ISSN: 2321-8169
3301 – 3306

A Comparative Study of Object Oriented Steganographic Techniques

Priya R. Sankpal[1] and P. A. Vijaya[2]
1: Research Scholar, Dept. of ECE, BNMIT, BANGALORE, INDIA (*Priya.bnmit@gmail.com*),
2: Professor, Dept. of ECE, BNMIT, BANGALORE, INDIA (*pavmkv@gmail.com*)

Abstract-- Steganography is defined as camoufling secret information within other information i.e. hiding information. The steganography's main objective is to communicate securely in such a manner that the true information/message is not visible to the intruder. Any unwanted parties should not be able to correlate any sense between cover image and stego image. Thus the stego image must be same as the original cover image. In this paper, a comparative study of steganographic methods that use skin tone detection is done. For comparison three methods are considered. At first steganography using DWT is discussed. It is done in frequency domain as we obtain more precise stego images. Here Haar transform is used which leads to four sub bands. The secret data is embedded into one of the high frequency sub band. In the second method, secret data is embedded within skin region of image that provides an excellent secure location for data hiding. Skin tone detection is performed using HSV and YC_bC_r color space models. The last implementation is performed by applying skin tone detection using YC_bC_r color space and the edge of those skin pixels is detected using canny edge detection filter and then the secret image is steganoflaged into cover image. Performances of the three techniques are compared based on the PSNR obtained.

Keywords : *Steganography; Skin tone detection; DWT ;HSV; YC_bC_r color space*

*****

I. Introduction

In this highly electronically connected world, the Internet plays a pivotal role for data transmission and sharing. However, since it is a publicized medium worldwide, an unintended observer may steal, copy, modify, or destroy some confidential data. Hence in this electronics age, security problems become an essential issue. A well known procedure for secured data transmission is encryption. Although encryption schemes provide certain security measures, they make the secret messages unintelligible or meaningless. The encrypted messages usually make some unintended observers' attracted to them. As a result a new security approach termed "Steganography" has arisen [2].

I.1 Steganography History

The word Steganography derives its original meaning from Greek history which means "*Covered Writing*". For thousands of years, it is used in various forms. In the 5th century BC Histaiacus shaved a slave's head, tattooed a message on his skull and was dispatched with the message after his hair grew back. In Saudi Arabia at the king Abdulaziz City of Science and Technology, a project was initiated to translate into English some ancient Arabic manuscripts on secret writing which are believed to have been written 1200years ago. Some of these manuscripts were found in Turkey and Germany. 500 years ago, the Italian mathematician Jérôme Cardan reinvented a Chinese ancient method of secret writing, its scenario goes as follows: A paper mask with holes is shared among two parties, this mask is placed over a blank paper and the sender writes his secret message through the holes then takes the mask off and fills the blanks so that the letter appears as an innocuous text. This method is credited to Cardan and is called Cardan Grille. In more recent history, the Nazis invented several Steganographic methods during WWII such as Microdots, invisible ink and null ciphers. As an example of the latter a message sent by a Nazi spy that read: "*Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils*." Using the 2nd letter from each word the secret message reveals: "*Pershing sails from NY June 1*".

"Steganography is the art and science of communicating in a way which hides the existence of the communication". The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present. Steganography can be used in a large amount of data formats in the digital world of today. The most popular data formats used are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav. These formats are popular because of the relative ease by which redundant or noisy data can be removed from them and replaced with a hidden message. Steganographic technologies are a very important part of the security and privacy concerns on open systems such as the Internet. In Steganography secret message is the confidential data that needs to be protected and may be text, image, audio, video, or any other data that which can be represented as a stream of bits. The cover or host is the medium in which the message is embedded and serves to hide the presence of the message [1].

I.2 Steganography Types

Steganography can be classified two groups on the basis of: type of cover being used to embed the message and on the level of secrecy/privacy. Most of the digital file formats can be used as the cover object, but the one that is most appropriate is the one which has a large number of redundant bits. Redundancy can be defined as those bits of an object which on being altered do not change the meaning of the object or those bits that carry the least information about the object. This criterion of having a large number of redundant bits is highly satisfied by Image and Audio file types, but research has proved that other forms of digital file types also need this criteria. The five major categories of file format that can be used for Steganography are: Text, Image, Audio, Video and Protocol.

I.3 Steganography Methods

A. Steganography in Spatial Domain

This is a simplest steganographic technique that embeds the bits of secret message directly into the least significant bit (LSB) plane of the cover image. In a gray level image, every pixel consists of 8 bits. The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly. The mathematical representation for LSB is:

$$x_i' = x_i - x_i \bmod 2k + m_i \qquad (1)$$

In equation (1), x_i' *represents* the *i* th pixel value of the stego-image and x_i *represents* that of the original cover image. m_i *represents* the decimal value of the *i* th block in the confidential data. The number of LSBs to be substituted is k. The extraction process is to copy the k-rightmost bits directly. Mathematically the extracted message is represented as:

$$m_i = x_i \bmod 2k \qquad (2)$$

Hence, a simple permutation of the extracted m_i *gives* us the original confidential data. This method is easy and straightforward but this has low ability to bear some signal processing or noises. And secret data can be easily stolen by extracting whole LSB plane [2].

B. Steganography in Frequency Domain

Robustness of steganography can be improved if properties of the cover image could be exploited. For example it is generally preferable to hide message in noisy regions rather than smoother regions as degradation in smoother regions is more noticeable to human HVS (Human Visual System). Taking these aspects into consideration working in frequency domain becomes more attractive. Here, sender transforms the cover image into frequency domain coefficients before embedding secret messages in it. Different sub-bands of frequency domain coefficients give significant information about where vital and non vital pixels of image resides. These methods are more complex and slower than spatial domain methods; however they are more secure and tolerant to noises. Frequency domain transformation can be applied either in DCT or DWT [2].

C Adaptive Steganography

Adaptive steganography is special case of two former methods. It is also known as “Statistics aware embedding” and “Masking”. This method takes statistical global features of the image before attempting to embed secret data in DCT or DWT coefficients. The statistics will dictate where to make changes [2].

II. Skin Tone Detection

In steganography, secret data can be embedded within the skin region of image, as it provides excellent secure location. Skin detection is the process of finding skin-colour pixels and regions in an image or a video. This process is typically used as a pre-processing step to find regions that potentially have human faces and limbs in images.

A skin detector typically transforms a given pixel into an appropriate color space and then uses a skin classifier to label the pixel whether it is a skin or a non-skin pixel. A skin classifier defines a decision boundary of the skin color class in the color space. Although this is a straightforward process but is quite challenging. Therefore, important challenges in skin detection are to represent the color in a way that is invariant or at least insensitive to changes in illumination and Another challenge comes from the fact that many objects in the real world might have skin-tone colors. This causes any skin detector to have much false detection in the background if the environment is not controlled. The simplest way to decide whether a pixel is skin color or not is to explicitly define a boundary. RGB matrix of the given color image can be converted into different color spaces to yield distinguishable regions of skin or near skin tone. There exists several color spaces. Mainly two kinds of color spaces are exploited in the literature of biometrics which is HSV (Hue, Saturation and Value) and YC_bC_r (Yellow, Chromatic Blue, Chromatic red) spaces.It is experimentally found and theoretically proven that the distribution of human skin color constantly resides in a certain range within those two color spaces. Color space used for skin detection in this work is HSV. Any color image of RGB color space can be easily converted into HSV color space. Sobottaka and Pitas defined a face localization based on HSV. They found that human flesh can be an approximation from a sector out of a hexagon with the constraints: S_{min}= 0.23, S_{max} =0.68, H_{min} =0^0 and H_{max}=50^0 [2-3].

III. Comparison of Steganographic Methods

In this section, comparisons of steganographic methods that use skin tone detection are discussed. The three methods compared are:

- Steganography using DWT in frequency domain.
- Steganography based on symmetric cryptography using skin tone detection.
- Steganography using skin tone detection and edge detection.

III.1 Steganography using DWT in frequency domain.

The flowchart of the steganography using DWT in frequency domain [5] is as shown in figure 1.The simplest type of DWT i.e. Haar DWT - has been applied [4]. In 1D-DWT average of fine details in small area is recorded. In case of 2D-DWT one step of the transformation is performed on all the rows. The matrix contains down sampled low pass coefficients of each row on the left side and the right side contains the high pass coefficients. In the next step, one step transformation is applied on all the columns. Application of transformation results in four different types of frequency bands: LL, HL, LH, HH. Since Human eyes are much more sensitive to the low frequency part (LL sub band) we can hide secret message in other three parts without making any alteration in LL sub band [12]. As other three sub-bands are high frequency sub-band they contain insignificant data. Embedding secret data in these sub-bands does not degrade the image quality.

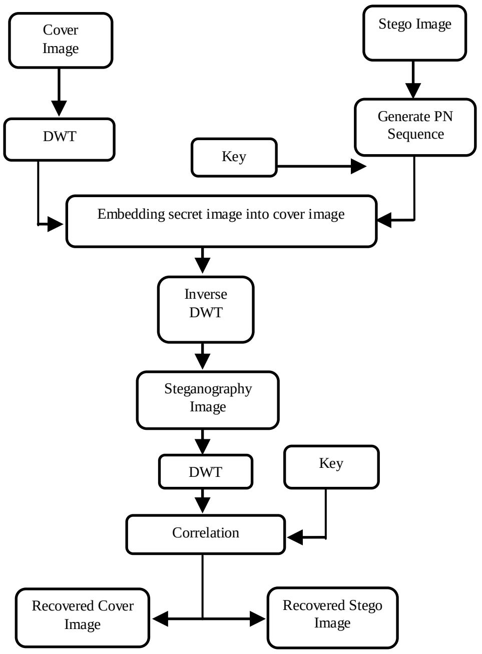

Figure 1: Flowchart for Steganography using DWT in frequency domain

A. *Embedding Procedure/ Algorithm*

Embedding procedure involves insertion of secret message onto cover object Additional components such as pseudo-random number is used rather than the usual Steganographic objects. Pseudo-random sequences typically exhibit statistical randomness while being generated by an entirely deterministic causal process generator. A pseudo-random number generator is a program that generates a seemingly random sequence of numbers when input seed is applied.

1. The cover image (x) is read.
2. Calculate the size of cover image (x).
3. The secret image (y) is read.
4. (y) is prepared as a message vector.
5. Haar wavelet transform is used to decompose The cover image(x).
6. Pseudo-random number (P_n) is generated.
7. Horizontal and vertical coefficients of wavelet decomposition are modified by adding P_n when message bit = 0.
8. Inverse DWT is applied.
9. Prepared stego image is displayed.

B. *Extraction Procedure/Algorithm*

In this step extraction of secret message is carried out. During extraction process correlation theory is also used. Correlation is the degree to which two or more quantities are linearly associated. The correlation between two same size matrices can be calculated by:

$$r = \frac{\sum_{m}\sum_{n}(A_{mn}-\bar{A})(B_{mn}-\bar{B})}{\sqrt{\left(\sum_{m}\sum_{n}(A_{mn}-\bar{A})^2\right)\left(\sum_{m}\sum_{n}(B_{mn}-\bar{B})^2\right)}} \quad (3)$$

1. The cover image (x) is read.
2. The stego image is read.
3. Haar wavelet transform is used to decompose the cover image(x) and stego image.
4. A message vector of all ones is generated.
5. Correlation between the original and modified coefficients is found.
6. If the correlation value is greater than the mean correlation value, turn the message vector bit to 0.
7. Message vector is prepared to display secret image.

III.2 Steganography based on symmetric cryptography using skin tone detection.

Skin tone detection is the method of embedding secret data within skin region, as it is less much sensitive to HVS (Human Visual System). This technique makes use of biometric features such as skin tone and not embedding data anywhere in the image. The data is embedded in selected regions [2].

A. *Embedding Procedure*

1. Skin tone detection of the input image is performed using HSV color space.
2. The cover image is transformed into frequency domain. This is performed by using Haar-DWT which results in four sub-bands.
3. The number of bits in which we can hide data termed as payload is calculated.
4. Secret data embedding is performed by tracing skin pixels in any one of the high frequency sub-band. The LL sub-band contains significant information and hence embedding in LL sub-band degrades the image quality greatly. In this method high frequency HH sub-band is chosen. Secret data is not embedded in all the pixels of DWT sub –band but to only the traced skin pixels. The skin pixels are traced using skin mask and secret data is embedded. Embedding is performed in B-plane and not in G/R-plane as skin color is largely contributed by the R plane than G/B plane. When the R plane pixel values are modified, at decoder the skin detection side gives different mask than encoder side and as a result data is not retrieved at the decoder. Secret data is embedded, coefficient by coefficient (raster scan)_in selected sub-band, if coefficient is skin pixel.
5. Perform IDWT to combine 4 sub-bands. Thus a stego image is obtained.

The embedding algorithm attempts to preserve histogram of DWT coefficients after embedding also. This protects from histogram based first order statistics attacks. The flowchart for steganography using skin tone detection is as shown if figure.

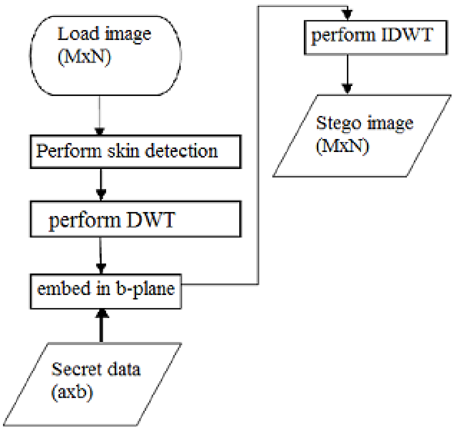

Figure 2: Embedding procedure flowchart

B. Extraction Procedure

- The cover image is loaded and skin detection is performed on it, which results in a binary mask. The obtained binary mask acts as the key in the retrieval of the secret data.
- The received stego image is loaded and this is the input at the retrieval process.
- DWT in performed on the stego image. Now from the Hi-Hi band obtained after applying DWT, the secret data has to be retrieved.
- Using the binary mask, apply the inverse process of embedding in the Hi-Hi band to retrieve the secret data. Thus from the stego image, the secret data is retrieved.

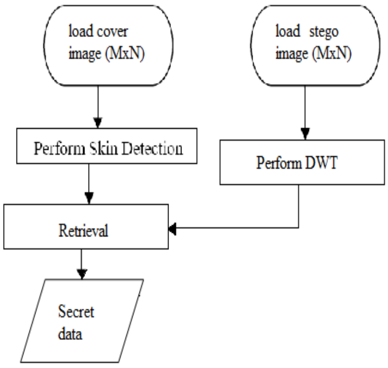

Figure 3: Extraction procedure flowchart

To enhance the security, we can first encrypt the secret image and then embed it with the Cover image to obtain the Stego image. This can be achieved as follows:

1. First, the secret image of size axb is converted into a vector of size 'a'.
2. We adopt a secret key with which we XOR each of the vectors to give the transformed vectors.
3. These transformed vectors are arranged to form a matrix which gives the transformed secret image.
4. This transformed secret image is embedded with the Cover image. Thus the Stego image is obtained.
5. At the receiving side first the transformed secret image is extracted. This is then decoded to obtain the actual secret image.

III.3 Steganography using skin tone detection and Edge detection.

A. Edge detection:

Edges define boundaries and therefore are of fundamental importance in image processing. Edges images are areas with strong intensity contrasts. Edge detection of an image significantly reduces the amount of data and filters out the unwanted information, while preserving the important structural properties of the image. There are different methods of edge detection. Either gradient and Laplacian edge detection can be used. In the gradient method edge detection is achieved by looking for the maximum and minimum in the first derivative of the image. The Laplacian method detects zero crossings in the second derivative of the image to detect edges. An edge has the one-dimensional shape of a ramp hence calculating the derivative of the image can highlight its location. Sobel, Prewitt, Canny are some of the edge detection techniques.

In the proposed method Canny edge detector algorithm is used. At first Canny edge detector is used to smoothen the image to eliminate noise. To highlight regions with high spatial derivatives image gradient is found and suppresses those pixels that are not at the maximum (non maximum suppression). The gradient array is reduced further by using hysteresis. The remaining non suppressed pixels are tracked by Hysteresis. For this purpose two threshold levels (T1 and T2) are defined. Threshold (T2) is set to zero (made a non edge) when the magnitude is less than T1. When the magnitude is above T2, it is made an edge. If the magnitude is lies between the 2 thresholds (T1 and T2), zero is set, unless there is a path from this pixel to a pixel with a gradient above T2.

B. Steganographic Process:

1. The cover image is read.
2. Skin tone detection is applied to the cover image.
3. Edge detection is performed using canny edge detection algorithm.
4. Secret message is embedded on to the cover image.
5. Final stego image is displayed.

III. Simulation Results

All the three methods discussed above were implemented using MATLAB 7.8. The simulation results of the three techniques are listed below. The cover image used for the three techniques is same and is of the size 512x512.

Figure 4: Cover Image (same for all three steganography techniques)

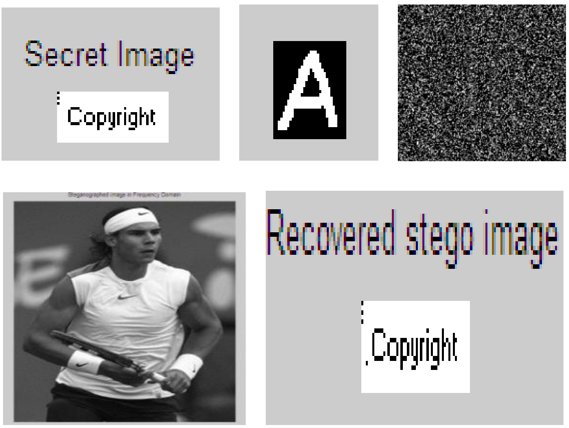

Figure 5: Steganography using DWT. (a) Secret Image,(b) Key (c) PN sequence,(d) Stego Image and (e) Recovered Stego Image.

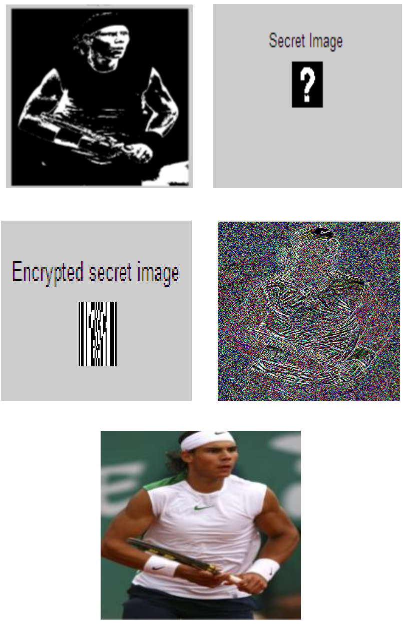

Figure 6: Steganographic technique based on symmetric cryptography using skin tone detection. (a) Skin tone detection,
(b) secret image, (c) Encrypted secret image,(d) Secret Message Embedded in CD1 Band and (e) Final embedded image.

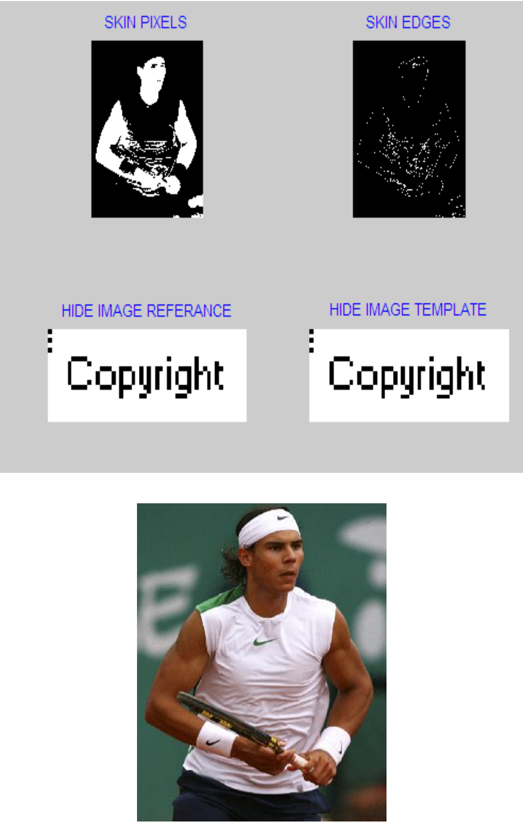

Figure 7: (a) Steganographic technique using shin tone detection and edge detection, (b) Steganographed image

IV. Performance Measure

As a performance measure [1] of image distortion, the well known Peak-Signal-to-Noise Ratio (PSNR) which is classified under the difference distortion metrics can be applied on the stego images. It is defined as:

$$PSNR = 10\log_{10}\left(\frac{C_{\max}^{2}}{MSE}\right) \qquad (4)$$

where *MSE* denotes the Mean Square Error which is given as:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy})^2 \qquad (5)$$

and holds the maximum value in the image, for example:

$$C_{\max} \le \begin{cases} 1 \text{ in double precision intensity images} \\ 255 \text{ in 8-bit unsigned integer intensity images} \end{cases} \qquad (6)$$

x and y are the image coordinates, M and N are the dimensions of the image, S_{xy} is the generated stego image and C_{xy} is the cover image. Many authors in the literature consider C_{max} =255 as a default value for 8-bit images. It can be the case, for instance, that the examined image has only up to 253 or fewer representations of gray colors. Knowing that C_{max} is raised to the power of 2 results in a severe change to the PSNR value. Thus we define C_{max} as the actual maximum value rather than the largest possible value. PSNR is often expressed on logarithmic scale in decibels (dB). PSNR values falling below 30dB indicate a fairly low quality (i.e., distortion caused by embedding can be obvious); however, a high quality stego should strive for 40dB or higher. The PSNR obtained for the three different steganographic techniques are tabulated in table 1.

Table 1: Performance Measure of all Implementations.

Steganographic Technique	PSNR
Using DWT	29.00
Using Skin tone and edge detection	36.00
Using Symmetric cryptography and skin tone detection	46.81

High quality stego image is obtained with symmetric cryptography based steganography using skin tone detection. The stego image of skin tone and edge detection steganographic technique is fairly better, but that obtained using DWT in frequency is of low quality.

V. Conclusion

Object oriented Steganography uses skin region of images in DWT domain for embedding secret data. Security can be enhanced by embedding data in only certain region (here skin region) and not in whole image. Features obtained from DWT coefficients are utilized for secret data embedding. This also increases the quality of Stego image because secret messages are embedded in high frequency sub-bands which human eyes are less sensitive to. A two-level security is provided, when the data is encrypted and then embedded.

Acknowledgment

The authors would like to thank to the earlier works on/regarding Steganography, which contributed significantly

to the comparative work done in this paper. All work done, images shown in this paper are for educational purpose and not for commercial purpose.

REFERENCES

[1] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, "Biometric inspired digital image Steganography", in: Proceedings of the 15th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS'08), Belfast, pp. 159-168, 2008.

[2] Anjali A. Shejul and U. L. Kulkarni, "A DWT based Approach for Steganography Using Biometric", International Conference on Data Storage and Data Engineering(DSDE'10), pp 39 - 43,2010.

[3] Rekha D.Kalambe, .Rakesh Pandit,and Sachin Patel,"A Hash-Based Approach on Secure Skin Tone Stegnography using Wavelet Transform ",International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 10, pp 973 – 980, October 2013.

[4] Chen, P. Y.and Liao, E.C.: A new Algorithm for Haar Wavelet Transform," 2002 IEEE International Symposium on Intelligent Signal Processing and Communication System, pp.453-457(2002). 43

[5] Barnali Gupta Banik and Samir K. Bandyopadhyay," A DWT Method for Image Steganography", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 6, pp 983-989, June 2013.

Authors

Priya R. Sankpal received post graduate degree from VisVeswaraya Technological University, Belgaum in 2005. She is currently working as a Assistant Professor in the Dept. of TCE, BNMIT, Bangalore and is pursuing research. Her areas of interest are Image Processing, Communication and Embedded Systems.

P.A. Vijaya received Phd from IISc, Bangalore in 2005. She is currently working as a Professor in Dept.of E & C, BNMIT,Bangalore.She has around 90 publications in reputed journals and conferences. She is guiding 6 research students. Her areas of interest are Pattern Recognition, Image Processing and Embedded systems.