ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Transformed IRIS Signature fabricated Authentication in Wavelet based Frequency Domain (TISAWFD)

Madhumita Sengupta and J. K. Mandal*
Department of Computer Science and Engineering,
University of Kalyani, Kalyani, Nadia
West Bengal, India.
madhumita.sngpt@gmail.com
jkm.cse@gmail.com

Abstract: In this paper a wavelet based steganographic technique TISAWFD has been proposed to automatically identify or authenticate prosecute to prevent or investigate crime. Secrete cameras or CCTV is used to take inputs from active mob, then iris of every visible eye are located and captured from where only IRIS are fetched and enhanced through scaling. IRIS are then transformed into signature through Hough transform and hide itself inside the documents/images in any of the three frequency components generated by wavelet transform using a secret key and a hash function. Experimental results are computed and compared with the existing steganographic techniques like PMEDF (Guo, 2011) and JIN's method (Jin, 2008) in terms of Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Standard Deviation (SD) and Image Fidelity (IF) which show better performances in TISAWFD.

Keywords: Hough Transform (HT); Wavelet; Transformed IRIS Signature fabricated Authentication in Wavelet based Frequency Domain (TISAWFD); Mean Square Error (MSE); Peak Signal to Noise Ratio (PSNR); Image fidelity (IF).

I. INTRODUCTION

Now a day's where criminal activities are growing rapidly, government of every country is eagerly waiting for new techniques of automation for surveillance. Surveillance is very useful to governments and law enforcement to maintain social control, recognize and monitor threats, and prevent/investigate criminal activity. Many contemporary gadgets such as CCTV, car keychain mini hidden camera, cordless button spy camera, night vision high resolution camera, swan wireless eagle eye, doorphones and many other are used for this purpose of surveillance to trace criminal activities and criminals by identifying them.

To identity individual external and internal parameters may be examined. External parameters includes photograph, birth certificate, school leaving certificate, identity card, library cards, driving licenses, passports, permanent account number and credit cards and so on, where as an internal identity parameters are biometric parameters such as voice, gait, iris and so on. External parameters, used in primordial time, now in digital forms can be tempered where as internal identity parameters also known as biometric characteristics can't be destroyed, stolen or tempered and are used to measure and analyze human physical and/or behavioral characteristics for authentication, identification, or screening purposes [1].

The main objective of this paper (TISAWFD) is collaborating steganography and forensic science by authenticating external parameters/documents/images with person's internal biometric parameter in transformed forms. Any type of document or images can be embedded with biometric characteristics of owner. These biometric characteristics can be categorized on the basis of scrutiny, under two categories, one where prosecute are unaware of the process of detection such as iris recognition from distance or gait analysis, and the other where prosecutes have to involve physically for detection process such as fingerprint, DNA testing, palm print. This technique is concerned with iris based authentication.

Various parametric tests are performed and results obtained are compared with most recent existing techniques such as, PMEDF [2] and JIN's method [3], based on Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), and Image Fidelity (IF) analysis [4] to show a consistent relationship with the existing techniques.

Overall procedure has been described in section II. Results and discussions are outlined in section III, real system applications are given in section IV, conclusions are drawn in section V and references are given at end.

II. THE SCHEME

This paper proposed a frequency domain based steganographic technique TISAWFD, which converts the cover image into its frequency domain through wavelet transform followed by embedding the IRIS signature of the owner obtained through Hough transform into diagonal coefficients of wavelet to authenticate the ownership and authenticity of image/document vise versa.

TISAWFD is divided into two major operations i.e. embedding operation, for generating IRIS signature through Hough transform of IRIS followed by embedding into cover image/document and decoding at receiving end for extraction and detection of IRIS signature to authenticate image/document.

Embedding process divided into five phases. At first IRIS of original owner is captured with high resolution camera and are passed through Sobel operator and thresholding mechanism [5] to generate edges from the IRIS (elaborated in section 2.1). In the next phase, the edges are passed through Hough transform to generate IRIS signature, which always be unique for each IRIS (discussed in section 2.2). The cover image passes through forward wavelet transform to generate four coefficient matrices [6] (elaborated in section 2.3) and 4th matrix is selected to embed the bits of IRIS signature. Inverse wavelet transformation is performed to generate stego-image. The schematic representation of process is given in fig 1.

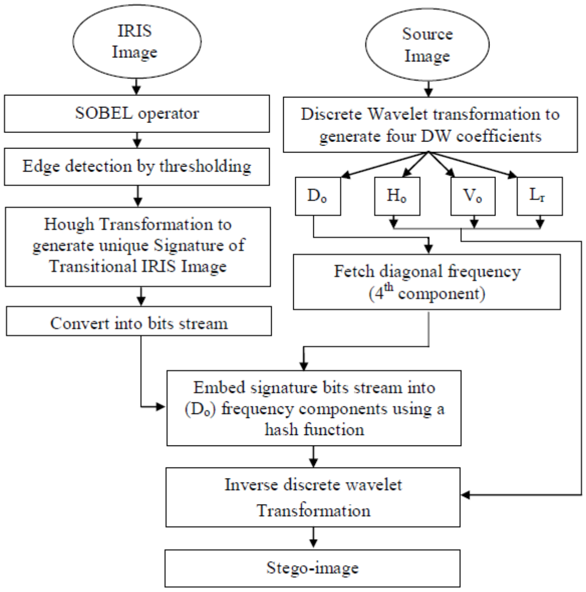

IRIS Image
Source Image
SOBEL operator
Edge detection by thresholding
Hough Transformation to generate unique Signature of Transitional IRIS Image
Convert into bits stream
Discrete Wavelet transformation to generate four DW coefficients
D_o
H_o
V_o
L_r
Fetch diagonal frequency (4th component)
Embed signature bits stream into (D_o) frequency components using a hash function
Inverse discrete wavelet Transformation
Stego-image

Figure 1. Schematic diagram of TISAWFD embedding algorithm

At the receiving end (fig. 2) the setgo-image passes through forward wavelet transformation to generate wavelet coefficients. Embedded bits of IRIS signature is fetched from 4th coefficient matrix using same hash function. Live IRIS image is taken through CCTV camera again passes all the steps to generate IRIS signature. On comparison of the generated IRIS signature verses extracted IRIS signature, image/document or owner may be authenticated or authorized. The same technique may be used in offline also.

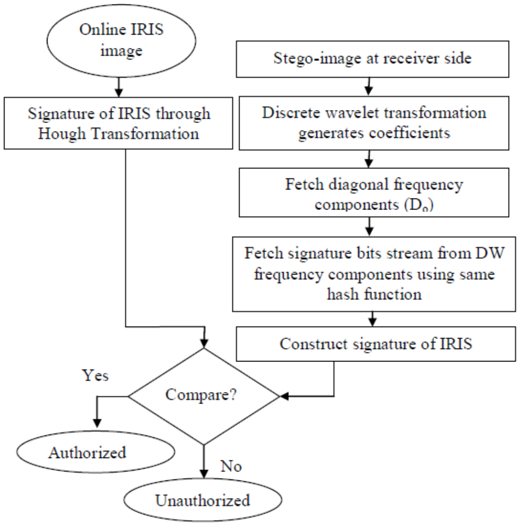
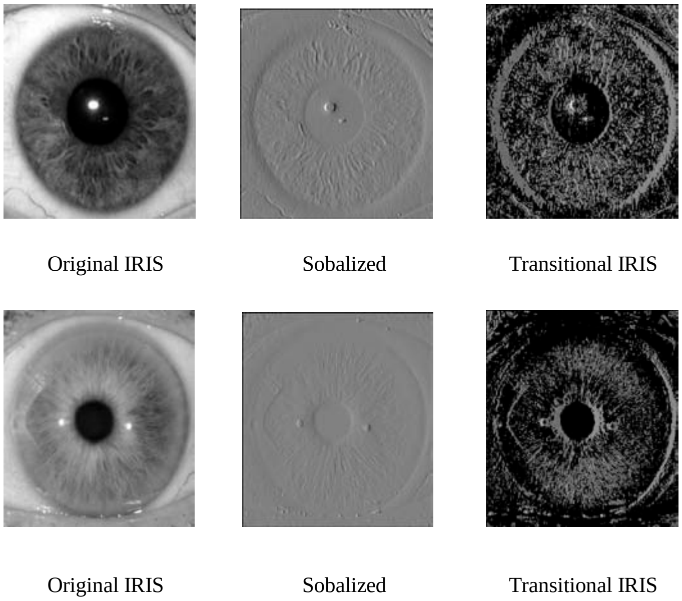

Online IRIS image
Signature of IRIS through Hough Transformation
Stego-image at receiver side
Discrete wavelet transformation generates coefficients
Fetch diagonal frequency components (D_o)
Fetch signature bits stream from DW frequency components using same hash function
Construct signature of IRIS
Yes
Compare?
No
Authorized
Unauthorized

Figure 2. Schematic diagram of TISAWFD extraction algorithm

A. *IRIS Information Extraction:*

IRIS images captured through high resolution camera, and stored in a form of gray scale image, as color information are not of any concern and from those information threshold based information are extracted termed as transitional IRIS image as shown in figure 3.


Original IRIS
Sobalized
Transitional IRIS

Original IRIS
Sobalized
Transitional IRIS

Figure 3. IRIS image, sobealized and IRIS transitional images

B. *Signature Generation*

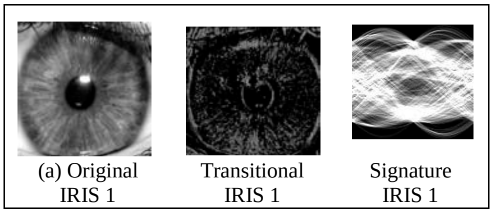
Hough transform is a feature extraction technique used in image analysis and concerned with the identification of lines in the image [7]. The IRIS image passes through a test of identifying the maximum intensity containing information of IRIS.

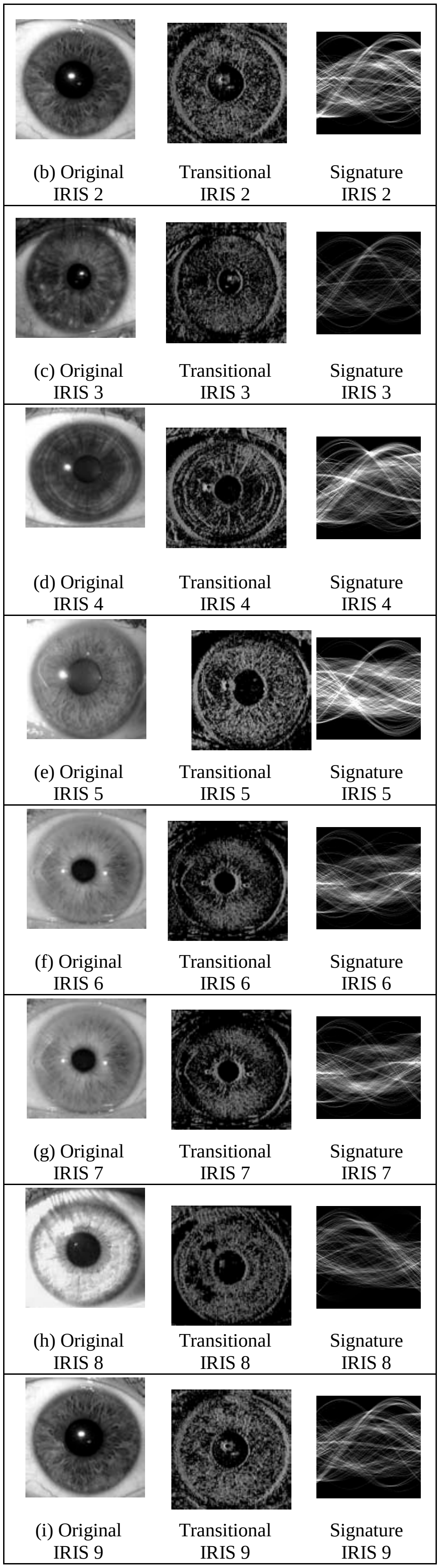
Grayscale image on passing through Hough transformation with threshold and origin as center of image generates a matrix of rho verses theta, by eq 1 and eq 2 where limits are $1 \leq \theta < \pi$ and $-N \leq \rho \leq N$.

$$N = \left(\left(\frac{\sqrt{Row^2 + Col^2}}{2}\right)\right) \qquad (1)$$

$$\rho_i = (x * \cos\theta + y * \sin\theta) \qquad (2)$$

On calculation of ρ for each value of θ and incrementing the matrix value of ρ verses θ a butterfly like structure obtained which is the signature for IRIS image as shown in figure 4. Ten such IRIS images with their transitional IRIS and signatures are given in figure 4.


(a) Original IRIS 1
Transitional IRIS 1
Signature IRIS 1



(b) Original IRIS 2 | Transitional IRIS 2 | Signature IRIS 2

(c) Original IRIS 3 | Transitional IRIS 3 | Signature IRIS 3

(d) Original IRIS 4 | Transitional IRIS 4 | Signature IRIS 4

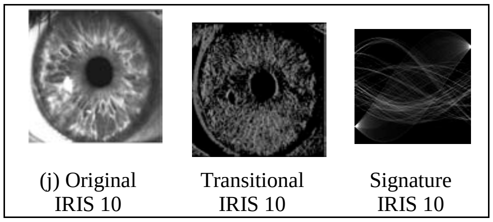
(e) Original IRIS 5 | Transitional IRIS 5 | Signature IRIS 5

(f) Original IRIS 6 | Transitional IRIS 6 | Signature IRIS 6

(g) Original IRIS 7 | Transitional IRIS 7 | Signature IRIS 7

(h) Original IRIS 8 | Transitional IRIS 8 | Signature IRIS 8

(i) Original IRIS 9 | Transitional IRIS 9 | Signature IRIS 9



(j) Original IRIS 10 | Transitional IRIS 10 | Signature IRIS 10

Figure 4. IRIS of dimension 256 x 256 with intermediate image and signature of 128 x 128

C. *Forward Transformation*

Transform equation is available in pair which is reversible and termed as forward and inverse transformation respectively [8]. In Wavelet based forward transformation the image converted from spatial domain to frequency domain using eq (3) and eq (4), and that of inverse transformation, the reverse procedure is followed (eq.(5)). Mathematically the image matrixes multiply with scaling function coefficients and wavelet function coefficients to generate the transformation matrix [9].

$$Y_{Low}[k] = \sum_n x[n].h[2k-n] \qquad (3)$$

$$Y_{High}[k] = \sum_n x[n].g[2k-n] \qquad (4)$$

$$x[n] = \sum_{k=-\infty}^{\infty}\left(Y_{High}[k].g[2k-n]\right) + (Y_{Low}[k].h[2k-n]) \qquad (5)$$

Where x[n] is original signal, h[x] is half band low pass filter, g[x] is half band high pass filter, $Y_{Low}[k]$ is output of high pass filter after sub sampling by 2, $Y_{High}[k]$ is output of low pass filter after sub sampling by 2. Cover images of 512 x 512 dimension are taken and Haar forward transform scaling function coefficients and wavelet function coefficients [9] $H_0 = ½$, $H_1 = ½$, $G_0 = ½$ $G_1 = -½$ are applied. The graphical representation of the results after forward DWT is shown in figure 5.

Low resolution sub-image $\psi(x, y) = \varphi(x)\varphi(y)$	*Horizontal Orientation sub-image* $\psi^H(x,y)=\varphi(x)\psi(y)$
Vertical Orientation sub-image $\psi^V(x, y) = (x)\varphi(y)$	*Diagonal Orientation sub-image* $\psi^D(x,y)=\psi(x)\psi(y)$

Figure 5. Image decomposition in Wavelet transforms

Inverse transformation is just the reverse of the forward transformation with column transformation done first followed by row transformation. But the coefficient values are different for column/row transformation matrices. The coefficient for reverse transformation are $H_0 = 1$, $H_1 = 1$, $G_0 = 1$, $G_1 = -1$ [9]. Reverse transform generate original image matrix as the technique is reversible.

D. *Embedding*

During first level forward transformation the cover image generates four quarter of frequency matrices as outputs. To embed secret information with minimum distortion diagonal coefficients [6] are used. A hash function is used to generate positions for embedding two bits per byte of coefficients matrix. Positions are selected using formula (B %P) and (B %(P +1)) where P varies from 0 to 4 and B equals to 2 to embed 2 bits of IRIS signature per byte of cover image up to fourth position from LSB towards MSB randomly.

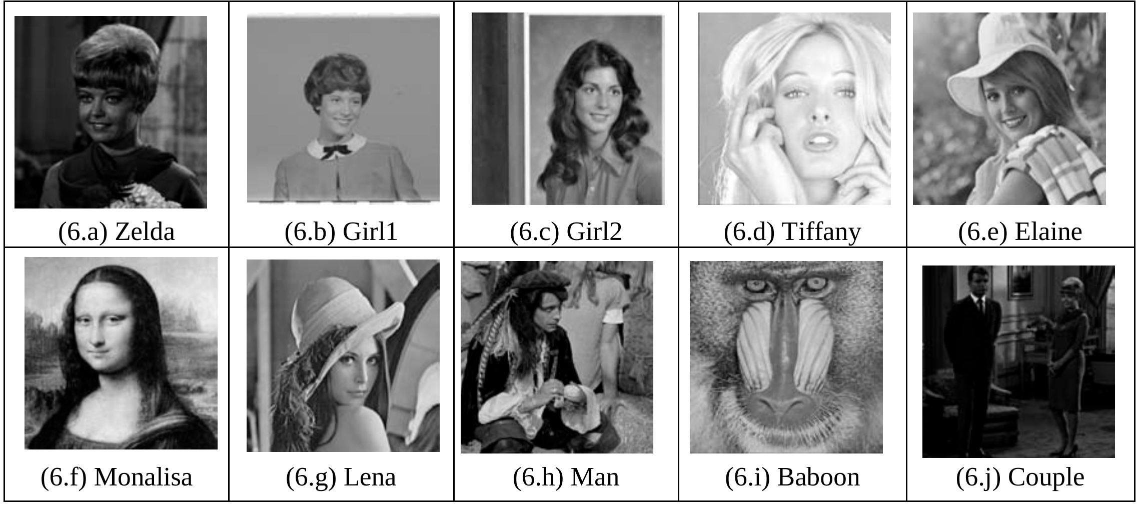
E. Authentication

To regenerate the IRIS signature at receiving end, stego-image passes through forward wavelet transformation, and two bits per bytes from diagonal coefficients are extracted based on hash function. Bit stream are compared with live IRIS image signature for the purpose of authentication.

III. RESULTS AND DISCUSSIONS

TISAWFD applied on ten PPM [11] images to formulate results. All cover images are 512 x 512 in dimension and IRIS signature used as authenticating image of 128 x 128 in dimension. The images are given in fig 6.

Table I, shows the MSE, PSNR, and IF for ten gray scale cover images (512 x 512) on embedding IRIS signatures (128 x 128), 2 bits per byte of cover image, where positions are selected through hash function. The average MSE, PSNR and IF obtained are 2.48, 44.27 and 0.9997 respectively.



(6.a) Zelda

(6.b) Girl1

(6.c) Girl2

(6.d) Tiffany

(6.e) Elaine

(6.f) Monalisa

(6.g) Lena

(6.h) Man

(6.i) Baboon

(6.j) Couple

Figure 6. Cover images of dimension 512 x 512

Table I. Data on applying TISAWFD over 10 Images with different IRIS signatures

Cover Image 512 x 512	**MSE**	**PSNR**	**IF**
(6.a) Zelda	3.791641	42.342531	0.999213
(6.b) Girl1	2.370743	44.381959	0.999883
(6.c) Girl2	1.941788	45.248786	0.999861
(6.d) Tiffany	2.450638	44.238012	0.999946
(6.e) Elaine	2.522552	44.112401	0.999878
(6.f) Monalisa	2.572540	44.027182	0.999871
(6.g) Lena	2.247620	44.613575	0.999859
(6.h) Man	2.318619	44.478510	0.999792
(6.i) Baboon	2.666580	43.871257	0.999856
(6.j) Couple	1.872742	45.406025	0.999068
Average	***2.4755463***	***44.2720238***	***0.9997219***

A comparative study of TISAWFD has been made with PMEDF and JIN's method in terms of peak signal to noise ratio. Comparison is made on randomly selected eight images for PMEDF and four images for JIN's the results are shown in table II and table III respectively. From the tables it is clear that the proposed data embedding/authentication TISAWFD obtained better performances.

Table II. Comparision of average performance for the eight cover images using PMEDF and TISAWFD method.

Average attributes			
Methods	***Watermark size***	***Cover image size***	***PSNR***
PMEDF	32 x 32	512 x 512	33.69 dB
PMEDF	64 x 64	512 x 512	32.50 dB
TISAWFD	128 x 128	512 x 512	44.18 dB

Table III. Comparision of PSNR between JIN's and TISAWFD

Image	***JIN's Method***	***TISAWFD***
Baboon	40.3533	43.8716
Lena	41.4818	44.6136

Boat	38.6725	42.5183
Sailboat	39.8301	42.9696
Average:-	***40.08443***	***43.49328***

IV. A REAL SYSTEM APPLICATION OF TISAWFD

Many applications are widely possible by incorporating proposed technique TISAWFD, especially authentication and verification oriented, like legal document, image authentication, ownership verification or criminal identification within mob.

A database regarding biometric enrolment, as Indian government is approaching towards UID program [12], is required with higher accuracy. Iris signature in transform domain may be embedded into any of the digital documents. During authentication online iris may be taken and compared with the embedded signature.

CCTV cameras are one of the most suitable gadgets for tracking mob by capturing pictures. Those pictures may be used for analysis of biometric parameters without the awareness of prosecute. For further process only iris are enhanced by scaling. The signature of the iris then compared with the database to identify any criminals/prosecute within the mob in a moment.

V. CONCLUSIONS

In this paper we addressed a technique to authenticate image/documents and ownership of the image/documents through biometric characteristics. On comparison to other standard techniques like PMEDF and JIN’s proposed technique obtained better MSE, PSNR and IF values. Online application of the proposed technique has also been elaborated.

VI. ACKNOWLEDGMENT

The authors express deep sense of gratuity towards the Dept of CSE, University of Kalyani and the IIPC Project AICTE, Govt of India and the infrastructure of Finishing School, Govt. of West Bengal, of the dept. where the computational resources are used for the work.

VII. REFERENCES

[1] Woodward, J; Christopher H, Julius Gatune, and Thomas A., Biometrics: A Look at Facial Recognition. RAND Corporation. ISBN 0-8330-3302-6. (2003).

[2] Guo Jing-Ming, Pei Soo-Chang, Lee Hua. Watermarking in halftone images with parity-matched error diffusion, Signal Processing, 91 (2011), pp 126–135. doi:10.1016/j.sigpro. 2010.06.017.

[3] Jin Cong, Jin Shu-Wei. Wavelet Packets-Based Robust Blind Digital Watermark Scheme. IEEE. Proceedings of the 2008 International Conference on Wavelet Analysis and Pattern Recognition, Hong Kong. (2008).

[4] M. Kutter, F. A. P. Petitcolas, A fair benchmark for image watermarking systems, Electronic Imaging '99. Security and Watermarking of Multimedia Contents, vol. 3657, Sans Jose, CA, USA,. The International Society for Optical Engineering, January 1999, http://www.petitcolas.net/fabien/publications/ei99-benchmark.pdf. (Last accessed on 12th Feb, 2011).

[5] Mehmet Sezgin and Bulent Sankur, Survey over image thresholding techniques and quantitative performance evaluation, Journal of Electronic Imaging 13(1), pp146–165. doi:10.1117/1.1631315. (2004).

[6] J.K. Mandal, Madhumita Sengupta. Authentication/Secret Message Transformation Through Wavelet Transform based Subband Image Coding (WTSIC). IEEE, International Symposium on Electronic System Design, pp 225--229, ISBN 978-0-7695-4294-2, DOI 10.1109/ISED.2010.50. (2010).

[7] V.F. Leavers, “Shape detection in computer vision using the hough transformation”, Springer-Verlag, Berlin, 1992, 201 pages, ISBN- 3-540-19723-0, Published online by Cambridge University Press 09 Mar 2009, doi: 10.1017/S0263574700016210.

[8] Robi Polikar. The Wavelet Tutorial. http://users.rowan.edu/~polikar/WAVELETS /WTpart1.html, Fundamental Concepts & an Overview of the Wavelet Theory. The Wavelet Tutorial is hosted by Rowan University, College of Engineering Web Servers, (Last accessed on 25thMarch, 2011).

[9] Ian Kaplan, http://www.bearcave.com/misl/misltech/wavelets/matrix /index.html, January 2002 (Last accessed on 25th May), 2010.

[10] Marc Antonini, Michel Barlaud, Pierre Mathieu, and Ingrid Daubechies. Image Coding Using Wavelet Transform, IEEE Transactions On Image Processing, Vol. I, (2), (1992).

[11] Allan G. Weber, The USC-SIPI Image Database: Version 5, Original release: October 1997, Signal and Image Processing Institute, University of Southern California, Department of Electrical Engineering. http://sipi.usc.edu/database/ (Last accessed on 25th January, 2011).

[12] Website: uidai.gov.in/ . (Last accessed on 7th June, 2011). Government of India.