

A Study on Digital Image and Video Watermarking Schemes using Neural Networks

Bibi Isac
School of Computing Science and
Engineering
VIT University
Vellore, India

V. Santhi
Associate Professor
School of Computing Science and
Engineering
VIT University
Vellore, India

ABSTRACT

The use of computer network communication makes information exchange and transmission relatively simple and quick. But with digital image, audio and video products like multimedia, copyright protected security questions will be exposed in such communication environments. Digital watermarks have been recently proposed for authentication of both video and still images. This paper gives a review of a few of the proposed image and video watermarking techniques using neural networks.

Keywords

Digital Watermarking, Neural Networks Based watermarking technique, Invisible Watermarking, Transform domain watermarking.

1. INTRODUCTION

1.1. Digital Watermarking

The rapid development of digital media provides a great convenience for adopting, using, modifying the information. The development in computer network communications make information transmission relatively simple and quick but, there can also be chances of attacks on the digital media that is being transmitted.

There has been an extraordinary growth of techniques for copyright protection of different types of data, especially multimedia information since the 1990s [1]. This has become necessary because of the simplicity in digital copying and dissemination: digital copies can be made similar to the original signal and later be reused or even manipulated. Perceptible marks of ownership or authenticity have been used for centuries in the form of stamps, seals, signatures. But, with the current situation of data manipulation technologies, imperceptible digital marks are required.

Cryptography [2] is one among the solutions that were suggested then but in most cases, a specialized and costly hardware is also involved. There is also an increasing need for software and in some cases, hardware that allows for protection of ownership rights. Another problem with cryptography is that, once the data is decrypted, it will no longer be secure.

Digital watermarks have been recently proposed for the authentication and copyright protection of audio, video and still images [3]. In such applications, the watermark is embedded within a cover image, audio sequence or video frame such that subsequent alteration to the watermarked image can be detected with high probability. A digital watermark is a visible or invisible

identification code that is permanently embedded in the data and remains present within the data even after any decryption process. In other words, a digital watermark is a distinguishing piece of information that is adhered to the data that it is intended to protect which means that it should be difficult to extract or remove the watermark from the watermarked object. The data may be audio, image or video. If the data is copied, then the information is also carried in the copy [4]. A particular signal may carry several different watermarks at the same time. Since watermarking can be applied to various types of data, the imperceptibility constraint will take different forms, depending on the properties of the recipient. In addition to imperceptibility, there are some desirable characteristics that a watermark should possess such as robustness. The watermark should be resistible to standard manipulations which may be intentional or unintentional and it should be statistically irremovable.

Digital watermarking can be of two types: (a) Visible watermarking and (b) Invisible watermarking [5]. In visible watermarking, the information is visible in the image or video. The information may be a text or a logo which identifies the owner of the media. In invisible watermarking, information is added as digital data to audio, picture or video, but cannot be perceived. The hidden information can be detected to some extent.

The concept of digital watermarking is derived from steganography [6]. Both steganography and watermarking describe techniques that are used to keep information by embedding it into the cover data. The methods used for steganography are usually not robust against modification of the data. Digital watermarking on the other hand should be robust against attempts to remove the hidden data. A popular application of watermarking is proof of ownership. As mentioned before, based on the host signal [7] in which the watermark is embedded, watermarking may be classified as:

- (a) Digital image Watermark- Both visible as well as invisible watermarking is applicable in images.
- (b) Digital video Watermark- A video sequence consists of many frames that can be taken as images. Hence, the process of watermarking in images can be extended to videos also.
- (c) Digital audio Watermark- Only invisible watermarking is possible.
- (d) 3D Multimedia based Watermark

Once the host signal is selected, the watermarking can be done in either the spatial domain i.e. where the watermark is directly embedded in the signal; or the frequency domain which involves applying any of the transformation techniques [8] on the signal

and then embed the watermark. Applications of digital watermarking include: copyright protection, covert communication, broadcast monitoring, content authentication, content description, and copy and usage control.

1.2. Neural Networks

Real neurons integrate hundreds or thousands of temporal signals through their dendrites. These signals modify their internal potential in a complex way that depends on the inhibitory or excitatory nature of the synapses at which the signals impinge on the cell [9]. A neural network represents a highly parallelized dynamic system with a directed graph topology that can receive the output information by means of a reaction of its state on the input actions [10]. The ensembles of interconnected artificial neurons generally organized into layers or fields include neural networks. The behavior of such ensembles varies greatly with changes in architectures as well as neuron signal functions. Artificial neural networks are massively parallel adaptive networks of simple non-linear computing elements called *neurons* which are intended to abstract and model some of the functionality of the human nervous system in an attempt to partially capture some of its computational strengths.

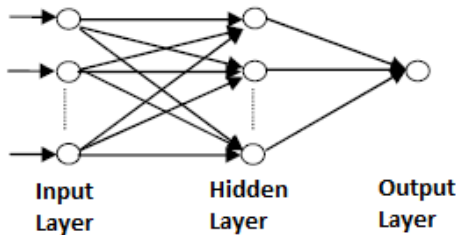


Figure 1: Basic Neural Network

In its most general form, a neural network can be viewed as comprising the following eight components [11]:

(a) Neurons

Neurons can be of three types: input, hidden and output. Input neurons receive the external stimuli presented to the network. Hidden neurons compute intermediate functions and their states are not accessible to the external environment. Outputs from the network are generated as signals of output neurons.

(b) Activation state vector

This is a vector that indicates the activation level of individual neurons in the neural network.

(c) Signal function

A function that generates the output signal of the neuron based on its activation is called a signal function. Functions may differ from neuron to neuron within the network; although most networks are field-homogeneous i.e. all neurons within a field or layer have the same signal function.

(d) Pattern of connectivity

This determines the inter-neuron connection architecture or the graph of the network.

(e) Activity aggregation rule

This aggregated the activity at a particular neuron.

(f) Activation rule

This function determines the new activation level of a neuron based on its current activation and its external inputs.

(g) Learning rule [12]

The learning rule provides a means of modifying correction strengths based on both the external stimuli and the network performance with the aim of improving the network performance.

(h) Environment

The environments in which neural networks can operate could be deterministic (noiseless) or stochastic (noisy).

A neural network can be viewed as a weighted directed graph in which artificial neurons are nodes and directed weighted edges represent connections between neurons. Local groups of neurons [13] may be connected in either:

(a) Feed-forward architecture

In this architecture, the network has no loops.

(b) Feedback architecture

Here, loops occur in the network because of feedback connections.

2. REVIEW ON DIGITAL IMAGE AND VIDEO WATERMARKING USING NEURAL NETWORKS

A number of techniques have been proposed for embedding and extracting a watermark in a digital medium using neural networks. A review has been done on the same area and it is given briefly below. Figure 2 shows the sample Lena and Baboon images that have been used for the analysis of most of these methods.



Figure 2: (a) Lena Image (b) Baboon Image

The work towards video authentication and copyright protection using neural networks started in 1999 [14]. In this paper an image comparison algorithm and cryptographic hash function on the regular array of cellular neural network (CNN) cells is given. These operations are necessary for message authentication and copyright protection in the multimedia service environment, serving both the interest of the copyright owner and the user. The hash function required for the authentication process is calculated using a cellular neural network. The basic motivations for multimedia copyright protection, some possible solutions, and the basic functions needed to protect multimedia data are explained in this paper. In the multimedia service environment, low capacity of transmission channels or storage media may result in the degradation of image quality. Therefore authentication of video data has to be performed based on image features which possibly resist lossy compression and corruption by noise. The proposed

authentication scheme is based on the comparison of segmentation results in an MPEG-4 coding/decoding process.

P.-T. Yu et al. [15] proposed a novel digital watermarking technique based on neural networks for color images. The proposed technique hides an invisible watermark into a color image and then uses a neural network to learn the relationship between the embedded watermark and the watermarked image. The relationship learnt by the neural network is then used as a digital signature in the extraction process. Multiple embedding is adopted in this technique to improve the performance. When a watermarked image is distorted by some attacks, such as rotation and filtering, the watermark information in the distorted and watermarked image may become tenuous. Due to the flexibility and adaptability of the neural network, the watermarking technique outperforms the conventional techniques against several attacks.

In [16], a technique which uses an artificial neural network (ANN) to model the human visual system (HVS) and an ANN-based image adaptive method for image DCT (Discrete Cosine Transform) coefficients is presented. In this technique, an ANN is used to model the HVS to decide the watermark strength of DCT coefficients and then watermark bits are embedded into the DCT coefficients adaptively. This paper presents the method of deciding watermarking strength in DCT domain using artificial neural network. It shows that an ANN can better model human visual system and that the watermarking strength calculated using ANN is much larger than conventional methods without causing visual degradation of watermarked images, so that the watermark robustness can be increased greatly.

A novel watermarking method for an image is proposed in 2002 by Jun Zhang [17], in which the logo watermark is embedded into a novel transform domain – multi-wavelet transform domain. Since the differences between the corresponding coefficients in two sub-blocks in the coarsest level of the multi-wavelet domain are small, the embedding strategy could ensure the quality of the image. A BPN (Back Propagation Network) model is used to learn the relationship between the watermark and the watermarked image.

A robust image-adaptive watermarking scheme is presented [18] which use a visually meaningful binary image as the watermark. The watermark was added to the mid-band frequency components of the block-based DCT domain. The algorithm's robustness against different attacks had increased as the strength of the added watermark increased with the help of RBF (Radial Basis Function) Neural Network.

Zhang [19] proposed a blind watermarking algorithm using Hopfield neural network and then analyzed the watermarking capacity based on the neural network. Hopfield neural network is a non-linear dynamical system that uses computational energy function to evaluate the stability property. The energy function always decreases toward a state of lowest energy. The neuron states in a Hopfield network are usually binary. The gray scale test image was decomposed and for each pixel, a decision had to be made whether the pixel should be modified or not. This was stored in a matrix. The watermark amplitude was decided based on this matrix. Basin of attraction is the set of points in the space of system. The radius of attraction basin is designed as the largest

Hamming distance within which almost all states are similar to the pattern. The attraction basin of Hopfield neural network decides the watermarking capacity.

Chang [20] presented a specific designed full counter-propagation neural network for digital image watermarking. Different from the traditional methods, the watermark was embedded in the synapses of the FCNN (Full Counter-Propagation Neural Network) instead of the cover image. The quality of the watermarked image was almost same as the original cover image. Since the watermark was stored in the synapses, most of the attacks could not degrade the quality of the extracted watermark image.

C.-R. Piao et al. [21] proposed a new blind watermarking scheme in which a watermark was embedded into the DWT (Discrete Wavelet Transform) domain. It also utilized RBF Neural network to learn the characteristic of the image, using which the watermark would be embedded and extracted. The embedding scheme resulted in a good quality watermarked image.

Wang [22] presented a novel blind digital watermarking scheme based on neural networks in the multi-wavelet domain. The watermark was embedded into the coefficients selected based on the weight factors calculated by exploiting the HVS characteristics. The neural network was fused properly with watermarking to enhance the performance of conventional watermarking techniques.

El' Arbi [23] proposed a video watermarking algorithm which combined neural networks with motion estimation in the wavelet domain in a way that was less perceptible and robust against common video processing attacks.

A novel digital video watermarking scheme based on 3D-DWT and Artificial neural network was later proposed [24]. First, a 3D wavelet transform was performed on each of the selected video shots and then the watermark was embedded in the LL sub-band wavelet coefficients of the low-pass frames. The scheme was found to have strong robustness against common video processing attacks. In order to ensure perceptual invisibility, the coefficient was selected adaptively to embed the watermark and the embedding intensity was adaptively controlled using statistical characteristics such as mean and standard deviation.

A digital watermarking scheme using neural networks was proposed later in 2007 [25] where, the original image was divided into some 8*8 blocks, and then neural networks were used according to different textural features and luminance of each block to decide adaptively different embedding strengths. The proposed watermarking scheme shows superior performance. By exploiting neural networks, it provides the maximum watermark embed strength which is robust to common attacks. By different embedding strengths decided by neural networks according to different textural features and the mean luminance of each block, the resulting watermarked image is extremely robust to a wide range of image JPEG compression. It does not require the original image for watermark detection.

In [26], a novel blind digital watermarking scheme based on BP neural network in the wavelet domain is presented. HVS characteristics were taken into consideration so as to make the watermark invisible during the process of watermark embedding. An artificial neural network was also applied to watermarking in order to enhance the performance of conventional watermarking

techniques. In order to test the robustness of the algorithm, Median filtering attack, Low-pass filtering attack, cropping attack, salt and pepper noise attack were among the few attacks that are taken into consideration.

Yongquiang [27] proposed a novel optimal color image watermarking scheme in the DWT domain to meet watermarking properties such as: security, imperceptibility and robustness. In the scheme, the watermark was a meaningful gray image encrypted by a two-dimensional chaotic stream encryption. Genetic algorithm was used to embed the watermark into the host color image so as to improve the imperceptibility of the watermarked image.

Paper [28] proposed a color image watermarking algorithm based on fractal and neural networks in Discrete Cosine Transform (DCT) domain. Firstly, the algorithm utilized the fractal image coding technique to obtain the characteristic data of a gray-level image watermark signal and encrypted it by a symmetric encryption algorithm before it was embedded. Secondly, by exploiting the abilities of neural networks and considering the characteristics of Human Visual System (HVS), a Just Noticeable Difference (JND) threshold controller was designed to ensure the strength of the embedded data adapting to the host image itself entirely. Thus the watermark scheme possessed dual security characteristics. CIELab color space was chosen to guarantee the stability of the results.

Yi [29] proposed a novel digital watermarking scheme based on improved Back-propagation neural network for color images. The watermark was embedded into the discrete wavelet domain of the original image and extracted by training the BPN which learnt the characteristics of the image. To improve the rate of learning and reduce the error, a momentum coefficient is added to the traditional BPN network.

Huang [30] proposed a novel watermarking technique based on image features and neural networks. The watermark used is a fusion of a binary copyright symbol and image feature label that is obtained by analyzing the image fractal dimension. The watermark not only visually represents the copyright symbol, but also reflects the feature of the image. Arnold transform is used to increase the security of watermark. The back propagation neural network is applied to improve its imperceptibility and robustness.

C.-Y. Chang et al. [31] used a full counter-propagation neural network (FCNN) for copyright protection where the ownership information was embedded and detected by a specific FCNN. The watermark is stored in the synapses of the FCNN. Since the FCNN has storage and fault tolerance, most attacks did not degrade the quality of the detected watermark image. The watermark embedding and retrieval procedures were integrated into the FCNN.

Arbi [32] proposed a video watermarking algorithm that embedded different parts of a single watermark into different shots of a video under the wavelet domain. Based on motion activity analysis, different regions of the original video are separated into perceptually distinct categories according to the motion information and region complexity. The watermark moves along with the moving objects and thus motion artifacts can be avoided.

Zhang and Li [33] proposed a novel watermarking algorithm for non-compressed video where, the original video frame is divided into 8×8 blocks. DCT (Discrete Cosine Transform) was applied on these 8×8 blocks to calculate the energy from the DCT coefficients. According to the energy calculated, the areas in the blocks were classified based on information contained and motion. The watermark embedding area was decided based on this area classification. In the watermark extraction process, a BPN (Back Propagation Network) was trained in order to detect the areas where the watermark is embedded based on the DCT coefficient energy values.

Table 1: Average PSNR values obtained using different neural network methods on a Blurred Baboon image

Neural Network	CNN	BPN	RBF	Hopfield	FCNN
Average PSNR Value	28.84	35.68	38.27	36.25	48.68

Table 2: Average PSNR values obtained using different neural network methods on a Filtered Lena image

Neural Network	CNN	BPN	RBF	Hopfield	FCNN
Average PSNR Value	22.62	33.51	38.68	34.45	37.49

A number of techniques have been proposed for digital image and digital video watermarking by training neural networks. Some of the watermarking techniques are categorized as blind watermarking and few techniques are classified as non - blind watermarking. Similarly in few works for embedding watermark neural network is used and in some works it is used for extracting watermark. The watermarking is carried in both spatial domain and frequency domain. Table 1 shows the average PSNR values that have been obtained using the different neural networks for a Blurred Baboon image and Table 2 shows the average PSNR values for different methods when they were applied on a Filtered Lena image. The results have been found to be better on using a BPN for the watermarking process.

3. CONCLUSION

In this paper a detailed description of watermarking works carried out using digital images and videos based on neural networks is given. Many of these techniques have been able to satisfy the basic requirement of watermarking i.e. the extraction process does not require the original signal or in other words, the algorithm is blind. Similarly in few papers it is found that work is carried out in spatial domain, while others work are carried out in frequency domain by using transformation techniques. The neural networks that are used include Back propagation Network (BPN), Counter Propagation Network (CPN), Full Counter Propagation Network and Cellular Neural Network (CNN). The robustness of these algorithms are tested with respect to various attacks like blurring, median filtering attack, low-pass filtering attack , cropping attack and salt and pepper noise attack. Each of these algorithms has

their own advantages and disadvantages which have been discussed briefly in Section 2. Thus, an ideal watermarking algorithm should be blind in nature and must be robust against attacks. Also it should guarantee correct and fast watermark detection with low error rate.

In future, a new algorithm can be designed to embed and extract a watermark using neural networks, where the neural network will be used in both the embedding process as well as the extraction process. The neural network used may be trained to detect the suitable place to embed the watermark based on Region of Interest (ROI). Once the watermark is embedded, the embedded area can be again detected from the watermarked signal using another trained neural network.

4. REFERENCES

- [1] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "A secure, robust watermark for multimedia," in *Information Hiding* (G. Goos, J. Hartmanis, and J. Leeuwen, eds.), vol. 1174 of *Lecture Notes in Computer Science*, (University of Cambridge, UK), pp. 185–206, Springer-Verlag, May 1996.
- [2] B. Macq and J. Quisquater, "Cryptology for digital TV broadcasting," *Proceedings of the IEEE*, vol. 83, pp. 944–957, February 1995.
- [3] M. Kutter, S. K. Bhattacharjee, and T. Ebrahimi, "Towards Second Generation Watermarking Schemes", in *Proceedings 6th International Conference on Image Processing (ICIP'99)*, volume 1, pp. 320-323, October 24-28, 1999, Kobe, Japan.
- [4] K. Tanaka, Y. Nakamura, and K. Matsui, "Embedding secret information into a dithered multi-level image," in *Proc. 1990 IEEE Military Communications Conference*, pp. 216–220, 1990.
- [5] J. R. Hernandez, F. Perez-Gonzalez, J. M. Rodriguez, and G. Nieto, "Performance analysis of a 2D-Multipulse Amplitude Modulation scheme for data hiding and watermarking of still images", *IEEE J. Select. Areas Communication*, Vol. 16, pp. 510–524, May 1998.
- [6] C. Cachin, "An information-theoretic model for steganography", In *Proc. of 2nd Workshop on information hiding*, 1998.
- [7] Jana Dittmann, David Megias, Andreas Lang, Jordi Herrera-Joancomarti, "Theoretical framework for a practical evaluation and comparison of audio watermarking schemes in the triangle of robustness, transparency and capacity", In *Transaction on Data Hiding and Multimedia Security I*, Springer LNCS 4300, Editor Yun Q. Shi, pp. 1-40, ISBN 978-3-540-49071-5, 2006.
- [8] Khan, A. and Mirza, A. M., "Genetic perceptual shaping: Utilizing cover image and conceivable attack information during watermark embedding", pp. 354-365, October 2007.
- [9] Laurene V. Fausett, "Fundamentals of Neural Networks: Architectures, Algorithms, and Applications", 9 December, 1993.
- [10] Howard B. Demuth, "Neural Network Design", ISBN 10: 0534943322, 29 December, 1995.
- [11] Brian D. Ripley, "Pattern Recognition and Neural Networks", ISBN-10: 0521460867, 18 January, 1996.
- [12] Christopher M. Bishop, "Pattern Recognition and Machine Learning", ISBN-10: 0387310738, 1 February, 2007.
- [13] Alexander I. Galushkin, "Neural Networks Theory", ISBN 978-3-540-48124-9, Springer Berlin Heidelberg, 2007.
- [14] Marton Csapodi, Joos Vandewalle and Bart Preneel, "CNN Algorithms for Video Authentication and Copyright Protection", *Journal of VLSI Signal Processing* 23, pp 449-463, 1999.
- [15] Pao-Ta Yu, Hung-Hsu Tsai, Jyh-Shyan Lin, " Digital watermarking based on neural networks for color images", *Signal Processing*, pp 663-671, 2001.
- [16] Mei Shi-chun, Li Ren-hou, Dang Hong-mei, Wang Yun-kuan, "Decision of Image Watermarking strength based on Artificial Neural Networks", In the *Proceedings of the 9th International Conference on Neural Information Processing*, Vol. 5, 2002.
- [17] Jun Zhang, Nenchao Wang, Feng Xiong, "Hiding a Logo Watermark into the Multiwavelet Domain using Neural Networks", In the *Proceedings of the 14th IEEE International Conference on Tools with Artificial Intelligence*, 2002.
- [18] Zhang Zhi-Ming, Li Rong-Yan, Wang Lei, " Adaptive Watermark scheme with RBF Neural Networks", *IEEE International Conference Neural Networks and Signal Processing*, December 14-17, 2003.
- [19] Fan Zhang, Hongbin Zhang, "Applications of Neural Network to Watermarking Capacity", *International Symposium on Communications and Information Technologies*, October 26-29, 2004.
- [20] Chuan-Yu Chang and Sheng-Jyun Su, "The Application of a Full Counterpropagation Neural Network to Image Watermarking", 2005.
- [21] Cheng-Ri Piao, Suenghwa Beack, Dong-Min Woo and Seung-Soo Han, "A Blind Watermarking Algorithm based on HVS and RBF Neural Network for Digital Image", *ICNC 2006, Part 1, LNCS 4221*, pp. 493-496, 2006.
- [22] Zhenfei Wang, Nenchango Wang and Baochang Shi, "A Novel Blind Watermarking Scheme based on Neural Networks in the Multiwavelet Domain", In the *Proceedings of the 6th World Congress on Intelligent Control and Automation*, June 21-23, 2006.
- [23] Maher El'Arbi, Chorki Ben Amar and Henri Nicolas, "Video Watermarking based on Neural Networks", 2006.

- [24] Xuefang Li, Rangding Wang, “A Video Watermarking scheme based on 3D-DWT and Neural Network”, 9th IEEE International Symposium on Multimedia, 2007.
- [25] Cong Jin and Shihui Wang, “Applications of a Neural Network to estimate Watermark Embedding Strength”, 8th International Workshop on Image Analysis for Multimedia Interactive Services, 2007.
- [26] Song Huang and Wei Zhang, Wei Feng and Huaqian Yang, “Blind Watermarking scheme based on Neural Networks”, In the Proceedings of the 7th World Congress on Intelligent Control and Automation, June 25-27, 2008.
- [27] Chen Yongquiang, Zhang Yangqing, Peng Lisen, “A Novel Optimal Color Image Watermarking Scheme”, 3rd International Conference on Genetic and Evolutionary Computing”, 2009.
- [28] Mao Li, Fan Yang-yu, Lv Guo-yun, Wang Hui-qin, “Adaptive Color Image Watermarking Algorithm based on Fractal and Neural Networks”, 2009.
- [29] Qianhui Yi and Ke Wang, “An Improved Watermarking method based on Neural Network for Color Image”, In the Proceedings of the 2009 IEEE International Conference on Mechatronics and Automation, August 9-12, 2009.
- [30] Song Huang, Wei Zhang, “Digital Watermarking based on Neural Network and Image Features”, 2nd International Conference on Information and Computing Science, 2009.
- [31] Chuan-Yu Cahng, Hung-Jen Wang, Sheng-Jyun Su, “Copyright authentication for images with a full counter-propagation neural network”, Expert Systems with Applications 37, 2010.
- [32] Maher El’Arbi, Mohamed Koubaa, Maha Charfeddine, Chokri Ben Amar, “A dynamic video watermarking algorithm in fast motion areas in the wavelet domain”, Multimedia Tools Application, August 11, 2010.
- [33] Lijing Zhang, Aihua Li, “A Novel Watermark Algorithm for Non-Compressed Digital Video”, 2nd International Workshop on Education Technology and Computer Science, 2010.

Prof. V. Santhi is currently working as Associate professor in VIT University, Vellore, India. She is having more than 15 years of teaching experience and more than 3 years of Industry experience. She has pursued her B.E degree in Computer Science and Engineering from Bharathidasan University, Trichy and M.Tech degree in Computer Science and Engineering from Pondicherry University, Pondicherry. She is currently doing PhD in VIT University. She is a member of IACSIT, IEEE and CSI. Her area of research includes Image Processing, Digital Signal Processing, Digital Watermarking and Data Compression. She has published many papers in international conferences and Journals.

Bibi Isac is currently doing her M.Tech degree in Computer Science and Engineering in VIT University, Vellore, India. She completed her B.E. degree in Computer Science and Engineering from Sathyabama University, Chennai, India. Her area of interest includes Image Processing, Signal Processing, and Digital Watermarking.