A Novel DWT Based Invisible Watermarking Technique for Digital Images

M.Mohamed Sathik¹ and S.S.Sujatha²

¹Sadakathullah Appa College, Tirunelveli ,India

²S.T. Hindu College, Nagercoil, India.

Abstract: With the rapid development of internet and multimedia technology, the requirement of copyright protection becomes more and more urgent. Digital Watermarking is a technique which finds solution to this problem. The aim of this paper is to propose an innovative watermarking scheme which utilizes the perceptual information of the image content to generate watermark. According to this, the disparity values between low frequency subband of wavelet domain and the rescaled version of original image are identified as the watermark and are disordered with the help of Arnold Transform. The operation of embedding and extraction of watermark is done in high frequency domain of Discrete Wavelet Transform since small modifications in this domain are not perceived by human eyes. This watermarking scheme deals with the extraction of the watermark information in the absence of original image, hence the blind scheme was obtained. Peak Signal to Noise Ratio (PSNR) and Similarity Ratio (SR) are computed to measure image quality. In addition, the competency of the proposed method is verified under common image processing operations and a comparative study is made against our previous technique [8].

Keywords: Robust watermarking, Discrete Wavelet Transform, Arnold Transform, Fibonacci Transform, Content based watermarking.

Received November 28, 2010; Accepted November 4, 2011

1. Introduction

The internet is an excellent distribution system for the digital media because of its inexpensiveness and efficiency. The use of internet and wireless applications has made it easy and fast to transmit data and with the availability of powerful computing, unauthorized operations such as digital copying and tampering of data can be performed relatively easily. As a result, there is the need for authentication digital to secure images. watermarking is a technique which embeds additional information called digital signature or watermark into the digital content in order to secure it. A watermark is a hidden signal added to images that can be detected or extracted later to make some affirmation about the host image. The commonly used watermarking applications include copyright related applications, medical forensic and military applications and content authentication applications.

The major point of digital watermarking is to find the balance among the aspects such as robustness to various attacks, security and invisibility. The invisibleness of watermarking technique is based on the intensity of embedding watermark. Better invisibleness is achieved for less intensity watermark. So we must select the optimum intensity to embed watermark. In general there is a little trade off between the embedding strength (the watermark robustness) and

quality (the watermark invisibility). Increased robustness requires a stronger embedding, which in turn increases the visual degradation of the images. For a watermark to be effective, it should satisfy the features such as imperceptibility, readily extractable, unambiguous and Robustness.

The digital image watermarking scheme can be divided into two categories. They are visible digital image watermarking and invisible image watermarking techniques. In visible watermarking, the information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the original document. In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such. Further, the invisible watermarks are categorized into watermarking techniques as fragile and robust.

Generally, a robust mark is used for copyright protection and ownership identification because they are designed to withstand attacks such as common image processing operations, which attempt to remove or destroy the mark. One solution to ownership protection is digital watermarking based on techniques for embedding a low energy signal (watermark) in an original multimedia data or host (i.e. audio, image and video data) in such a way that the perceptual quality is not degraded. These algorithms ensure that the image processing operations do not erase the embedded watermark signal.

On the other hand a fragile or semi-fragile watermark and integrity verification because they are very sensitive to attacks, i.e., it can detect slight changes to the watermarked image with high probability. In this case, the watermark breaks as soon as any processing is applied to the watermarked signal.

Several methods have been proposed in literature. A survey is in [7]. Two categories of Digital watermarking algorithms are spatial-domain techniques and frequency-domain techniques. Least Significant Bit (LSB) is the simplest technique in the spatial domain techniques [5] which directly modifies the intensities of some selected pixels. The frequency domain technique transforms an image into a set of frequency domain coefficients [4]. The transformation adopted may be discrete cosine transform (DCT), discrete Fourier transforms (DFT) and discrete wavelet transforms (DWT) etc. After applying transformation, watermark is embedded in the transformed coefficients of the image such that watermark is not visible. Finally, the watermarked image is obtained by acquiring inverse transformation of the coefficients.

In feature based watermarking scheme, watermark is generated by applying some operations on the pixel value of host image rather than taking from external on secure Recent researches source. digital watermarking techniques have revealed the fact that the content of the images could be used to improve the invisibility and the robustness of a watermarking scheme [13]. In the proposed watermarking scheme, watermark is created from the content of the host image and discrete wavelet transform (DWT) is used for embedding watermarks, since it is an excellent time-frequency analysis method, which can be well adapted for extracting the information content of the image [6]. A detail survey on wavelet based watermarking techniques can be found in [14].

To improve the security, Wang et.al [8] adopt a key dependent wavelet transform. To take the advantage of localization and multiresolution property of the wavelet transform, Wang and Lin [10] proposed wavelet tree based watermarking algorithm. Tao et al.[9] put forward a discrete-wavelet transform based multiple watermarking algorithm. The watermark is embedded into LL and HH subbands to improve the robustness. Luo et al.[3] introduced an integer wavelets based watermarking technique to protect the copyright of digital data by utilizing encryption technique to enhance the security.

Yuan et al.[15] proposed an integer wavelet based Multiple logo watermarking scheme. The watermark is permuted using Arnold transform and is embedded by modifying the coefficients of the HH and LL subbands. Lin et al.[2] put forward a DWT based blind watermarking scheme by scrambling the watermark using chaos sequence. Many of the algorithms proposed meet the imperceptibility requirement quite easily but robustness to different image processing

are mainly applied to content authentication attacks is the key challenge and the algorithms in literature addressed only a subset of attacks.

This paper proposes a novel frequency domain based blind robust watermarking scheme, in which watermark is constructed from the spatial domain and is embedded in the high-frequency band. According to this algorithm, a DWT is performed on the host image and values in LL1 subband forms the first matrix. The second matrix is formed by finding average values from every 2x2 blocks. Watermark construction process finds the disparity values between those two matrices and is converted into a binary matrix. The resultant matrix is disordered with the help of Arnold Transform. The extraction is done without using original image. This method is robust against many common image attacks and experimental results verify this. The security of the proposed method lies on the multifaceted procedure used to construct watermark.

The rest of this paper is organized as follows: Section 2 gives an overview of Discrete Wavelet Transform, Arnold Transform and the previous method. The details of watermark generation, embedding and extraction processes are explained in Section 3. Section 4 shows experimental results and discussion. Finally section 5 provides concluding remarks.

2. Related Background

This section briefly describes the techniques and methods that have been adopted by the watermarking schemes, including DWT, Scrambling using Arnold Transform, Fibonacci Transform and watermark construction process adopted in our previous watermarking algorithm.

2.1. Discrete Wavelet Transform

The DWT decomposes input image into four components namely LL, HL, LH and HH where the first letter corresponds to applying either a low pass frequency operation or high pass frequency operation to the rows, and the second letter refers to the filter applied to the columns [12], which is shown in Figure 1. The lowest resolution level LL consists of the approximation part of the original image. The remaining three resolution levels consist of the detail parts and give the vertical high (LH), horizontal high (HL) and high (HH) frequencies. In the proposed algorithm, watermark is embedded into the host image by modifying the coefficients of high-frequency bands i.e. HH subband.

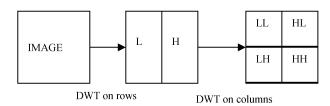


Figure 1. DWT decomposition of image.

For a one level decomposition, the discrete twodimensional wavelet transform of the image function f(x, y) can be written as [1]

$$LL = [(f(x,y)*\phi(-x)\phi(-y))(2n,2m)]_{(n,m)\in z^{2}}$$

$$LH = [(f(x,y)*\phi(-x)\psi(-y))(2n,2m)]_{(n,m)\in z^{2}}$$

$$HL = [(f(x,y)*\psi(-x)\phi(-y))(2n,2m)]_{(n,m)\in z^{2}}$$

$$HH = [(f(x,y)*\psi(-x)\psi(-y))(2n,2m)]_{(n,m)\in z^{2}}$$

where ϕ (t) is a low pass scaling function and ψ (t) is the associated band pass wavelet function.

2.2. Arnold Transform & Fibonacci Transform

A digital image can be considered as a two unit function f(x,y) in the plane Z. It can be represented as Z = f(x, y) where $x, y \in \{0,1,2,3...N-1\}$ and N represents order of digital image. In order to enhance the security, a scrambled version of the image matrix can be changed into a new matrix by the Arnold transform or Fibonacci Transform. Arnold Transformation is a mapping function which changes a point (x, y) to another point (x^1, y^1) by the equation (1), whereas Fibonacci Transformation obtains new points as defined in equation (2).

$$\begin{bmatrix} x^1 \\ y^1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mod N \tag{1}$$

$$\begin{bmatrix} x^1 \\ y^1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mod N \tag{2}$$

2.3. Overview of Previous Method [8]

This section briefly describes about the watermarking generation algorithm of our previous work [8]. The watermark is generated from the spatial domain information. It includes the following steps:

- The original image X of size M x N is partitioned into non-overlapping blocks of size 2 x 2.
- Compute one feature value from each block using equation (3)

$$M_{b}(p,q) = \frac{\sum_{i=1}^{2} \sum_{j=1}^{2} X(p*2+i,q*2+j)}{4}$$
 (3)

where $0 \le p \le M/2$, and $0 \le q \le N/2$.

- Perform Fibonacci Transformation for three times to scramble the elements and obtain the matrix $M_f(p,q)$.
- Find median value M_d for the elements in $M_f(p,q)$.
- Form the watermark pattern to be embedded into original image as

$$W(p,q) = \begin{cases} 0 & \text{if } M_f(p,q) > M_d \\ 1 & \text{otherwise} \end{cases}$$

• The resultant matrix has size M/2 x N/2, which is the watermark pattern to be embedded into original image.

In this method, watermark is generated by performing some operations on image pixels rather than taking from external source, hence the name feature based watermark. This watermark is embedded in the HH1 subband of the original image and resultant image is called watermarked image. This embedded watermark is extracted in detection phase, and is compared with the calculated watermark to decide authenticity.

3. Proposed Method

In the proposed scheme, there are three significant phases: Watermark generation, Watermark embedding and Watermark Detection. The watermark is generated from pixel value of original image and so there is no need of external image or logo. Hence it is necessary to devise a method to generate watermark. The resolution of watermark is assumed to be half of that of original image.

For embedding the watermark, a 1-level Discrete Wavelet Transform is performed. Watermark information is embedded in the high frequency bands (HH1) since it is robust against various normal image processing and malicious attacks. In detection phase, watermark is once again generated from watermarked image and also extracted the embedded watermark from HH1 subband. Comparison is made between those watermarks to decide authenticity.

3.1. Watermark generation

The watermark pattern is generated from the content information of host image. Watermark generation procedure includes the following steps and is shown in figure 2.

- Consider the original image P of size M x M.
- Perform 1-level DWT on the original image and acquire the LL1 component, which is of size M/2 x M/2. Let this matrix be 'A'.

- A reduced size (M/2 x N/2) image 'B' is obtained from original image by performing the following steps.
- 1) Partition the original image into non- overlapping blocks of size 2x2.
- 2) One feature value from each block is calculated according to equation (4).

$$B(x, y) = \frac{\sum_{i=1}^{2} \sum_{j=1}^{2} P(x * 2 + i, y * 2 + j)}{4}$$
 (4)
where $0 \le x \le M/2$, and $0 \le y \le N/2$.

- Find the difference between A and B. Let it be C.
- A binary sequence 'W' can be obtained by applying the following constraint.

$$W(x, y) = \begin{cases} 0 & \text{if } C(x, y) \text{ is even} \\ 1 & \text{otherwise} \end{cases}$$

• Disorder the matrix 'W' with the help of Arnold Transform, the resultant is the required watermark pattern to be embedded in to the host image.

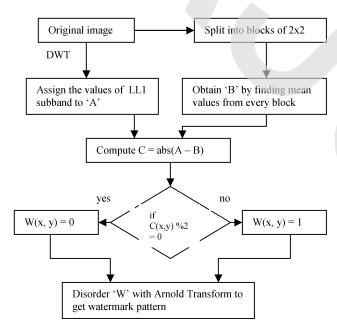


Figure 2. Watermark Generation Procedure

3.2. Watermark embedding

The watermark is embedded in the high frequency subband of DWT as follows:

- Apply 1-level DWT to original image.
- It divides the image into four parts namely LL1, HL1, LH1 and HH1.
- The HH1 part is replaced with the watermark.
- Perform inverse wavelet transform to obtain the watermarked image.

3.3. Watermark Detection

Proposed watermarking scheme extracts and generates watermark information from watermarked image and so original image is not essential. So it can be referred as blind watermarking.

The authentication process includes the following steps:

- Watermark is derived from the content of watermarked image using the steps described under watermark generation in section 3.1.
- Apply 1-level DWT to the watermarked image and extract the embedded watermark from HH1 subband.
- Compare the two watermarks (derived and extracted). If two values match, authenticity is preserved. Otherwise the authenticity is suspected.
- Quality of watermarked image and the watermark is found out according to equation (5) and (7).

4. Experimental Results

In this paper, we consider the images with number of rows and columns are of equal size since the embedded watermark is a square matrix. For testing, the size of the original image is considered as 512x512. Figure 3 (a) shows original image. A 256x256 binary watermark signal is constructed from original image and is embedded within itself. The proposed method is tested using MATLAB.

After embedding the watermark, there is no visual difference between the original and watermarked images. Figure 3(b) shows watermarked image. The absolute difference of the pixel intensities of the watermarked image and the original image is shown in figure 3(c). The difference image shows that the technique ensures high degree of fidelity.



(a) Original Image.



(b) Watermarked Image.



(c) Difference Image.

Figure 3. Test results.

The visual quality of watermarked and attacked images is measured using the Peak Signal to Noise Ratio, which is defined in equation (5). The PSNR value of watermarked image is 59.1168, which indicates that there is very little deterioration in the quality of original image. So, the watermark embedding process produced high-quality watermarked images.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{5}$$

where MSE is Mean Squared Error between original and distorted images, which is defined in equation (6).

$$MSE = \sum_{i=0}^{M-1N-1} \frac{[OI(i,j) - DI(i,j)]^2}{MxN}$$
 (6)

where OI is original image and DI is the distorted image. The MSE value computed by proposed method is 0.0797, which is a very least value.

A comparison between extracted and original watermark can be done by computing Similarity Ratio (SR) between these two patterns as defined in equation(7), which is the metric used for identifying robustness of the watermarking process.

$$SR = \frac{S}{S+D} \tag{7}$$

where 'S' denotes number of matching pixel values and 'D' denotes number of different pixel values. In the proposed scheme, similarity ratio evaluated between extracted and calculated watermark is 0.8496 which indicates that the number of matching pixels are quite high and hence authenticity is preserved. The simulation results of our previous Method [8] and the proposed one are exposed in Table 1.

Table 1. Quality Evaluation of Watermarking Schemes

Metric used	Method [8]	Proposed
PSNR	54.1047	59.1168
MSE	0.2527	0.0797
SR	1	0.8496

The data provided in Table 1 illustrates that the invisibleness of watermark is high in the proposed method, whereas a high robustness is achieved in our previous method.

Table 2. Assessment of PSNR under Attacks.

Attacks		PSNR (dB)	
		Method [8]	Proposed
Adding Gaussian noise	0.01, 0	37.8092	38.3272
(mean, variance)	0, 0.001	30.0770	30.0997
Adding Salt & Pepper noise	0.002	31.8352	32.1381
Median filtering	3x3	29.5819	29.5727
Linear filtering	3x3	27.7808	27.7761
Salt & pepper noise and Median Filtering	0.002 3x3	29.5995	29.5891
Salt & pepper noise and Linear Filtering	0.002 3x3	27.6109	27.5918
Gaussian noise and Median filtering	0, 0.001 3x3	29.3644	29.3649
Gaussian noise and Linear filtering	0, 0.001 3x3	27.4947	27.4988
Image Adjustment		18.7003	18.5312
Blurring		37.8265	37.8322
Histogram Equalization		19.0083	19.0944
JPEG (Quality Factor)	90	43.0162	43.1448
	70	37.4432	37.4799
	50	35.2062	35.4799
	30	33.1842	33.2002
	10	29.1816	29.1867
Scaling (512-256-512)		51.0944	56.1065
Rotation	5°	13.9454	13.9492
	10°	12.0291	12.0325

In the proposed as well the previous watermarking techniques, the watermarked image has been subjected to several types of image manipulations including compression, additive noises, filtering. adjustment, scaling and rotation. Using image compression before storing and transmitting images is very common. So we evaluated the robustness of the proposed scheme by compressing the watermarked images with different JPEG quality factors. The robustness of proposed method has been evaluated by Gaussian noise with mean=0 adding variance=0.001 and Salt&Pepper noise with density 0.002 on the watermarked images.

Also filtering such as median filtering, linear filtering, histogram equalization and blurring has been applied on the watermarked image and the robustness of the watermarking scheme has been tested. The intensity values of watermarked image are adjusted to new values such that 1% of data are saturated at low and high intensities. Also a clockwise rotation with cropping operation has been applied on the image. Apart from those individual attacks, both the algorithms have been executed under combined operations such as additive noises and filtering. Results of the metrics Peak Signal to Noise Ratio and Similarity Ratio on the test image 'cameraman' are shown in Table 2 & 3 respectively.

The imperceptibility of watermark in the proposed method has been evaluated against incidental attacks by using the metric PSNR and compared with [8]. A comparative study on Table 2 reveals the fact that the quality of watermarked image under various incidental image processing operations is more or less similar in both methods.

Robustness of the proposed method under the common image processing operations has been identified with the help of Similarity Ratio and is compared against our previous method [8]. Table 3 shows the experimental results. The simulation results of both methods in the case of additive Gaussian noises show that the robustness of watermark is high with constant variance 0. An increase in variance slightly affects the robustness in both cases. The watermarked image is attacked with salt & pepper noise with density 0.002, the results obtained show that both techniques are highly robust in this case. An analytical study demonstrates that the watermark in previous method [8] shows more robustness than the proposed one under such kinds of attacks.

Watermarked image is smoothed with a 3x3 median filter. Experimental results disclose that the proposed technique is more robust than the technique in [8]. Similar is the case with linear filtering. Experimental results against Image adjustment and Histogram equalization attacks reveal that the robustness of watermark is high in both the methods.

A Gaussian lowpass filter of size 3x3 and a standard deviation sigma 0.5 is applied on the image. Similarly

the watermarked image is compressed with lossy JPEG compression by applying the quality factor from 10 to 90. Experimental results of the proposed system against the operations such as blurring, histogram equalization, JPEG compression and scaling show a high Similarity Ratio than [8], which in turn indicates that the robustness of currently devised technique is higher than the previous method. For the rotation with cropping operation, the observed results dictate that the robustness of the proposed method is better than that of the previous one.

Table 3. Assessment of SR under Attacks.

Attacks		Similarity Ratio	
		Method [8]	Proposed
Adding Gaussian noise	0.01, 0	1	0.8371
(mean, variance)	0, 0.001	0.5229	0.5042
Adding Salt & Pepper noise	0.002	0.9880	0.8370
Median filtering	3x3	0.5200	0.6629
Linear filtering	3x3	0.5300	0.6696
Salt & pepper noise and Median Filtering	0.002 3x3	0.4595	0.6635
Salt & pepper noise and Linear Filtering	0.002 3x3	0.4863	0.6672
Gaussian noise and Median filtering	0, 0.001 3x3	0.3982	0.5449
Gaussian noise and Linear filtering	0, 0.001 3x3	0.4381	0.5600
Image Adjustment		0.8434	0.8435
Blurring		0.6656	0.8083
Histogram Equalization		0.7645	0.7598
JPEG (Quality Factor)	90	0.4665	0.6488
	70	0.4717	0.6956
	50	0.4708	0.7418
	30	0.4730	0.7736
	10	0.4734	0.8158
Scaling (512-256-512)		0.4991	0.8463
Rotation	5°	0.5191	0.7135
	10°	0.4865	0.6957

5. Conclusion

In this paper, we proposed a new robust watermarking scheme, which provides a complete algorithm that embeds and extracts the watermark information effectively. In this method, a binary watermark pattern was constructed from the content of the host image itself and was disordered with the help of Arnold Transform. The watermark embedding process does not degrade the visual quality of the image. The designed method makes use of the Discrete Wavelet Transform which provides a frequency spread of the watermark within the host image. Moreover the authentication process provides qualities like imperceptibility, The robustness security. and algorithm was tested with several standard test images and the experimental results demonstrated that it created high quality images and it was robust versus different attacks. Moreover the simulation results of currently devised method are compared with that of our previous work [8], the results obtained show that the proposed technique is highly robust against attacks such as image adjustment, blurring, histogram

equalization, compression, scaling, rotation and that of combined attacks. Future work will aim at making suitable enhancements to identify malicious attacks.

References

- [1] Kumar S., Raman B., Thakur M. "Real Coded Genetic Algorithm based Stereo image Watermarking", IJSDIA, Vol. 1 No.1 pp 23-33, 2009.
- [2] Lin. Q, Liu Z., Feng G. "DWT based on watermarking algorihthm and its implementing with DSP", IEEE Xplore, pp. 131-134, 2009.
- [3] Luo Y., et al. "Study on digital elevation mode data watermark via integer wavelets", Journal of software, 16(6), pp.1096-1103, 2005
- [4] Parthasarathy A.K., Kak S. "An Improved Method of Content Based Image Watermarking", IEEE Transaction on broadcasting, Vol.53, no.2, pp.468-479, June 2007.
- [5] Podilchuk C.I., Delp E.J. "Digital watermarking: algorithms and applications" IEEE Signal Processing Magazine, pp. 33-46, July 2001.
- [6] Reddy R., et al. "Robust Digital Watermarking of Color Images under Noise Attacks", International Journal of Recent Trends in Engineering, Vol.1, No. 1, May 2009.
- [7] Rey C., Dugelay J. "A survey of watermarking algorithm for Image authentication", Journal on Applied Signal Processing, Vol.6, pp.613-621, 2002.
- [8] Sujatha S.S., Sathik M.M. "A Novel Pixel Based Blind Watermarking Algorithm by Applying Fibonacci Transform", Proc. of ACM, The First Amrita ACM-W Celebration of Women in Computing (A2CWIC 2010), pp.197-202, Sept 2010.
- [9] Tao P., Eskicioglu A.M. "A robust multiple watermarking scheme in the discrete wavelet transform domain", Proceedings of the SPIE, Vol.5601, pp.133-144, 2004.
- [10] Wang S.H., Lin Y.P. "Wavelet Tree quantization for copyright protection for watermarking", IEEE Trans. Image Process, pp.154-165, 2002.
- [11] Wang Y., Doherty J.F., Dyck V.R.E.. "A wavelet-based watermarking algorithm for ownership verification of digital images", IEEE Trans. Image Process, 11, pp.77-88,2002.
- [12] Xia X., Boncelet G. "Wavelet Transform based watermark for digital images", OPTICS EXPRESS, Vol.3, No.12, pp 497-511, 1998.
- [13] Xie L., et al. "A class of authentication digital watermarks for secure multimedia communication IEEE Transactions on Image Processing, Vol.10, No.11, pp.1754-1764.
- [14] Ying Q., Ying W. "A survey of wavelet-domain based digital image watermarking algorithm",

Computer Engineering and Applications, Vol.11, pp.46-49, 2004.

[15] Yuan Y., Huang D., Liu D.: An Integer Wavelet Based Multiple Logo-watermarking Scheme. In IEEE, Vol.2 pp.175-179, 2006.



S.S.Sujatha received the M.C.A degree from Alagappa University, Karaikudi, in 1993 and M.Phil degree from Manonmanium Sundaranar University, Tirunelveli in 2003. She is working as an Associate Professor in Department

Computer Science at S.T.Hindu College, Nagercoil, India since 1994. Currently she is a Ph.D candidate at Mother Teresa Womens University, India. She has presented fifteen papers in National and International conferences and Journals. Her current research interest focuses on digital Image Processing, Digital watermarking and image authentication.



M.Mohamed Sathik received the M.Sc (Mathematics) degree from Bharathidhasan University in 1986, and the M.Phil and Ph.D. in Computer Science degrees from Manonmanium Sundaranar University in 1997 and 2006

respectively. Currently he is the Principal of Sadakathullah Appa College, Tirunelveli, India. His research interest includes Virtual Reality Techniques and Digital image processing. He had presented number of papers in National and International conferences and Journals.