International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958, Volume-9 Issue-1S3, December 2019

A Robust Watermarking Method for an Authentication of Video Surveillance Applications

Satish D. Mali, AgilandeeswariL

***Abstract:** The problem of authenticating the video content is the major role of any automated video surveillance systems (AVS). This research work delivers an approach to authenticate the surveillance video which can be used by attorneys to prove their clients using Digital Watermarking. The digital watermark gives an assurance that the provided video surveillance frame is not tampered. In this paper, we proposed a robust video watermarking approach for an authentication of video surveillance applications. The digital watermark is embedded into the Discrete Wavelet domain of the identified key frames using holoentropy. Here, the pixel map will be optimallygenerated for the watermarking and the image embedding using the proposed classifier using Moth – flame - Rider optimization based Neural Network (MF-ROA-based NN) will generate the optimal map prediction based on the fitness measure, such as wavelet coefficient, energy, entropy, loop coefficient, and standard deviation, respectively. This optimal map is used for both embedding and extraction. The experimental results proves that the proposed systems can authenticate the surveillance video frames against various attacks when compared to the existing systems.*

***Keywords:** Automated Video Surveillance Systems (AVS), Digital Watermarking, Discrete Wavelet Domain, holoentropy, optimal map*

I. INTRODUCTION

Video surveillance systems play a major role in forensic evidence in court. The video files of digital surveillance systems need to be authenticable. Thus a technique like watermarking is applied for tamper detection purposes. The watermark must not have any effect on visual information and or compromise the video evidence in any way. High imperceptible watermarks can meet these requirements [1]. Video tamper detection is a major challenge for today's researchers in the field of multimedia security [1]. Tamper-resistant watermarks are designed for copyright protection to declare the ownership. The tamper resistant watermark must be robust in nature so that it is impossible or difficult to remove watermark without visibly damaging the watermarked media. While fragile watermarks designed to detect the tampering of the watermarked media as these are very sensitive to modifications. The tampering will modify or destroy the watermark. Fragile watermark provides basis for the tamper detection as well as tamper localization [2]. Most tampered media have part of the medium altered using objects in the medium itself.

Revised Manuscript Received on December 20, 2019.
***Correspondence author:** Dr.L.Agilandeeswari
Sathish D Mali, Puranmal Lahoti Government Polytechnic, Latur, Maharashtra, India. Email: 2satish.mali@gmail.com
Dr.L.Agilandeeswari*, Associate Professor, School of Information Technology and Engineering, VIT University, Vellore, India. Email: agila.l@vit.ac.in

Parts of a medium can be altered geometrically to change their appearance. The commonly used by forgers include cropping, rotation and scaling [2]. An alteration using scaling changes the size of objects, often creating an illusion. Rotational modification, on the other hand, changes the angle of alignment of an object in the medium [1].The continuous growth of Internet Technologies has made the communication and circulation of digital multimedia contents very easy. However, this leads to an increase in illegal operations such as duplication, modification, forgery, and copyright infringement. Therefore, the copyright protection, content authentication, and ownership identification have become critical requirements of the multimedia content security [3]. Watermarking is the process of embedding data into a multimedia element such as image, audio or video. This embedded data can later be extracted from, or detected in, the multimedia element for different purposes such as copyright protection, access control, and broadcast monitoring [4]. A basic watermarking system has three major requirements, such as transparency, robustness and blind detection [5]. The watermark is concealed as additional information to the original video which may degrade the visual quality of watermarked video content. Hence, maintaining the perpetual transparency of video content after watermark concealing is vital [5]. Introducing watermarks in digital videos can be useful to safeguard copyright. The watermark can be inserted either in uncompressed (raw) video or compressed video. Video signals are often stored and transmitted in a compressed format. Application of uncompressed watermarking techniques for compressed video sequences, however, needs complete decoding and re-encoding of the video for watermark embedding or detection [6]. Although digital video watermarking, which is the process of hiding digital information in a host video signal, is a solution to this problem, there are some important issues, such as imperceptibility, blind detection, security and robustness to attacks that need to be considered during the design of the watermarking algorithm [7]. Despite video watermarking in the compressed domain, which may cause error propagation due to embedding, watermarking in the uncompressed domain is easier. In this case, the designer does not care about the video bit-rate [8]. Although video watermarking has many properties, the main three ones are imperceptibility, robustness and payload or capacity. All three are closely related to each other: for example, when robustness increases, imperceptibility decreases, and vice-versa [1]. A robust video watermarking scheme must maintain the integrity of watermark transparency plus robustness to pirate attacks [5].

Video watermarking algorithms can be divided into three groups including pixel domain, transformed domain, and compressed domain based on the place in which the embedding is directly applied. Pixel domain algorithms directly embed the watermark into video frame pixels. The main advantage of these algorithms is that they have low computational complexity and as a consequence can be implemented easily. However, they are less robust against attacks; in this regard, statistical and geometrical techniques are utilized to improve the robustness [8].

The above study motivates us to develop a robust watermarking scheme which authenticates the surveillance video frames. The proposed system identifies the key frames using holoentropy, then identifies the optimal map using the Moth flame – rider – based Neural Network classifier. Such optimal map is used for both embedding and extraction which makes the system robust against various attacks.

The rest of the paper is organized as follows: section 2 elaborates related works, section 3 describes proposed methodology, section 4 demonstrates the experimental results and finally conclusions were drawn in section 5.

II. RELATED WORKS

Digital watermarking method was developed to enhance the effectiveness of the compression ratio. However, it was not secure against geometric attacks. In [2], Bi-directional Extreme Learning Machine (B-ELM) was developed to makes the embedding and extraction process quite fast. However, the performance was not effective. In [3], Bi-orthogonal

Wavelet Transform was introduced to enhance the efficiency and security in the surveillance system, but this system was not robust. Zero-watermarking scheme was developed in [4] to exhibits strong robustness against various video attacks. Conjugate Symmetric Sequency-Complex Hadamard Transform (CS-SCHT) was modelled in [5] to resists various attacks like RS, BD and HEVC compression. However, the computational cost is high. Multi-BAM-FUZ was developed to enhance the embedding capacity of the scheme [6]. Novel video watermarking approach was developed to identify the malicious consumers from the video services [7]. The robust video watermarking technique was introduced to detect the video surveillance accurately even very fine cutand- paste blocks. It focuses on video watermarking, particularly with respect to the Audio Video Interleaved (AVI) form of video file format. However, it offered a high degree of imperceptibility and efficient tamper detection. It requires a large quantity of sequences to be processed, which makes computational efficiency an additional constraint on video watermarking for surveillance systems. It proved to be equally efficient in detecting tampering and in their overall robustness, but not in terms of their imperceptibility. It was able to embed confidential and integrity information into hosts effectively and also improved the efficiency of detecting tampering [8].

This section elaborates the work related to the authentication of video.

Authors	Methods	Pros	Cons
Asikuzzaman M *et al.* [7]	Digital watermarking method	It was robust and effective against H.264/AVC compression, additive noise, baseline distance adjustment, and both 2D and 3D camcording.	It was not secure against geometric attacks.
Rajpal A *et al.* [3]	Bi-directional Extreme Learning Machine (B-ELM)	It makes the embedding and extraction process quite fast. It was robust against the preocessing interferences, like cropping, filtering, and scaling.	However, the performance was not effective.
Sake A. and Tirumala R [4]	Bi-orthogonal Wavelet Transform	It improved the imperceptibility, efficiency and security in watermarking.	However, it was not robust.
Liu X *et al.* [9]	Zero-watermarking scheme	It does not cause any distortion to the synthesized 3D videos, exhibits strong robustness against various video attacks.	It failed to enhance the robustness of the content-based features against geometrical attacks such as rotation and cropping.
Meenakshi K *et al.* [5]	Conjugate Symmetric Sequency-Complex Hadamard Transform (CS-SCHT)	This scheme is resilient to various attacks like RS, BD and HEVC compression.	However, the computational cost is high.
Loganathan A. and Kaliyaperumal G [10]	Multi-BAM-FUZ	The embedding capacity of this scheme is far better than the existing algorithms.	However, it was not suitable for fast motion videos.
Mareen H *et al.* [11]	Novel video watermarking approach	It effectively identifies the malicious consumers of video services.	The detection rate was vey less.
Arab F *et al.* [1]	Robust video watermarking technique	It attained better detection capabilities and better imperceptibility	It failed to accurately detect the fine cutand- paste blocks.

1.1. Contributions:

The issues on the above study motivate us towards the following contributions:

- Develop an effective watermarking scheme in the video surveillance system to enhance the performance of the watermarking mechanism.
- Develop a novel watermarking concepts this helps to inquire the features of the embedding characteristics.

III. PROPOSED METHODOLOGY

The primary intention of this research work is to design and develop a new method for video watermarking. This work performs the video watermarking framework by involving four phases, as (i) Key frame identification, (ii) pixel map generation, (iii) embedding phase, and (iv) extraction phase, respectively. Initially, the input video is collected from the video surveillance system and will be fed to the latent frame identification phase, where the key frames will be effectively identified using the concept of holoentropy. The selected latent frames will be allowed to the pixel map generation module. Here, the pixel map will be optimally generated for the watermarking and the image embedding using the proposed classifier. The proposed Moth-flame-rider optimization algorithm-based Neural network (MF-ROA-based NN) classifier will be the integration of the standard RideNN [14] and moth-flame optimization (MFA) [15] such that the proposed classifier will generate the optimal map prediction based on the fitness measure, such as wavelet coefficient, energy, entropy, loop coefficient, and standard deviation, respectively.

Then, the generated optimal pixel map will be forwarded to the embedding phase, where the watermark image will be embedded in the video. In the embedding phase, the video watermarking will be carried out using the Haar wavelet-based embedding. Moreover, the extraction process will be carried out using the inverse Haar wavelet-based embedding. In the extraction phase, key will be used to extract the embedded watermark image in the video by applying the inverse Haar wavelet-based embedding and it is tested for robustness. Figure 1 shows the architecture of the proposed video watermarking approach for surveillance video applications.

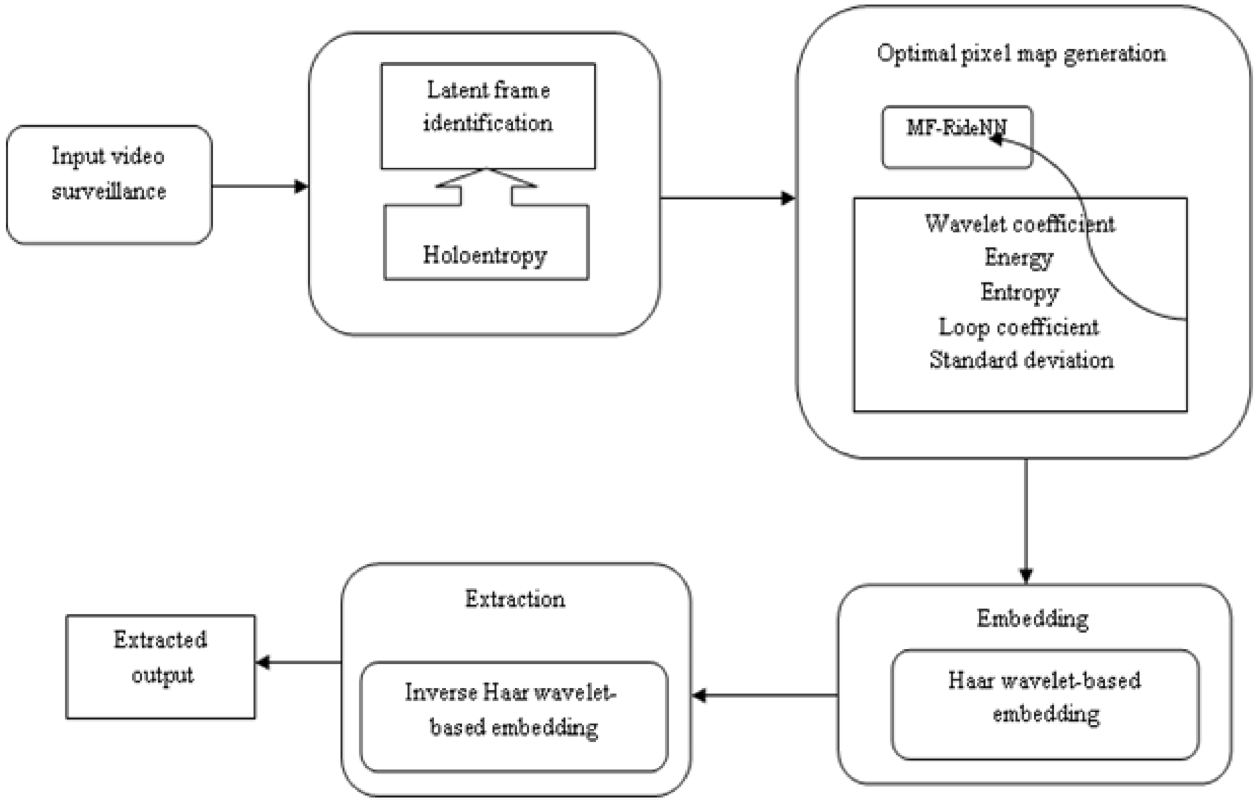

Fig. 1. Architecture of the proposed MFA-Ride- based NN approach for Video Surveillance

IV. EXPERIMENTAL RESULTS

The simulation experiments were carried out in this section to test the efficiency of the proposed system. This approach is tested with large data set of popular surveillance videos and CAVIAR dataset [16] as shown in Fig. Due to page constraint, we have shown few surveillance video samples namely ‘*suzie*’ ‘*abcnews’*, *‘blanchardtownhouse’*, *‘oldstreet’*, *‘sporecctvfootage’*, *‘taximeter’*, *‘wnycnews’*, *‘womaninstreet’ and ‘caviar’*and watermark image as ‘lena’ as shown in Fig.2

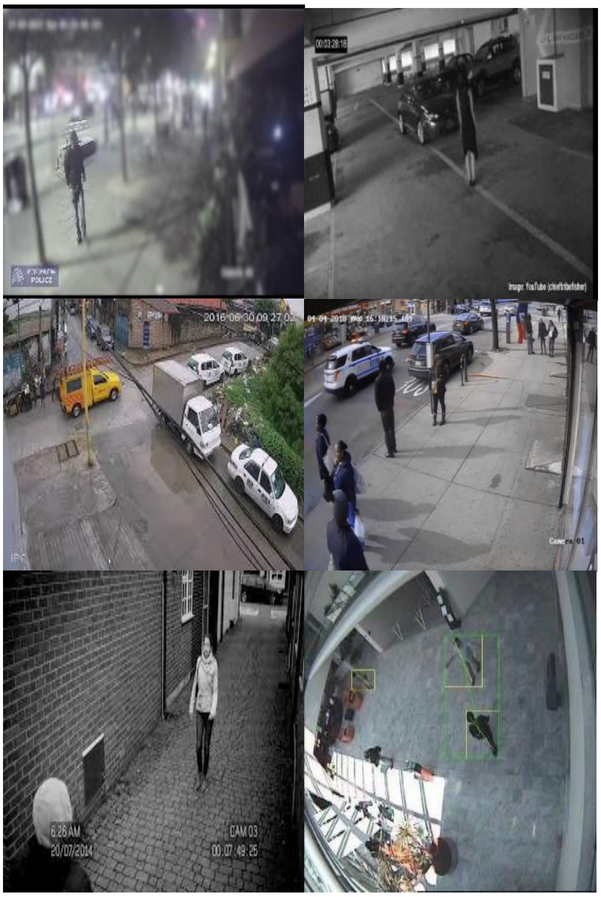

Fig. 2.A sample cover video frames

Moreover, the watermarks choosen to verify the robustness of the proposed system are the benchmark test images such as *lena*,as given in Fig.3

Fig. 3 A sample watermark images

The Fig. 4 shows the watermarked video frames *blanchardtownhouse_w*and the extracted watermark *lena1*

Fig. 4 Watermarked Video frames and extracted watermarks

4.1 Performance Metric

The performance of the proposed method in terms of imperceptibility and robustness were evaluated using the performance metrics, namely Peak Signal to Noise Ratio (PSNR), and Normalized correlation coefficient respectively.

4.2 Attacks:

To investigate the performance of the proposed video watermarking system, we voluntarily introduced some attacks on each watermarked videos such as, Frame Noisingintroduces various noises on the watermarked video such as, gaussian noise of variance 0.05, Salt and pepper noise with density 0.05. Frame cropping is an attack performed by an illegitimate users by cropping the significant portion of the video frames at the rate of 50%. Frame Insertion is an attack involves inserting the frames randomly at various locations in the rate of 50%. Frame Dropping is anattack dealt with dropping the frames randomly at the rate of 50%. Frame Swapping involves swapping of frames randomly at the rate of 50%, Frame Rotate, Frame Rate conversion attack dealt with changing the number of frames shown per second. The various frame rates used for testing purposes are varying in the range 50fps. Temporal redundancy is evaluated by embedding the watermark weight matrix on the test videos with temporal redundancy of r=6 frames and MPEG Compression.The proposed scheme shows high resistance to all the mentioned attacks with good and acceptable quality factor (see Fig. 5)

Type of attack	Watermarked frame	Extracted Watermark	Type of attack	Watermarked frame	Extracted Watermark
Gaussian noise (variance = 0.05)	 PSNR = 51.51	 NCC = 0.99	Salt and pepper noise (density = 0.05)	 PSNR = 49.99	 NCC = 0.98
Frame Cropping(20%)	 PSNR = 49.89	 NCC = 0.97	Frame Insertion (Rate = 50%)	 PSNR = 51.88	 NCC= 0.99
Frame Dropping (Rate = 50%)	 PSNR = 51.01	 NCC = 0.99	Frame Swapping (Rate = 50%)	 PSNR = 50.62	 NCC = 0.99
Frame Rotation (30^o)	 PSNR = 46.74	 NCC = 0.91	Frame Rate conversion (20fps)	 PSNR = 49.99	 NCC = 0.95
Frame Resizing (Upscaling to W=429 H = 240)	 PSNR = 51.67	 NCC = 0.99	Frame Resizing (Downscaling to W=114 H = 64)	 PSNR = 48.77	 NCC = 0.94
Temporal redundancy R=6 frames	 PSNR = 49.56	 NCC = 0.97	MPEG Compression	 PSNR = 50.12	 NCC = 0.99

Fig. 5 Watermarked Video Frames (Attacked *blanchardtownhouse*) and Corresponding Extracted watermark (*lena*)

4.3 Comparative Study

The proposed video watermarking scheme for video surveillance applications was tested and compared with the relevant watermarking systems Arab et.al. (Video watermarking for tamper detection of surveillance systems). From Table 1, we infer that the proposed system is more robust when compared to the related system for all kinds of attacks.

Table. 1 Comparison of Proposed Approach with Existing System [1]

Attacks	Existing System [1]			Proposed Approach		
	Tamper Detect	Watermark Extract	NCC	Tamper Detect	Watermark Extract	NCC
Gaussian Noise	NA	NA	NA	Yes	Yes	0.9999
Salt and Pepper Noise	Yes	Yes	0.9995	Yes	Yes	0.9876
Frame Cropping	Yes	Yes	NA	Yes	Yes	0.9789
Frame Insertion	Yes	Yes	0.8885	Yes	Yes	0.9999
Frame Dropping	Yes	Yes	0.905	Yes	Yes	0.9987
Frame Swapping	Yes	Yes	0.999	Yes	Yes	0.9995
Frame Rotation	Yes	Yes	0.9786	Yes	Yes	0.9123
Frame Rate Conversion	NA	NA	NA	Yes	Yes	0.9564
Frame Resizing (Upscaling)	NA	NA	NA	Yes	Yes	0.9964
Frame Resizing (Downscaling)	NA	NA	NA	Yes	Yes	0.9493
Temporal Redundancy	NA	NA	NA	Yes	Yes	0.9756
MPEG Compression	NA	NA	NA	Yes	Yes	0.9912

V. CONCLUSIONS

In this research work, we have designed a new robust Moth – Flame – Rider based Neural Network (MF – ROA – based NN) technique to identify the optimal map for both embedding and extraction in the wavelet domain. The proposed technique is suitable for authenticate the surveillance video frames which can be used for law evidence. The proposed approach satisfies the imperceptibility, robustness and security in all kinds of attacks when compared to the existing system.

REFERENCES

1. F. Arab, S.M. Abdullah, S. Z. M. Hashim, A. A. Manaf and M. Zamani, “A robust video watermarking technique for the tamper detection of surveillance systems”, Multimedia Tools and Applications, vol. 75, no. 18, pp.10855-10885, 2016.
2. R. D. Patil and S. Metkar, “Fragile video watermarking for tampering detection and localization”, IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 1661-1666, August 2015.
3. A. Rajpal, A. Mishra and R. Bala “A Novel fuzzy frame selection based watermarking scheme for MPEG-4 videos using Bi-directional extreme learning machine”, Applied Soft Computing, vol. 74, pp.603-620, 2019.
4. A. Sake and R. Tirumala, “Bi-orthogonal wavelet transform based video watermarking using optimization techniques”, Materials Today: Proceedings, vol. 5, no. 1, pp.1470-1477, 2018.
5. K. Meenakshi, K.S. Prasad and C.S. Rao, “Development of Low-Complexity Video Watermarking With Conjugate Symmetric Sequency–Complex Hadamard Transform”, IEEE Communications Letters, vol. 21, no. 8, pp.1779-1782, 2017.
6. T. Dutta, and H.P. Gupta, “A robust watermarking framework for High Efficiency Video Coding (HEVC)–Encoded video with blind extraction process”, Journal of Visual Communication and Image Representation, vol. 38, pp.29-44, 2016.
7. M. Asikuzzaman, M. J. Alam, A. J. Lambert and M.R. Pickering, “Robust DT CWT-based DIBR 3D video watermarking using chrominance embedding”, IEEE Transactions on Multimedia, vol. 18, no. 9, pp.1733-1748, 2016.

8. F. Madine, M. A. Akhaee, and N. Zarmehi, "A multiplicative video watermarking robust to H. 264/AVC compression standard", Signal Processing: Image Communication, vol. 68, pp.229-240, 2018.
9. X. Liu, R. Zhao, F. Li, S. Liao, Y. Ding and B. Zou, "Novel robust zero-watermarking scheme for digital rights management of 3D videos", Signal processing: Image communication, vol. 54, pp.140-151, 2017.
10. A. Loganathan and G. Kaliyaperumal,"An adaptive HVS based video watermarking scheme for multiple watermarks using BAM neural networks and fuzzy inference system", Expert Systems with Applications, no. 63, pp.412-434, 2016.
11. H. Mareen, J. D. Praeter, G. V. Wallendael and P. Lambert, "A novel video watermarking approach based on implicit distortions", IEEE Transactions on Consumer Electronics, vol. 64, no. 3, pp.250-258, 2018.
12. B. Goel, and C. Agarwal, "An optimized un-compressed video watermarking scheme based on svd and dwt", IEEE Sixth International Conference on Contemporary Computing (IC3), pp. 307-312, August 2013.
13. L. Wei, "A improved video watermarking scheme based on spread-spectrum technique", IEEE International Conference on Networking and Digital Society, vol. 1, pp. 511-514, May 2010.
14. D. Binu and B.S. Kariyappa, "RideNN: A New Rider Optimization Algorithm-Based Neural Network for Fault Diagnosis in Analog Circuits", IEEE Transactions on Instrumentation and Measurement, vol. 99, pp.1-25, 2018.
15. S. Mirjalili, "Moth-Flame Optimization Algorithm: A Novel Nature-inspired Heuristic Paradigm", Knowledge-Based Systems, vol.89, pp.228-249, November 2015.
16. Caviar dataset, http://groups.inf.ed.ac.uk/vision/CAVIAR/CAVIARDATA1/ accessed on July 2019.

AUTHORS PROFILE

Satish D Maliis currently working as a Lecturer in the Puranmal Lahoti Government Polytechnic, Latur Maharashtra. He is also pursuing his PhD in Video watermarking as an External Part Time Scholar in Vellore Institute of Technology, Vellore Tamilnadu, India**.**His areas of interests includes Image processing, Image and Video watermarking, etc.

Agilandeeswari Lcompleted her PhD and working as HOD & Associate Professor in the Department of Digital Communications, School of Information Technology & Engineering (SITE), VIT Vellore. She received her Bachelor's degree in Information Technology and Master's in Computer Science and Engineering from Anna University during 2005 and 2009 respectively.She got best researcher award for the past four years from 2015 to till date. She is having around 13+ years of teaching experience and published 50+ papers in the peer reviewed reputed journals. Her reputed publications includes research articles in peer reviewed journals namely Expert Systems with Applications, Journal of Ambient Intelligence and Humanized Computing, Multimedia Tools and Applications, Journal of Applied Remote Sensing indexing at Thomson Reuters with average impact factor of 5. She is the peer reviewer in journals include IEEE Access, Journal of Super computing, International journal of Fuzzy Systems, Array, Artificial Intelligence Review, Informatics in Medicine Unlocked, Neuro computing, Computers and Electrical Engineering, Journal of King Saud University – Computer and Information Sciences, IET ReView, Journal of Engineering Science and Technology (JESTEC), etc. She also published about 13 engineering books as per Anna University Syllabus. She is a life time member in Computer Society of India. Her areas of interests include Image and video watermarking, Image and Video processing, Neural networks, Fuzzy Logic, Machine Learning, Cryptography, IoT, Information Centric Networks and Remote Sensing.