Design and Implementation of SDRAM controller based Digital Watermarking with combined DWT-DCT Technique on FPGA

Prof Pramod Kumar Naik[1], Prof Arun S Tigadi[2], Dr.Hansraj Guhilot[3]

[1] Department of Electronics & Communication Engineering, VCET, Puttur, Karnataka, India
[2] Department of Electronics & Communications, KLE DR. M.S.S CET, Belgaum, Karnataka, India
[3]Principal K.C.College of Engineering & Management Studies and Research, Thane, Maharashtra, India

Abstract- Safeguarding creative content and intellectual property in a digital form has become increasingly difficult as technologies, such as the internet, broadband availability and mobile access advance. It has grown to be progressively easier to copy, modify and redistribute digital media, resulting in great declines in business profits. Digital watermarking is a technique which has been proposed as a possible solution to this problem. Digital Watermarking is a technology which is used to identify the creator, owner, distributor of a given video or image by embedding copyright marks into the digital content, hence digital watermarking is a powerful tool used to check the copy right violation. A robust watermarking technique based on DWT (Discrete Wavelet Transform), DCT (Discrete Cosine Transform) and combined DWT-DCT is presented. In these techniques the insertion and extraction of the watermark in the gray scale image is found to be simpler than other transform techniques. All three methods are simulated using two watermarking algorithms. The performance of the two algorithms is evaluated by applying various attacks on the watermarked image and results tabulated. This paper describes SDRAM control which enhances the overall performance.

Index Terms- DWT, DCT, SDRAM.

I. Introduction

Digital watermarking can be defined as the process of embedding a certain piece of information (technically known as watermark) into multimedia content including text documents, images, audio or video streams, such that the watermark can be detected or extracted later to make an assertion about the data [14].In the digital watermarking system, information carrying the watermark is embedded in an original image. The watermarked image is transmitted or stored, and then decoded to be resolved by the receiver. The goal of the watermarking system is not to restrict access to the original image, but to ensure that embedded data remain recoverable. The essential factors of a good watermarking scheme are robustness, imperceptibility, watermark capacity and security. Robustness refers to the ability to survive intentional attacks as well as accidental modifications, for instance, lossy compression, and noise insertion, region cropping, local and global geometrical transformations.

Imperceptibility or fidelity refers to the perceptual similarity between the watermarked image and its cover image. Watermarking methods with highly complex algorithms that incur more computational costs compared to low complexity. Higher robustness often offsets imperceptibility of a watermark [3].The number of watermark bits encoded in a message is data payload and the maximum repetition of data payload within an image is the watermark capacity. A watermark may have higher capacity but lower data payload. Higher capacity would comprise its imperceptibility because more modifications to the cover image are needed to embed the watermark. Many of the watermark properties have conflicting characteristics. Therefore, designing a watermarking method usually requires finding a balance among these conflicting factors. The main focus is on image watermarking. Image watermarking can be done in the spatial domain as well as in the frequency domain. The most common and the simplest watermarking technique in the spatial domain is the least significant bit (LSB). The watermark to be embedded is placed in the LSB of the source image. Spatial domain methods are less complex as no transform is used, but are not robust against attacks. To obtain better imperceptibility as well as robustness, the addition of the watermark is done in a transform domain/frequency domain. DCT and DWT are popular transforms widely used in transform based watermarking. Frequency based techniques are robust against attacks involving image compression and filtering, because the watermark is actually spread throughout the image, not just operating on an individual pixel [11].Frequency domain methods are similar to spatial domain watermarking in that the values of selected frequencies can be altered. Because high frequencies will be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies containing important elements of the original picture. Upon inverse transformation, watermarks applied to frequency domain will be dispersed over the entire spatial image, so these methods are not as susceptible to defeat by cropping as the spatial technique.

II. LITERATURE SURVEY

Digital watermarking can be defined as the process of embedding a certain piece of information (technically known as watermark) into multimedia content. Watermarking techniques can be divided into four categories according to the type of document to be watermarked, their working domains, based on human perception and area of application [14].To understand watermarking methods and determine their applications, one needs to know the properties of digital watermarks. The fundamental properties include: robustness, imperceptibility and computational cost [3]. Watermarks added to digital content serve a variety of purposes. The applications include owner identification, copy protection, finger printing, content authentication, broadcast monitoring, medical applications etc [14].In order to resist attacks, many approaches to robust watermarking have been investigated throughout the years. Some of them can be implemented in the spatial domain while others utilize the frequency domain. The frequency domain includes DFT, DCT, DWT and many others. With the standardization process of JPEG2000 and the shift from DCT to wavelet based image compression methods, watermarking schemes operating in wavelet transform domain have become more interesting. The proper selection of the frequency transform is dependent on the fact, the better the image transform approximates the properties of the HVS (Human Visual System) the easier is to put more energy in the embedded signal without causing perceptible distortion [6]. According to the HVS the high frequencies are less visible than the low frequencies. The wavelet transform is used because it is more close to the Human Visual System than DCT. Wavelet-based watermarking methods exploit the frequency information and spatial information of the transformed data in multiple resolutions to gain robustness [14]

III. WAVELET TRANSFORM

Wavelet transforms are the most powerful and most widely used tools in the field of image processing due to its flexibility in representing non-stationary image signals and its ability in adapting to human visual characteristics. A wavelet transform divides a signal into a number of segments, each corresponding to a different frequency band. The wavelet transform can be broadly classified into continuous and discrete wavelet transform. For long signals, continuous wavelet transform can be time consuming since it needs to integrate over all times. To overcome the time complexity, discrete wavelet transform was introduced. Discrete wavelet transforms can be implemented through sub-band coding. The DWT is useful in image processing because it can simultaneously localize signals in time and scale, whereas the DFT and DCT can localize signals only in the frequency domain [11].

Frequency transform is a powerful tool that has been available to signal analysts for many years. It gives information regarding the frequency content of a signal. However, the problem with using Fourier transform is that frequency analysis cannot offer both time resolution and frequency resolution at the same time. A Fourier transform does not give the time at which a particular frequency has occurred in the signal. Hence, a Fourier transform is not an effective tool to analyse non-stationary signal. To overcome this problem, windowed Fourier transform, or short time Fourier transform, was introduced. Even though a short time Fourier transform has the ability to provide time resolution, multi-resolution is not possible with the short time Fourier transforms. Wavelet is the answer to the multi-resolution problem. A wavelet has the property of not having a fixed-width sampling window.

IV. DIGITAL IMAGE WATERMARKING

DWT Image Watermarking: Wavelet based watermarking methods exploit the frequency information and spatial information of the transformed data in multiple resolutions to gain robustness [9]. The wavelet transform is closer to the human visual system since it splits the input image into several frequency bands that can be processed independently. It is a multi-resolution transform that permits to locate image features such as smooth areas, edges or textured areas.

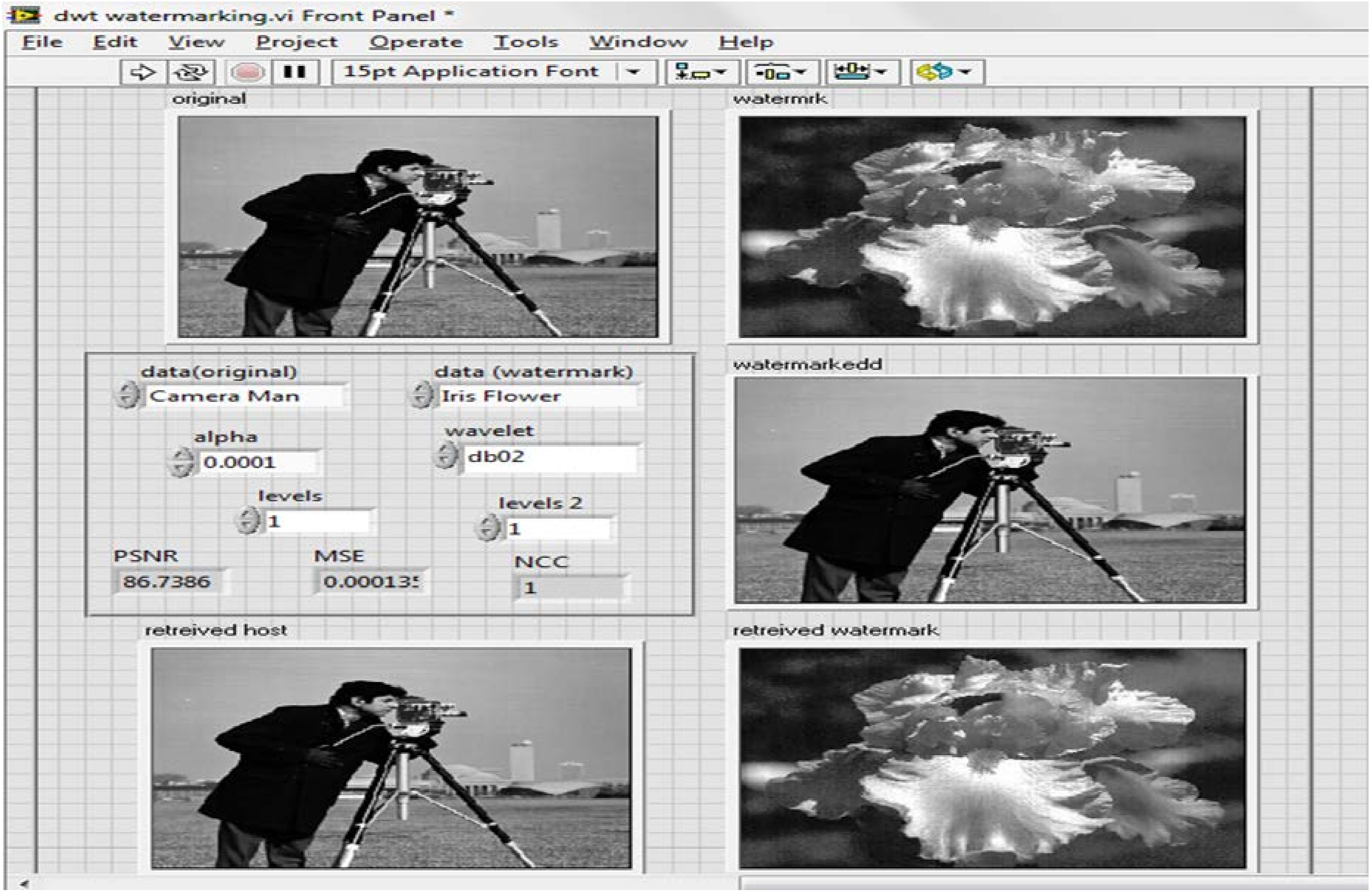
DCT Image Watermarking: Discrete Cosine Transform (DCT) is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers to orderly express data points in terms of a sum of cosine functions oscillating at different frequencies. DCT is equivalent to DFT of roughly twice the length, operating on real data with even symmetry, wherein some variants of the input and/or output data are shifted by half a sample. Discrete Cosine Transform is a general orthogonal transform for digital image processing and signal processing, with advantages such as high compression ratio, low bit error rate, good information integration ability and good synthetic effect of calculation complexity.

Combined DWT-DCT Image Watermarking: Further performance improvements in DWT-based digital image watermarking algorithms could be obtained by combining DWT with DCT. The idea of applying two transform is based on the fact that combined transforms could compensate for the drawbacks of each other, resulting in effective watermarking. Watermarking is done by altering the wavelet coefficients of carefully selected DWT sub-bands, followed by the application of the DCT transform on the selected sub-bands.In this method, the benefits of DWT is to choose the most proper sub-bands in case of robustness and imperceptibility. Then, the block based DCT is applied on these selected band to embed watermark in middle frequencies of each block to augment further robustness of watermarked image against different attacks. In fact by combining the two common frequency methods, we take the advantageous of both the algorithms to increase robustness and imperceptibility. At the same time, we suppress the effect of attack that is designed for each of these frequency methods such as jpeg and jpeg2000 compression [2].

V. RESULTS

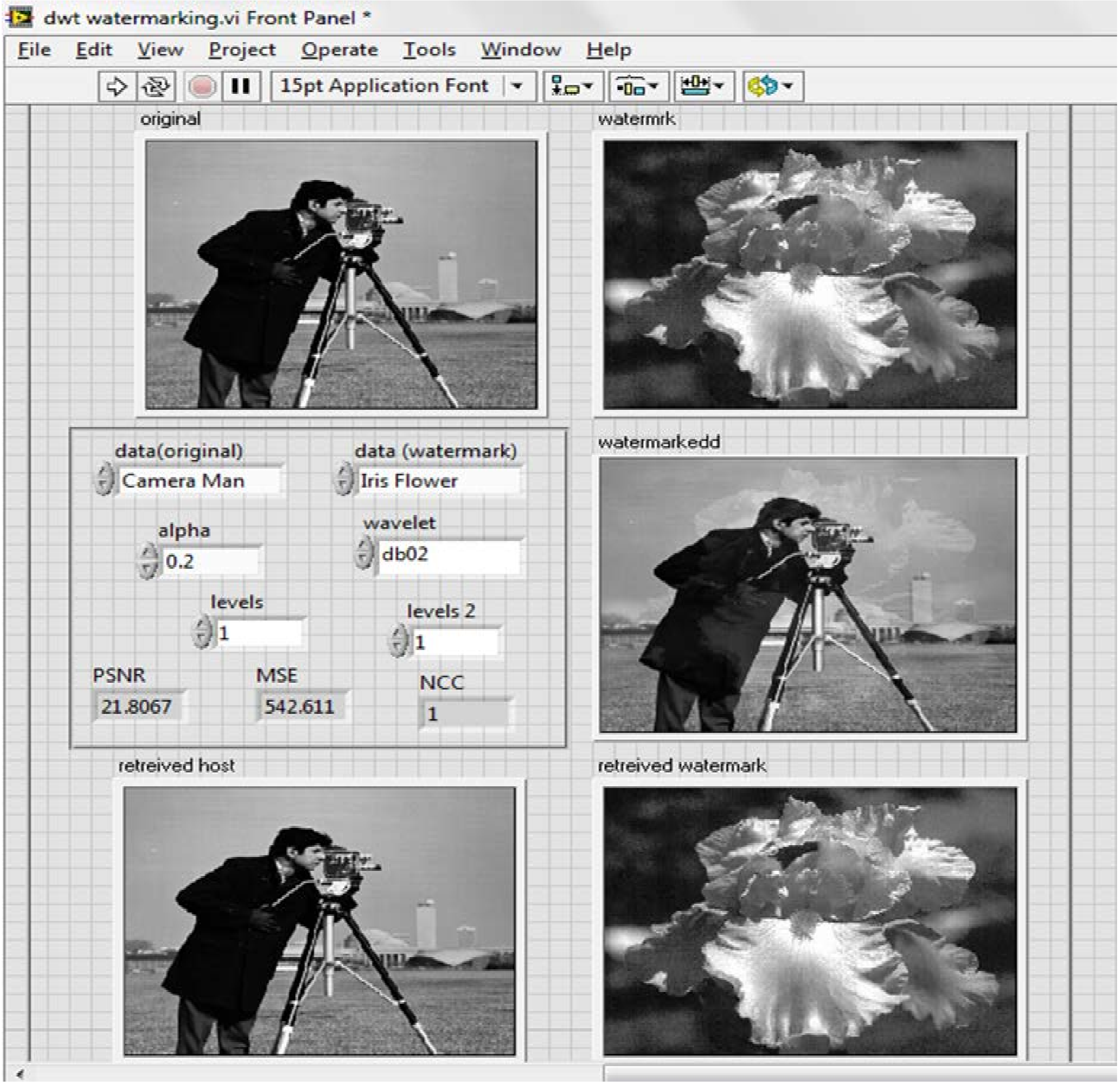
The project is implemented in NI LABVIEW and standard database gray-scale images are used for testing. In this process two gray-scale images, “Cameraman” image is used as original host image and the “Iris flower” image is used as the watermark. Both the images are of equal size of 256x256. The performance evaluation is done by two performance evaluation metrics: Perceptual transparency and Robustness. In our experiments for additive modification and alpha blending techniques, we performed fidelity tests to analyse the unobtrusiveness of the watermarks after watermark embedding, whether perceptual distortion occurred to the host images or not. Also different attacks like noise, rotation, compression were applied on the watermarked images and the visual quality of watermarked and attacked images was measured using the Peak-Signal-To-Noise Ratio (PSNR) and Mean Square Error (MSE) between the original and distorted images. For our results we supposed that the correlation coefficient of about 0.75 or above is assumed as an acceptable value for the extracted watermarks from noisy images.

The watermark can be embedded into the cover image using DWT, DCT and combined DWT-DCT methods



data(original): Camera Man
data (watermark): Iris Flower
alpha: 0.0001
wavelet: db02
levels: 1
levels 2: 1
PSNR: 86.7386
MSE: 0.00013!
NCC: 1

Figure 5.1 DWT based image watermarking using scaling factor α = 0.0001



data(original): Camera Man

data (watermark): Iris Flower

alpha: 0.2

wavelet: db02

levels: 1

levels 2: 1

PSNR: 21.8067

MSE: 542.611

NCC: 1

Figure 5.2 DWT based image watermarking using scaling factor α = 0.2

The wavelet used here is the wavelets of daubecheis (db02). The value of α can be varied from 0.0001 to 0.2. As the value of α is decreased further to 0.2 the watermark in the watermarked image becomes darker and finally becomes invisible. For the process of recovering the original watermark image from the watermarked image the scaling factor α is used.

TABLE I.The values of the mean square error (MSE) & PSNR are calculated for different values of the scaling factors α.

Scaling factor α	PSNR (db)	MSE
0.0001	86.8065	0.000135653
0.0005	72.8271	0.00339132
0.001	66.8065	0.0135653
0.005	52.8271	0.339132

0.01	46.8065	1.35653
0.05	32.8271	33.9132
0.1	26.8065	135.653
0.2	21.8067	542.611

The mean square error gradually decreases as the value of the PSNR increases. It can be observed that the PSNR value for cover image and the watermarked image decreases as the scaling factor value is increased. This is because the content of the watermark in watermarked image increases with scaling factor.

TABLE II. Experimental results for various attacks on the watermarked image with α =0.2.

	Using DWT			**Using DCT**			**Combined DWT-DCT**		
Attack	NCC	PSNR	MSE	NCC	PSNR	MSE	0.998761	22.1223	529.69
No attack	1	21.8067	542.611	0.996311	20.8173	538.699	0.9951	20.9061	711.506
JPEG compression	0.99629	20.8512	719.764	0.996548	20.8512	719.764	0.97998	21.1449	630.928
Median filtering (3x3)	0.97899	20.8506	639.957	0.988964	20.0842	637.77	0.89551	16.8253	1159.3
Blurring effect	0.89908	16.8056	1166.28	0.990091	16.7507	1161.8	0	8.49814	9948.03
Resize (scale=2)	0.663907	15.2431	2290.44	0.970625	15.2431	2290.44	0.99615	21.1285	531.7
Noise insertion(σ=5)	0.99629	21.0235	554.389	0.99746	21.117	564.289	0.99465	22.938	2323.22
Sharpening	0.995942	22.8108	2432.54				0.998761	22.1223	529.69

TABLE III. Experimental results for various attacks on watermarked image with β=0.9 and α =0.2.

	Using DWT			**Using DCT**			**Combined DWT-DCT**		
Attack	NCC	PSNR	MSE	NCC	PSNR	MSE	0.998768	24.8188	248.249
No attack	1	24.1648	265.514	1	23.8889	265.578	0.998422	22.7011	434.03
JPEG compression	0.99774	22.3913	444.474	0.998174	22.3861	445.196	0.98061	22.8923	356.297
Median filtering (3x3)	0.980944	22.3847	373.144	0.989744	22.3752	373.373	0.905265	16.8938	955.147
Blurring effect	0.908616	16.839	916.658	0.987788	16.8413	961.576	0	8.8253	8969.28
Resize (scale=2)	0.661034	15.525	265.514	0.958025	15.5247	1987.45	0.999033	24.1976	272.365
Noise insertion(σ=5)	0.997935	23.8799	290.308	0.997835	23.9477	289.227	0.998016	23.5676	2036.58
Sharpening	0.997501	23.6919	1700.76						

Synchronous RAM Controller Results: The usual memory hierarchy of a FPGA includes the data path, Main Memory Controller (MMC) and Local Memory Controller (LMC) as shown in the below figure1.The MMC will control the SDRAM (Synchronous Dynamic Random Access Memory) and generates the burst signals for the remaining units of the device. The LMC controls the data path and waits for the burst signals from the MMC. The main aim of our paper is to design Synchronous Ram Controller which is the main part of MMC [1].

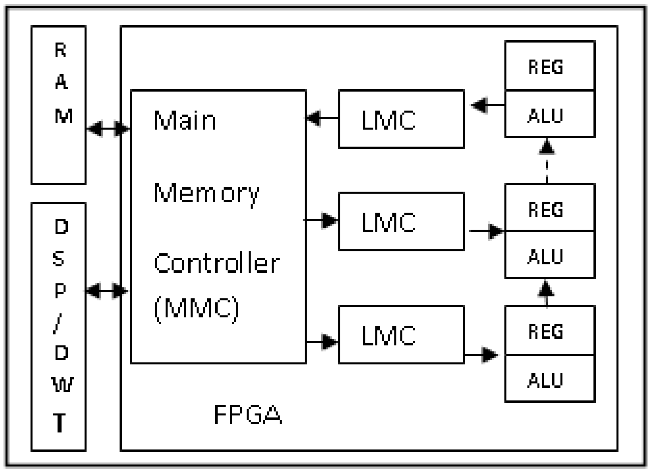


Figure 5.3 Memory Hierarchy

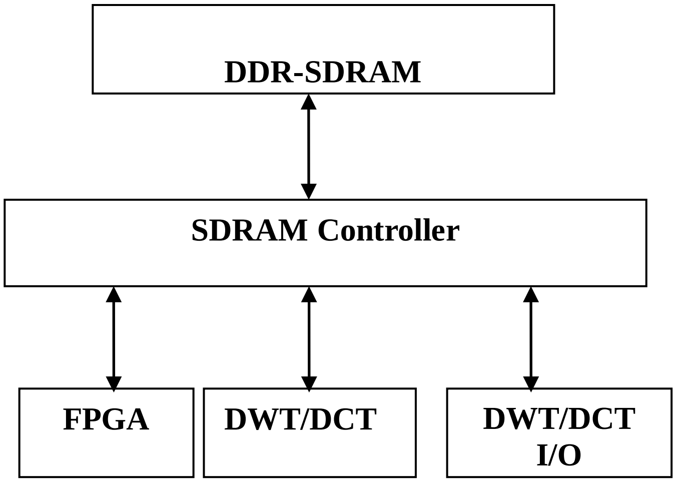


Figure 5.4 Memory Hierarchy

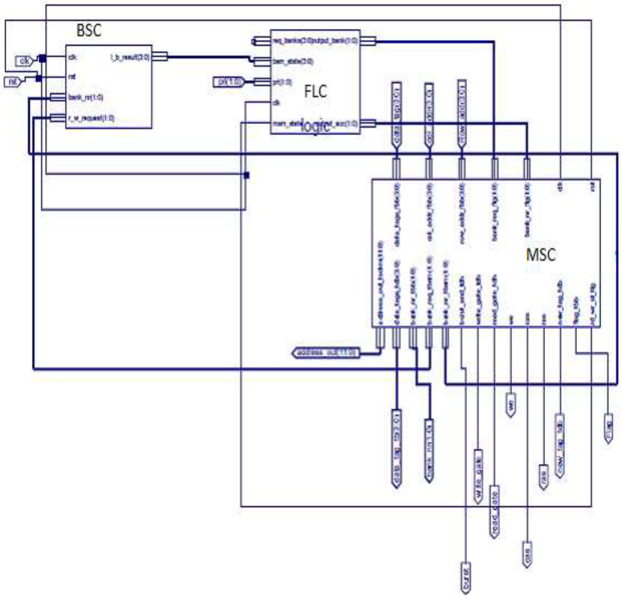


Figure 5.5 RTL schematic of top module of the design

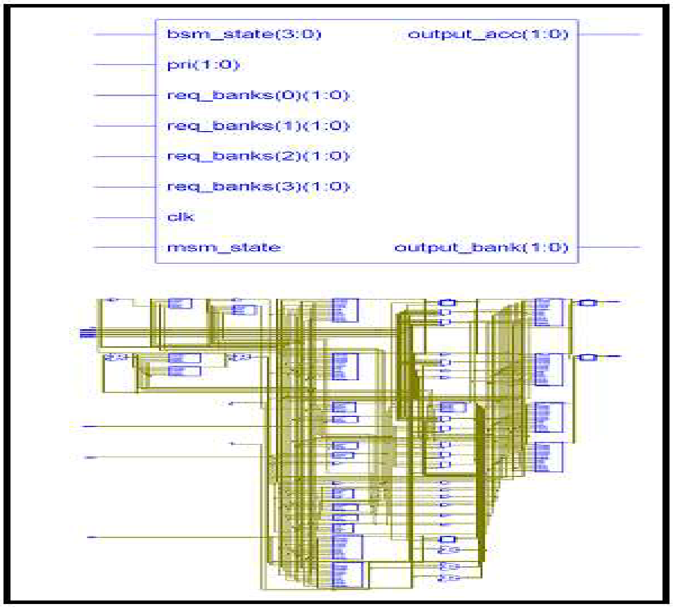


Figure 5.6 RTL schematic of FLC module

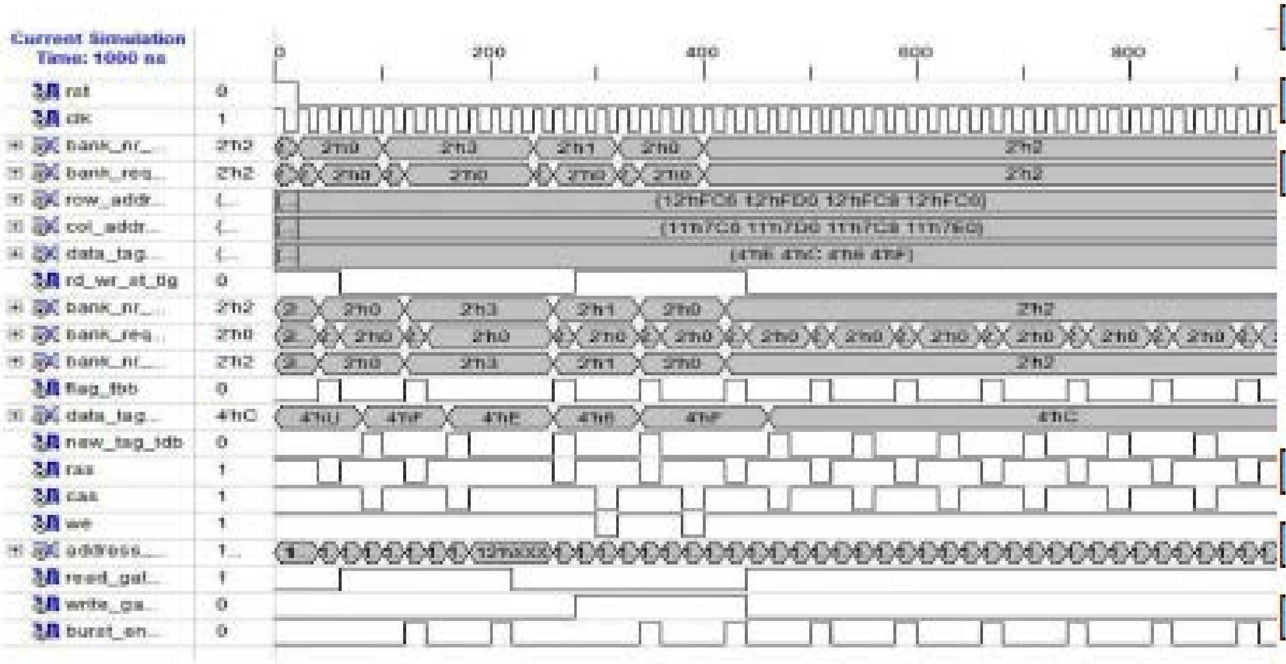


Figure 5.7 Simulation result of MSC module

VI. CONCLUSION

A robust watermarking scheme is implemented using NI LabVIEW. Two watermarking algorithms, additive modification and alpha blending were simulated using DWT, DCT and combined DWT-DCT in detail to analyse the robustness for copyright scenario. Both the algorithms were found non-obtrusive in gray level images. The performance of the watermarking scheme is evaluated with common image processing attacks using DWT, DCT and combined DWT-DCT and the results compared. For robustness, DWT technique showed better results when compared with DCT and combined DWT-DCT technique. Based on experimental setup an architecture for reconfigurable image processing system was implemented which increases the level of controllability.

. References

[1] FPGA realization of multi-port SDRAM controller in real time image acquisition system, Multimedia Technology (ICMT), 2011 International Conference 26-28 July 2011.

[2] D. N. Vizireanu and R. O. Preda, "A New Digital Watermarking Scheme for Image Copyright Protection using Wavelet Packets", 7th Int. Conf. Telecomm. In Modern satellite, Cable and Broadcasting Services, vol. 2, pp. 518-521, Sept. 2005.

[3] J. Cummins, P. Diskin, S. Lau and R. Parlett, "Steganography and Digital Watermarking", Student Seminar Report, School of Computer Science, University of Birmingham, 2004.

[4] J. F. Delaigle, C. Devleeschouwer, B. Macq and I. Langendijk, "Human Visual System Features Enabling Watermarking", IEEE Int. Conf. on Multimedia and Expo (ICME '02), vol. 2, pp. 489- 492, 2002.

[5] Jonathan M. Bloom, "Revolution by the Ream: A History of Paper", Saudi Aramco World May/June 1999 print edition, vol. 50, pp. 26-39, May/June 1999.

[6] J. Zan, M. O. Ahmad and M. N. S. Swamy, "Object- based Image Watermarking Technique Using Wavelets", Proc. IEEE Canadian Conf. on Electrical & Computer Engin., vol. 2, pp. 1143-1146, May 2004.

[7] Peining Taoa and Ahmet M. Eskicioglu, "A robust multiple watermarking scheme in the Discrete Wavelet Transform domain" Department of Computer and Information Science, Brooklyn College, New York

[8] S Jayaram, S Esakkirajan and T Veerakumar, "Digital image processing", Tata McGraw-Hill Publications.

[9] X. Wu, J. Hu, Z. Gu and J. Huang, "A Secure Semi-Fragile Watermarking for Image Authentication Based on Integer Wavelet Transform with Parameters", Proc. 3rd Australasian Information Security Workshop (AISW2005), CRPIT, vol. 44, pp. 75-80, 2005.

[10] Yusnita Yosuf and Othman O. Khalifa, "Digital watermarking for digital images using wavelet transform",Proc.IEEE International Conf. on telecommunications, May 2007.

[11] C. S. Woo, J. Du and B. Pham, "Performance Factors Analysis of a Wavelet-based Watermarking Method", Proc. 3rd Australasian Information Security Workshop (AISW2005), CRPIT, vol. 44, pp. 89-97,

AUTHORS

First Author – Prof Pramod Kumar Naik, B.E, M Tech, Vivekananda College of Engineering &Technology, Puttur. Karnataka, India. pramodkumarnaik.ece@vcetputtur.ac.in.

Second Author – Prof Arun S Tigadi, B.E, M Tech, KLE DR. M.S.S CET, Belgaum, Karnataka, India.

Third Author – Dr.Hansraj Guhilot Principal,K.C.College of Engineering & Management Studies and Research ,Thane, Maharashtra, India.

Correspondence Author – – Prof Pramod Kumar Naik, B.E, M Tech, Vivekananda College of Engineering &Technology, Puttur. Karnataka, India.pramodkumarnaik.ece@vcetputtur.ac.in. Mobile: 9886362690.