

Performance Evaluation of Steganography and AES encryption based on different formats of the Image.

Farhan R. Patel¹, Dr. A. N. Cheeran²

M.Tech Student, Department of Electrical Engineering, V.J.T.I. College, Mumbai City, India¹

Associate Professor, Department of Electrical Engineering, V.J.T.I. College, Mumbai City, India²

Abstract: During the recent times, there has been tremendous growth in transfer of data across the globe which ultimately has boosted data communication over the computer networks. For any data communication network, the information content security of the messages is of prime concern. Steganography and Cryptography are two different data hiding techniques. Steganography puts a cover onto the messages by some other form of digital media whereas Cryptography on the other hand performs the encryption of the message. In this paper, we present a combination of both these techniques wherein the text is first hidden into some form of cover image using Least significant bit (LSB) hiding method and then encryption using Advanced Encryption Standard (AES) is performed on to the stego image. The combination of both these algorithm will certainly ensure high degree of security, integrity, capacity and robustness to the embedded data. Using GUI based MATLAB simulation, a comparative analysis is being made by employing different formats of the images for learning variations in performance evaluation parameters such as delay, Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), and Absolute Mean Square Error (AMSE). The objectives of this paper are to provide security against visual as well as statistical attacks and to ensure better quality of received information.

Keywords: Steganography, Cryptography, LSB hiding, AES encryption standard, Human Visual System (HVS), PSNR, MSE, AMSE.

I. INTRODUCTION

With the increase in data communication over the network, security of the data is of major concern and hence is the theme of our paper. Digital data can be transmitted over the network with little error and least interference, however to ensure unauthorized access of the data, we need to preserve confidentiality and data integrity of the message which is being transmitted [2]. Steganography techniques are used to protect information by concealing secret data [1]. We employ LSB substitution technique for hiding of the data into cover image. Cryptography technique provides encryption to the original content thereby changing the representation of the information, which becomes difficult to understand by the attacker or intruder. In our paper, we make use of AES encryption standard to provide cryptography. Hence, the paper involves a combination of Steganography and Cryptography which will certainly be more robust for the information security of the data which is being transmitted. This paper also presents comparison of performance by employing different formats of the image, analysing it gives the information of which format is most suitable under this technique. The remainder of this paper is organized as follows: Section II describes the previous work done. Section III describes the Flowchart representation of the work. Section IV describes the concept of previous work done in this area. Section V explains LSB substitution technique of steganography and AES method of encryption. Then, the following section VI gives the information of simulation and experimental results achieved and the conclusion of the paper.

II. LITERATURE REVIEW

This section overview on the main components of a traditional steganographic and cryptographic system and briefly introduces the current approach, title and author details. A significant work was carried on by Peticolas F. A., R. Anderson in [1], [2] wherein the classification of steganography is being carried out. The authors have discussed some of the ancient and the modern steganography approaches.

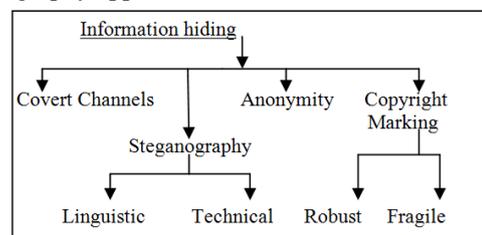


Fig. 1: Classification of Information hiding techniques

On the other hand, the work presented by S.J. Wang was involving increased level of security by first embedding the secret image into the host image and then multiplying it with substitution matrix. Here, an increased level of security was provided due to the involvement of substitution matrix which acts as a key [4]. In another work presented by G. Vanjare claims that LSB substitution is the most adapted method to increase the capacity of the system by reducing the quality of the cover image being used [5]. In their work, the author has also presented DWT as a compression technique after performing

steganography. V. K. Sharma, V. Shrivastava explained the algorithm for first component alteration technique which indicates that for a colour image each pixel is a combination of three components Red (R), Green (G), Blue (B), however this technique signifies that the first component alone is sufficient for data hiding. This first component can be either R or G or B, but E. Hetch in his research of hyper physics signifies that visual perception of intensely blue objects is less distinct than perception of objects of red and green [6]. Also, in their research work the author explains improved LSB technique where in the text is hidden into the cover image using Logic-Gates [6]. According to R. S. Gutte and Y. D. Chincholkar in the year 2012, Steganography method along with cryptography are the best method for secret communication [7]. In their research work, by calculating entropy, standard deviation, and other statistical parameters, performance evaluation is carried out on both 1bit LSB and 2bit LSB substitution and it signifies that even 2bit LSB substitution results in negligible variations in the original image but gives almost double the data hiding capacity. For the encryption purpose, they used Extended Square Substitution Algorithm [7]. With the combination of both steganography and cryptography a two level security can be obtained and the performance can be improved. Scharinger designed a Kolmogorov flow based image encryption technique in which the whole image is taken as a block and permuted through a key controlled chaotic system [11]. Block permutation found to be faster and gave computationally efficient results. On comparing with Data Encryption Standards (DES), Triple Data Encryption Standard (3DES) and other symmetric key cryptographic methods, AES found to be more efficient and robust symmetric form of cryptosystem [12]. Mitra carried out performance analysis by comparing cryptography when done on pixel, bit, block level and evaluates degree of security [13].

III. STEGANOGRAPHY AND CRYPTOGRAPHY

A. Steganography

Steganography relies on hiding message in unsuspected multimedia and is generally used in secret communication between acknowledged parties [3]. The technique of Steganography takes advantage of the psycho visual redundancy of the Human Visual System (H. V. S.) that is taking advantage of the fact that human eye cannot distinguish between two highly correlated pixels. This can be easily accomplished if the carrier to hide the text is in the form of digital image, wherein adjacent pixels are highly correlated. Any Steganography system model must satisfy the following three properties:

- i. Invisibility: The secret data must be invisible with the naked eye view.
- ii. Capacity: A cover image must hold more embedded secret data, consequently image quality is degraded, and hence there is a trade-off between image quality and capacity [4].
- iii. Robustness: The stego image must hold the secret data even after some noise gets added to it.

The above 3 conditions are the qualitative measures which indicates how much is our system model capable to handle the various attacks [6].

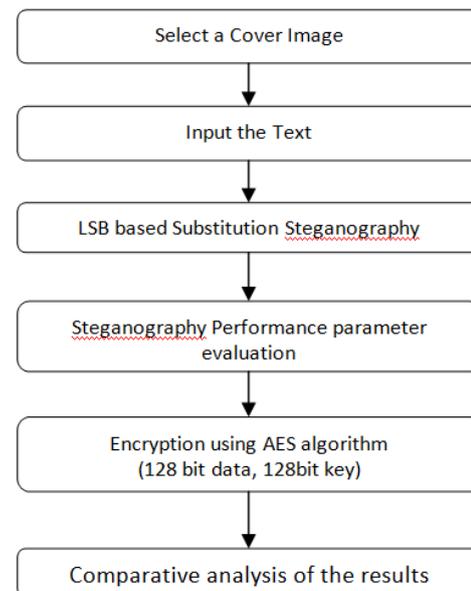


Fig. 2: Flow Chart of the proposed method

Steganography is divided into two main categories:

- (i) Spatial domain approach: In this method, the secret message is directly hidden by modifying the pixels of the image. Advantage of this technique is high data embedding capacity. Examples are LSB substitution technique, watermarking etc.
- (ii) Transform domain approach: In this method, the secret message is indirectly embedded by taking some type of transforms such as DCT, DWT, etc. Advantage of this technique is more robustness.

The important concepts such as LSB inserting, followed by the types of cryptosystem etc. are discussed in the following sections.

LSB substitution method of Steganography: LSB substitution is the most adapted method to increase the capacity of data hiding by making some compromise in the image quality. The LSB in the 8bit grey level image contains very less significant information, while the MSB of the image contains significant information. LSB bit substitution technique makes the use of this bit position and smartly replaces LSB of image with the secret data. The mathematical representation of LSB method can be given as [7]:

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

In the above equation,

x_i denotes the i^{th} pixel value of the stego image.

m_i denotes the decimal value of the i^{th} block in the secret image.

k is the number of LSB substituted.

On the other hand, the mathematical representation of extracted image is given as [7],

$$m_i = x_i \bmod 2^k \quad (2)$$

Now, if desire choice is capacity then even the last second bit can be substituted but this will result in degradation of the image quality. Hence, there is a trade-off between image quality and capacity of data hiding.

B. Cryptography

Cryptography is the process of scrambling the original text by rearranging and substituting the original text making it unreadable for others [1].

In the process of cryptography a secret key is used to convert the plain text into the cipher text, this key ensures the data integrity. Depending upon the type of the key being used in the system, we have two types of the cryptography methods:

(i) Symmetric Cryptosystem: In this method, both the sender and the receiver uses the same key, hence this method is named as Private key Cryptosystem. Advantages: Less chance of breaking of cryptography method and key, highly secure, coherent system and hence least probability of error. Examples: AES encryption, DES encryption, 2DES, etc.

(ii) Asymmetric Cryptosystem: In this method, both the sender and the receiver uses different key, hence this method is named as Public key Cryptosystem.

Advantages: since the key is public key, hence there is more chance of breaking of cryptography method, not highly secure, non coherent system and hence more probability of error.

Examples: RSA, ECC algorithm, etc.

1) AES Encryption Standard:

We employ AES standard of symmetric cryptosystem. AES is a block cipher technique with a data block length of 128 bits.

AES allows for three different key length sizes such as 128 bits, 192 bits, 256 bits. Depending upon the key length different numbers of processing rounds are required for any AES algorithm.

Data block length: 128bits.

Key length: 128bits, 192bits or 256bits.

AES is an iterative algorithm in which single complete iteration is called as "Round". The total number of rounds N_r depends upon the key length N_k .

The 128 bit data is divided into 16 Bytes. These bytes are mapped to a 4×4 array called as the state and all operations of AES are performed on this state.

Each round involves four steps namely:

- Byte substitution step
- Row wise permutation step
- Column wise mixing step
- Addition of Round key

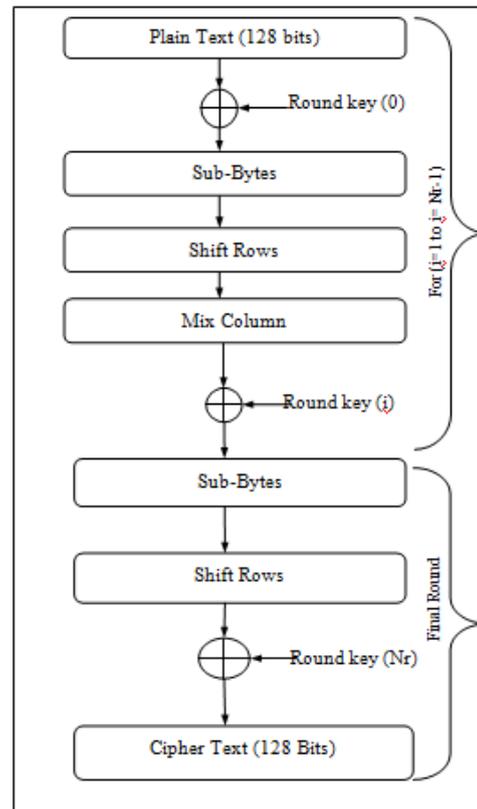


Fig. 3: AES encryption block diagram different steps which are performed based upon N_r and N_k .

The following are the variations of the key size and their corresponding rounds:

Table I. AES parameters

Key length(N_k)	Block size(N_b)	No. of rounds(N_r)
$4 \times 32 = 128$ bits	$4 \times 32 = 128$ bits	10
$6 \times 32 = 192$ bits	$4 \times 32 = 128$ bits	12
$8 \times 32 = 256$ bits	$4 \times 32 = 128$ bits	14

If the key length is less than the required number of bits for a specific AES algorithm then it must be expanded by zero padding method to bring it to desired length. However, if the required key length is more than the data bits as in AES-192, AES-256 than the key expansion algorithm is used to expand the key length.

IV. PROPOSED METHODOLOGY

We perform the combination of both Steganography and Cryptography thereby ensuring high degree of security for the data. For the steganography we employ LSB substitution technique and then carrying out encryption using AES technique which involves 128 bit block size of data and 128 bit block size of the key.

The process of hiding text into the image is done using the spatial domain approach named as LSB substitution technique, wherein LSB of the cover image is being

replaced by the data. This method ensures larger data holding capacity with negligible compromise on the image quality. This is because in an image there is high degree of redundant information as adjacent pixels are highly correlated and HVS cannot distinguish among correlated pixels.

A. Steganography Implementation Using LSB Substitution

The complete algorithm of data hiding in an image is given in [14] as follows:

Let C be the original 8-bit greyscale cover-image of

$M_c \times N_c$ pixels represented as

$$C = \{X_{ij} \mid 0 \leq i < M_c, 0 \leq j < N_c\}$$

$$X_{ij} \in \{0, 1, \dots, 255\} \quad \dots \dots \dots (1)$$

M be the n-bit secret message represented as

$$M = \{m_i \mid 0 \leq i < N, m_i \in \{0, 1\}\} \quad \dots \dots \dots (2)$$

For embedding the n-bit secret message M into the k rightmost LSBs of the cover-image C, the secret message M is rearranged to form a conceptually k-bit virtual image M' which is represented as,

$$M' = \{m'_{ij} \mid 0 \leq i < n', m'_i \in \{0, 1, \dots, 2^k - 1\}\} \quad \dots \dots \dots (3)$$

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:

$$m'_i = \sum_{j=0}^{k-1} m_{i \times k + j} \times 2^{k-1-j} \quad \dots \dots \dots (4)$$

A subset of n' pixels $\{x_{11}, x_{12}, \dots, x_{1n}\}$ is chosen from the cover-image C in a predefined sequence. The embedding process is completed by replacing the k LSBs of x_{ij} by m'_i . Mathematically, the pixel value x_{ij} of the chosen pixel for storing the k-bit message m'_i is modified to form the stego-pixel x'_{ij} as follows:

$$x'_{ij} = x_{ij} - x_{ij} \bmod 2^k + m'_i \quad \dots \dots \dots (5)$$

Also, Algorithm [15] for LSB Based extracting process is given as:

In the extraction process, given the stego-image S, the embedded messages can be directly extracted. Using the same sequence as in the embedding process, the set of pixels $\{x_{11}, x_{12}, \dots, x_{1n}\}$ storing the secret message bits are selected from the stego-image. The k LSBs of the selected pixels are extracted and lined up to reconstruct the secret message bits.

B. Implementation of Encryption using AES method

Designing Steps

State array

The input to the encryption algorithm is a single 128 bit block; now this block is required to be copied into a state array. State Array is a square matrix of bytes. This state array is modified at each stage of encryption.

Key Expansion

This stage is the most important stage for both encryption as well as decryption. The AES key expansion algorithm

[15] takes as input a 4-word key and produces a linear array of 44 words. Each round uses 4 of these words as shown in Fig. 4. Each word contains 32 bytes which means each sub key is 128 bits long.

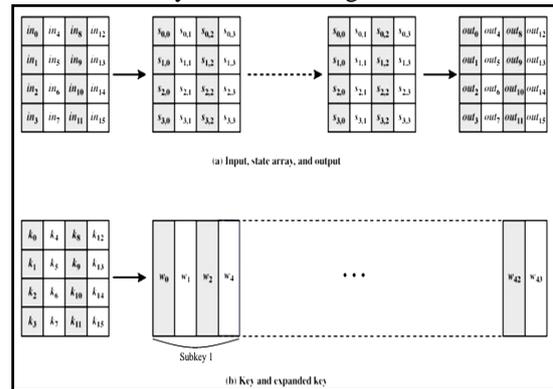


Fig. 4: Key Expansion

Add Round Key Expansion

The 128 bits of State array are bitwise XORed with the 128bits of the round key(4 words of the expanded key).The operation is viewed as a column wise operation between the 4 bytes of the State array column and one word of the round key (Fig. 5).



Fig.5: Add Round Key Expansion

S-Box Substitution

AES defines a 16 x 16 matrix of byte values, called an S-box which contains a permutation of all possible 256 8-bit values. Each byte of State array is mapped into a new byte in the following way: The leftmost 4 bits of the byte are used as a row designated value and the leftmost 4 bits are used as a column designated value. These row and column designated values serve as indexes into the S-box to select a unique 8-bit output value.

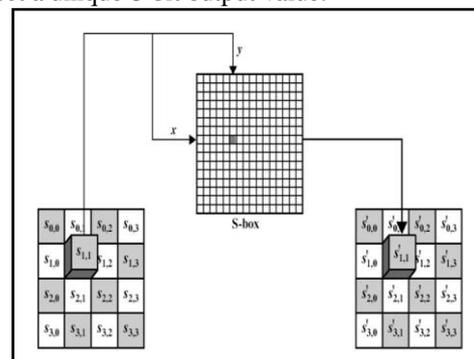


Fig. 6: S-Box Substitution

Row Shifting

For the second row, a 1-byte circular left shift is performed. For the third row, a 2- byte circular left shift is performed. For the third row, a 3- byte circular left shift is performed. For the first row, no shifting is performed.

Column Mixing

It operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in the column. The transformation can be defined by following matrix multiplication on State array.

V. SOFTWARE SIMULATION

Evaluation of parameters:

A. PSNR:

It is the ratio between maximum possible power and corrupting noise that corrupts the representation of the image. Higher is the value, better is the quality of the image.

$$PSNR = 10 \log_{10} \frac{(2n-1)^2}{MSE} \dots\dots\dots (6)$$

B. MSE:

It is a “figure of merit” which indicates the degree of similarity or differences between two images. Lesser the MSE value of an image better is the quality and less distortion from the original.

$$MSE = \frac{1}{M} \times \frac{1}{N} \sum_{i=0}^M \sum_{j=0}^N (x(i,j) - y(i,j))^2 \dots\dots\dots (7)$$

C. Delay:

It is the time taken by the process of steganography or cryptography with steganography.

On performing GUI based MATLAB simulation, we get the following results.

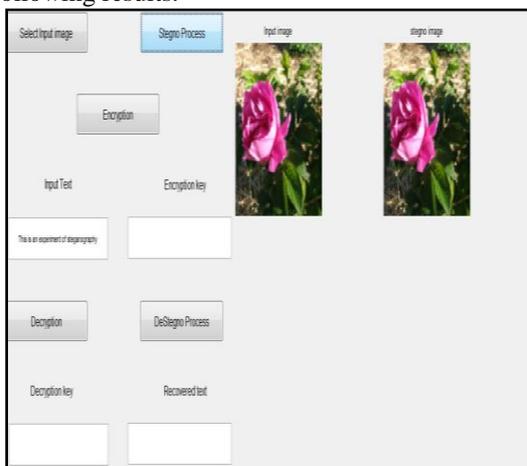


Fig.7: Steganography implementation on color image

The figure 7, demonstrates the result of hiding a text into a color image without making a considerable change in the image.

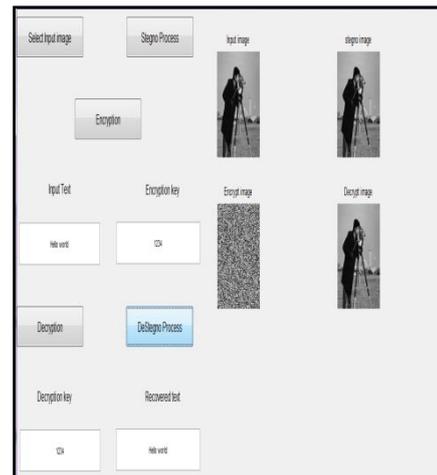


Fig. 8: Implementation of AES encryption on Stego image.

The figure 8, demonstrates the result of hiding a text into a color image and then encryption-decryption involving AES method of Cryptography. It also shows the recovered text.

VI. RESULTS AND CONCLUSION

Table II. Results showing the performance parameters for both steganography alone and combination of steganography and cryptography

Image name	Type	PSNR (dB)	MSE	Delay (sec)	MSE	Delay (sec)
	.tif	68.2843	0.0103	5	0.010305	95
	.png	71.8420	0.0038	4	0.003852	104
	.jpg	72.5661	0.0036	5	0.003645	85
	.bmp	79.7225	0.0010	10	0.001013	70
	.gif	70.4979	0.0058	12	0.005829	120

Observing the results in table 2, and evaluating the performance based upon only Steganography we learn that .bmp is the best format which supports steganography, also the criteria of minimum MSE and maximum PSNR both are together satisfied by the bmp format. However, in terms of delay in processing .png and .jpg takes least processing time. Only Steganography implementation using LSB substitution algorithm generally has a delay of fewer seconds which can be tolerated. But when we perform both cryptography and steganography we find

different results. We observe that on performing both LSB steganography and AES encryption on different formats of the image, the delay of the process increases. This delay is the total delay, wherein number of rounds involving in AES expansion results in increase in the delay.

VII. FUTURE SCOPE

Implementation of Steganography and Cryptography together were performed with text and images, but this method can be further be extended to audio, video as well thereby adding up the security in the audio and video processing.

REFERENCES

- [1]. Anderson, R. J. and Petitcolas, F. A.P. (1998) "On the Limits of Steganography", IEEE Journal of Selected Areas in Communications, Vol.16 No.4, pp.474-481, ISSN 0733-8716.
- [2]. Petitcolas, F.A.P., Anderson, R. J. and Kuhn, M.G. (1999) "Information Hiding- A Survey", Proceedings of the IEEE, Special issue on Protection of Multimedia Content, vol. 87, no. 7, pp.1062-1078.
- [3]. Rabah, K. (2004), "Steganography – The Art of Hiding Data", Information Technology Journal, Vol.3, no.3, pp. 245-269.
- [4]. Cheng-HsingYang and Shih-Jeng Wang, "Transforming LSB substitution for image-based steganography in matching algorithms", Journal of information Science and Engineering 26, 1199-1212 (2010).
- [5]. Gauresh Vanjare and Sayalee Gharghe "Performance evaluation of LSB substitution and DWT method for steganography" International Journal of advance researches in computer science and software engineering vol.5, issue 3, March-2015.
- [6]. Vijay Kumar Sharma And Vishal Shrivastava, "A Steganography algorithm for hiding image in image By Improved LSB Substitution by Minimize detection", Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1
- [7]. Gutte, R. S. and Chincholkar, Y. D. (2012) "Comparison of Steganography at One LSB and Two LSB Positions", International Journal of Computer Applications, Vol.49,no.11, pp.1-.
- [8]. S. A. Laskar, K. Hemachandran, "High capacity data hiding using LSB Steganography and Encryption", International journal of database management system, Vol.4, issue 6, Dec-2012.
- [9]. Farhan R. Patel, Dr. A. N. Cheeran, "AES grade encryption security on steganography", International journal of emerging trends in engineering and basic sciences", volume 2, issue1, (Jan-Feb) 2015.
- [10]. Manupriya, Tarun Kumar, "Analysis of Wavelets with Watermarking through Wavelet Transformation", International Journal of Computer Applications (0975 – 8887) Volume 96– No.22, June 2014
- [11]. J. Scharinger, "Fast encryption of image data using chaotic Kolmogrov flow, International journal of Electronic Engineering 7 (1998) (2), pp. 318–325.
- [12]. Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani "New Comparative Study between DES, 3DES and AES within Nine Factors", Journal of Computing, Volume 2, Issue 3, March 2010, ISSN 2151-9617.
- [13]. Mitra, Y. V. Subba Rao, and S. R. M. Prasanna, A new image encryption approach using combinational permutation techniques, International Journal of Computer Science, vol. 1, no. 2 , pp. 1306-4428, 2006.
- [14]. Chan, C.K., Cheng, L.M., 2004. "Hiding data in images by simple LSB substitution". Pattern Recognition 37(March), 469–474.
- [15]. P.Karthigaikumar and S.Rasheed "Simulation of Image Encryption using AES algorithm", IJCA special issue on computational science-new dimensions and perspectives" NCCSE 2011.

BIOGRAPHIES

Patel Farhan Rehman, He received his Bachelor degree in Electronics and Telecommunication Engineering from the University of Mumbai, in India in 2012 and he is

currently pursuing M.Tech degree in the department of Electrical Engineering, Veermata Jijabai Technological Institute (VJTI), Mumbai, India. His research interest is Digital signal processing, image processing and Steganography.

Dr. Alice Noble Cheeran, She received her B.E. in Electrical Engineering from the Kerala University, India in 1984. She joined the Electrical Engineering department, Veermata Jijabai Technological Institute (V J T I), Mumbai, India as lecturer in 1987. She completed Masters in Electrical Engineering with specialization in control systems in 1994 from Mumbai University, India. Subsequently she completed Masters in Electronics Engineering in 1996 from the same university. Further did Ph. D. in the topic of signal processing for hearing aids in 2005 from IIT, Bombay, India. Currently she is an Associate Professor. Her topics of interest include Signal and Image Processing Applications in various fields like biomedical, partial discharge etc.