Volume 4, No. 4, March-April 2013
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Triple DES Algorithm for Hiding Amorphous Secret Data into Predictive Coding Based on Reversible Image Steganography

Ananthi. S*
*Ph.D Scholar, Dept. of CSE
Annamalai University
Chidambaram, India.
ananthi68@gmail.com

Dhanalakshmi. P**
**Associate Professor, Dept. of CSE
Annamalai University
Chidambaram, India.
abi_dhana@rediffmail.com

Abstract: Cryptography is the art of converting one form of message into another form which hides the content of the original data. In this method the content alone kept secret but it fails to hide the existence of secret data. While using this crypt method the malicious people can easily identify the existence of secret image. So we are in need of transferring the secret data which should not be hacked by the third party. For avoiding this kind of problem we propose Predictive coding technique based on Steganography Scheme. Steganography is the process of hiding the existence of secret message. Secret message is embedded into the host image and the cover image is transfer to the beneficiary. In our work we propose Triple DES Algorithm for converting the structured data into unstructured data. Triple DES is widely used technique for converting huge amount of document. By using this Triple DES the abuser can convert large document into unreadable form. This unreadable document is hided into the original cover image or host image using Predictive Coding Method. The proposed work embeds the secret data into a particular block which is chosen by abuser so it is difficult to identify where the secret data is located. While this predictive coding is combined with Cryptography using Triple DES it gives stronger security for the hidden information.

Keywords: Cryptography, Data Encryption Standards, Data Hiding, Irreversible, Median Edge Detective Predictor (MED), Predictive Coding, Reversible Image, Steganography, Triple DES.

I. INTRODUCTION

The word Cryptography comes from the Greek cryptology, which means hides the contents of a secret message. In cryptography the content of the message alone is kept secret. The structure of a message is scrambled to make it meaningless. Data hiding conceals the existence of secret messages while cryptography protects the content of message. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. Since World War - I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. The original message is said to be as Plain Text and the encrypted or converted secret message is called as Cipher Text.

The abuser will transfer the Cipher Text to the beneficiary which should not be guessed or hacked by the third party. The beneficiary will receive the Cipher Text. After receiving the Cipher Text the end user will transform the Cipher Text into Plain Text to obtain the original message. In our work we use Triple DES algorithm for converting the original documents into unreadable form. Triple is the process of combining three Data Encryption Standards together. Triple DES is the best method which is often widely used in Cryptography. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. But in some cases, the system is broken when the attacker can read the secret message [1]. To avoid this kind of problem we propose both Cryptography and Steganography together.

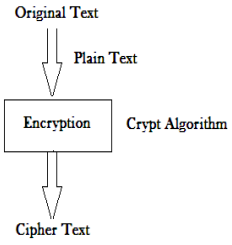

Figure 1 Encryption Process in Cryptography

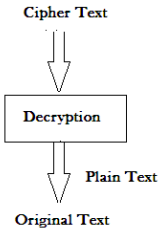

Figure 2 Decryption Process in Cryptography

The word Steganography comes from the Greek Steganos, which mean covered or secret and graphy mean writing or drawing i.e., the art of hiding information in ways that prevent detection[2],[3]. In Steganography the secret message or file is hidden into another image. The image used to hide data is called as cover image or host image [4]. After embedding the secret message into the cover image that image is transferred to another. This embedded image is called as stego-image [1].

i.e., Stego-Image = Cover Image + Secret Message -- (1)

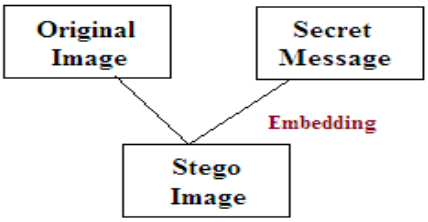

Figure 3 Embedding in Steganography

Steganography scheme consist of Embedding procedure and Extracting procedure. In embedding procedure secret message is embedded into original image for security purpose [2]. Original image is otherwise called as cover image or host image [5] [6]. This procedure varies depending upon the type of algorithm used. Extracting procedure is the reverse process of Embedding. It expands the embedded secret data from the cover image. We can separate the cover image and secret message from the stego image is called as Extraction Procedure [3].

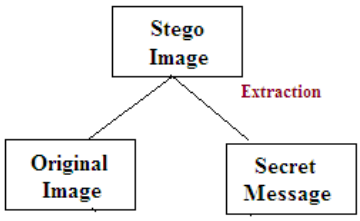

Figure 4 Extraction Process in Steganography

Steganography is classified as two categories called Reversible data hiding and Irreversible Data hiding. If there is any loss in the host image, while extracting the secret data from the cover image then that type of Steganography is called as Irreversible data hiding [7]. If there is no loss in the host image, while extracting the secret data from the host image then that process is called as Reversible Data Hiding. In our work we develop the Steganography based on Reversible data hiding. For achieving Reversible Steganography we introduce Predictive Coding Method.

Predictive coding method is used for hiding the secret data into the host image. Median Edge Detective Predictor is used in Predictive coding method. This MED predictor hides the data in an effective manner. This is the method for embedding secret data into the cover image while compared to other Steganography method.

II. TRIPLE DES

In cryptography, Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm. Triple DES uses a "key bundle" which comprises three DES keys, K1, K2 and K3, each of 56 bits (excluding parity bits).

Triple DES is simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Private Encryptor, you simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually. The Triple DES DLL then breaks the user provided key into three sub keys, padding the keys if necessary so they are each 64 bits long. The procedure for encryption is exactly the same as regular DES, but it is repeated three times. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key.

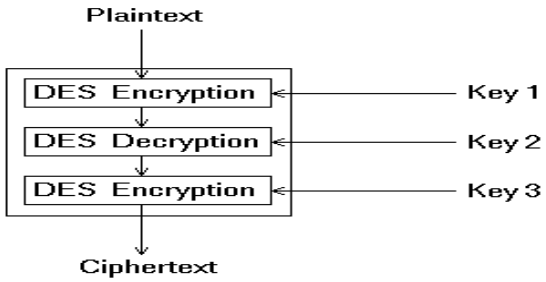

Figure 5 Triple DES Representations

Consequently, Triple DES runs three times slower than standard DES, but is much more secure if used properly. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Unfortunately, there are some weak keys that one should be aware of: if all three keys, the first and second keys, or the second and third keys are the same, then the encryption procedure is essentially the same as standard DES. This situation is to be avoided because it is the same as using a really slow version of regular DES.

Encryption and Decryption:

The Encryption algorithm is: defined as

Ciphertext=EK3(DK2(EK1(plaintext))) -- (2)

That is DES Encrypt with K1, DES decrypt with K2, then DES encrypt with K3. The Decryption is the reverse process of the Encryption

Plaintext=DK1(EK2(DK3(ciphertext))) -- (3)

That is decrypt with K3, encrypt with K2, and then decrypt with K1. Each triple encryption encrypts one block of 64 bits of data.

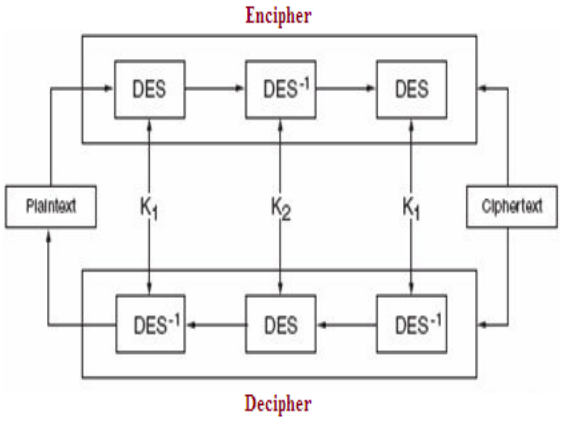

Figure 6 Working of Triple DES

III. PREDICTIVE CODING

In this work, we will introduce the Median Edge Detector (MED) predictor. The MED predictor is commonly used for lossless and near-lossless image compression techniques.

Embedding Procedure:

The MED predictor is used for the Low Complexity Lossless Compression for Image (LOCO-I) scheme. LOCO-I is the core algorithm for the lossless and near-lossless image compression of ISO/ITU standard. The MED predictor is used in the predictive coding stage. For each image pixel, the predictive values are generated by a MED predictor, which is called the predictive image. By finding the difference between the original image and the predictive image, the error values are generated, and then coded in the entropy coding stage. The predictive template shown in fig 1 uses neighboring pixels to generate the predictive value. *X* is the current pixel designated to be predictive, and *a*, *b* and *c* are neighboring pixels of *x*. The MED predictor uses past data, *a*, *b* and *c*, in order to detect vertical or horizontal edges in the predictive template. When a vertical edge appears on the left side of *x*, the MED predictor will use *b* as the predictive value. When a horizontal edge is on the upper side of x, the MED predictor will use *a* as the predictive value. If no edge appears in the predictive template, the MED predictor will use a + b - c for the predictive value.

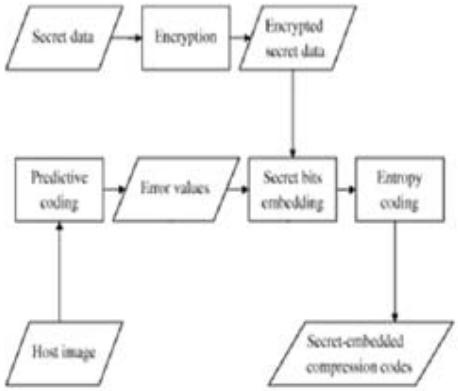

Figure 7 Embedding Procedure

c	***B***
a	***X***

Figure 8 Host Image Template

If *x′* is the predictive value of *x*, the predictive rule can be represented as

C	***b***
A	***x'***

Figure 9 Predictive Image Template

Predictive images are calculated by using the below formula for N X N pixels in the selected block.

Where max (*a*, *b*) and min (*a*, *b*) are the functions that find the maximum and minimum values of *a* and *b*, respectively. In the recovery stage, the predictive image also can be generated by the same MED predictor with the error values of entropy decoding. The original image can be recovered by adding the predictive image and error values [8].

An image-hiding scheme via predictive coding that is based on the concept of lossless and near-lossless image compression. They embed the secret data by modification of error values during the predictive coding stage. In their scheme, each error value can embed three secret bits at most [9].

164	159	155	149
209	127	119	118
166	169	170	175
207	205	200	198

0	164	159	155
164	204	127	119
209	127	161	169
156	207	205	200

Figure 10 Example of *HI* and *PI*

164	-5	-4	-6
45	-77	-8	-1
-43	42	9	6
41	-2	-5	-2

Figure 11 Example of *EV*

164	5	4	6
45	77	8	1
43	42	9	6
41	2	5	2

Figure12 Example of *AEV*

Let *HI* be gray-scale host image with NXN pixels represented as,

$HI = \{h_{ij} \mid 0 \le i < N, 0 \le j < N, h_{ij} \in \{0,1,\ldots.225\}$ -- (4)

Let *PI* be the predictive image with NXN pixels represented as,

$PI = \{p_{ij} \mid 0 \le i < N, 0 \le j < N, p_{ij} \in \{0,1,\ldots.225\}$ -- (5)

The encrypted secret data is embedding into the error value. Error values are the differences between HI and PI.

Let *EV* be the Error value set for N X N error value represented as,

$EV = \{e_{ij} \mid 0 \le i < N, 0 \le j < N, e_{ij} \in \{-255,-254,\ldots.225\}$ -- (6)

Where, eij – error value

$eij = hij - pij$ -- (7)

The range of each e_{ij} is [−255, 255]. AEV be the Absolute Error Value,

$AEV = \{a_{ij} \mid 0 \le i < N, 0 \le j < N, a_{ij} \in \{0, 1,..,225\}$ -- (8)

Where,

$a_{ij} = \mid a_{ij} \mid$ -- (9)

There are two basic ways to manipulate GIS videos images for hiding data. The first class of approaches changes low-level features such as flipping a black pixel to white or vice versa [10]. The second class of approaches changes high-level features such as modifying the thickness of strokes, curvature, spacing, and relative positions. Since the number of parameters that can be changed by the second class of approaches is limited, especially under the requirements of invisibility and blind detection (i.e., without using the original image in detection), the amount of data that can be hidden is usually limited except for special types of images [11].

Embedding of Secret Message:

Directly encoding the hidden information in flippable pixels (e.g., set to black if to embed a "0" and to white if to embed a "1") may not allow the extraction of embedded data without the original image. The reason is that the embedding process may change a flippable pixel in the original image to a pixel that may no longer be black pixels that are immediately adjacent to white pixels are considered as "flippable" [12].

One such flippable pixel, marked by thick boundary in Figure1, is changed to white to carry a "1", as shown in Fig.1. It can be seen that after embedding, this pixel is no longer considered flippable if applying the same rule. This simple example shows the difficulty for the detector to correctly identify which pixel carries hidden information without using the original image.

Extraction Procedure:

The hidden data in the Image or Video or Audio is extracted by referring the Absolute Error Value (AEV).

During the predictive decoding the hidden data's are extracted and MED Predictor is applied to regenerate the original information. While extracting the hidden data there is no loss in the original information by using the Reversible Image steganography [8].

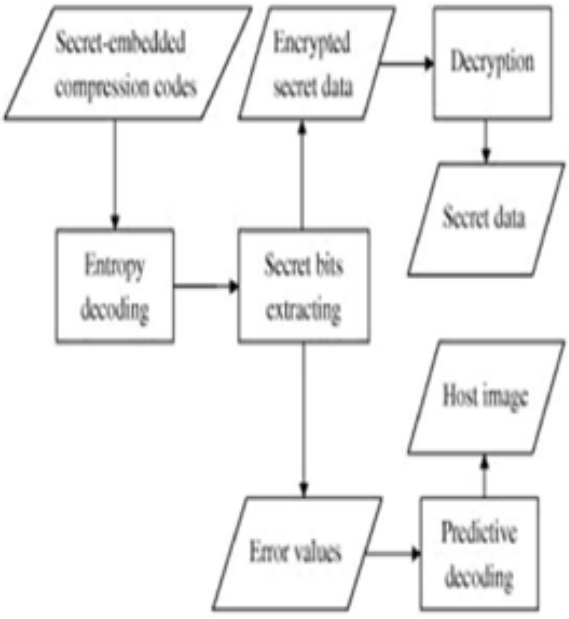

Figure 13 Extraction Procedure

IV. EXPERIMENTAL RESULTS AND DISCUSSION

In our work, we choose a Text file with huge amount of document. This document consists of data with readable structure. This readable form of data is converted into indecipherable (unreadable) structure which cannot be understand or hacked by the malicious person. This indecipherable structure of data is embedded or hided into the cover image. The generated stego-image is transferred to the beneficiary. Stego image consist of cover image and hidden data. Stego- image is compressed using lossless compression.

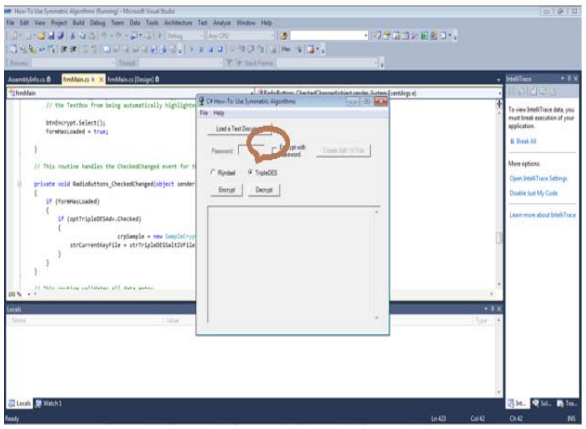

Figure: 14 Cryptography using Triple DES

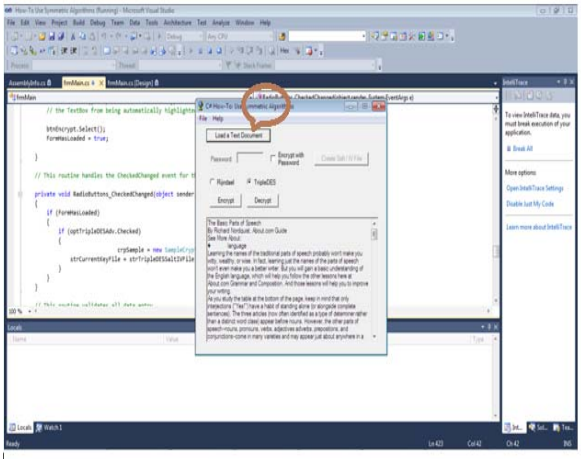

Figure: 15 Original text document before converting

Figure: 16 Converting the text document into unreadable form using Triple DES

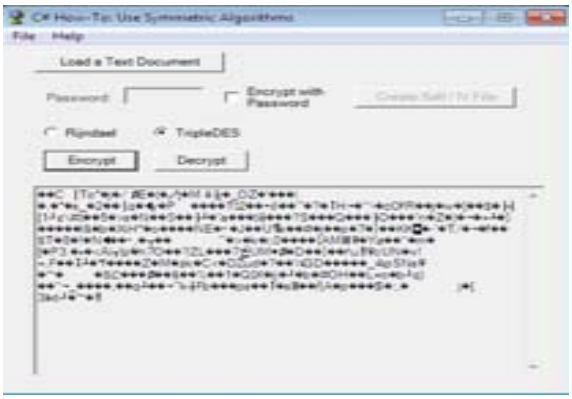

Figure: 17 After converting using Triple DES

Figure: 18 Unstructured document for embedding into host image

After applying Triple DES Algorithm based on Cryptography to the file import the crypt file into the stego document. This document is hidden into the image to transfer data in a secure manner to the beneficiary.

Figure: 19 Master file to transfer Crypt document

Figure: 20 Master file information

This Master file consists of original image uploaded with secret data, even if we extract this secret data the third party cannot hack the content of the secret data. After transferring the stego-image the beneficiary extract the cover image and secret data from the stego-image.

The principle of Reversible image data hiding is achieved. That is while extracting the secret data there should not be any loss in the cover image.

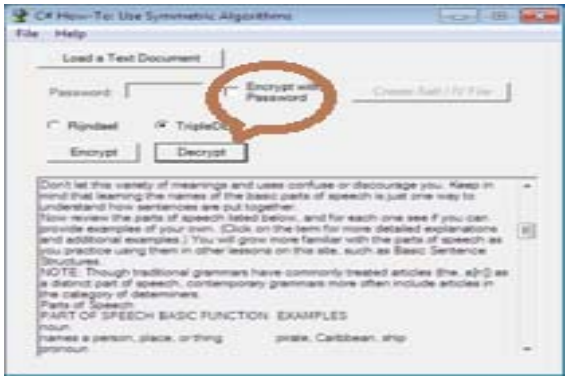

Figure: 21 After extracting the secret document from stego image

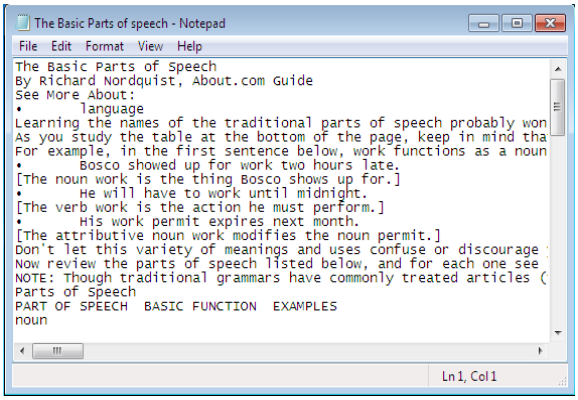

Figure: 22 Extracted original document

V. CONCLUSION

In our proposed work we combine both Triple DES Algorithm and Predictive coding Method. Cryptography is used to convert original plain text into cipher text. That is original text is converted into unreadable form. The content of message is kept secret. Steganography is used to hide the secret data into an image. The existence of message is hidden secret. We propose a scheme to combine the advantages of both Cryptography and Steganography. i.e., hiding the existence of message from Steganography and the hiding the content of message from Cryptography is combined together to form the effective Security System. Conversion of structured data into unstructured data using Triple DES is achieved successfully. This Triple DES Algorithm in Cryptography is widely used technique for converting huge amount of document. By using this Triple DES the abuser can convert large document into unreadable form. This unreadable document is hided into the original cover image using Predictive Coding Method. By combing this predictive coding and Triple DES Algorithm gives stronger security for hiding the information.

VI. REFERENCES

[1] Bruce Schneier, "Applied Cryptography," Second Edition, published by Wiley, New York, 1996. ISBN 0-471-11709-9

[2] N. Provos, P. Honeyman, "Hide and seek: an introduction to steganography", IEEE Security and Privacy Magazine 1 (2003) 32–44.

[3] Ki-Hyun Jung, Kee-Young Yoo, "Data Hiding method using Image Interpolation", Republic of Korea**,** in Journal of Computer Standards & Interfaces, Volume 31 Issue 2, February, 2009..

[4] Armin Bahramshahry, Heasm Ghasemi, "Design of Data Hiding Application using Steganograhy", April 2007.

[5] A.M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform", IEEE Transactions on Image Processing 13 (2004) 1147–1156.

[6] J. Mielikainen, "LSB matching revisited", IEEE Signal Processing Letters 13 (2006) 285–287.

[7] M.U. Celik, G. Sharma, A.M. Tekalp, E. Saber, "Reversible data hiding", Proceedings of the IEEE International Conference on Image Processing (2002) 157–160.

[8] Y.H. Yu, C.C. Chang, Y.C. Hu, "Hiding secret data in images via predictive coding", Pattern Recognition 38 (2005) 691–705.

[9] R.Z. Wang, C.F. Lin, J.C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm", Pattern Recognition 34 (2001) 671–683.

[10] C.C. Thien, J.C. Lin, A simple and high-hiding capacity method for hiding digit by- digit data in images based on modulus function, Pattern Recognition 36 (2003) 2875–2881.

[11] S. Ananthi, A.Anjanadevi," Reversible Image Data Hiding Using Predictive Coding Technique Based on Steganograpic Scheme", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 1, July 2012. ISSN: 2277-3754.

[12] S. Ananthi, A.Anjanadevi," Reversible Image Data Hiding Using Predictive Coding Technique Based on Steganograpic Scheme", IOSR Journal of Engineering (IOSRJEN) ISSN: 2250-3021 Volume 2, Issue 7(July 2012), PP 27-33

Short Bio Data for the Author

S. Ananthi received her B.E Degree in Computer Science from Dhanalakshmi Srinivasan Engineering College, Perambalur and M.E Degree in Computer Science from Annamalai University, Chidambaram. She is working as an Assistant Professor in M.A.M College of Engineering, Siruganur, Trichy. She had presented a paper about Steganography in National Conference on Multimedia Signal Processing, NCMSP' 2011 in Annamalai University on 2011. Her Paper got Selected in the National Conference on Information Security (NCIS-2012) held at SASTRA University, Thanjavur, during June 14-15, 2012. She participated in the National Conference on Confluence of Multidisciplinary in Engineering Fields NCCME'12. She had published a paper in International Journal of Engineering and Innovative Technology (IJEIT). She had published a paper in International Organization of Scientific Research (IOSR) International Journal on the topic of Steganography. Her research interests include cryptography and Steganography.

Dr. P. Dhanalakshmi received her Bachelor's degree in Computer Science and Engineering from Government College of Technology, Coimbatore in the year 1993. She received her M.Tech degree in Computer Applications from the reputed Indian Institute of Technology, New Delhi under the Quality Improvement Programme in the year 2003. She completed her Ph. D in Computer Science and Engineering from Annamalai University in the year 2011. She joined the services of Annamalai University in the year 1998 as a faculty member and is presently serving as Associate Professor in the Department of Computer Science & Engg. She has published 11 papers in international conferences and journals. She is guiding several students who are pursuing doctoral research. Her research interests include speech processing, image and video processing, pattern classification and neural networks.