

# Digital Design for Image-Adaptive Watermarking using CDF 5/3 Wavelet

Pankaj U. Lande, Sanjay N. Talbar, G. N. Shinde

**Abstract:** Paper This paper presents a hardware architecture for image-adaptive watermarking in the wavelet domain. The embedding strength factor is selected by calculating the energy present between the different frequency bands. The current algorithm is constructed on a CDF 5/3 wavelet based on the model of lossless compression JPEG 2000. Wavelet filters are implemented using a parallel architecture with a lifting scheme, which makes them more efficient in terms of speed and hardware utilization. The top module of the system is built with the combination of serial-parallel architecture to balance the speed and power consumption. The presented watermarking system is tested using hardware in the loop-testing technique. The objective is to develop an image-adaptive, real time, low power consumption and robust watermarking system, which can be incorporated into existing hardware such as digital cameras, scanners, and camcorders. The watermarking system's efficiency against different assaults has been evaluated using the StirMark software. The proposed watermarking system showed robustness against most of the geometric and non-geometric attacks.

**Keywords:** Discrete Wavelet Transform (DWT), Field Programmable Gate Array (FPGA), Hardware in the loop (HIL), Watermarking, Cohen–Daubechies–Feauveau wavelet (CDF).

## I. INTRODUCTION

In manipulating digital material, the fast growth of computer and internet technologies has provided consumers the ultimate power. These electronic contents are most often altered without the permission of its owner. This is often referred to as digital piracy. Digital piracy involves illegally copying, using and distributing copyrighted digital data. Using the free internet software can readily create, copy, process, store and distribute digitized multimedia. Digital Rights Management (DRM) is a technology compilation that addresses problems linked to digital property rights. Digital watermarking is one of DRM's technologies [1]. The term watermark has been introduced from the paper industry. Digital world brought the same concept of paper watermarking and called digital watermarking. Watermarking is a process that integrates an informed signal, called a watermark, into a multimedia object such as an authentication image to protect the rights of ownership. It is possible to decode the integrated data to define the copyright owner [2][3].

Revised Manuscript Received on December 15, 2019.

\* Correspondence Author

**Pankaj U. Lande** \*, Department of Electronics ,Rajaram College,Kolhapur (Maharashtra) India. E-mail: landepankaj@gmail.com

**Sanjay N. Talbar**, Professor, Department of Electronics & Telecommunication Engg., SGS Institute of Engineering & Technology Nanded, India. E-mail: sntalbar@yahoo.com

**G. N. Shinde**, Principal, Yashwant college, Nanded, India E-mail: shindegn@yahoo.co.in

In many respects, watermarking methods can be split into different classifications. Depending on the domain of insertion and removal used, watermarking can be grouped into three main techniques. These are methods of space-domain, transform-domain, and color-space. The space-domain technique includes an algorithm that operates directly on the host image's pixel values [4]. In the transform-domain method, the pixel values are transformed into another domain by applying appropriate transform techniques like Discrete Cosine Transform (DCT) [5][6], Discrete Wavelet Transform (DWT) [7][8] and Hadamard Transform [9][10]. It has been observed that the spatial domain watermarks are weaker than the frequency-domain watermarking methods [11]. However, compared to the frequency-domain scheme, the spatial-domain watermarking scheme requires fewer computations. The color image is transformed from one color space to another in the color space, then the watermark is embedded into one of the color planes [12]. A number of literature exist on the software approach for image watermarking [6][7][13][14][15]. The hardware implementation of digital watermarking has the following advantages [16][17][18]:

1. It provides an optimized particular layout that is a tiny, quick, and possibly inexpensive watermarking device.
2. It is best suited for real-time applications with deterministic and brief computation time.
3. Digital cameras and scanners, graphics handling systems, and others can readily integrate the hardware-based watermarking device.
4. The watermarking system based on hardware also consumes less energy than the software, which needs a general-purpose processor to make it suitable for battery-operated applications.
5. The price of using system-on-chip (SoC) technology is small relative to software explicitly used for watermarking.

This paper is organized in eight parts: related work, novel contribution, watermarking algorithm, watermark detection, hardware implementation, quality measures of watermarked images and performance evaluation under various attacks.

## II. RELATED WORK

Hardware-based watermarking has been the subject of a few studies as mentioned here.

Jana et al. [19] presented an FPGA prototype of the reversible watermarking method in the DCT domain. The image is divided into 8 by 8 blocks of pixels and then DCT is calculated. Random blocks are selected to embed the watermark. The binary watermark is created from the DC coefficient of the transformed DCT blocks. This binary watermark is then inserted into

the coefficients of the DCT using the modulation process of the spread spectrum (SS). In decoding processes, a suspected image is divided into blocks and IDCT is calculated. The random sequence is generated from the user key and correlation is calculated. If the correlation is above the desired threshold value, then the watermark is detected in the suspected image. The embedding effect can be reversed to obtain the original image.

In [20], the author has proposed the watermarking processor in FPGA and an application-specified integrated circuit (ASIC) version of the same. The algorithm converts the cover image into a binary image by applying the threshold. The binary image is then portioned into  $3 \times 3$  blocks and the central pixel value is flipped by using logical operations. XOR or a concatenate operation is performed with the payload watermark to generate the watermarked image. The watermarked image and the original image are compared to verify authentication. The synthesis of the chip is performed using the XILINX ISE tools targeting Xilinx VIRTEX-E FPGA technology (XCV50E-8-CS144).

Very large scale integration (VLSI) architecture for visible image watermarking is presented in [21]. The proposed watermarking scheme is implemented on FPGA. The image is tiled into  $8 \times 8$  pixels blocks and for each block 1D DCT is calculated. The scaling factors are computed from the DCT coefficients. The watermark DCT coefficients and the image coefficients are added together to form a watermarked image. The proposed architecture is implemented on Xilinx Virtex V technology-based FPGA targeting device as XC5VLX330 (DSP 48E).

Elias Kougianos et al. proposed a spatial domain watermarking architecture and chip in [17]. The authors have implemented an invisible robust spatial domain. A ternary image watermark is inserted in the image by modifying its nearest neighborhood with an appropriate scaling factor. The watermark can be extracted by comparing the original image and the watermarked image. The synthesis of the chip is carried out using Synplify Pro<sup>TM</sup> tool and implemented on Xilinx VIRTEX-II technology with the XCV50-BG256-6 target device. The simulations were done using the ModelSim.

The advance encryption standard (AES) and wavelet-domain watermarking method are described in [22]. The cover image is transformed into wavelet domain and the watermark is encrypted using AES. The encrypted watermark and transformed image are added together to obtain a watermarked image. The watermark is embedded into the low frequency components of the transformed image. The algorithm was implemented on Virtex 6 FPGA (XC6VCX75T) using Xilinx 14.1 ISE tools.

Ahmed et al. [23] proposed a quantization-based image watermarking method in the wavelet domain. The cover image is transformed into the wavelet domain using CDF 5/3 filter. In the transformed image, the LL3 band is selected for embedding processes. A binary watermark is then embedded in the LL3 band by modifying the relationship between the coefficients. In the detection processes, the wavelet coefficients are compared, and if the relation is above the threshold limit, then it is treated as '1' and if it is less, then it is '0'. The method was implemented using the Xilinx system generator software and targeting the VIRTEX4

(VLX100FFL148-2) device from Xilinx. Note that the watermark detection processes are blind. The design operates on a 141.9-MHz clock frequency.

The dual-mode watermarking algorithm for spatial and fast Walsh-Hadamard (FWH) domain is proposed in [24]. In spatial-domain watermarking, the cover image and watermark image is divided into  $B \times B$  blocks. The binary watermark image is embedded into the cover image by adding a pseudo random sequence. For transform-domain watermarking, the cover image is divided into blocks and then FWH is calculated. A binary watermark is then embedded by adding a pseudo random sequence into the transformed coefficients. To detect a watermark, the suspected image is divided into blocks and FWH is calculated for each block. Correlation is calculated between the pseudo random sequence and the transformed block. If the correlation that exists is greater than the threshold limit, then the watermark bit '1' is recovered, otherwise it is '0'. The proposed watermarking algorithm was implemented on Virtex 4 series (XC4VLX200-11FF1513) from Xilinx. The transform-domain design consumes 1146 mW power and the spatial domain consumes 627 mW of power. Both designs operate on a 90.131-MHz clock frequency.

A secure digital camera for real-time DRM is proposed by Mohanty in [25]. The proposed prototype embeds an encrypted watermarking logo image within the cover image. In the proposed algorithm, the color image is divided into YCbCr, and the luminance component is chosen for watermarking. The luminance component is divided into equal-size blocks, and the DCT is calculated for each block separately. The DC and lower frequency components are selected for the watermarking. A  $2 \times 2$  block of the encrypted image is embedded in the cover image using additive and subtractive equitations. For the DC and lower frequency components, separate gain values are used to minimize visual distortion. The prototype was implemented on Xilinx Virtex-II technology. The proposed architecture consumes 3.7 mW of power and operates on a 256-MHz clock frequency.

### III. NOVEL CONTRIBUTION

The data in Table I shows that less contribution has been made to the hardware implementation of image watermarking on FPGA. We have presented a parallel architecture for CDF 5/3 wavelet with a lifting scheme. A parallel approach makes the filter faster in terms of calculation and the lifting scheme makes it hardware-efficient. The top module (i.e. block processing unit) is implemented with the combination of serial and parallel architectures. This approach is used to increase the speed, but at the same time requires less hardware and power. This paper also presents the multiplier-less approach to implement the CDF 5/3 filter and the watermark-embedding equation. The image quality parameters of the watermarked image are calculated and presented in this paper. We have also discussed the simulation as well as synthesis results. This paper also describes the performance of the watermarking system under various geometric and non-geometric attacks.

Table I Watermarking Methods

No .	Proposed Work	Type of Watermark	Domain	Technology	Parallel Architecture	Adaptive	Hardware-In-The-Loop Test	Performance Against Attacks	Watermarked-Image Parameters
1	Jana Poulami et al. [19]	Invisible	DCT	FPGA	N	N	N	N	N
2	P. Karthigaikumar [19]	Invisible	Spatial	FPGA & ASIC	N	Y	N	N	N
3	V.E. Jayanthi [20]	Visible	DCT	FPGA	N	Y	N	N	N
4	G. Singh [21]	Invisible	DWT	FPGA	N	N	N	N	N
5	J. Ahmed[22]	Invisible	DWT	FPGA	N	N	N	N	N
6	S. Ghosh[23]	Invisible	Spatial & FWH	FPGA	N	N	N	N	N
7	S. P. Mohanty[24]	Invisible	DCT	FPGA	N	N	N	Y	Y
8	Present paper	Invisible	DWT (CDF 5/3)	FPGA	Y	Y	Y	Y	Y

IV. PROPOSED WATERMARKING SCHEME

In the domain of image compression, the wavelet transformation is gaining significance. The latest compression standard JPEG2000 offers a fresh compression engine that enables many neighboring features such as progressive transmission. It also has the ability to identify Regions of Interest (ROI) in a picture, the scalability of the spatial and signal to noise ratio (SNR), the resilience of errors and the option of security of intellectual property rights [26][27]. It has appeared with a range of important characteristics that would enable it to be used effectively across a broad range of pictures. Interestingly enough, a unified algorithm incorporates all these characteristics. JPEG2000 is the latest verse.

The scheme presented is built on CDF 5/3 wavelet filters, which are also the foundation for the JPEG2000 lossless compression system. A revised version of the lifting system was implemented as outlined in [28][29]. The benefit of the lifting scheme is that the amount of multiplications and additions is lowered relative to the application of the filter-bank, resulting in a much more efficient use of energy and chip region. Its modular design is suitable for hardware implementation.

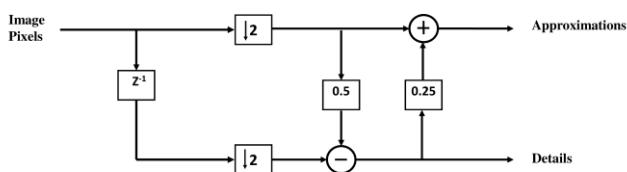


Fig. 1. Lifting scheme

The incoming pixels are split into two odd and even sample of disjoint sets, and the predicted stage calculates results in the odd set of pixels where  $\alpha = -0.5$  is called as a predict coefficient. The update step is to update the even set using the fresh wavelet coefficients in the strange set, where  $\beta = 0.25$  is called as the update-step coefficient. Instead of multiplying the update and predicting values, the value is right-shifted by two in the predicted stage and then subtracted to calculate the results information. Data is right-shifted by four in an update phase and inserted to get approximation values.

The cover image  $I_{MN}$  cover image is split into non-overlapping size  $B \times B$  blocks. For each block, the CDF 5/3 wavelet transformation is calculated separately. The

wavelet energy coefficients are calculated using equations (1) and (2) for the sub-bands LL and HH. Using equation (3), the energy between LH and HL band is drawn on average. The gain factor is determined in the sub-bands depending on the energy. The Following abbreviations are used in the paper.

- $E_L$  -Energy in LL Band
- $E_H$  -Energy in HH band
- $E_M$  -Average energy in HL and LH band
- $I_{(m,n)}$  - Cover image (size  $m \times n$ )
- $I_W$  -Watermarked image
- N-block number
- g- gain

$$E_H = \frac{1}{B \times B} \sum |I_{HH}| \tag{1}$$

$$E_L = \frac{1}{B \times B} \sum |I_{LL}| \tag{2}$$

$$E_M = \left( \frac{\frac{1}{B \times B} \sum |I_{HL}| + \frac{1}{B \times B} \sum |I_{LH}|}{2} \right) \tag{3}$$

V. WATERMARK DETECTION

Blind and non-blind methods can detect watermarks and a program has been developed to detect the watermark using the MatLab software. The presumed image and the original image are split into  $B \times B$  blocks in a non-blind technique. For each block, CDF 5/3 is calculated. Using equation (4), the binary watermark is retrieved.

$$W(x, y) = \begin{cases} 1 & \text{if } I_{W,N}(x, y) - I_N(x, y) > \sigma \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

$\sigma$  represents the threshold for converting the difference into binary.

In blind watermark detection method, the binary logo image is perceived as a PN sequence and the correlation is calculated between the alleged image and watermark. The alleged image is divided into  $B \times B$  blocks and DWT coefficients are calculated. The equation (5) calculates the correlation between the watermark and the wavelet-transformed matrix.



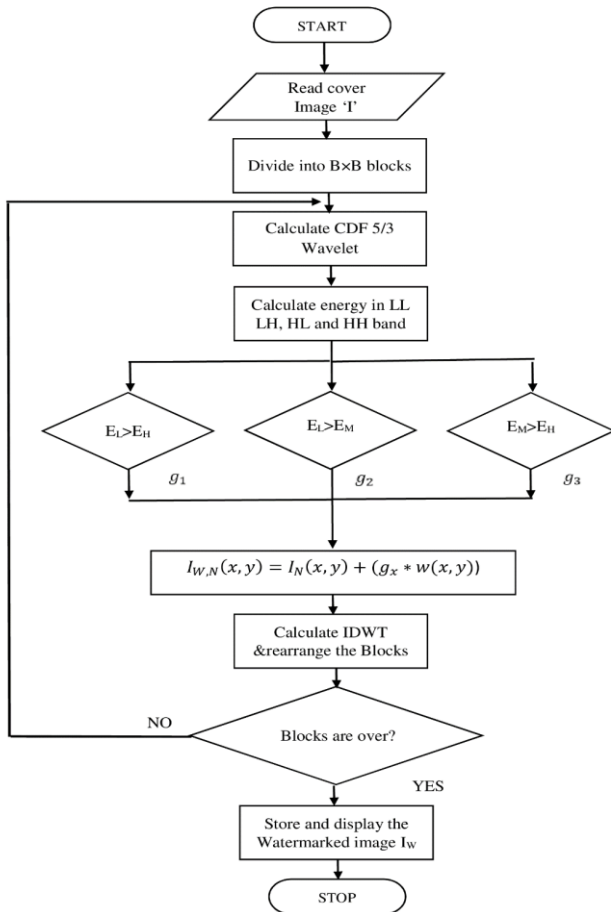


Fig. 2. Watermarking algorithm

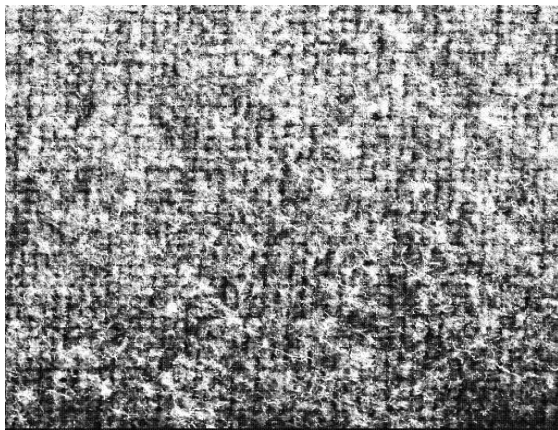


Fig. 3. Watermarked image

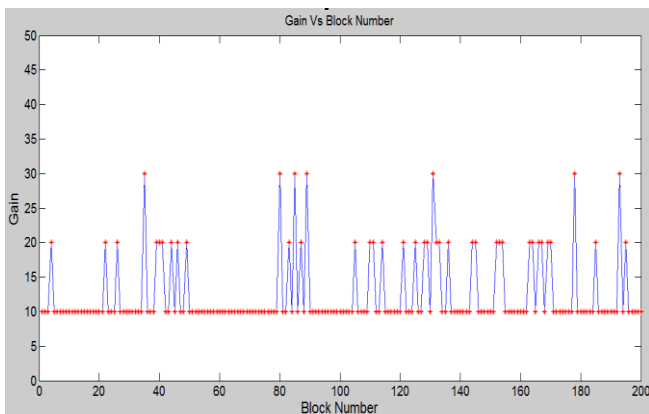


Fig. 4. Block number vs gain

VI. WATERMARK DETECTION

Blind and non-blind methods can detect watermarks and a program has been developed to detect the watermark using the MatLab software. The presumed image and the original image are split into BxB blocks in a non-blind technique. For each block, CDF 5/3 is calculated. Using equation (4), the binary watermark is retrieved.

$$W(x,y) = \begin{cases} 1 & \text{if } I_{W,N}(x,y) - I_N(x,y) > \sigma \\ 0 & \text{otherwise} \end{cases} \quad (4)$$

$\sigma$  represents the threshold for converting the difference into binary.

In blind watermark detection method, the binary logo image is perceived as a PN sequence and the correlation is calculated between the alleged image and watermark. The alleged image is divided into BxB blocks and DWT coefficients are calculated. The equation (5) calculates the correlation between the watermark and the wavelet-transformed matrix.

$$\gamma = \frac{\sum_m \sum_n (I_{W,N}(x,y) - \bar{I}_{W,N})(W^*(x,y) - \bar{W}^*)}{\sqrt{\sum_m \sum_n (I_{W,N}(x,y) - \bar{I}_{W,N}) \sum_m \sum_n (W^*(x,y) - \bar{W}^*)}} \quad (5)$$

If the value of  $\gamma$  is greater than 0.8, then the watermark is detected.

VII. ARCHITECTURES FOR THE WATERMARKING ALGORITHM

In this section, we describe the VLSI architectures for the invisible-watermarking unit. Figure 5 shows the top module of the watermarking system. It consists of the memories for the image storage, block-processing unit and address generator. Two separate memories are used to store the cover image and watermarked image. Address generator block generates a sequence of address in such a way that the block of pixels is extracted from the memory. Same addresses are used to store the watermarked image block with delay. This delay is equal to the time taken by the block-processing unit to insert the watermark. Note that the block-processing unit is the most important unit. This unit calculates CDF 5/3 wavelets, inserts a watermark and calculates inverse CDF 5/3 wavelets.

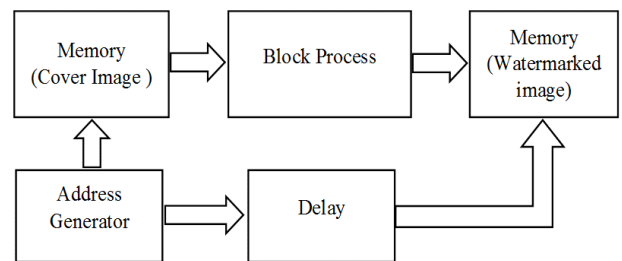


Fig. 5. Block diagram of the watermarking unit

A. Address Generator

The address-generator module generates the sequence of addresses to extract the block of pixels from the cover image. In the proposed algorithm, the block size is 8x8 and the cover image size is 512x512. Equation (6) is used to generate the address.

$$Add = (x + (y \times 512) + (P \times 8) + (Q \times 4096)) \quad (6)$$

where x, y, p and q are the counters. Counter x counts from 0 to 7; each time when the counter finishes its count, counter y is incremented by one. When one block pixels are over, p is incremented by one, and when 64 blocks are completed, q is incremented by one. This process continues till all the 4096 blocks are over. Figure 6 shows the address generation mechanism.

### B. Block-Processing Unit

The block-processing unit consists of Time Division Multiplexer (TDM), Time Division Demultiplexer (TDD), forward CDF 5/3 wavelet filter bank, watermarking block, adaptive gain block, and inverse CDF /3 wavelet filter bank. Figure 10 shows the block-processing unit. Serial and parallel combinations are used to optimize the area, power and speed. In the block-processing unit, image pixels are transformed into wavelet domain using CDF 5/3 wavelet filters. These transformed coefficients are modified to embed a watermark and inverse wavelet is calculated.

The block-processing unit consists of Time Division Multiplexer (TDM), Time Division Demultiplexer (TDD), forward CDF 5/3 wavelet filter bank, watermarking block, adaptive gain block, and inverse CDF /3 wavelet filter bank. Figure 10 shows the block-processing unit. Serial and parallel combinations are used to optimize the area, power and speed. In the block-processing unit, image pixels are transformed into wavelet domain using CDF 5/3 wavelet filters. These transformed coefficients are modified to embed a watermark and inverse wavelet is calculated.

The TDD (1:8) is used to divide the input data into even and odd samples. These samples are fed to the forward CDF 5/3 wavelet filter bank. Lifting scheme is implemented in a parallel way so that all the coefficients are calculated at the same time. Figure 7(a) shows the implementation of forward CDF 5/3 filters.

The transformed coefficients are then sent to watermarking block as well as to adaptive gain block. In adaptive gain block, the energy in each sub-band is calculated by equations (1), (2) and (3).  $E_L$  is the energy present in the lower frequency band;  $E_H$  is the energy present in the higher frequency band and  $E_M$  is the energy present in the middle band.  $E_M$  is calculated by taking an average value of the energy present in vertical and horizontal bands. These calculated energies are then compared to select one of the gain factors. If the value of  $E_L$  is greater than  $E_M$ , then the gain is small. The gain will be moderate if  $E_M$  is greater than  $E_H$  and if  $E_H$  is greater than  $E_M$ , then the gain will be large. Figure 8 shows the logical implementation of the adaptive gain block. This adaptive gain value and transformed coefficients are fed to the watermarking block. The watermarking block then modifies these transformed values according to the watermarking block consists of eight such units in one watermarking block. In the block-processing unit, such eight blocks are used in parallel to modify the pixel values.

Modified transformed values are then fed to the inverse CDF 5/3 filters. The parallel eight filters are used to calculate the inverse wavelet. Figure 7(b) shows the implementation of the inverse CDF5/3 wavelets. TDMs are used to convert these

equation shown in the watermarking algorithm. If the watermarking bit is one then the gain value is added to the transformed pixel value, otherwise, zero is added. Figure 9 shows the implementation of the watermarking equation. The parallel coefficients into serial. The memory addresses from the address generator are delayed and are used to store watermarked pixel values.

## VIII. EXPERIMENTAL RESULTS

### A. Synthesis and Implementations

The architecture was designed using VHDL and using Xilinx ISE technology, functional modeling was conducted. The algorithm has been synthesized from Xilinx Spartan-3A DSP technology on XC3SD1800A-4FGG676C device. The overview of the use of hardware is provided in Table II.

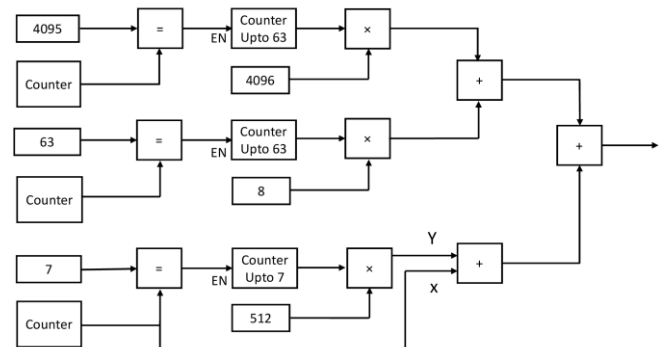


Fig. 6. Address generator unit

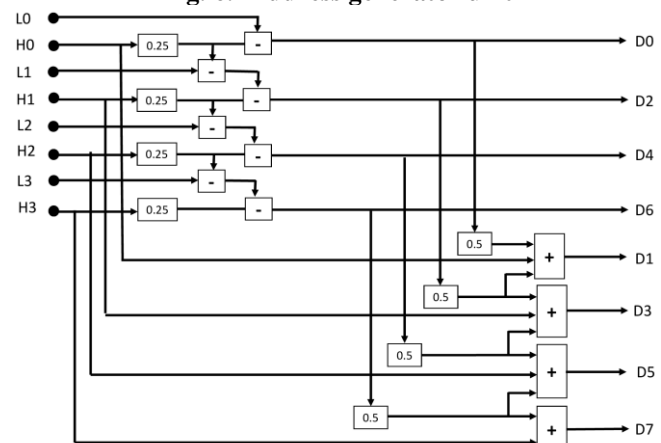


Fig. 7(a). Forward CDF 5/3 wavelet filter

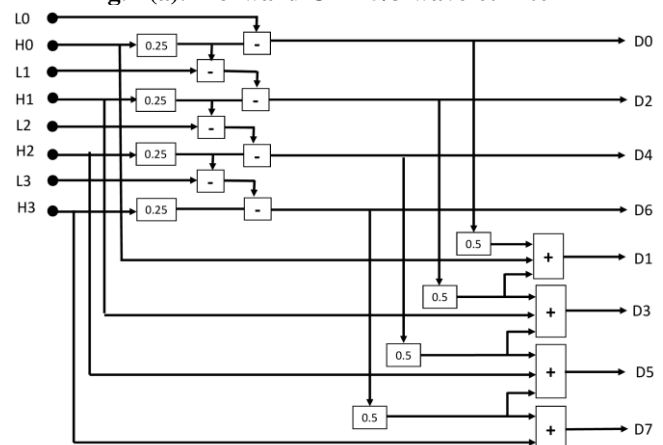


Fig. 7(b). Inverse CDF 5/3 wavelet filter



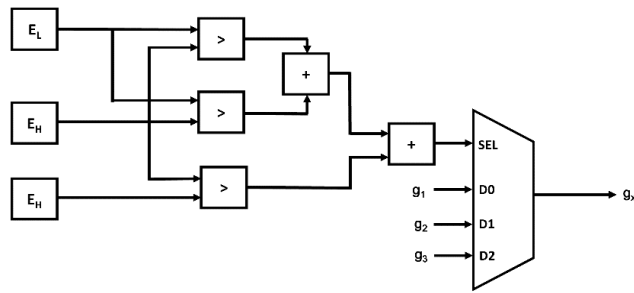


Fig. 9. Watermark embedder

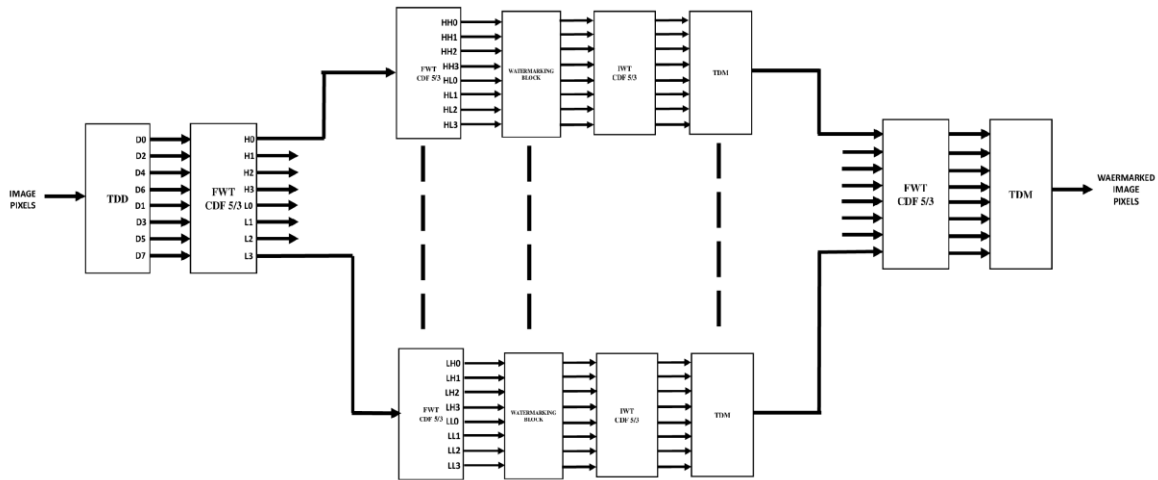


Fig. 10. Block-processing unit

IX. EXPERIMENTAL RESULTS

A. Synthesis and Implementations

The architecture was designed using VHDL and using Xilinx ISE technology, functional modeling was conducted. The algorithm has been synthesized from Xilinx Spartan-3A DSP technology on XC3SD1800A-4FGG676C device. The overview of the use of hardware is provided in Table II.

The Hardware co-simulation technique [30] was used to verify the results. The HIL was operating at a frequency of 50 MHz clock. The power analysis is performed using Xilinx Xpower analyzer and it is estimated that the power consumption will be 211 mW. The design can operate with the maximum frequency of 63.910 MHz. Maximum path delay was estimated as 15.647ns for the design. Figure 11 shows the RTL schematic and Figure 12 shows the floor plan for the chip.

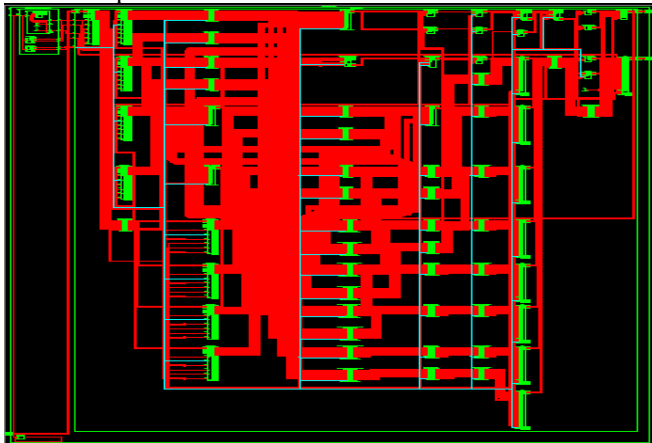


Fig. 11. RTL schematic of the chip

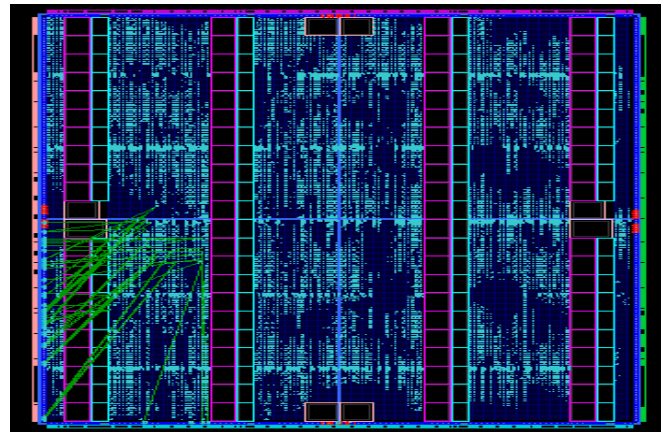


Fig. 12. Floor plan of the chip

Table II Hardware Utilization

Logic Utilization	Used	Available	Utilization %
Number of slice flip flops	2789	33280	8
Number of 4-input LUTs	1591	33280	47
Number of occupied slices	1072	16640	64
Number of slices containing only related logic	1072	10722	100
Total number of 4-input LUTs	1822	33280	54
Number of bonded IOBs	39	519	7

## B. Image Quality Measures

The image quality assessments are discussed in various papers [31][32]. Fair benchmarking and quality assessment [33] as well as visual degradation due to embedding are major issues that need to be addressed. Based on subjective and qualitative demands, image quality criteria are classified. A human member offers the subjective needs efficiency rating. Figure 13 shows the initial picture and Figure 14 shows the watermarked picture. Note that in this case it is difficult to discover the distinction between the original and watermarked images with the naked eyes.

Qualitative criteria use numerical methods to find the difference between two images. It can be further classified into two broad classes univariate and bivariate. A univariate measure gives a numerical significance to a single image based on picture field measurements, and a bivariate measure is a numerical comparison of two pictures. In the evaluation of image quality, bivariate tests are used more frequently. Different efficiency assessment metrics such as PSNR (dB), image fidelity (IF), standardized cross correlation, and quality of correlation are calculated. Table III describes the performance metric for low-medium and high-texture images. The image dataset provided by the University of Southern California was used for the experiments. As the watermarking algorithm is image adaptive it can be seen from Table III, the image with the high texture is having the low PSNR and others factors like MSE and MD are high. Comparatively the Lena image is having high PSNR value as it is having a minimum texture.

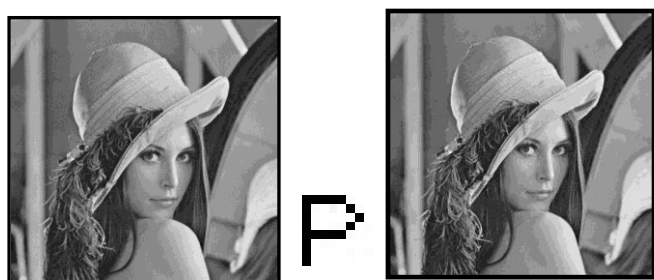


Fig. 13. Original image and watermark Fig. 14. Watermarked image

Table III Quality Metric of Watermark Images

Quality Measures	Lena	Wood	Fabri c
Mean Square Error	144.35	168.52	405.12
PSNR	26.53	25.86	22.05
Normalized Absolute Difference	0.0814	0.082	0.1213
Average Difference	9.62	9.24	13.64
Structural Content	0.8751	0.9024	0.8647
Maximum Difference	44	64	106
Normalized Mean Square Error	0.0082	0.0076	0.0186
Image Fidelity	0.9918	0.9924	0.9814

## X. PERFORMANCE EVALUATIONS ON VARIOUS ATTACKS

In this section, we use a benchmark software to assess the watermarking algorithm's performance against multiple attacks[34]. StirMark[35] is a generic software designed by the University of Cambridge, Markus Kuhn, Computer Laboratory. StirMark is used to assess the robustness of algorithms for image-watermarking and other methods for steganography. This software includes multiple attacks with medium compression such as JPEG compression, addition of noise, rotation, cropping, scaling and geometric transformation. These attacked images are processed with the software program to detect watermarks. In non-blind detection, the original and recovered watermarks are compared to find the Bit Error Rate (BER). For watermark detection, BER should be less than 20%. In a blind detection technique, the threshold is kept at  $\gamma=0.80$  for watermark from the results, the suggested watermarking scheme can be seen to be strong against geometric assaults such as cropping, rotation, lines removal, lateral distortion and other assaults such as affine transformation, JPEG compression assaults. Table IV(A) and (B) summarize some of the outcomes of these evaluations. In Table IV(A) CROPT\_50 means the image is cropped by 50% still the watermark is able to detect. The watermark shows its existence even if the image is rotated by anticlockwise by 0.5 degrees in ROT\_-0.5. it also survives in compound attacks like ROTCROP\_2 which means the image is rotated by 2 degrees anti-clockwise and then cropped. RML\_30 attacks mean some of the horizontal pixels is removed from the image. Watermark survives well even after affine transform and lateral distortion attack.

Table IV indicate the maximum cross-correlation values (CCR) for the detected watermark. The false positive rate of watermark detection algorithm is 20%.

## XI. CONCLUSION

In this paper, we presented novel architecture in the wavelet domain for an image-adaptive watermarking. We also discussed various aspects of the digital design such as hardware Co-simulation test, which is most important for result validation. Serial and parallel architecture gives low power consumptions, minimum hardware utilization and better speed. Our algorithm performance well than the architectures described in a [23] and [24] in terms of clock speed and power dissipation. Additionally, we discussed the performance of the watermarking system under various attacks. Its dual detection technique makes it more robust against attacks, as one or another technique can be used to detect watermarks. In the future, we plan to develop a full parallel architecture model for image-adaptive watermarking system, which will consider all the aspects of an image including luminance, texture and frequency sensitivity.

Table IV (A) Performance Evaluation



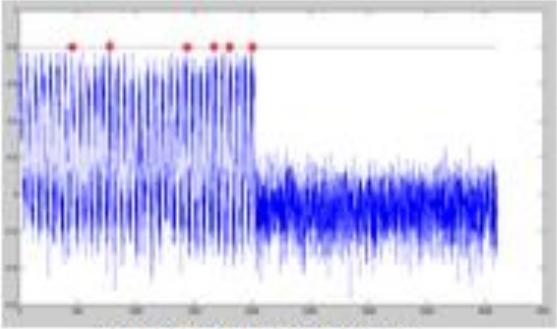


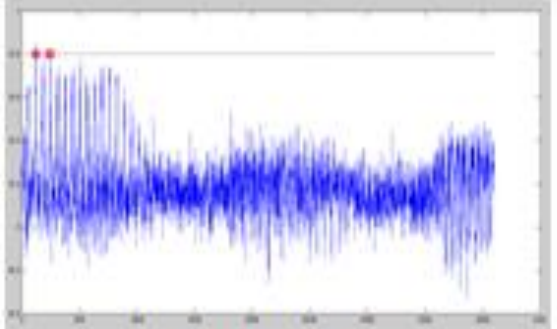


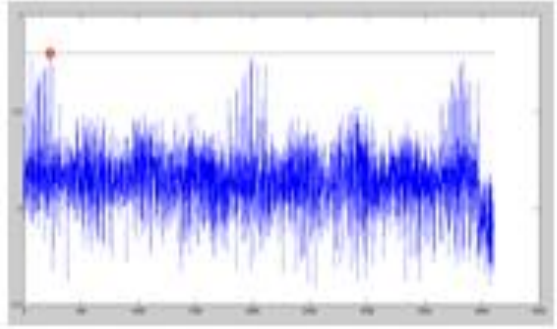


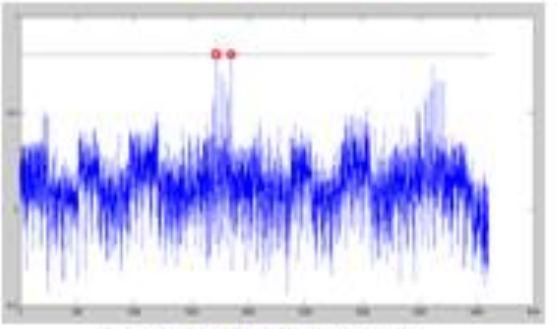


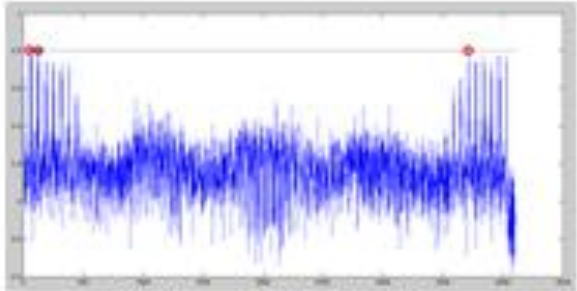


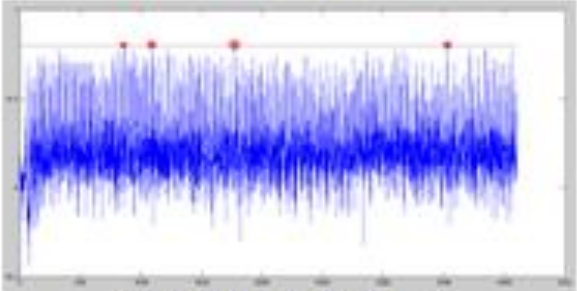


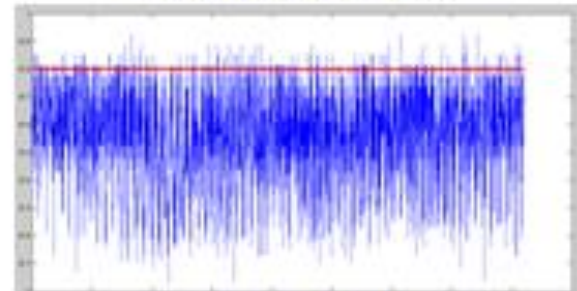


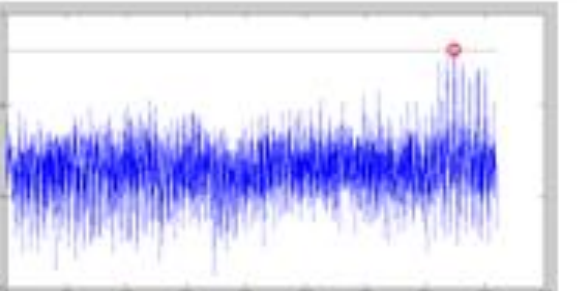
Attacks	Non-Blind Detection	Blind Detection
 <p>CROP_50</p>	 <p>BER=6.25</p>	 <p>Maximum CCR value =0.85</p>
 <p>ROT_-0.5</p>	 <p>BER=7.81</p>	 <p>Maximum CCR value =0.81</p>
 <p>ROTCROP_-2</p>	 <p>BER=7.81</p>	 <p>Maximum CCR value =0.81</p>
 <p>RML_30</p>	 <p>BER=7.81</p>	 <p>Maximum CCR value =0.81</p>



Table IV (B) Performance Evaluation

Attacks	Non-Blind Detection	Blind Detection
 ROTCROP_1	 BER=7.81	 Maximum CCR value =0.81
 AFFINE_2	 BER=7.81	 Maximum CCR value =0.81
 JPEG_50	 BER=3.12	 Maximum CCR value =0.92
 LATESTRNDDIST_1.1	 BER=7.81	 Maximum CCR value =0.81

REFERENCES

1. D. KUNDUR, K. KARTHIK, Video fingerprinting and encryption principles for digital rights management, Proc. IEEE. 92 (2004) 918–932. doi:10.1109/JPROC.2004.827356.
2. E. Fu, Literature survey on digital image watermarking, Lect. NotesEE381KMultidimens.Signal.(1998).http://users.ece.utexas.edu/~bevans/courses/ee381k/projects/fall98/fu/literatureSurvey.pdf (accessed July 25, 2016).
3. N. Memon, P.W. Wong, Protecting digital media content, Commun. ACM. 41 (1998) 35–43. doi:10.1145/278476.278485.
4. P.A. Fordjour, I. Engineering, Spatial Domain Technique for Visible Watermarking, J. Shanghai Univ. 7 (2003) 384–388.
5. J.R. Hernandez, M. Amado, F. Perez-Gonzalez, DCT-domain watermarking techniques for still images: detector performance analysis and a new structure, IEEE Trans. Image Process. 9 (2000) 55–68. doi:10.1109/83.817598.
6. S.N.T. and G.N. shinde Pankaj U. Lande, Adaptive DCT Domain Watermarking For Still Images, in: International Conf. RACE-07, 2007.
7. S. Agreste, G. Andaloro, D. Prestipino, L. Puccio, An image adaptive , wavelet-based watermarking of digital images, J. Comput. Appl. Math. 210 (2007) 13–21. doi:10.1016/j.cam.2006.10.087.
8. P. Meerwald, A. Uhl, Survey of wavelet-domain watermarking algorithms, in: P.W. Wong, E.J. Delp III (Eds.), Proc. SPIE 4314, Secur. Watermarking Multimed. Contents III, 505 (August 1, 2001), 2001: pp. 505–516. doi:10.1117/12.435434.
9. A.T.S. Ho, J. Shen, S.H. Tan, Robust digital image-in-image watermarking algorithm using the fast Hadamard transform, in: M.S. Schmalz (Ed.), Proc. SPIE 4793, Math. Data/Image Coding, Compression, Encryption V, with Appl. 76 (January 1, 2003),



- International Society for Optics and Photonics, 2003: pp. 76–85. doi:10.1117/12.451250.
10. P.U. Lande, S.N. Talbar, FPGA Implementation of Image Adaptive Watermarking Using Human Visual Model, ICGST-PDCS J. 9 (2009) 17–22.
  11. I.J. Cox, J. Kilian, T. Leighton, T. Shamoon, A secure, robust watermark for multimedia, in: Inf. Hiding, Springer Berlin Heidelberg, 1996: pp. 185–206. doi:10.1007/3-540-61996-8\_41.
  12. M.A. Soni, S.P. Metkar, P.U. Lande, Blind and invisible watermarking techniques for color images, in: Thinkquest–2010, Springer India, New Delhi, 2011: pp. 227–233. doi:10.1007/978-81-8489-989-4\_42.
  13. I.J. Cox, J. Kilian, T. Leighton, T. Shamoon, Secure spread spectrum watermarking for images, audio and video, in: Proc. 3rd IEEE Int. Conf. Image Process., IEEE, 1996: pp. 243–246. doi:10.1109/ICIP.1996.560429.
  14. C.-C. Chang, J.-C. Chuang, An image intellectual property protection scheme for gray-level images using visual secret sharing strategy, Pattern Recognit. Lett. 23 (2002) 931–941. doi:10.1016/S0167-8655(02)00023-5.
  15. N.M. Makbol, B.E. Khoo, A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition, Digit. Signal Process. 33 (2014) 134–147. doi:10.1016/j.dsp.2014.06.012.
  16. E. Kougiianos, S.P. Mohanty, R.N. Mahapatra, Hardware assisted watermarking for multimedia, Comput. Electr. Eng. 35 (2009) 339–358. doi:10.1016/j.compeleceng.2008.06.002.
  17. S.P. Mohanty, R.K. C. S. Nayak, FPGA Based Implementation of an Invisible-Robust ImageWatermarking Encoder, in: Intell. Inf. Technol., Springer Berlin Heidelberg, 2004: pp. 344–353. doi:10.1007/978-3-540-30561-3\_36.
  18. A.M. Joshi, P.D. Scholar, Design and Implementation of Real-Time Image Watermarking, in: 2010 Annu. IEEE India Conf. Publ. IEEE, 2010: pp. 1–4.
  19. P. Jana, A. Phadikar, G.K. Maity, Reversible Data Hiding for Content Verification and Quality Access control of Image and its Hardware Implementation, Proc. Int. Conf. Electr. Electron. Optim. Tech. IEEE Explor. Chennai, Tamil Nadu, (2016) 3324–3329.
  20. P. Karthigaikumar, K. Baskaran, An ASIC implementation of a low power robust invisible watermarking processor, J. Syst. Archit. 57 (2011) 404–411. doi:10.1016/j.sysarc.2010.03.008.
  21. V.E. Jayanthi, V. Rajamani, P. Karthikeyan, High performance VLSI architecture for block based visible image watermarking, Int. J. Electron. 99(2012)1191–1206.
  22. G. Singh, M.S. Lamba, Efficient hardware implementation of image watermarking using DWT and AES algorithm, 2015 39th Natl. Syst. Conf. (2015) 1–6. doi:10.1109/NATSYS.2015.7489093.
  23. J. Ahmed, A. Aziz, P. Akhtar, FPGA based efficient architecture for image watermarking using Wavelet Co-efficients Quantization, in: 2014 Int. Conf. Open Source Syst. Technol., 2014: pp. 105–112. doi:10.1109/ICOSST.2014.7029329.
  24. S. Ghosh, S. Talapatra, J. Sharma, N. Chatterjee, H. Rahaman, S.P. Maity, Dual Mode VLSI Architecture for Spread Spectrum Image Watermarking using Binary Watermark, Procedia Technol. 6 (2012) 784–791. doi:10.1016/j.protcy.2012.10.095.
  25. S.P. Mohanty, A secure digital camera architecture for integrated real-time digital rights management, J. Syst. Archit. 55 (2009) 468–480. doi:10.1016/j.sysarc.2009.09.005.
  26. A. Skodras, C. Christopoulos, T. Ebrahimi, The JPEG 2000 still image compression standard, IEEE Signal Process. Mag. 18 (2001) 36–58. doi:10.1109/79.952804.
  27. M. Charrier, D.S. Cruz, M. Larsson, JPEG2000, the next millennium compression standard for still images, in: Proc. IEEE Int. Conf. Multimed. Comput. Syst., IEEE Comput. Soc, 1999: pp. 131–132. doi:10.1109/MMCS.1999.779134.
  28. Y.H. Seo, D.W. Kim, VLSI architecture of line-based lifting wavelet transform for motion JPEG2000, IEEE J. Solid-State Circuits. 42 (2007) 431–440. doi:10.1109/JSSC.2006.889368.
  29. I. Saeed, H. Agustianwan, Lifting-based VLSI Architectures for Two-Dimensional Discrete Wavelet Transform for Effective Image Compression, I (2008) 19–21.
  30. P.A.V.G. Neha.P.Raut, FPGA Implementation for Image Processing Algorithms Using Xilinx System Generator, IOSR J. VLSI Signal Process. 2 (2013) 26–36.
  31. A.M. Eskicioglu, P.S. Fisher, A Survey of Quality Measures for Gray Scale Image Compression, in: Proc. 1993 Sp. Earth Sci. Data Compression Work., 1993: pp. 49–61.
  32. M. Kutter, F. a P. Petitcolas, A fair benchmark for image watermarking systems, SPIE 3657, Secur. Watermarking Multimed. Contents. 3657 (1999) 25–27. doi:10.1117/12.344672.
  33. F.A.P. Petitcolas, Watermarking schemes evaluation, IEEE Signal Process. Mag. 17 (2000) 58–64. doi:10.1109/79.879339.
  34. F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Attacks on Copyright Marking Systems, in: Springer, Berlin, Heidelberg, 1998: pp. 218–238. doi:10.1007/3-540-49380-8\_16.
  35. M. Kutter, F.A.P. Petitcolas, Fair benchmark for image watermarking systems, in: P.W. Wong, E.J. Delp III (Eds.), International Society for Optics and Photonics, 1999: pp. 226–239. doi:10.1117/12.344672.

## AUTHORS PROFILE

**Pankaj U. Lande** Assistant Professor and Head, Department of Electronics in Government of Maharashtra's Rajaram College, Kolhapur. The author has 9 years' experience of teaching Electronics to undergraduate college and 4 years of experience teaching Electronics at postgraduate at SPPU University, Pune. He has published 11 international paper and four textbooks for Shivaji university.



from SGGS Institute



**Sanjay N. Talbar** received his B.E and M.E degrees of Technology, Nanded, India in 1985 and 1990 respectively. He obtained his PhD from SRTM University, Nanded, India in 2000. He received the "Young Scientist Award" by URSI, Italy in 2003. He had Collaborative research programme at Cardiff University Wales, UK. Presently he is working as Professor, Department of Electronics & Telecommunication Engg., SGGS Institute of Engineering & Technology Nanded, India. He has published more than 50 journal papers, 10 books and more than 125 papers in referred National as well as International Conferences. His research interests includes Image Processing, Medical Image processing, Multimedia Computing and Embedded System Design. He is a member of IEEE, IET, IETE, AMPI, ISTE, and worked on many prestigious committees in academic field of India.



He has awarded Benjoni Jalnawala award for securing highest marks at B.Sc. Seventeen research scholars were awarded Ph.D. degree under his guidance. He has published more than 80 papers in the International Journals and presented more than 50 papers in International Conferences. He was more than the five times Chairperson for International Conference in abroad. In his account one book is published, which is reference book for different courses in different Universities. He is also member of different academic & professional bodies such as IAENG (Hon Kong), ANAS (Jordan). He is in reviewer panel for different Journals such as IEEE (Transactions on Neural Networks), International Journal of Physical Sciences (U.S.A.), Journal of Electromagnetic Waves and Applications (JEMWA, U.S.A.). His abroad Visit includes U.S.A., Thailand, Portugal, Germany, Switzerland, Italy, Vatican City, Monaco, France, Maldives, Sri Lanka, U. K., Scotland, China , New Zealand and Hong Kong. His research interest includes Filters, Wireless Sensor Network System, Image processing and Multimedia analysis and retrieval system.

**Dr. G. N. Shinde** is presently Principal of Yashwanth College Nanded, India. He was Pro-Vice Chancellor, SRTM University, Nanded, Maharashtra, INDIA. He has received "Ideal State Teacher Award" from Government of Maharashtra, India for 2008-09 and "Best Principal Award" for 2009-2010 from S.R.T.M. University, Nanded, Maharashtra. He has received M. Sc. & Ph.D. degree from Dr. B.A.M. University, Aurangabad.