.1, the one obtained by low-pass filtering the rows and columns is referred to as the LL image.
The one obtained by low-pass filtering the rows and high-pass filtering the columns is referred to as the LH images. The one obtained by high-pass filtering the rows and low-pass filtering the columns is called the HL image. The subimage obtained by high-pass filtering the rows and columns is referred to as the HH image. Each of the subimages obtained in this fashion can then be filtered and subsampled to obtain four more subimages. This process can be continued until the desired subband structure isobtained[9].

IV. DISCRETE WAVELET TRANSFORM

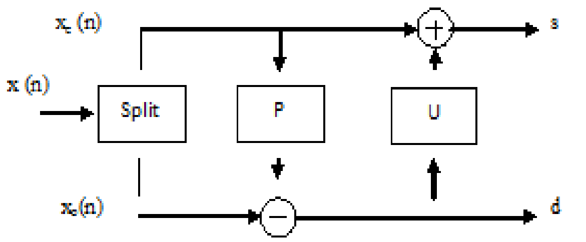
The discrete wavelet transform (DWT) was developed to apply the wavelet transform to the digital world. Filter banks are used to approximate the behavior of the continuous wavelet transform. The signal is decomposed with a high-pass filter and a low-pass filter. The coefficients of these filters are computed using mathematical analysis and made available to us[2].

V. LIFTING SCHEME

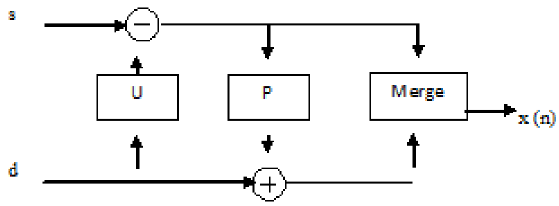
The wavelet transform of image is implemented using the lifting scheme. The lifting operation consists of three steps. First, the input signal x[n] is down sampled into the even position signal x_e (n) and the odd position signal x_o(n) , then modifying these values using alternating prediction and updating steps.

x_e (n) = x [2n] and x_o(n) = x [2n+1]

A prediction step consists of predicting each odd sample as a linear combination of the even samples and subtracting it from the odd sample to form the prediction error. An update step consists of updating the even samples by adding them to a linear combination of the prediction error to form the updated sequence. The prediction and update may be evaluated in several steps until the forward transform is completed. The block diagram of forward lifting and inverse lifting is shown in figure 5.1.



(a)



(b)Figure 5.1: The Lifting Scheme. (a) Forward Transform (b) Inverse Transform

The inverse transform is similar to forward. It is based on the three operations undo update, undo prediction, and merge. The simple lifting technique using Haar wavelet is explained in next section.

VI. LIFTING USING HAAR

The lifting scheme is a useful way of looking at discrete wavelet transform. It is easy to understand, since it performs all operations in the time domain, rather than in the frequency domain, and has other advantages as well. This section illustrates the lifting approach using the Haar Transform [6].

The Haar transform is based on the calculations of the averages (approximation co-efficient) and differences (detail co-efficient). Given two adjacent pixels a and b, the principle is to calculate the average $s = \frac{(a+b)}{2}$ and the difference $d = a - b$. If a and b are similar, s will be similar to both and d will be small, i.e., require few bits to represent. This transform is reversible, since $a = s - \frac{d}{2}$ and $b = s + \frac{d}{2}$ and it can be written using matrix notation as

$$(s,d) = (a,b)\begin{pmatrix} 1/2 & -1 \\ 1/2 & 1 \end{pmatrix} = (a,b)A,$$

$$(a,b) = (s,d)\begin{pmatrix} 1 & 1 \\ -1/2 & 1/2 \end{pmatrix} = (s,d)A^{-1}$$

Consider a row of 2^n pixels values $S_{n,l}$ for $0 \le l < 2^n$. There are 2^{n-1} pairs of pixels $S_{n,2l}, S_{n,2l+1}$ $for l = 0,2,4,.....,2^{n-2}$. Each pair is transformed into an average $S_{n-1,1} = (S_{n,2l} + S_{n,2l+1})/2$ and the difference $d_{n-1,l} = S_{n,2l+1} - S_{n,2l}$. The result is a set $S_{n-1} of 2^{n-1}$ averages and a set $d_{n-1} of 2^{n-1}$ differences.

VII. DATA HIDING BY SIMPLE LSB SUBSTITUTION:

In this, the general operations of data hiding by simple LSB substitution method are described[9].

Let C be the original 8-bit grayscale cover-image ofMc× Ncpixels represented as,

$$C = \{x_{ij} | 0 \leqslant i < M_c, 0 \leqslant j < N_c,$$
$$x_{ij} \in \{0, 1, \ldots, 255\}\}.$$

M be the n-bit secret message represented as

$$M = \{m_i | 0 \leqslant i < n, m_i \in \{0, 1\}\}.$$

Suppose that the n-bit secret message M is to be embedded into the k-rightmost LSBs of the cover-image C. Firstly, the secret message M is rearranged to form a conceptually k-bit virtual image M_ represented as

$$M' = \{m'_i | 0 \leqslant i < n', m'_i \in \{0, 1, \ldots, 2^k - 1\}\},$$

Where $n' < M_c \times N_c$. The mapping between the n-bit secret message.

$M = \{m_i\}$ And the embedded message $M' = \{m'_i\}$ can be defined as follows:

$$m'_i = \sum_{j=0}^{k-1} m_{i \times k + j} \times 2^{k-1-j}.$$

Secondly, a subset of n_ pixels {xl1; xl2 ,…….. xln_ } is chosen from the cover-image C in a predefined sequence. The embedding process is completed by replacing the k LSBs of xli by mi' . Mathematically, the pixel value xli of the chosen pixel for storing the k-bit message mi' is modified to form the stego-pixel xli' as follows:

$$x'_{l_i} = x_{l_i} - x_{l_i} \bmod 2^k + m'_i.$$

In the extraction process, given the stego-image S, the embedded messages can be readily extracted without referring to the original cover-image. Using the same sequence as in the embedding process, the set of pixels{xl1', xl2',…. Xln'} storing the secret message bits are selected from the stego-image[5]. The k LSBs of the selected pixels are extracted and lined up to reconstruct the secretmessage bits. Mathematically, the embedded message bits mi' can be recovered by,

$$m'_i = x'_{l_i} \bmod 2^k.$$

Suppose that all the pixels in the cover-image are used for the embedding of secret message by the simple LSB substitution method. Theoretically, in the worst case, thePSNR of the obtained stego-image can be computed by,

$$\text{PSNR}_{worst} = 10 \times \log_{10} \frac{255^2}{\text{WMSE}}$$
$$= 10 \times \log_{10} \frac{255^2}{(2^k - 1)^2} \text{ dB}.$$

Table 1 tabulates the worst PSNR for some k = 1–5. It could be seen that the image quality of the stego-image is degraded drastically when k>4.

VIII. EXPERIMENTAL RESULT

We can use uncompressed color image as input (Fig.1) and after converting it in grayscale image we apply our algorithm on it. Then apply Haar transform on the grayscale image. This type of transform gives four type of frequency bands of image which is approximate, vertical, horizontal anddiagonal details coefficients.From these bands we can find out high-high frequency component pixels which show the edge areas of images for hiding the text data in it.

One of the important properties of our steganographic method is that it can first choose the sharper edge regions for data hiding according to the size of the secret message by adjusting a threshold T.WhenT is 0, all the embedding units within the cover become available. In such a case, our method can achieve the maximum embedding capacity of 100% (100% means 1 bpp on average for all the methods in this paper).It can also be observed that most secret bits are hidden within the edge regions when the embedding rate is low, while keeping those smooth regions such as they are. The subjective quality of our stegos would be improved&based on the human visual system (HVS) characteristics.

Now we will see all the stages according with the results. In that first step is Histogram Modifications. The histogram of an image which shows the intensity of the image (Fig. 2) represents the relative frequency of occurrence of the various gray levels in the image.Modify an image so that its histogram has desired shape.In histogram equalization ,the goal is to obtain a uniform histogram for the output image. The input gray level is first transformed nonlinearly and output is uniformly quantized.

Fig. 1: LENA Image in JPEG-2000 LS

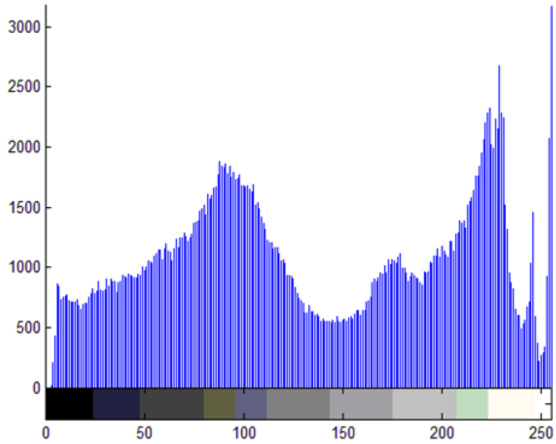


Fig.2 : Histogram of LENA Image

Fig.3 :After Histogram Modification

The histogram of the image can be adjusted in between 15(min value) and 240(max value) if the image size is taken 512×512(Fig.3& Fig.4). And secret message is going to hide in between these values of histogram.Basically after histogram modifications, we got output image having matrix, if this image matrix will subtract from input image matrix then anyone cannot get easily the hidden secret message bits.

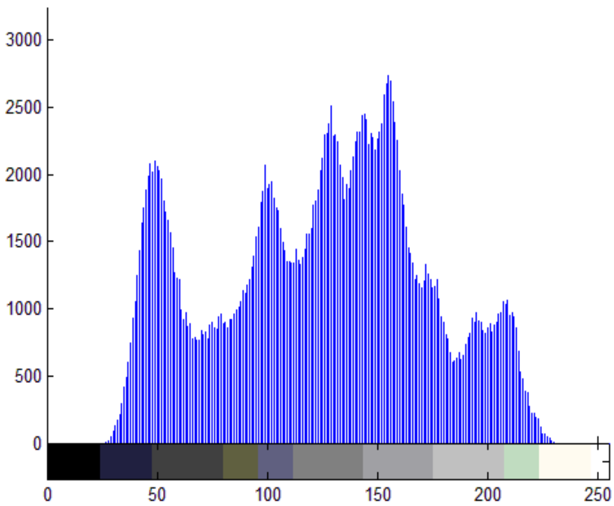


Fig.4 : Histogram of modified LENA Image.

Basically Integer Wavelet Transform is used for image compression method as explain above.

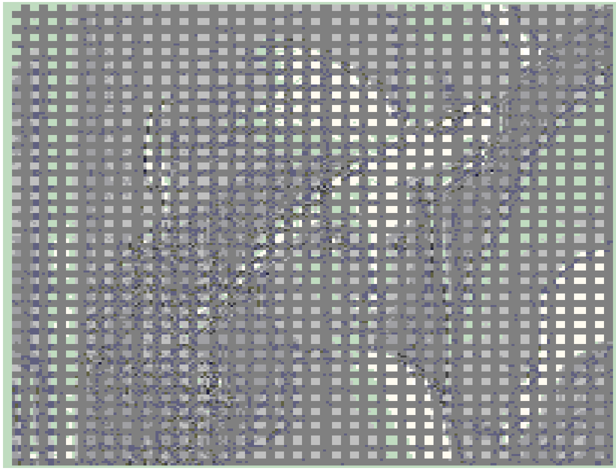


Fig.5 : After using Integer Wavelet Transform (DWT)

After the DWT we can embed the message into the edges of image(Fig.5). We will get the image which is slightly disturbed due to secret message hiding in the image. The LSB matching techniques can convert the last bit of pixels into message bits. The another method to remove the disturbance of the image is to use the filtering methods. But by using these methods, message bits which are hided into that pixels of the image will be lost. So we can't use any filtering method to remove the disturbance or noise from that image.

Fig.6 : After Embedding the secret message into image

PSNR for Grayscale LENA image is15.954db & the MSE for this image is11555.3. Hence the quality of image can be decreases in some manner(Fig.6). If we increase the size of image pixelwise, then the PSNR of image also increases means MSE decreases and distortions (noise) decreases. The following graph shows the image size, PSNR & MSE.

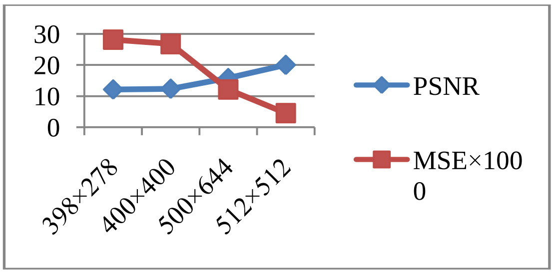


Fig.7: Increasing pixel size of the image as message size kept constant (PSNR, MSE)

As a message size of image increases then it does not much affect on the stego image distortion. The following graph (Fig.8) shows the distortions of the image due to increasing message size as pixel size of image keep constant:

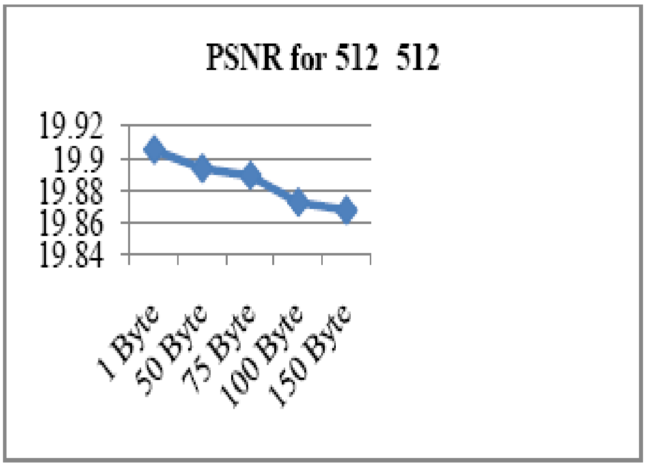


Fig.8: PSNR of image for increasing message size for image size 512×512

Also we can improve the quality of image by using filtering method. But by using any filtering method, the hidden secret message will destroy. Hence we can't use any filter for these stego image.

IX. CONCLUSION

In this paper we proposed a novel data hiding scheme that hides data into the integer wavelet coefficients of an image. The system combines an adaptive data hiding technique and the optimum pixel adjustment algorithm to increase the hiding capacity of the system compared to other systems. The proposed system embeds secret data in a random order using a secret key only known to both sender and receiver.

It is an adaptive system which embeds different number of bits in each wavelet coefficient according to a hiding capacity function in order to maximize the hiding capacity without sacrificing the visual quality of resulting stego image. The proposed system also minimizes the difference between original coefficients values and modified values by using the optimum pixel adjustment algorithm.

The proposed scheme was classified into three cases of hiding capacity according to different applications required by the user. Each case has different visual quality of the stego-image. Any data type can be used as the secret message since our experiments was made on a binary stream of data. There was no error in the recovered message (perfect recovery) at any hiding rate. From the experiments and the obtained results the proposed system proved to achieve high hiding capacity up to 48% of the cover image size with reasonable image quality and high security because of using random insertion of the secretmessage. On the other hand the system suffers from low robustness against various attacks such as histogram equalization and JPEG compression.

The proposed system can be further developed to increase its robustness by using some sort of error correction code which increases the probability of retrieving the message after attacks, also investigating methods to increase visual quality of the stego-image (PSNR) with the obtained hiding capacity.

REFERENCES

[1] WeiqiLuo, Fangjun Huang and Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 2, JUNE 2010

[2] C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 488–497, Sep. 2008.

[3] F. Huang, B. Li, and J. Huang, "Attack LSB matching steganography by counting alteration rate of the number of neighborhood gray levels," in *Proc. IEEE Int. Conf. Image Processing*, Oct. 16–19, 2007, vol. 1, pp. 401–404.

[4] G. J. Simmons, "The prisoners' problem and the subliminal channel," inProceedings of Crypto' 83, pp. 51-67, 1984.

[5] N. Wu and M. Hwang. "Data Hiding: Current Status and Key Issues," International Journal of Network Security, Vol.4, No.1, pp. 1-9, Jan. 2007.

[6] W. Chen, "A Comparative Study of Information Hiding Schemes UsingAmplitude, Frequency and Phase Embedding," PhD Thesis, National Cheng Kung University, Tainan, Taiwan, May 2003.

[7] C. Chan and L. M. Cheng, "Hiding data in images by simple LSBsubstitution," Pattern Recognition, pp. 469-474, Mar. 2004.

[8] H. H. Zayed, "A High-Hiding Capacity Technique for Hiding Data in images Based on K-Bit LSB Substitution," The 30th International Conference on Artificial Intelligence Applications (ICAIA – 2005) Cairo, Feb. 2005.

Mr. Ajinkya S. Jamdar received the B.E. degreein Electronics & Telecommunication from Dr. J. J. Magdum College of Engineering, Jaysingpur underShivaji University, Kolhapur, India, in 2010. Now he is perusing the M.E. in Electronics from D.K.T.E.S. Textile & Engineering Institute, Ichalkaranji under Shivaji University, Kolhapur, Maharashtra, India. Now, he is with the faculty at the Navsahyadri Group of Institution's Faculty of Engineering, Naigaon, Pune under the Pune University, Pune, Maharashtra, IndiaFrom July of 2012.HE has a teaching experience of over 2.5 years. His work has been published in 1 International Conferences and 1 National Conferences.

Prof. Atul V. Shah received the M.E. in Electronics from Walchand College of Engineering, SangliUnderShivaji University, Kolhapur onics Engineering, India, in 2005. Now, he is working as an Assistant Professor at the Department of Electronics & Telecommunication Engineering at D.K.T.E.S. Textile & Engineering Institute, Ichalkarnji, Maharashtra, India. His area of research is Computer Networking & Image Processing.

Prof. Dhananjay D. Gavali received the B.E. degree from Walchand College of Engineering, Sangli Under Shivaji University, Kolhapur of Electrical Engineering, India, in 2008 & completed M.Tech. in Electrical from Walchand College of Engineering, Sangli, Maharashtra, India. Now, he is working as an Assistant Professor & Head of the Department of Electrical Engineering at Navsahyadri Group of Institution's Faculty of Engineering, Naigaon, Pune under the Pune University, Pune, Maharashtra, India From September of 2012. HE has a teaching experience of over 06 years. His work has been published in 2 International papers, 6 National Conferences.

Prof.Sanjay L. Kurkute became a member of **IEEE** in 2002, a Life Member of ISTE in 2000. He has completed his B.E.(Electronics) M. Tech in Electronics. Presently he is doing the Research/ PhD in Power Electronics. He is working as Associate Professor in the Department of Electronics & Telecommunication Engineering at Navsahyadri Group of Institutions, Faculty of Engineering, Pune-412213. Also he was working as Principal Investigator for Research Project (2008, 2009) under BCUD, University of Pune. HE has a teaching experience of over 18 years. His work has been published in 5 International Journal, 1 International IEEE papers, 5 International Conferences and various National Conferences.