IMAGE ADAPTIVE WATERMARKING USING FUZZY LOGIC ON FPGA

Pankaj U.Lande
Dept. instrumentation science
University of Pune, Pune
pul@usic.unipune.ac.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 novel hardware architecture for watermarking unit which can be used with the JPEG2000 compression standard. We have presented dual watermark detection which is also novelty of our algorithm. Hardware assisted watermarking offers advantages over the software implementations in terms of less area, power consumption, real time. The objective is to develop the real time low cost and robust watermarking hardware which can be incorporated with existing systems such as digital camera, scanners, camcorders etc. We have implemented CDF 5/3 wavelet filters with lifting scheme which requires less hardware and memory efficient. The present algorithm was tested with standard benchmark software StirMark. The experimental result shows that the proposed scheme of watermarking is robust against most of the geometric attacks scaling, rotation, remove lines and cropping.

Keywords- *Watermarking, FPGA, CDF 5/3, JPEG200*

1. INTRODUCTION

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]. This needs the gives rise to the new technology of hiding the information in the digital content which is called as watermarking.

Watermarking techniques can be divided into various categories in numerous ways. According to human perception, the digital watermarking can divided into visible [3] and invisible watermarking [4][5].On the basis of performance against various attacks watermarking techniques can be divided into invisible fragile[6] or robust watermarking [5].

The watermarking method can be divided into three primary methods depending on the insertion and extraction domain used for watermarking. These are spatial domain, transform domain and color space methods. The spatial domain method [7] involves an algorithm that directly operates on the pixel values of the host image. It is been observed that the spatial domain watermarks are weaker than the frequency domain watermarking methods [4][5]. However the spatial domain watermarking scheme requires less computations compared to frequency domain scheme.

In the transform domain method the pixel values are transformed into another domain by applying appropriate transform technique like discrete cosine transform (DCT) [4],discrete wavelet transform (DWT) [5] and discrete Hadamard transform(DHT) [8]. A watermark is then embedded by modifying these coefficients. A DCT based watermarking algorithm has been described in many literatures; however DWT based watermarking algorithms are more effective for several reasons [9].

There are several software based watermarking scheme are available in literatures [4][5] but hardware implementation has advantages over software. Hardware implementations offer an optimized specific small design, fast and potentially cheap watermarking solutions. A hardware based watermarking unit can be easily integrated with digital cameras, scanners graphics processing units, camcorders etc. Watermarking unit consumes lesser power than software, which requires a general purpose processor so that hardware based watermarking unit is ideal for battery operated applications. It is most suitable for real-time applications, where the computation time is deterministic and short.

JPEG2000 is the newest version of one of the most popular image formats and it includes the DWT. Efficient VLSI implementations of DWT processors with watermarking unit became more important[10][11].The hardware assisted watermarking scheme implemented on FPGA has been presented in following literatures.

An FPGA based invisible robust spatial domain watermarking is described in [13]. The watermark insertion is carried out by replacing original image pixel value by watermark encoding function. 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 [14] based on DCT. The algorithm work for both gray and color image and the biometric image is selected as watermark. The prototype was modeled using VHDL and implemented on XC2V500-6FG256 device from Xilinx.

Saraju P. Mohanty et. al. [15] 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. 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. For the watermark detection the difference is calculated to detect a watermark.

Image adaptive watermarking and its hardware architecture is described in DHT domain[8]. The proposed scheme of watermarking is invisible and robust against JPEG attacks. 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.

In [16] spread spectrum based image watermarking scheme is described. The watermark is embedded in cover image using bi-phase modulation. The watermark detection method is blind. The behavioral simulation is done using Modelsim XE 6.1e and chip operates at 219.542MHz.

The objective of this paper is to develop an image watermarking hardware architecture that can serve the purpose of image authentication and secured communication of images in real time environment. The proposed scheme is an invisible robust wavelet domain watermarking method.

2. FUZZY INTERFACE SYSTEM (FIS)

Human visual system (HVS) has been characterized with several phenomenon that permits to adjust the pixel values to elude perception. These phenomenons are luminance sensitivity, frequency sensitivity and texture sensitivity. The distortion visibility is very low if the back ground is with the high texture..

Fuzzy logic approach is used to estimate the optimal gain with a proper scaling factor so that the watermark remains imperceptible. This approach enables the texture sensitivity membership function to be adjusted in such a manner to best fit the image's properties. Each input is composed of three member ship function based on the variance distributed among smooth, slightly rough and rough. The output of the FIS is gain factor for the particular block is based on the three membership function minimum, medium and maximum. This block calculates the variance of the image block. The calculated variance is fed to the FIS. The fuzzy rules and the membership function were developed using intuition logic. The image with low texture is called as smooth and with medium texture is called as slightly rough and so on. The following rules calculated corrected the amount of gain for the particular block. The following simple fuzzy rules illustrated are as follows

1. If the image block is smooth (low variance) then gain is minimum.
2. If the image block is slightly rough (medium variance) then gain is medium.
3. If the image block is rough (high variance) then gain is maximum.

The defuzzified output D, is calculated for the composite output set, using a volume defuzzification method.

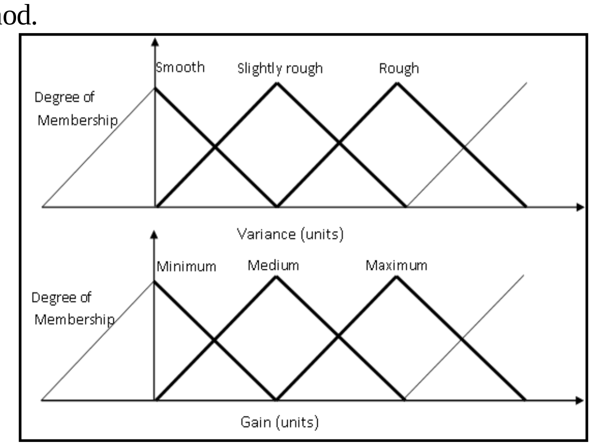


Fig.1. Fuzzy Membership for Variance And Gain

3. PROPOSED WATERMARKING SCHEME

The original image I is divided into non-overlapping blocks of size B×B. the image block is fed to CDF 5/3 filters to calculate wavelet transform. A binary watermark is embedded into cover image using equation (1).

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

$$\text{Whereas} \quad K = \beta \times D \quad (2)$$

β is a global scaling factor and D is defuzzified out of FIS.

$I_{W,N}$ is the N^{th} block of the watermarked image ; W is a binary watermark logo. x and y are index numbers. In each block of B×B one watermark is implemented.

TABLE I. PSNR FOR DIFFERENT TEXTURE IMAGES

Image	PSNR
Wall	56.14 dB
Lena	43.97dB
Grass	42.18dB

4. HARDWARE ARCHITECTURE FOR PROPOSED SCHEME

. The watermarking chip mainly consists of a block processing unit, FIS and control.

4.1 Block Processing Unit

The block processing unit considers the original image block as input. This unit consists of CDF 5/3 wavelet filters and watermarking unit. Image block is wavelet transformed and the watermark is embedded using equation (1).

We have used the lifting scheme descried in[11]. 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 the predict step predicts values in the odd set where α= -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 β=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 2.

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.

The watermarking unit consists of two multipliers and adder. The watermark is embedded using equation (1). 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.

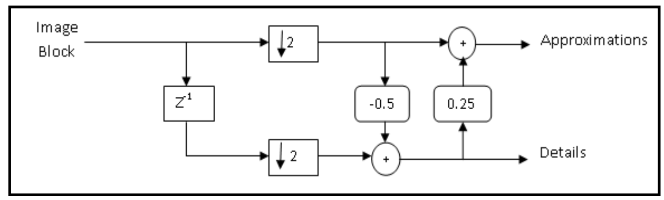


Fig.2.CDF 5/3 Wavelet Filter

4.2 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

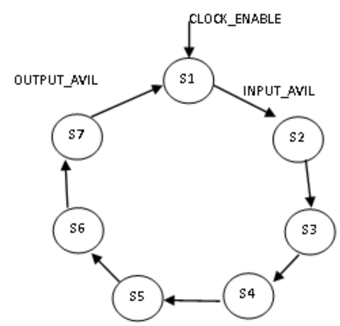


Fig.3.Control System as FSM

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 a 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: calculate variance of the block

S4: α is calculated by using FIS

S5: embedded the watermark

S6: calculate inverse DWT

S7: generate OUTPUT_AVIL signal

4.3 Watermark Detection

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

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

τ represents threshold for blind detection

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

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

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

5. EXPERIMENTAL RESULTS

5.1 Device Utilization

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 the hardware in the loop configuration using AccelDSP. The HIL was run at 33.3 MHz and the samples were fed to the target device at a rate of 287.67 KSPS through a JTAG USB cable. The proposed design utilizes 391 startup clock cycles and 130 clock cycles per function call. The device utilization summary is given in Table II. Figure 4 shows the RTL of the watermarking chip. The power consumption is calculated using XPower tool and it is 175mW.

TABLE II. DEVICE UTILIZATION

Logic Utilization	Utilization
Number of Slices	15%
Number of Slice Flip Flops	7%
Number of 4 input LUTs	11%
Number of bonded IOBs	94%
Number of GCLKs	4%
DSP48 blocks	15%

5.2 Image Quality Measures

In [17] 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. 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 III.

Quality Measures	Lena	Wall	Grass
Mean square error	6.80	6.74	6.80
PSNR	43.97	56.14	42.18
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 III. IMAGE QUALITY MEASUURES

5.3 Performance Evaluations against Various Attacks

In this section we discuss performance of the watermarking algorithm against various attacks by standard bench mark software. StirMark is the one of the earliest benchmark software. The StirMark includes several attacks like compression, geometric transformation, noise addition etc. the geometric attacks includes rotation, cropping, scaling and geometric transformation with medium compression. Some of the results are summarized in the Table IV.

Results show that the proposed watermarking scheme is robust against the geometric attacks.

6. CONCLUSION

In this paper, we have proposed a novel image adaptive invisible watermarking algorithm and developed the efficient hardware architecture. The importance of fuzzy logic to calculate the gain factor with respect to the texture sensitivity of the image was also proved. The proposed design utilizes the less hardware resources as it can be seen from device utilization summary. The experimental results showed that the proposed watermarking scheme is imperceptible and robust against geometric attacks. This was achieved because of the space and frequency localizing property that is characteristics to the discrete wavelet transform technique. In future we are planning to develop the image adaptive watermarking system which will consider the luminance, texture and frequency sensitivity to construct the full human visual model.

Refrances

[1].S. Katzenbeisser and F. A. P. Petitcolas: *Information Hiding techniques for steganography and digital watermarking*, Artech House, Inc., MA, USA, 2000.

[2].N. Memon and P. W. Wong.:Protecting Digital Media Content. *Communications of the ACM*, vol. 41, no. 7, pp. 34–43, Jul 1998.

[3].S. P. Mohanty.:Watermarking of Digital Images.M.S. thesis, Indian Institute of Science, Bangalore, India, 1999.

[4].Pankaj U. Lande,Sanjay N.Talbar and G.N. shinde.:Adaptive DCT Domain Watermarking For Still Images.;*International Conference RACE-07*,Bikaner, Rajastan, India,2007.

[5].Pankaj U.lande,Sanjay N.Talbar and G.N. shinde.: Hiding A Digital Watermark Using Spread Spectrum At Multi-Resolution Representation. *International conference ACVIT07*, Aurangabad, India, 2007.

[6].C. T. Li.:Digital fragile watermarking scheme for authentication of JPEG images. IEE Proc.-Vis. Image Signal Processing, Vol. 151, No. 6, , pp. 460-466, December 2004.

[7].N. Nikolaidis, I. Pitas.:Robust Image Watermarking in Spatial Domain. *International journal of signal processing, 66*(3), 385-403, 1988.

[8].Pankaj U.Lande,S.N. Talbar,G.N. Shinde.:FPGA iplimentation of image adaptive watermarking using human visual model.ICGST-PDCS,Vol.9,Issue1,Oct. 2009.

[9].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.

[10].M. Nagabushanam,Cyril Prasanna Raj P, S. Ramachandran "Design and Implementation of Parallel and Pipelined Distributive Arithmetic Based Discrete Wavelet Transform IP Core" European Journal of Scientific Research ISSN 1450-216X Vol.35 No.3 pp.378-392,2009.

[11]. 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.

[12]. Abhishek Basu, Tirtha Sankar Das, Somnath Maiti, Nurul Islam and Subir Kumar Sarkar.:FPGA Based Implementation of Robust Spatial Domain Image Watermarking Algorithm. International Conference on Computers and Devices for Communication, 2009.

[13]. S. P. Mohanty, R. K. C., S. Nayak, FPGA Based Implementation of an Invisible-Robust Image WatermarkingEncoder, in: Lecture Notes in Computer Science, Vol. 3356, pp. 344–353, 2004.

[14]. 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.

[15].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, pp. 468-480, October-December 2009.

[16] Sudip Ghosh and santi P. Maity, "spread spectrum watermarking with digital design"IEEE international advance computing conference(IACC 2009)Patiala,2009.

[17].M. Kutter and F.A. Petitcolas, "A Fair Benchmark for Image Watermarking Systems",*Electronic imaging ,Security and Watermarking of Multimedia Contents, VOL. 3657*, pp. 25-32,1999.

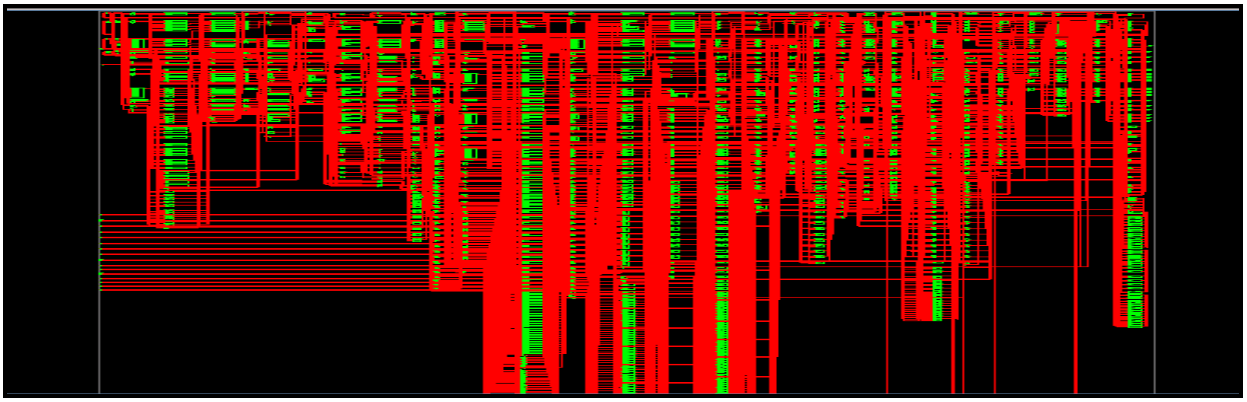
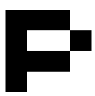
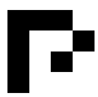
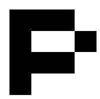
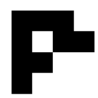
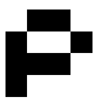
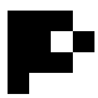
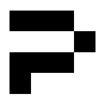
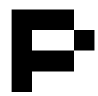
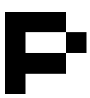
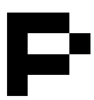
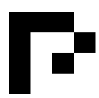
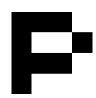
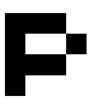
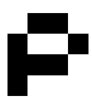
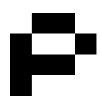
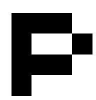


Fig 4. RTL of Watermarking Chip

TABLE IV. PERFORMANCE AGAINST ATTACKS

 AFFINE_5	 CONV_2	 Crop_25	 MEDIAN_7
 NOISE_20	 RESC_75	 RESC_110	 RML_10
 RML_50	 RNDDIST_1.1	 ROT_15	 ROT_-1
 ROTSCALE_-0.75	 ROTSCALE_1	 ROTCROP_-0.5	 ROTCROP_0.75

ISBN: 978-960-474-276-9