

FPGA Prototype of Robust Image Watermarking For JPEG 2000 With Dual Detection

Pankaj U.Lande

Dept. Instrumentation Science,
University of Pune,
Pune

pul@usic.unipune.ernet.in

Sanjay N. Talbar

S.G.G.S. Institute of Engineering and Technology,
Nanded.

sntalbar@yahoo.com

G.N. Shinde

Indira Gandhi College CIDCO,
Nanded.

shindegn@yahoo.co.in

Abstract

This paper presents a novel robust invisible watermarking method for still images. The scheme is implemented on hardware, and it can be incorporated with the lossless JPEG2000 compression standard. We have implemented Cohen-Daubechies-Favreau (CDF) 5/3 wavelet filters with lifting scheme which requires less hardware and they are also the basis of lossless JPEG2000. Its modular structure is well suitable for hardware implementation and it is more efficient use of power and chip area. The objective of the hardware assisted watermarking is to achieve low power usage, real-time performance, robust and ease of integration with existing consumer electronic devices such as scanners, cameras and handy camcorders. The proposed scheme of watermarking is tested with StirMark software which is a one of the benchmarking software for watermarking scheme. The experimental result shows that the proposed scheme of watermarking is robust against most of the geometric attacks such as scaling and rotation. We have proposed a dual detection technique for watermark detection which is a novelty of our algorithm.

Keywords: CDF 5/3 wavelet, FPGA, watermarking

1. INTRODUCTION

The recent proliferation and success of the internet, together with the availability of relatively inexpensive digital recording and storage devices has created an environment in which it becomes very easy to obtain, replicate and distribute digital content without any loss in quality. This growth of applications in the past decade gave rise to the new set of problems like *digital piracy*: illegal copying, use, and distribution of copyrighted digital data. This has become a great concern to the multimedia content such as music, video and image to the publishing industries, because technologies or techniques to protect intellectual property rights for digital media and to prevent unauthorized copying did not exist. Exactly identical copies of digital information, be it images, text or audio, can be produced and distributed easily. In such a scenario, who is the artist and who the plagiarist? It's impossible to tell or was, until now. Digital right management (DRM) is a collection of technologies and a technique that enables the licensing of digital information including the multimedia content such as image, video and music. DRM consist of two prominent technologies those are encryption and watermarking. Encryption technologies can be used to prevent unauthorized access to digital content. However, encryption has its limitations in protecting intellectual property rights, because once digital content is decrypted, there is nothing to prevent an authorized user from illegally replicating it [1][2].

Digital watermarking is a process in which an informed signal (watermark) is incorporated in multimedia content such as images to protect the owner's copyright over that content. The watermark can be later be extracted from a suspected image and be verified in order to identify the copyright owner. Watermarking technique for paper manufacturing have been in use since the middle ages, same concept was adopted by digital world and extended this concept for digital images, video and music.[3]. A watermarking scheme consists of three parts: the watermark, the encoder, and the decoder. The watermarking algorithm incorporates the watermark in the object, whereas the verification algorithm authenticates the object by determining the presence of the watermark and its actual data bits [4].

Watermarking techniques can be divided into various categories in numerous ways [5]. In the case of still digital images, there are three primary methods for insertion and extraction of a watermark. These are spatial domain, transform domain and color space methods. The spatial domain method [6] involves an algorithm that directly operates on the pixel values of the host image. In the transform domain method the pixel values are transformed into another domain by applying appropriate transform technique like discrete cosine transform (DCT) [7][9][10], discrete wavelet transform(DWT)[8][11] and Hadamard transform[12]. A watermark is then embedded by modifying these coefficients. However it is observed that spatial domain watermarks are weaker than frequency domain ones [13][14]. A DCT based watermarking algorithm has been described in many literatures; however DWT based watermarking algorithms are more effective for several reasons [15].

Wavelet is a small wave whose energy is concentrated in time and still possesses the periodic characteristics. An arbitrary signal can be analyzed in terms of scaling and translation of a single mother wavelet function. Properties of wavelet allows both time and frequency analysis of signals simultaneously. They offer excellent space-frequency localization of salient image features such as textures and edges. DWT can analyze the data in different scales and resolutions this principal is called as multi-resolution analysis [16]. DWT decomposed the signal into lower and higher frequency signal components. The high-frequency content of an image corresponds to a large coefficient in the detail sub-band. Hence, watermark encoders operating in the wavelet domain can easily locate the high-frequency features of an image and embed most of the watermark energy. Such a method of embedding results in an implicit visual masking of the watermark, because the ability of human visual system (HVS) to detect high frequency signals is limited [17]. It is also a basis of a compression standards like JPEG2000 [18] and MPEG-4[19].

1.1 Related Work

Software approach for image watermarking have been proposed in many literatures; but hardware implementations has few advantages over software approach such as

1. It gives optimized specific design which is a small, fast, and potentially cheap watermarking unit.
2. It is most suitable for real-time applications, where the computation time is deterministic and short.
3. Hardware based watermarking unit can be easily integrated with digital cameras and scanners, graphics processing units etc.
4. Hardware watermarking unit consumes lesser power than software, which requires a general purpose processor so that they are ideal for battery operated applications.
5. The cost is low compared to that software used explicitly for watermarking; this is because a hardware based watermarking unit can be monolithically built on a single unified system in the context of system-on-chip (SoC) technology.

6. The hardware can be implemented as a soft core expressed in the structural hardware description language like VHDL and Verilog. The soft core can be modified as algorithm changes and can be resynthesized into new silicon technology.

A hardware based watermarking is presented in few literatures illustrated bellow.

Seo and Kim [20] presented a field programmable gate array (FPGA) based implementation of blind and invisible watermarking on Altera FPGA. This watermarking algorithm was presented in DCT domain and the DC coefficients are replaced by watermark. The two dimensional DCT was calculated for one or more than one bit planes and the DC coefficients are replaced in such a way that it will be imperceptible to human eyes. The watermarking algorithm was integrated with JPEG2000 encoder and it operates on 66MHz.

An FPGA based invisible robust spatial domain watermarking is described in [21].the watermark insertion is carried out by replacing original image pixel value by watermark encoding function. The watermark is generated through user key. The watermarking scheme is evaluated by standard benchmark like StirMark software. The original image is required for watermark detection. The algorithm was implemented on XCV50-BG256-6 device from Xilinx and operated on 50.398MHz.

An FPGA prototype of Biometric based watermarking is described in [22]. The algorithm work for both gray and color image and the biometric image is selected as watermark. The original image is divided in 8x8 blocks and DCT is calculated for each block. The biometric image (watermark) is divided into blocks and embedded into perceptually significant region of cover image. This approach makes the watermark robust against the common signal processing attacks. Original image is required watermark detection. The prototype was modeled using VHDL and implemented on XC2V500-6FG256 device from Xilinx.

Saraju P. Mohanty et. al. [23] proposed a novel algorithm for encrypted watermarking based on block-wise DCT. The watermarking can work for gray scale image as well as color image. In the case of color image the cover image in RGB format is converted into YCbCr and the Y component is selected for watermarking. The image is divided in 8x8 blocks and DCT is calculated for each block. The encrypted watermark is embedded into transformed image by four different embedding factors. The embedding strength factor is chosen such that the image quality will not degrade. The watermark detection process requires original image. The block-wise DCT is computed for both image and the difference is calculated to detect a watermark. The extracted watermark is compared with original watermark to authenticate the suspected image.

Image adaptive watermarking and its hardware architecture is described in [12]. The proposed scheme of watermarking is invisible and robust against JPEG attacks. Cover image is divided in 8x8 blocks and DHT is calculated. PN sequence is generated through user key and embedded into DHT coefficients. The strength factor is calculated from quantization table for DHT domain. Watermark detection method is blind. The proposed method is robust against the common signal processing attacks like median filtering and noise addition. The algorithm was implemented on XC3SD1800A-4FGG676C and functional simulation was performed using Xilinx tools. The chip was tested using hardware co-simulation which was run at 33.3MHz.

In this paper we have presented a watermarking scheme using the CDF 5/3 wavelet filter which can be incorporated with JPEG2000 lossless image compression. Hardware architecture was implemented on FPGA. The proposed scheme is an invisible robust wavelet domain watermarking method. We have also proposed a dual watermark detection technique that is the watermark can be detected by blind and non blind method to verify the suspected image. The blind watermark detection can be used with the images from digital cameras where the original image is not present. The non-blind technique can be used with the digital scanners where the original image is present.

The scheme described in [24] is used to implement CDF 5/3 wavelet filters. The proposed architecture uses the lifting scheme technique and provides advantages that include small memory requirements, fixed-point arithmetic implementation, and a small number of arithmetic computations. The chip was modeled using Verilog and a function simulation was performed. This chip was tested using AccelDSP in hardware in the loop (HIL) arrangement. The proposed scheme is robust against several geometric attacks. We have tested our watermarking scheme using standard benchmark such as StirMark software.

2. PROPOSED WATERMARKING SCHEME

The proposed scheme is based on CDF 5/3 wavelet filters which is the basis of lossless JPEG2000 compression standard. The new still compression image standard, JPEG2000 has emerged with a number of significant features that would allow it to be used efficiently over a wide variety of images. The JPEG2000 standard exhibits a lot of features, the most significant being the possibility to define regions of interest in an image, the spatial and SNR scalability, the error resilience and the possibility of intellectual property rights protection. Interestingly enough, all these features are incorporated within a unified algorithm. This compression standard uses the Cohen-Daubechies-Favreau (CDF) 5/3 and CDF 9/7 DWT for lossless and lossy image compression respectively. Since JPEG2000 is the newest version of one of the most popular image formats and it includes the DWT, efficient VLSI implementations of DWT processors became more and more important.

We have used the lifting scheme described in[24].the advantages of using lifting scheme is that, the number of multiplications and additions compared to the filter-bank implementation are reduced resulting in more efficient use of power and chip area. The modular structure is well suitable for hardware implementation. The lifting scheme calculates the DWT using spatial domain analysis, and consists of a series of *Split*, *Predict* and *Update* steps. The split step separates odd and even samples, and predict step predicts values in the odd set where $\alpha = -0.5$ as the predict step coefficient. The Update step uses the new wavelet coefficients in the odd set to update the even set, where $\beta = 0.25$ as the update step coefficient. Lifting scheme is shown in figure 1 and Lifting operation for the CDF 5/3 synthesis filter is shown in Figure 1.

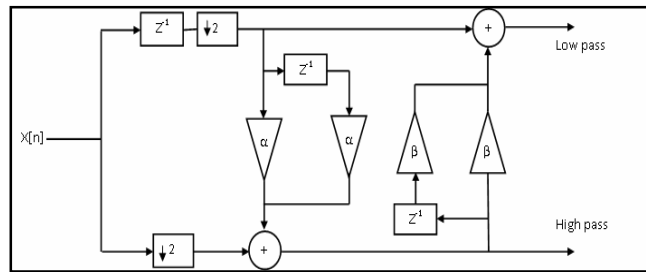


FIGURE 1: CDF 5/3 with lifting scheme

The watermarking algorithm embeds same multiple watermarks in cover image. The cover image I is divided into non-overlapping blocks of size BxB. CDF 5/3 wavelet transform is calculated for block separately. A binary watermark is embedded into cover image using equation (1).

$$I_{W,N}(x, y) = I_N(x, y) + a \times W(x, y) \quad (1)$$

Where 'a' is gain

$I_{W,N}$ is a N^{th} block of watermarked image and W is a binary watermark logo. x and y are index numbers.

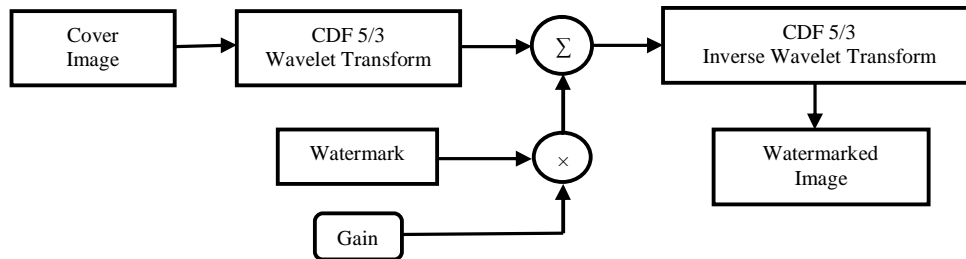


FIGURE 2: Watermarking Scheme

2.1 Hardware Architecture for Proposed Scheme

In this section, we discuss the hardware architecture for the scheme discussed in the previous section. The watermarking chip mainly consists of a block processing unit and control.

2.1.2 Block processing unit

The block processing unit considers the original image block as input. Image block is wavelet transformed and the watermark is embedded using equation (1). This unit consists of CDF5/3 wavelet filters and watermarking unit. To meet the real time constrain, we have used two filters in parallel to calculate forward and inverse transform. In order to calculate the 2D wavelet, these filters first calculate the coefficients first row-wise and then column-wise. The intermediate results are stored in the memory. Inverse wavelet is calculated in similar manner.

2.1.3 Watermarking unit

The watermarking unit consists of a multiplier and adder. The watermark is embedded using equation (1). Because a multiplier requires more hardware, only one multiplier is implemented. The wavelet transformed block is fed serially to the watermarking unit. The gain is multiplied by watermark and added to the wavelet transformed coefficients. The intermediate results are stored in the memory.

2.1.4 Control unit

The control unit generates the necessary control signals for the entire system during the watermarking process. The control unit generates four main signals and these signals are as follows

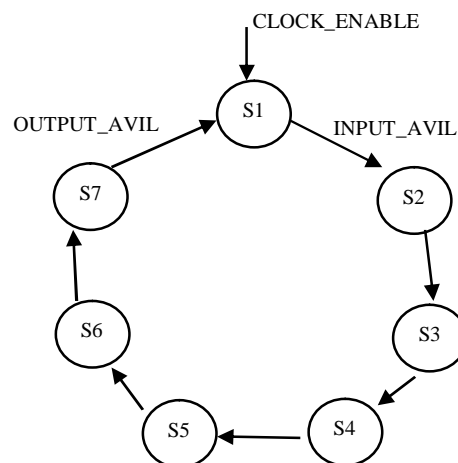


FIGURE 3: Control Unit as FSM

INPUT_AVIL: Image block is available at input.

OUTPUT_AVIL: Watermarked image block is available at output

CLOCK: Clock signal for chip

CLOCK_ENABLE: When clock enable is high chip is in an active mode for processing

This unit undergoes seven states in each state; the particular task is performed in each state and the finite state machine (FSM) begins to the next state. Figure (3) shows the state diagram of FSM.

S1: if the clock enable is high and INPUT_AVIL is high then read image block

S2: calculate DWT

S3: read the watermark

S4: multiply the watermark with 'a'

S5: embedded the watermark

S6: calculate inverse DWT

S7: generate OUTPUT_AVIL signal

2.1.5 Watermark detection

The watermark detection algorithm is implemented using MatLab. The watermark can be detected using two methods blind and non-blind. In non blind method original and watermarked image both are required to detect a watermark. The suspected image and original image are divided into BxB blocks, and DWT coefficients are calculated for both images. The watermark is recovered using equation (4).

$$W(i, j) = \begin{cases} 1 & \text{if } I_{WN}(x, y) - I_N(x, y) > \tau \\ 0 & \text{other wise} \end{cases} \quad (4)$$

τ represents threshold for blind detection

In the blind watermark detection method the binary logo image is considered as PN sequence and the correlation between the suspected image and watermark is calculated. The suspected image is divided into BxB blocks, and DWT coefficients are calculated. The correlation between encrypted watermark and wavelet transformed block is calculated using equation (5)

$$\gamma = \frac{\sum_m \sum_n (I_{WN}(x, y) - \bar{I}_{WN})(w(x, y) - \bar{w})}{\sqrt{\sum_m \sum_n (I_{WN}(x, y) - \bar{I}_{WN}) \sum_m \sum_n (w(x, y) - \bar{w})}} \quad (5)$$

If $\gamma > \rho$ then the watermark is detected. ρ is threshold for blind detection.

If $\gamma > \rho$ then the watermark is detected. ρ is threshold for blind detection.

3. EXPERIMENTAL RESULTS

3.1 Synthesis and Implementation

The chip was modeled using a Verilog and functional simulation was performed. The code was synthesized on Xilinx Spartan-3A technology on XC3SD1800A-4FGG676C device using the AccelDSP. The results are verified by hardware in the loop (HIL) configuration using AccelDSP. The HIL was run at 33.3 MHz clock frequency, and the samples were fed to the target device at a rate of 319.585 Ksps through a JTAG USB cable. The design utilizes 2 startup clock cycles and single clock cycles per function call. The device utilization summary is given in Table 1.

Logic Utilization	Used	Available	Utilization %
Number of Slices	628	16640	3.77 %
Number of Slice Flip Flops	290	33280	0.87 %
Number of 4 input LUTs	1077	33280	3.23 %
Number of bonded IOBs	293	309	94.82 %
Number of GCLKs	1	24	4.16 %

TABLE 1: Device Utilization Summary

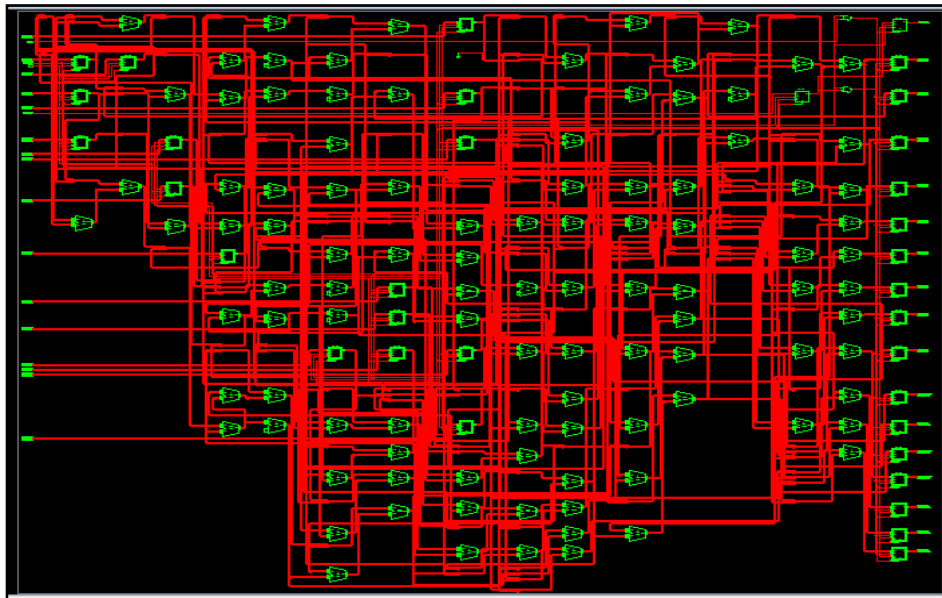


FIGURE 4: RTL of Watermarking Chip

3.2 Image Quality Measures

In [25] Kutter and Petitcolas have discussed various parameters to estimate any watermarking scheme. For fair benchmarking and performance evaluation, the visual degradation due to embedding is an important issue. Most distortion measure (quality metrics) used in visual information processing belongs to a group of difference distortion measures. The watermark images are acceptable to the human visual system if the distortion introduced due to watermarking is less.

The various performance evaluations metrics such as PSNR (db), Image Fidelity (IF), Normalized cross correlation, correlation quality etc. are calculated. Results for few popular images are given in Table 2.

Quality Measures	Lena	Mandrill	Woman
Mean square error	6.80	6.74	6.80
PSNR	39.79	39.84	39.80
Normalized cross correlation	1	1	1
Average Difference	-0.8135	-0.8055	-0.8146
Structural content	0.98	0.99	0.98
Maximum difference	3	3	3
Normalized absolute error	0.031	0.017	0.017
Image Fidelity	1	1	1
correlation quality	1	1	1

TABLE 2. Image Quality Measures



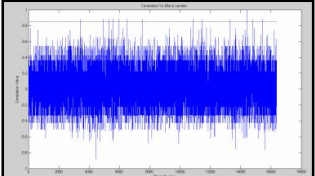


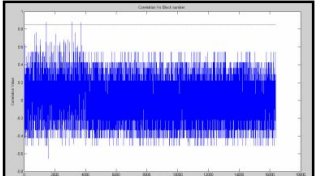
3.3 Performance Evaluations on Various Attacks

In this section, we evaluate the performance of the watermarking algorithm against various attacks using standard benchmark software. The StirMark software includes several attacks such as JPEG compression geometric transformation, noise addition etc. The geometric attacks includes rotation, cropping, scaling and geometric transformation with medium compression. Some of the results of these evaluations for blind and non-blind detection are summarized in Table 3. For blind detection threshold is $\rho=0.85$. These results indicate that the proposed watermarking scheme is robust against the geometric attacks.

The proposed scheme of watermarking embeds multiple watermarks in cover image. The objective was, at least a single watermark will survive after attacks. In detection algorithm all the watermarks are detected, and the watermark which is having highest correlation with the original watermark is treated as the recovered watermark. We have also proposed a dual watermark detection technique. The watermark can be detected by blind or non-blind method and both detection techniques can be used to verify suspected image. Scheme implements several watermark in the cover image, due to which scheme is robust against various geometric attacks.

4. Conclusion

In this paper, we proposed a novel invisible image watermarking algorithm and developed efficient the hardware architecture which can be used with JPEG2000. The watermarking scheme utilizes minimal hardware resources as it can be seen from the device utilization summary table. Because of the lifting scheme is used in CDF 5/3 filters it requires minimum hardware and it requires less clock cycles. The experimental results showed that the proposed scheme of watermarking scheme is imperceptible and robust against geometric attacks. The proposed algorithm outperforms than the presented algorithm in [12][21]. This was achieved because of space and frequency localizing property that is the characteristics of the discrete wavelet transform. In the future we want to develop a image adaptive watermarking hardware using fuzzy logic or neural network.

Attacks	Non – Blind Detection	Blind Detection
 AFFINE_2		 Max corr value =0.86
 CROP_25		 Max corr value =0.87

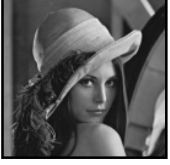

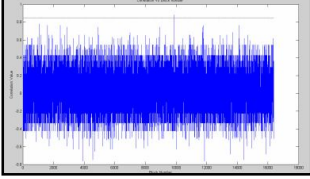


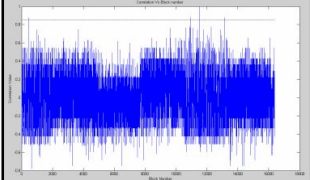


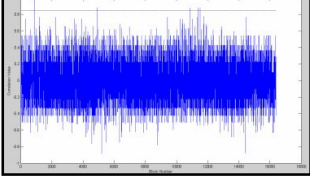


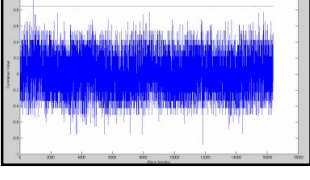
 MEDIAN_3		 Max corr value 0.88
 RML_90		 Max corr value =1
 ROTCROP_-75		 Max corr value 1
 ROTSCALE_0.5		 Max corr value 1

TABLE 3. Performance Evaluation

5. REFERENCES

1. Er-Hsinen, "Literature Survey on Digital Image Watermarking," *EE381K-Multidimensional Signal Processing* 8/19/98.
2. S. Katzenbeisser and F. A. P. Petitcolas: *Information Hiding techniques for steganography and digital watermarking*, Artech House, Inc., MA, USA, 2000.
3. N. Memon and P. W. Wong.:Protecting Digital Media Content. *Communications of the ACM*, vol. 41, no. 7, pp. 34–43, Jul 1998.
4. C.C. Chang and J. C. Chuan, "An image intellectual property protection scheme for gray-level images using visual secret sharing strategy," *Pattern Reconition Letters*, vol. 23, pp. 931-941, June 2002.
5. S. P. Mohanty.:Watermarking of Digital Images.M.S. Thesis, Indian Institute of Science, Bangalore, India, 1999.
6. N. Nikolaidis, I. Pitas, "Robust Image Watermarking in Spatial Domain", *International journal of signal processing*, 66(3),385-403,1998.

7. Pankaj U. Lande, Sanjay N. Talbar and G.N. shinde "Adaptive DCT Domain Watermarking For Still Images", *Internatational Conference RACE-07*, Bikaner, Rajasthan, India
8. Pankaj U. Lande, Sanjay N. Talbar and G.N. shinde "Hiding A Digital Watermark Using Spread Spectrum At Multi-Resolution Representation", *Internatational conference ACVIT07*, Aurangabad, India.
9. Juan R. Hernandez, Martin Amado, Fernando Perez-Gonzalez "DCT Domain watermarking technique for still Image :Detectors Performance analysis and New Structure", *IEEE transaction on image processing*, VOL.9, no.1, Jan 2000.
10. Juan R. Hernandez, Martin Amado, Fernando Perez-Gonzalez "DCT Domain watermarking technique for still Image: Detectors Performance analysis and New Structure", *IEEE Transaction on Image Processing*, VOL.9, No.1, Jan 2000.
11. Pik Wah Chan, Michael R. Iyu and Roland T. Chin, "A Novel scheme For Hybrid Digital Video Watermarking : Approach, Evaluation And Experimentation", *IEEE Transactions on circuits and system for video technology*, VOL 15, No. 12, Dec 2005.
12. Pankaj U. Lande, S.N. Talbar, G.N. Shinde, "FPGA implementation of image adaptive watermarking using human visual model", *ICGST-PDCS*, Vol.9, Issue1, Oct. 2009.
13. I. J. Cox, J. Kilian, T. Shamoan, T. Leighton, Secure Spread Spectrum Watermarking of Images, Audio and Video, in: Proc IEEE International Conf on Image Processing, Vol. 3, 1996, pp. 243–246.
14. I. J. Cox, J. Kilian, T. Shamoan, T. Leighton, A Secure Robust Watermarking for Multimedia, in: Proc. of First International Workshop on Information Hiding, Vol. 1174, 1996, pp. 185–206.
15. P. Meerwald and A. Uhl, (2001) "A survey of wavelet-domain watermarking algorithms," Proceedings of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents III, San Jose, California, vol. 4314.
16. Burrus, C., Gopinath, R., and Guo, H.: *Introduction to Wavelets and Wavelet Transforms: A Primer*.: Prentice Hall 1998.
17. R. Dugad, K. Ratakonda, and N. Ahuja, (1998) "A new wavelet-based scheme for watermarking images," *Proceedings of the IEEE International Conference on Image Processing, ICIP '98*, Chicago, Illinois, pp. 419-423.
18. D. Taubman and M. Marcellin.: *JPEG2000: Image compression fundamentals, standards, and practice*.: springer, 2002.
19. T. Ebrahimi and F. Pereira.: *The MPEG-4 Book*.: Prentice Hall 2002.
20. Y. H. Seo, D. W. Kim, Real-Time Blind Watermarking Algorithm and its Hardware Implementation for Motion JPEG2000 Image Codec, in: Proceedings of the 1st Workshop on Embedded Systems for Real-Time Multimedia, 2003, pp. 88–93.
21. S. P. Mohanty, R. K. C., S. Nayak, FPGA Based Implementation of an Invisible-Robust Image Watermarking Encoder, in: Lecture Notes in Computer Science, Vol. 3356, 2004, pp. 344–353.

22. S. P. Mohanty, O. B. Adamo, and E. Kougianos, "VLSI Architecture of an Invisible Watermarking Unit for a Biometric-Based Security System in a Digital Camera", in *Proceedings of the 25th IEEE International Conference on Consumer Electronics (ICCE)*, pp. 485-486, 2007.
23. S. P. Mohanty, "A Secure Digital Camera Architecture for Integrated Real-Time Digital Rights Management", *Elsevier Journal of Systems Architecture (JSA)*, Volume 55, Issues 10-12, October-December 2009, pp. 468-480. Kanchan H. Wagh, Pravin K. Dakhole, Vinod G. Adhau.: Design & Implementation of JPEG2000 Encoder using VHDL. Proceedings of the World Congress on Engineering 2008 Vol I, WCE 2008, , London, U.K July 2 - 4, 2008.
24. Kanchan H. Wagh, Pravin K. Dakhole, Vinod G. Adhau.: Design & Implementation of JPEG2000 Encoder using VHDL. Proceedings of the World Congress on Engineering 2008 Vol I, WCE 2008, , London, U.K July 2 - 4, 2008.
25. M. Kutter and F.A. Petitcolas, "A Fair Benchmark for Image Watermarking Systems", *Electronic imaging ,Security and Watermarking of Multimedia Contents, VOL. 3657*, 25-32,1999.