ISSN No. 0976-5697

Volume 6, No. 1, Jan-Feb 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Blind Wavelet Based Watermarking Technique for Image Authentication

Dr.S.S.Sujatha
Associate Professor in Computer Science,
South Travancore Hindu College, Nagercoil, India.

Abstract: The central idea of this paper is to propose an innovative wavelet based watermarking scheme which embeds watermark signal into the host image in order to authenticate it. In this novel technique, some pixels are randomly selected from original image, so that all of them have a valid 3x3 neighborhoods. A binary sequence is constructed from those pixels by comparing them against average values of neighborhoods. The binary sequence is then converted into a watermark pattern in the form of a Toeplitz matrix to improve security of watermarking process and is then embedded within the host image. 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. A blind watermarking scheme is attained because the extraction of the watermark information is done in the absence of original image**.** The proposed algorithm is more secure and robust against most of the common image processing attacks. Finally computer simulations demonstrate that the proposed method is better than the recent algorithm proposed in [1] by Lin Q. et al. in terms of Peak Signal to Noise Ratio.

Keywords: Digital watermarking, Discrete Wavelet Transform, Toeplitz Matrix, Image Authentication, Content based watermarking.

I. INTRODUCTION

Now-a-days, the Internet plays an important role in distributing digital contents in an excellent, efficient and inexpensive way. Since the digital contents are easily used, processed and transmitted, it causes severe problems such as modification, unauthorized use and exploitation of digital content. Hence, the reseachers focuses on the need for authentication techniques to secure digital images. Digital 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.

Several methods for authenticating digital content have been proposed in literature by many researchers. A survey is in [2]. Digital watermarking algorithms are categorized into two namely: spatial-domain techniques and frequency-domain techniques. The simplest technique is the Least Significant Bit (LSB) method in the spatial domain [3] 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 [5].

A detail survey on wavelet based watermarking techniques can be found in [6]. Luo et al.[7] introduced an integer wavelets based watermarking technique to protect the copyright of digital elevation mode data. The method utilized encryption technique to lift the security. In oreder to enhance the robustness and security of the embedded watermak, Wei P. et al. [8] generated a chaotic sequence by coupled Chebyschev map, and the original binary watermark is masked by the chaotic sequence. Yuan et al.[9] 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.[1] put forward a DWT based blind watermarking scheme by scrambling the watermark using chaos sequence and embedded the watermark in LL1 subband. Many of the algorithms proposed have utilized an external image as the watermark and meet the imperceptibility requirement quite easily. The ability to withstand against to different image processing attacks is the key challenge and the algorithms in literature addressed only a subset of attacks. Moreover, combinations of incidental image processing operations were not taken into account.

This paper proposes a novel DWT based blind watermarking scheme, which shows robustness against incidental image processing attacks and their combinations. The watermark is constructed from the spatial domain, which ensures the uniqueness of the watermark and is embedded in the high-frequency sub-band. The security of the proposed method lies on the multifaceted procedure used to construct watermark. The watermark construction process selects pixels in a random method and adopts Toeplitz matrix and thereby offer better security. The watermark extraction is done without initial carrier image. This method attains better imperceptibility and is robust against many common image attacks and experimental results verify this.

The rest of this paper is organized as follows: Section 2 introduces the concept behind image representation, neighborhoods, Discrete Wavelet Transform and Toeplitz matrix. Next, Section 3 describes the procedures for watermark generation, embedding and extraction process. Section 4 shows experimental results and discussion. Finally section 5 provides concluding remarks.

II. RELATED BACKGROUND

This section briefly describes the techniques and methods that have been adopted by the proposed scheme,

© 2015-19, IJARCS All Rights Reserved

including image representation and neighborhoods, DWT and watermark construction by Toeplitz matrix.

A. *Image Representation:*

A grey-level image X with size MxN can be defined by X= $[x_p]_{M \times N}$, where $x_p \in \{0, 1, 2, \dots, 255\}$. Here x_p represents the pixel value located at position p(i, j) over X, where $i \in [0, 1, M-1]$ and $j \in [0, 1, N-1]$.

B. *Neighbors:*

Consider a pixel P at coordinates (x, y) has two horizontal and two vertical neighbors whose coordinates are (x+1, y), (x-1, y), (x, y-1), (x, y+1).

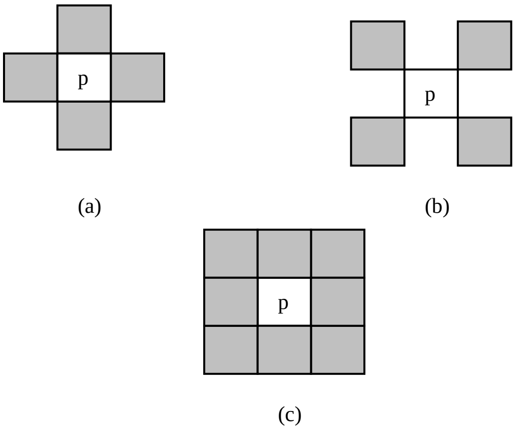


Figure 1. Neighbors of a pixel (a) 4-neighbors (b) Diagonal -neighbors (c) 8-neighbors

This set of 4-neighbors of P is denoted as $N_4(P)$ and is shaded in figure 1(a). The four diagonal neighbors of P have coordinates (x+1, y+1). (x+1,y-1),(x-1,y+1) and (x-1, y-1). These neighbors are denoted as $N_D(P)$ and is shaded in figure 1(b). The union of $N_4(P)$ and $N_D(P)$ form the 8-neighbors of P and is denoted as $N_8(P)$ [10] and is given in figure 1(c).

C. *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 [11], which is shown in figure 2.

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) frequency. In the proposed algorithm, watermark is embedded into the host image by modifying the coefficients of high-frequency bands i.e. HH subband. 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 [12].

For a one level decomposition, the discrete two-dimensional wavelet transform of the image function f(x, y) can be written as [13]

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

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

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

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

Where ϕ (t) is a low pass scaling function and $\psi(t)$ is the associated band pass wavelet function.

D. *Toeplitz Matrix:*

In mathematical discipline of linear algebra, a Toeplitz matrix or diagonal constant matrix is a matrix in which each descending diagonal from left to right is constant. It was named after Otto Toeplitz and is frequently encountered in applications where matrix computation is exploited in order to devise very effective numerical solution algorithm. For instance, a Toeplitz matrix is a square matrix with constant diagonals and for constructing a Toeplitz matrix of order NxN, we need 2N-1 elements [14].

Let P= {a, b, c, d, e, f, g, h, i}. Since there are 9 elements in this vector, a Toeplitz matrix of size 5x5 may be constructed so that its first row is first 5 elements and first column except the first element is last 4 elements, which is given in equation (1). The remaining elements are calculated according to equation (2).

$$\mathrm{T} = \begin{pmatrix} a & b & c & d & e \\ f & a & b & c & d \\ g & f & a & b & c \\ h & g & f & a & b \\ i & h & g & f & a \end{pmatrix} \qquad (1)$$

$$A(i,\ j) = A(i-1,\ j-1) \qquad (2)$$

III. PROPOSED METHOD

The three significant phases in the proposed scheme are Watermark generation, Watermark embedding and Watermark Detection. The primary objective of the proposed work is to generate watermark generated from pixel value of original image and so there is no need of external image or logo. The resolution of watermark is assumed to be half of original image.

A 1-level Discrete Wavelet Transform is performed on the host image and the watermark information is embedded in the high frequency bands (HH1) so as to get the watermarked image. Further, detection phase comprises of three steps: watermark generation from watermarked image, watermark extraction from HH1 subband and comparison of them to decide authenticity.

A. *Watermark Generation:*

Watermark generation procedure constructs the watermark pattern from the spatial domain information by performing the following steps. The framework of watermark generation is shown in figure 2.

a) Consider the original image P of size MxM.
b) Randomly select M-1 elements from P so that all the pixels have valid 3x3 neighborhoods.
c) Let the neighborhoods of the selected pixel P(x, y) are P(x-1, y-1), P(x-1, y), P(x-, y+1), P(x,y+1), P(x+1,y+1), P(x+1,y),P(x+1,y-1), and P(x, y-1)

d) Find average value of those neighborhoods. Let it be $P_a(x, y)$.

e) A binary sequence 'B' can be obtained by applying the following constraint.

$$B_i = \begin{cases} 0 & if \;\; P(x,y) > P_a(x,y) \\ 1 & otherwise \end{cases}$$

where i=1, 2, 3, …, M-1.

f) A Toeplitz matrix of size M/2 x M/2 is constructed from the binary sequence B using the following procedure. First row elements are calculated according to equation (3), first column elements except the first are calculated according to equation (4) and remaining elements are computed by using equation (2).

$$T(1, j) = B(i + j - 1) \qquad (3)$$

$$T(i,1) = B(i + M/2 - 1) \qquad (4)$$

Where $2 \le i \le M/2, \quad and \quad 1 \le j \le M/2$

Now T is the watermark pattern to be embedded within host image.

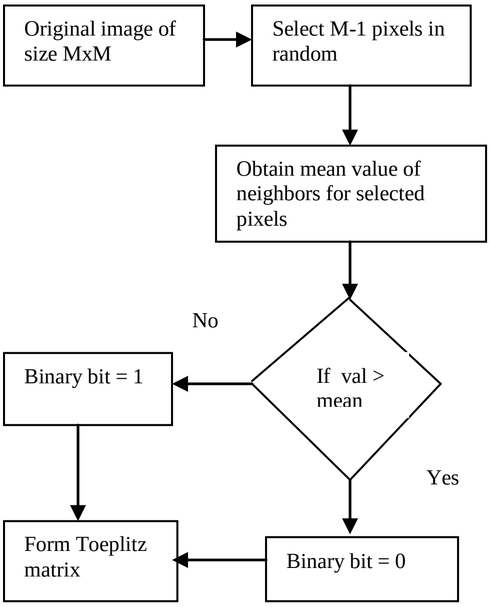

Original image of size MxM
Select M-1 pixels in random
Obtain mean value of neighbors for selected pixels
No
If val > mean
Binary bit = 1
Yes
Form Toeplitz matrix
Binary bit = 0

Figure 2. Watermark generation procedure

B. *Watermark embedding:*

The proposed algorithm embeds watermark in the high frequency subband of DWT by using Haar wavelet as follows:

a) Use 'haar' wavelet and apply 1-level DWT on original image.

b) It decomposes the image into four sub-bands namely LL1, HL1, LH1 and HH1.

c) The watermark is embedded in the high frequency component HH1 of DWT by replacing it with the watermark.

d) Perform inverse wavelet transform to obtain the watermarked image.

C. *Watermark Detection:*

Proposed watermarking scheme extracts the embedded watermark and also regenerates watermark information from the watermarked image. The authentication process includes the following steps:

a) Watermark is derived form the content of watermarked image using the steps described under watermark generation in section 3.1.

b) Apply 1-level DWT to the watermarked image and extract the embedded watermark from HH1 subband.

c) Compare the two watermarks (derived and extracted). If two values match, authenticity is preserved. Otherwise the authenticity is suspected.

d) Quality of watermarked image and the watermark is found out according to equation (5) and (7).

IV. EXPERIMENTAL RESULTS

In this paper, images with equal number of rows and columns are considered since the Toeplitz matrix is a square matrix. The performance of the proposed algorithm is tested on various images under various common image processing attacks. Here, the results are presented for grayscale Leena image of size 512x512. Figure 3(a) shows original image. A 256x256 Toeplitz matrix (binary watermark signal) is constructed from original image and is embedded within itself.

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.

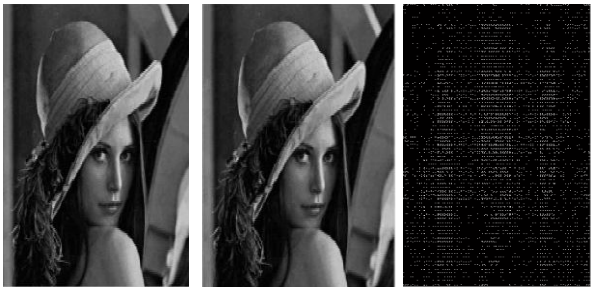


Figure 3. Input and processed images

(a) Original Image b) Watermarked Image (c) Difference Image

The visual quality of original and watermarked images is measured using the Peak Signal to Noise Ratio, which is defined in equation (5). The PSNR value of watermarked image is 46.5921dB, which is greater than the empirical value 35 db and in turn indicates that there is a little deterioration in the quality of original image.

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

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

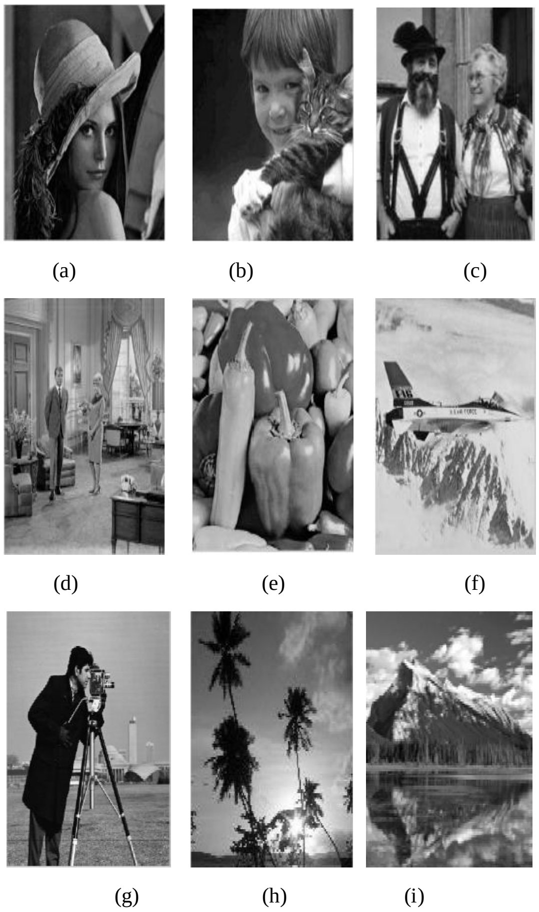
$$MSE = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\frac{[OI(i,j) - DI(i,j)]^2}{MxN} \qquad (6)$$

Where OI is original image and DI is the distorted image.

A comparison between extracted and original watermark is carried out by computing Similarity Ratio (SR) between the two patterns as defined in equation(7).

$$SR = \frac{S}{S+D} \qquad (7)$$

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 0.9803 which indicates that the number of matching pixels is at the maximum and hence authenticity is preserved.


(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Figure 4. Sample Images

(a) Leena (b) Boy (c) Couple (d) House (e) Vegetables (f) Sea (g) Cameraman (h) Tree (i) Cloud

Watermark invisibility and robustness are evaluated on different images. A set of sample images are shown in figure 4. The experimental results obtained for PSNR and SR values are tabulated in Table 1. The calculated PSNR values are greater than 35.00 db, which is the empirical value for the image without perceivable degradation.

Table 1: Performance of the proposed scheme

Picture	PSNR	SR
4.a	46.5921	0.9803
4.b	46.6253	0.9261
4.c	48.1898	0.9768
4.d	46.0477	0.9820
4.e	47.1756	0.9801
4.f	44.9179	0.9725
4.g	43.7014	0.9694
4.h	46.6971	0.9414
4.i	49.2975	0.9379

The attacks chosen are JPEG compression, adding noises such as Gaussian and salt & pepper noises, median filtering, and low pass filtering, rescaling, image adjustment and rotation. Apart from individual attacks, the proposed scheme is experimented with combined attacks such as additive noise and filtering operations. Table 2 gives the performance of proposed watermarking scheme under various attacks.

Table 2: Quality Evaluation of Proposed Scheme

Attacks		PSNR(dB)	SR
No		46.5921	0.9803
JPEG	90%	38.2824	0.7512
	70%	38.2824	0.7785
	50%	36.1642	0.7990
	30%	34.1884	0.8276
Adding Noise	Gaussian noise 0.001	30.1496	0.5044
	Salt & pepper 0.01	24.6911	0.9489
Filtering	Low pass filtering	38.9415	0.8539
	Median filtering	34.5248	0.7227
	Blurring	39.5532	0.8015
Rescaling(512-256-512)		30.4421	0.8145
Image Adjustment		21.3204	0.7509
Rotation with cropping	10^0	11.6206	0.5340
	20^0	10.7030	0.3774
	30^0	10.3672	0.3255
Salt&Pepper and Median filtering		30.5678	0.7978

Simulation results against JPEG compression attack show that a decrease in quality factor decreases the imperceptibility of watermarked image but increases the robustness of watermark. The high value of Similarity Ratio indicates that the proposed method is able to withstand such kind of attacks.

Quality of watermarked image is degraded little in the case of additive Gaussian noise, but the robustness is moderate. The watermarked image is attacked with salt & pepper noise with density 0.01 and observed a less PNSR value, with a high similarity ratio.

Experimental results against Filtering attacks disclose that the robustness of watermark is high with an acceptable PSNR value. In addition, the values obtained for similarity ratio conveys that the proposed method is robust against scaling operation. Simulation results for attack with rotation show that both the imperceptibility of watermarked image and robustness of watermark are degraded.

The performance is verified under combined attacks. Image is first corrupted by salt and pepper noise in which both the black and white points have a probability of occurrence of 0.2. Median filtering is a useful tool for reducing salt and pepper noise in an image. So median filtering is applied to the noisy image and the robustness is observed. The evaluated value of SR indicates that the new scheme is robust against the combined attacks.

The simulations of proposed scheme are compared with the technique in [1] and the results are tabulated in Table 3.

© 2015-19, IJARCS All Rights Reserved

Table 3: Comparison results with [1]

Attacks		**PSNR(dB)**	
		Lin Q.[1]	Proposed
No		36.7350	46.5921
JPEG	90%	34.0694	42.5139
	70%	32.3515	38.2824
	50%	31.3426	36.1642
	30%	30.2435	34.1884
Adding Noise	Gaussian noise 0.001	26.2434	30.1496
	Salt & pepper 0.01	21.9358	24.6911
Filtering	Low pass filtering	28.3791	38.9415
	Median filtering	31.5238	34.5248
Rotation with cropping	10^0	14.0534	11.6206
	20^0	10.7326	10.7030
	30^0	10.5539	10.3672

An observation demonstrates that the proposed scheme attains a greater PSNR values for most of the attacks than [1]. But the performance is slightly degraded in the case of rotation with cropping operation.

V. CONCLUSION

This study has proposed a robust watermarking algorithm, in which the watermark is designed with the help of Toeplitz matrix such that the integrity is proven in the case of some mild image processing operations. Security is enhanced by selecting random pixels and building Toeplitz matrix. The designed method makes use of the HH sub-band of Discrete Wavelet Transform for embedding the watermark since it provides a frequency spread of the watermark within the host image. Moreover qualities like imperceptibility, robustness and security have been realized efficiently.

The performance of the watermarking scheme is evaluated with common image processing attacks such as JPEG compression, adding noises, filtering, scaling and rotation with cropping. The combined attacks are also addressed. Experimental results demonstrate that watermark is robust against most of the attacks with high quality of watermarked image. However the proposed method is not maintaining quality of watermarked images against rotation. Further, the performance of proposed method is compared with a recent existing method and observed fine results. Future work will aim at making suitable enhancements to attain semi-fragile watermarking and detect malicious attacks.

VI. REFERENCES

[1] Lin Q., Liu Z., Feng G., "DWT based on watermarking algorihthm and its implementing with DSP", IEEE Xplore, pp. 131-134, 2009.Dittmann J., "Content-fragile Watermarking for Image Authentication" Proc. of SPIE, Security and Watermarking of Multimedia Contents III, vol.4314, pp.175-184, 2001.

[2] Rey C., and Dugelay J., "A survey of watermarking algorithm for Image authentication," Journal on Applied Signal Processing, Vol.6, pp.613-621, 2002.

[3] Podilchuk C I, and Delp E J., "Digital watermarking: algorithms and applications," IEEE Signal Processing Magazine, pp. 33-46, July 2001.

[4] Parthasarathy A., Kak S., "An Improved Method of Content Based Image Watermarking," IEEE Transaction on broadcasting, Vol.53, no.2, pp.468 -479, June 2007.

[5] Sujatha S S and Mohamed sathik M., "A Novel Technique for Digital Watermarking with Feature Based Disparity Values", International Journal of Advanced Research in Computer Science, Vol.2, No.1, pp.203-207, Jan-Feb 2011.

[6] Ying Q., and Ying W., "A survey of wavelet-domain based digital image watermarking algorithm", Computer Engineering and Applications, Vol.11, pp.46-49, 2004.

[7] Luo Y., Cheng L.Z., Chen B., and Wu Y., "Study on digital elevation mode data watermark via integer wavelets", Journal of software, 16(6), pp.1096-1103, 2005.

[8] Wei P., Zhang W., Yang H. and Haung S., "Combining the Neural network and the Chaotic map to construct Blind Digital Watermarking Scheme", Proceedings of IEEE International Conference on Intelligent Systems Design and Applications", Vol.2, pp.338-341, 2006.

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

[10] Gonzalez R C., Woods R E., and Eddins S L., "Digital Image Processing Using MATLAB", India ,2008.

[11] Xia X., Boncelet C G., and Gonzalo, "Wavelet Transform based watermark for digital images," OPTICS EXPRESS, Vol.3, No.12, pp 497-511, 1998.

[12] Reddy R, Prasad M.V.N., and Rao D S., "Robust Digital Watermarking of Color Images under Noise Attacks" International Journal of Recent Trends in Engineering, Vol.1, No. 1, May 2009.

[13] Kumar S., Raman B., Thakur M, "Real Coded Genetic Algorithm based Stereo image Watermarking," IJSDIA, Vol. 1 No.1 pp 23-33, 2009.

[14] www.mathworks.com/help/matlab/ref/toeplitz.html

Short Bio Data for the Author

Dr.S.S.Sujatha received the M.C.A degree from Alagappa University, Karaikudi, in 1993, M.Phil degree from Manonmanium Sundaranar University, Tirunelveli in 2003 and Ph.D from Mother Teresa Womens University, India. She is working as an Associate Professor in Department Computer Science at S.T.Hindu College, Nagercoil since 1994. She had presented more than fifteen papers in National and International conferences and Journals. Her current research interest focuses on digital watermarking and image authentication.