A NOVEL TECHNIQUE FOR SECURE, LOSSLESS STEGANOGRAPHY WITH UNLIMITED PAYLOAD AND WITHOUT EXCHANGE OF STEGOIMAGE

Rahna E[1] and V K Govindan[2]
Department of Computer Science and Engineering, NIT Calicut, Calicut, India

ABSTRACT

Steganography is the technique of sending messages hidden in images for secured communication. The major components of a steganographic framework are secret message, cover image, stegoimage. At present, most of the steganographic methods are based on substitutions. All these approaches for hiding messages are lossy since the image will be modified without causing much visually detectable change. The other major issues yet to be addressed satisfactorily are the degree of security of the communication, key size and the payload capacity. Hence, this paper proposes a novel technique which attempts to solve all the above issues in steganography. In the proposed method, instead of substitutions we are using the notion of matches between secret data and cover image. And we also use the concept of fixed frequency for each character in English. The proposed method is lossless, has infinite payload capacity, has key size which is only about 10 to 20 percentage of the message size and has improved security.

KEYWORDS: *Lossless Steganography, Secure Steganography, Unlimited Payload, Less Overhead*

I. INTRODUCTION

The difficulties in ensuring individual's privacy become progressively challenging with advancements in digital technologies of communication and the growth of computer power and storage. Different persons will appreciate different degrees of privacy. To protect personal privacy, various methods have been investigated and developed. Encryption is probably the most obvious one, and next comes steganography. Encryption is adaptable to noise and is generally observed whereas steganography is not.

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity [1]. The word "Steganography" is of Greek origin and means "concealed writing". The main aim of steganography is to hide the existence of the message in the cover medium.

Cryptography and steganography are cousins in the spy craft family [2]. Cryptography scrambles a message with the help of certain cryptographic algorithms for converting the secret data into unintelligible form. On the other hand, steganography hides the message in cover image so that it becomes invisible. Sending a message in the form of cipher text might arouse suspicion on the part of the recipient whereas an "invisible" message created with steganographic algorithms will not. Anyone who needs to perform secret communication can use cryptographic algorithms to scramble the data before performing steganography to achieve additional security. The purpose of steganography is defeated once the presence of secret data is revealed or even suspected, even if the message is not extracted or deciphered.

For a steganography algorithm, a cover image is given or chosen, and the embedding process generates a stego-image using stego-key. The extraction method takes the stego image and applies the inverse algorithm using the shared key to extract the hidden message [3].

1.1. Challenges

The major challenges of steganography are [4]:

1. Security of Hidden Communication: The hidden contents must be invisible both perceptually and statistically so as to avoid the suspicions of eavesdroppers.
2. Size of Payload: Steganography requires sufficient embedding capacity.

Requirements for higher payload and secure communication are often contradictory. Depending on the specific application scenarios, a tradeoff has to be sought.

1.2. Applications

Steganography can be used when we need to hide data [5]. The main reason for hiding data is to prevent unauthorized persons from being aware of the existence of a message. Steganography can be used to hide secrets of a company or plans of a new invention. With the help of steganography, we can send out trade secrets without anyone at the company being aware and hence prevents corporate espionage. Steganography can also be used in the non-commercial sector for number of purposes such as secret data hiding and copyright protection.

The rest of the paper is organized as follows: Section II presents a brief review of some of the papers in the literature of steganography. Section III deals with the frequency of letters and the Huffman codes required to compress the key. Section IV presents the proposed approach of hiding messages using a cover image without causing any loss of data. Section V deals with the experimental results and analysis, and Section VI presents the future work that can be taken up to further reduce the key size and enhance the utility of the technique. Finally, the paper is concluded in Section VII highlighting the major features of the approach.

II. LITERATURE SURVEY

Steganography is an active field of research; many attempts are already been done. Most of them are based on LSB based lossy techniques. This section briefly reviews some of the major work in this topic of research.

2.1. Spatial Domain Method

Basic spatial domain systems try to encode secret information by substituting insignificant parts of the cover by secret message bits. The receiver can extract the information if he has knowledge of the positions where secret information has been embedded. Since only minor modifications are made in the embedding process, the sender assumes that they will not be noticed by an attacker [6]. Brief description of various papers on this method is given below:

Ashok et al. [7] proposed a steganographic technique based on matrix matching. In this method, they wrote their message as an information matrix of 8 columns. Then they selected 8 pixels using pseudo random number generator for insertion of one row of information matrix. From the 8 selected pixels they made selected pixel image matrix of size 8X8. The row of information matrix is inserted in that column of selected pixel image matrix which has the minimum effective change. The experimental results show that it provides better PSNR values than some previous existing methods. Also, the NCC values come closer to 1, which shows that stego images are visually indistinguishable from their corresponding cover images.

Patel and Dave [8], Swati and Mahajan [9], Hassan Mathkour et al. [10] and Masud Karim et al. [11] proposed variations of LSB substitutions. In the first paper, both the parties will have to agree upon a set of carrier images and certain required parameters. Then the sender will select an image, from the set of carrier images which requires least number of bit manipulations on LSB substitution of secret data, and produce stegoimage. Whereas in second paper, the secret data is first encrypted using recipient's RSA public key. Then each bit of the encrypted message is inserted to the LSBs of image in different images so as to find the best cover image. Best cover image is the one which requires minimum number of LSB changes. In the third paper, the idea was to divide the image into many segments and apply a different processing on each segment. Whereas in the fourth one, data is encrypted using a key and is replaced with the LSB of RGB color image. And the length of the hidden message is stored in the 1st row of stego image.

Johri and Asthana [12] proposed a steganography technique in which data is embedded using alteration component technique. In this, key and secret message will replace each pixel. Then for the security of stegoimage palette based image technique is applied by stretching process. The receiver having the same secret key applies destretching palette process on stegoimage using alteration component extraction process to extract the data.

Ching-Yu Yang [13] proposed a steganography method based on the module substitutions. The secret bits to be embedded in the block are first determined by the base-value (BV) of the block in R-, G-, and B-component of a RGB trichromatic system. Then, the data bits are embedded in each component respectively by Mod u, Mod u-v, and Mod u-v-w module substitutions.

Piyush and Paresh [14] presented a technique that combines the features of cryptography, steganography along with multimedia data hiding. In order to provide higher security levels the algorithm uses a reference database. In this method, they first encrypted the message using DES. And then the cipher is saved in the image using a modified bit encoding technique. For each byte of data one cover pixel will be edited.

Mohammad and Adnan proposed [15] an algorithm which uses actual color value of a pixel to determine the number of bits stored in each channel (R, G or B) of that pixel. In this, one of the channels is selected randomly as indicator. Data will be stored in the least significant bits of the channel, having lowest color value among the two channels other than the indicator.

2.2. Transform Domain Method

It has been noted early in the development of steganographic systems that embedding information in frequency domain of a signal can be much more robust than embedding rules operating in the time domain. Most robust steganographic systems known today actually operate in some sort of transform domain. Transform domain methods hide messages in significant areas of the cover image which makes them more robust to attacks, such as compression, cropping, and some image processing, than the LSB approach [6].

Jisha and Geevarghese [16] had proposed a method of steganography which hides data in video using pixel level motion estimation. In this method, they produced a motion histogram and the histogram data is used as the cover sequence for hiding. The proposed method is found to be less complex and maintains the steganographic distortion within the desired level.

Neda and Amir [17] proposed a steganographic approach based on Integer Wavelet Transform and Assignment algorithm. In this method, IWT is used to transform both cover and secret images from spatial domain to frequency domain, and assignment algorithm is used for best matching between blocks for embedding. They embedded the secret image in different coefficients of cover image bands such as horizontal detail, vertical detail and diagonal detail and observed the effect of embedding on the performance of stego image in terms of Peak Signal to Noise Ratio (PSNR). Their experimental results showed that stego image and extracted secret image have high visual quality and they are perceptually similar to their original versions. And this method is also has high robustness.

Velagalapalli et al. [18] proposed a technique known as SteganPEG to hide data in jpeg images. They perform JPEG compression on the data to be hidden. This method uses a new cryptography technique known as ‘Rotatocrypt’ to encrypt or decrypts data using rotations. A list called ‘PassStore’ is created from the password used. Then encryption is done by right rotating the bits as guided by the value in PassStore.

Debnath Bhattacharyya et al. [19] presented a discrete Fourier transformation based Image authentication technique. In this technique they selected 2 x 2 windows for better result of authentication. For achieving more security, insertion and extraction is done in frequency domain rather than on spatial domain. In this they first took 2X2 window of cover image in sliding window manner and applied DFT. Then they replaced the LSB of DFT component by the data bit and applied Inverse DFT.

LIU Tong and QIU Zheng-ding [20] and Vladimir Banoci et al. [21] proposed a DWT based color image steganography method. In the former method the secret information is hidden into a publicly accessed color image by a quantization-based strategy. Whereas, the latter case method processes grey scale images as cover object for creating subliminal channel and it utilizes transform coefficients of 2-Dimensional Discrete transform for embedding process.

2.3. Combination of Spatial Domain and Transform Domain Method

Work by Raja et al. [22] is based on a technique that combines Least Significant Bit (LSB), Discrete Cosine Transform (DCT), and compression techniques on raw images to enhance the security of the payload. Initially, the LSB algorithm is used to embed the payload bits into the cover image to derive the stegoimage. The stego-image is transformed from spatial domain to the frequency domain using DCT. Finally quantization and run length coding algorithms are used for compressing the stego-image to enhance its security.

2.4. Spread Spectrum Method

Lisa M. Marvel et al. [23] presented an embedding method, called Spread Spectrum Image Steganography (SSIS). In this method, the data to be hidden is first encoded and a spreading sequence is generated using a wideband pseudorandom noise generator. Then the modulation scheme is used to spread the narrowband spectrum of encoded image with the spreading sequence, thereby composing the embedded signal, which is then input into an interleaver and spatial spreader. The output signal is then combined with the cover image to get the stegoimage.

2.5. Steganography in MMS

Mohammad [24] proposed a technique for steganography in MMS. In this, he hides the data in two media, text and image, so this is more resistant. The approach he followed is that, first the data is broken into two parts. Each part size is proportionate to the capacity of the text and the image for hiding data. Then he hides the first bit in the text and the next 5 in the image. Then he hides the 7th bit in the text and next 5 bits in the image again. He does this loop until reach the end of data. In this method, the order of hidden data is not continuous; therefore the possibility of breaking this method is low.

2.6. Other Techniques

Yu-Chen Shu, Wen-Liang Hwang and Dean Chou [25] proposed a new paradigm in which the receiver does not necessarily require stego-text to retrieve the message content. Under the proposed approach, the sender can produce keys without modifying the cover-image, and the intended recipient can use the keys and an image that resembles like the cover-image to recover the message. They had proposed a subspace approach to implement the paradigm. In this method, the message is not embedded in the cover-text and the recipient can produce his/her own images to extract messages.

Hassan Mathkour et al. [26] proposed a technique which emphasizes undetectability. It allows for the change of intensity of image planes of (24 bit) colored image to embed secret message in a specific distance between them. It is based on changing the distance of two random selected pixel channels in a specific range that represent hidden data.

Han-ling Zhang et al. [27] presented an approach which is based on pixel value differencing. It makes use of the largest difference value between the three pixels nearer to the target pixel to calculate how many secret bits will be embedded into the pixel. In order to enhance the image quality of the stego-image, they applied optimal pixel adjustment process (OPAP).

Subba Rao et al. [28] presented an image steganography technique that randomizes the sequence of cipher bits. They computed the suitability measure of the various random sequences of the cipher bits against a given image and select the random sequence closest to the image. Then they generated those random sequences by the use of an L.F.S.R. They then embed these random sequences of cipher bits in the image.

The survey carried out reveals that the main issues yet to be further addressed in the field of steganography are payload limitation, quality of stegoimage and the concern of security. We need to develop steganography techniques where we can embed data equal or more than the size of cover image and without any distortion in stego image so that the security of the message is enhanced. In this paper, we propose a method that overcomes the issues associated with the method proposed by Rahna E and V K Govindan [29].

III. BACKGROUND REQUIRED

3.1. Frequency of Letters

Michael and Mewhort [30] have calculated the single-unit frequency counts for lower case and upper case alphabets and 32 non alphabetic characters including the 10 digits (ASCII 32–64) from NYT

Corpus. It has demonstrated that upper- and lowercase letters do not have equivalent relative frequencies in print. And the results shows that the frequency is highest for space (ASCII 32) and lowest for non alphabetic characters like ~ (ASCII 126) and ^ (ASCII 94).

3.2. Huffman Coding

The Huffman encoding algorithm starts by constructing a list of all the alphabet symbols in descending order of their probabilities [31]. It then constructs, from the bottom up, a binary tree with a symbol at every leaf. This is done in steps, where at each step two symbols with the smallest probabilities are selected, added to the top of the partial tree, deleted from the list, and replaced with an auxiliary symbol representing the two original symbols. When the list is reduced to just one auxiliary symbol (representing the entire alphabet), the tree is complete. The tree is then traversed to determine the codewords of the symbols.

IV. PROPOSED METHOD

In case of LSB or any other bit substitutions, we have to modify the cover image. Though the change is invisible to human vision system it might be visible to some other visions. So we can go for a system which will not even change a bit of the cover image.

The proposed algorithm makes an array of locations of each possible character in an English message in the image. Then for each character in the secret message we will search the array; the array index of the exact character is sent to the receiver. Receiver will then reverse the process so as to get the secret data. The three procedures required for this purpose, the *preprocessing step*, *embedding* and the *extraction* of messages are given below:

4.1. Preprocessing Step

Select around 10-20 color images which on equalization will serve the purpose of hiding data eminently. And these set of images are send to the receiver once both parties agree upon this algorithm.

4.2. Embedding Procedure

- *Input:* Cover image, Secret message
- *Output*: Key
    a) Scan the image and find the locations of different characters of the message alphabet in the image. Form and array of such locations, say *ArrayLoc.*
    b) Considering the frequencies as per [30] perform Huffman encoding of the index of *ArrayLoc*.
    c) For each element of secret message
        - Get the index of *ArrayLoc* where the location of that element is stored.
        - Concatenate the huff code of that index to a string Temp.
    d) Attach the *image Id* to the beginning of the string *Temp.*
    e) Compress the *Temp* to obtain the compressed *Key* and send it to the receiver.

4.3. Extraction Procedure

- *Input:* Key, Cover image
- *Output:* Secret message
    a) Take the *Key* and uncompress it to get the *Temp*.
    b) Extract *Temp* to get the image Id.
    c) Take the specified image and scan it to find the locations of different characters of the message alphabet in the image. Form an array of such locations, say *ArrayLoc*.
    d) Considering the character frequencies as per [30] perform Huffman decoding of *Temp.*
    e) For each element in Temp, that is, Index:
        - *Location= ArrayLoc[Index]*; // get the location of message char in the image
        - *Message = Message + Image [Location]. // assemble the message from each char.*

V. Experimental Results and Analysis

The system was implemented in MATLAB R2012a version 7.14.0.739. We have used many Matlab functionalities to get the things done. By using the proposed algorithm we have embedded secret data into image 'Picture.bmp'. When we tried to embed a message of size 196 characters in an image of size 1024 X 1024 we got a key of size 21 characters which is only about 10 percentage of the message. Hence the amount of data that we need to send to receiver is reduced to a great extend. Table 1 gives the number of bits required for hiding messages of different sizes. It is seen that the number of bits required depends on both size of the message and the frequency of letters in message. It is seen that size of key is very less in array method with Huffman coding. The storage required for key is only around 10 to 12 percentage of the secret message size. Hence we are achieving a reduction of 80 to 90 percentage in data that we need to send to receiver.

Figure 1. Picture.bmp

Table 1. Storage requirements for message and key (in bits).

Message size in characters	Storage Required for Message(in bits)	Storage Required for Key using Simple matching method (in bits)	Storage Required for Key using Array method with Huffcoding (in Bits)
196	3136	1680	336
1386	22176	10280	2241
4897	78352	36200	8029

From the above table, we can see that the size of key depends on the frequency of each character in a message and it is mainly proportional to the size of the message. Most of the existing steganographic method's performance is analyzed on the basis of histogram similarity and Peak Signal to Noise Ratio (PSNR) between cover image and the stegoimage. Here, since we are not sending the stegoimage the cover image itself is considered as the stegoimage. Therefore, the histograms will be identical and the PSNR value will be infinite, and hence such an analysis not required in this case.

VI. Future Work

A major drawback of the approach is that the key size, though it is about 12 percent of the message size, is proportional to the message size. The acceptability of the approach can be further improved if a technique is devised to achieve fixed key size independent of message or to reduce the key size further. So, future work on this topic can address this important issue of bringing down the key size.

VII. Conclusion

The ultimate aim of steganography is to hide the very existence of message in the cover medium. There are a number of methods suggested by various researchers attempting to achieve this goal of hiding the messages securely in the cover images. Most of the approaches in the literature surveyed are based on

LSB manipulation and their variant. The major issues still unresolved are the payload limitation, quality of stegoimage and the lack of security. In this paper, we have proposed a method that looks for exact matches between message and the cover image data. The main advantage of the proposed approach is that the stegoimage will be the cover image itself. Hence, the stegoimage need not be send to the receiver along with every message; it needs to be sent only once for all subsequent messages. And also, the payload capacity is higher than the cover image, no limit; it can be infinitely large. This technique is a highly secure lossless robust steganography technique unlike the other lossy LSB techniques in the literature. The result we have obtained shows that the amount of data we need to send to receiver is only around 10 to 15 percentage of the secret data.

ACKNOWLEDGEMENTS

We express our gratitude to God almighty for his incessant blessings on us during this project. Our family and friends have been very supportive. We are thankful for all that we have learnt from them.

REFERENCES

[1]. "Steganography." *Wikipedia*. Wikimedia Foundation, 20 Nov. 2012. <http://en.wikipedia.org/wiki/Steganography>.

[2]. N. F. Johnson, and S. Jajodia, “Steganography: Seeing the Unseen,” IEEE Computer, Feb. 1998, pp. 26-34.

[3]. Al-Mohammad A., “Steganography-based secret and reliable communications improving steganographic capacity and imperceptibility,” School of Information Systems, Computing and Mathematics, 2010.

[4]. P. Goel., “Data Hiding in Digital Images: A Steganographic Paradigm,” PhD thesis, Indian Institute of Technology, Kharagpur, 2008.

[5]. Riasat R., Bajwa I.S., Ali M.Z., “A hash-based approach for colour image steganography,” IEEE International Conference on Computer Networks and Information Technology, 2011, pp. 303-307.

[6]. Z. K. AL-Ani, A. Zaidan, B. Zaidan, H. Alanazi, et al., “Overview: Main fundamentals for steganography," arXiv preprint arXiv:1003.4086, 2010.

[7]. J. KAUR, M. DUHAN, A. KUMAR, and R. K. YADAV, “Matrix matching method for secret communication using image steganography,"

[8]. H. J. Patel and P. K. Dave, “Least signi_cant bits based steganography technique," IJECCE, vol. 3, no. 1, pp. 97-103, 2012.

[9]. S. Tiwari, R. Mahajan, and N. Shrivastava, “Steganography-an approach for data hiding based on encryption and lsb insertion,".

[10]. H. Mathkour, G. M. Assassa, A. Al Muharib, and I. Kiady, “A novel approach for hiding messages in images," in Signal Acquisition and Processing, 2009. ICSAP 2009. International Conference on, pp. 89-93, IEEE, 2009.

[11]. S. Masud Karim, M. Rahman, and M. Hossain, “A new approach for lsb based image steganography using secret key," in 14th International Conference on Computer and Information Technology (ICCIT), 2011, pp. 286-291, IEEE 2011.

[12]. A. Asthana and S. Johri, “An adaptive steganography technique for gray and colored images," International Journal, vol. 2, no. 5, 2012.

[13]. C.-Y. Yang, “Color image steganography based on module substitutions," in Intelligent Information Hiding and Multimedia Signal Processing, 2007. IIHMSP 2007. Third International Conference on, vol. 2, pp. 118-121, IEEE, 2007.

[14]. P. Marwaha, “Visual cryptographic steganography in images," in Computing Communication and Networking Technologies (ICCCNT), 2010 International Conference on, pp. 1-6, IEEE, 2010.

[15]. M. Parvez and A. Gutub, “Rgb intensity based variable-bits image steganography," in Asia-Paci_c Services Computing Conference, 2008. APSCC'08. IEEE, pp. 1322-1327, IEEE, 2008.

[16]. J. A. Jose and G. Titus, \Data hiding using motion histogram," in Computer Communication and Informatics (ICCCI), 2013 International Conference on, pp. 1-4, IEEE, 2013.

[17]. N. Raftari and A. M. E. Moghadam, “Digital image steganography based on integer wavelet transform and assignment algorithm," in Modelling Symposium (AMS), 2012 Sixth Asia, pp. 87-92, IEEE, 2012.

[18]. V. Reddy, A. Subramanyam, and P. Reddy, “Steganpeg steganography+ jpeg," in International Conference on Ubiquitous Computing and Multimedia Applications, 2011, pp. 42-48, IEEE, 2011.

[19]. D. Bhattacharyya, J. Dutta, P. Das, R. Bandyopadhyay, S. Bandyopadhyay, and T.-h. Kim, “Discrete fourier transformation based image authentication technique," in Cognitive Informatics, 2009. ICCI'09. 8th IEEE International Conference on, pp. 196-200, IEEE, 2009.

[20]. T. Liu and Z. Qiu, “A dwt-based color image steganography scheme," in 6th International Conference on Signal Processing, 2002, vol. 2, pp. 1568-1571, IEEE, 2002.

[21]. V. Banoci, G. Bugar, and D. Levicky, “A novel method of image steganography in dwt domain," in Radioelektronika (RADIOELEKTRONIKA), 2011 21st International Conference, pp. 1-4, IEEE, 2011.

[22]. K. Raja, C. Chowdary, K. Venugopal, and L. Patnaik, “A secure image steganography using lsb, dct and compression techniques on raw images," in Third International Conference on Intelligent Sensing and Information Processing, 2005. ICISIP 2005., pp. 170-176, IEEE, 2005.

[23]. L. M. Marvel, C. T. Retter, and C. G. Boncelet Jr, “A methodology for data hiding using images," in Military Communications Conference, 1998. MILCOM 98. Proceedings., IEEE, vol. 3, pp. 1044-1047, IEEE, 1998.

[24]. M. Shirali-Shahreza, “Steganography in mms," in Multitopic Conference, 2007. INMIC 2007. IEEE International, pp. 1-4, IEEE, 2007.

[25]. Y.-C. Shu, W.-L. Hwang, and D. Chou, “Message passing using the cover text as secret key," in Biometrics and Security Technologies (ISBAST), 2012 International Symposium on, pp. 102-107, IEEE, 2012.

[26]. H. Mathkour, B. Al-Sadoon, and A. Touir, “A new image steganography technique," in Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on, pp. 1-4, IEEE, 2008.

[27]. H. Zhang, G. Geng, and C. Xiong, “Image steganography using pixel-value differencing," in Electronic Commerce and Security, 2009. ISECS'09. Second International Symposium on, vol. 2, pp. 109-112, IEEE, 2009.

[28]. Y. Subba Rao, S. Brahmananda Rao, and N. Rukma Rekha, “Secure image steganography based on randomized sequence of cipher bits," in Information Technology: New Generations (ITNG), 2011 Eighth International Conference on, pp. 332-335, IEEE, 2011.

[29]. Rahna E. and V. K. Govindan, "A Novel Technique for Secure, Lossless Steganography with Unlimited Payload,"International Journal of Future Computer and Communication vol. 2, no. 6, pp. 638-641, 2013.

[30]. M. N. Jones and D. J. Mewhort, “Case-sensitive letter and bigram frequency counts from large-scale english corpora," vol. 36, pp. 388-396, Springer, 2004.

[31]. Mamta Sharma. “Compression using Huffman coding”. IJCSNS International Journal of Computer Science and Network Security, Volume 10, pp.133-141, 2010.

AUTHORS

Rahna E is currently doing the final semester of MTech in computer science and engineering in the National Institute of technology Calicut. She has received Bachelor’s degree in computer science and engineering from AWH Engineering College (University of Calicut) in the year 2010. She was born in Calicut, Kerala on 30th October 1988

V K Govindan received Bachelor’s and Master’s degrees in electrical engineering from the National Institute of technology Calicut in the year 1975 and 1978, respectively. He was awarded PhD in Character Recognition from the Indian Institute of Science, Bangalore, in 1989. His research areas include Image processing, pattern recognition, data compression, document imaging and operating systems. He has more than 100 research publications in international journals and conferences, and authored ten books. He has produced six PhDs and reviewed papers for many Journals and conferences. He has more than 34 years of teaching experience at UG and PG levels and he was the Professor and Head of the Department of Computer Science and Engineering, NIT Calicut during years 2000 to 2005. He is currently working as Professor in the Department of Computer Science and Engineering, and Dean Academic at National Institute of Technology Calicut, India.