International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 4, Number 5 (2014), pp. 545-552

http://www. irphouse.com /ijict.htm

Implementation of Blind Image Watermark Encoder in FPGA

Waikhom Mona Chanu[1], Bitan Chakraborty[2] and Diwarkar R Marur

[1]Dept. of ECE, NIT Manipur, Imphal, Manipur, India.
[2]Dept. of ECE, VELTECH University, Chennai, India.
[3]Dept. of ECE, SRM University, Chennai, India.

Abstract

To protect our ownership rights and authenticity, many digital watermark techniques has been proposed. When watermarking comes in the digital data, the information is no longer present in the physical material like in documents or paper. Here in order to prevent image from fraudulent the digital watermarks is embedded into image data. In this paper we proposed a new blind digital image watermarking technique based on DCT where the original image is not required for watermark recovery. It is resistant to compression and other frequency based attacks. And the watermark encoder part is implemented in the Xilinx Spartan FPGA board. The motivation to implement watermark in FPGA comes from the hypothesis that the performance of the system could be significantly improved in terms of speed considering the optimal parallelism environment that hardware provides.

Keywords: Discrete Cosine Transform, Digital image Watermarking, Subsampling and FPGA.

1. Introduction

Digital watermark is a signal which is embedded into digital data such as audio, video, images and text to protect our ownership. In 1988, Komatsu and Tominaga first used the term “Digital Watermarking”. Digital watermark is a technology for embedding various type of information in the digital content and the watermarks cannot be removed or altered.it becomes a very important tool when fighting copyright infringement on the Web. Over the past few years, there has been tremendous growth in computer networks and more specifically, the World Wide Web. This phenomenon,

coupled with the exponential increase of computer performance, has facilitated the distribution of multimedia data such as images. Publishers, artists, and photographers, however, may be unwilling to distribute pictures over the Internet due to a lack of security. Images can be easily duplicated and distributed without the owner's consent. Digital watermarks have been proposed as a way to tackle this tough issue. This digital signature could discourage copyright violation, and may help determine the authenticity and ownership of an image [1], [2]. Digital image watermarking techniques can be categorized into one of the two domains, viz., spatial and transform, according to the embedding domain of the host image. The simplest technique in the spatial domain methods is to insert the watermark image pixels in the least significant bits (LSB) of the host image pixels [3]. But it is found that the transform domain watermarking schemes are typically much more robust to image manipulation as compared to the spatial domain schemes. Watermarking has been an exciting topic and there have been many watermarking schemes proposed. Among these schemes, those requiring both the original data and the secret keys for the watermark bit decoding are called private watermark schemes. Those requiring the secret keys but not the original data are called public or blind watermark schemes. Those requiring the secret keys and the watermark bit sequence are called semi-private or semi-blind watermark schemes [4]. Blind watermark schemes, on the other hand, detect the watermarks without the original data and are feasible in those situations. Cox *et al.* [1] uses spread spectrum to embed watermark in the discrete cosine transform (DCT) domain. There are also many blind watermark schemes. Zhang *et al.* [5] embeds a watermark pattern by modifying the DC and low-frequency coefficients in the DCT domain. Piva *et al.* [6] developed a DCT-based scheme where the watermark can be identified by calculating the correlation between the watermark sequence and the DCT coefficients of the watermarked image. A similar scheme was proposed by Dugad *et al.* [7] applied to the DWT domain. In these methods, a significant correlation can be obtained only through a big number of coefficients (typically more than 10 000 [8]).A method has been developed where a binary-valued watermark is inserted to the low-frequency region based on a mapping function and a spread spectrum signal is added to the mid frequency region.

2. DCT Watermarking System

DCT based watermarking is resistant to compression and other frequency-based attacks, and this results in the scheme being very robust as well as imperceptible than most other schemes. The system block diagram consists of encoder and decoder.

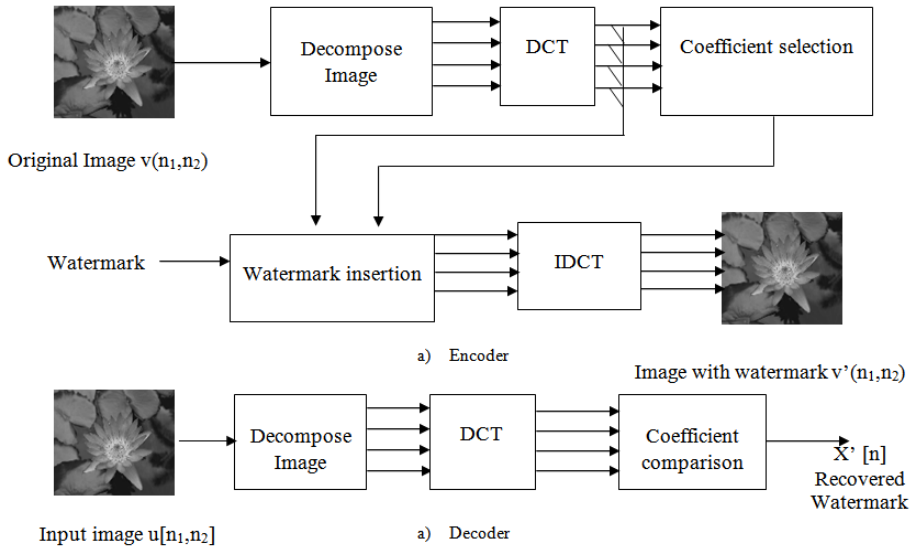

Fig. 1: System Block a) Encoder, b) Decoder.

Fig. 2: Implementation in FPGA.

Fig. 3: RGB to gray scale

Fig. 4: Subsampling of image.

2.1.1 Watermark insertion

Watermark insertion in the DCT domain can be performed by modifying the DCT coefficients. In our scheme, one pair of coefficients from two different subimages situated in the same DCT domain location is used to insert one watermark sample. Since there are four subimages available for every location in the DCT domain, two consecutive samples of the watermark sequence can be inserted to one DCT domain location. The order sequence can be fixed, or generated as a random sequence. In these cases four consecutive numbers in the sequence must be different, so as to ensure that the watermark is inserted to pairs of different subimages. The operation can be performed to the selected pairs of coefficients V_i and Vj, ———.And if ——— then the modification must not be done in V_i and Vj. Instead the watermark is inserted with . Finally, the block containing the watermarked DCT coefficients is inverse transformed to obtain the final watermarked image. Each block containing the watermarked coefficients in the transformed domain is converted back to the image block in the pixel domain. Hence we obtain the final watermarked image. The algorithm used in MATLAB to compute the inverse DCT is shown below:

for $x,y = 0, 1, 2, \ldots N-1$.

$$\alpha(u) = \begin{cases} \sqrt{(1/N)} \text{ for } u = 0 \\ 2/N) \text{ for } u = 1, 2 \ldots N-1 \end{cases}$$

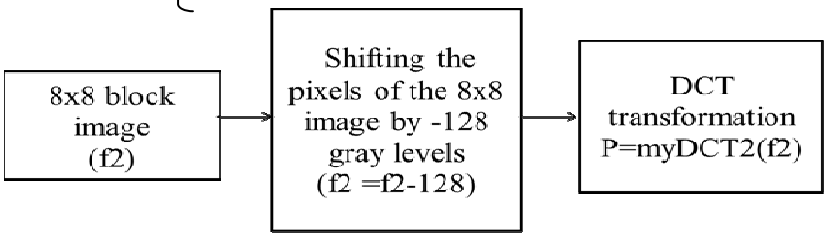

Fig. 5: DCT Block.

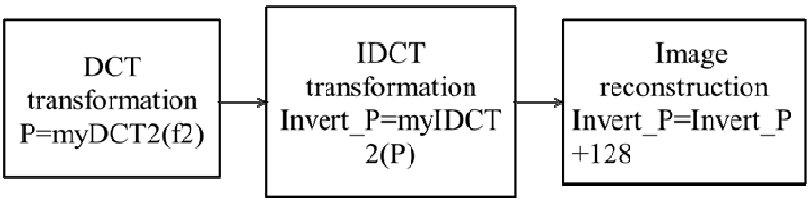

Fig. 6: IDCT Block.

2.2 Decoder

For the decoder, input image u $[n_1, n_2]$ where, $n_1=0\ldots N_1-1$, $n2=0\ldots N_2-1$is decomposed i.e., the image is first broken down into the same 8x8 blocks as done in watermark embedding and then the DCT is performed on each block. The same

watermark insertion order sequence is used to select the pairs of coefficients. Hence, the watermark as $X'[n]$ is recovered.

2.2.1 Watermark Recovery

Denoting the recovered watermark as $X'[n]$, the following operations are performed to each selected pair of coefficients *Ui, Uj*.$\mathrm{U} = \frac{(\mathrm{Ui}+\mathrm{Uj})}{2}$. If $\frac{(Ui-Uj)}{U} > 6 \propto$ then we have to set X =0, otherwise$X' = \frac{1}{\propto}(\frac{Ui-Uj}{Ui+Uj})$. Therefore, assuming that the input is the watermarked image, the decoder can replicate the exact threshold verification procedure as the encoder, since U=V .One advantage is that under noiseless condition, the inserted watermark samples can be recovered exactly where, $X'=X$. The algorithm utilizes the blind watermark detection technique which means that the original image was not required for the watermark detection. The suspected image was divided in to 8X8 blocks and the DCT is calculated for each block.

3. Simulation and Experimental Results

Here 256x256 Lena image has been used with α=0.1 shown in fig 7. Re-watermarking is considered next. First, a watermarked image is generated.

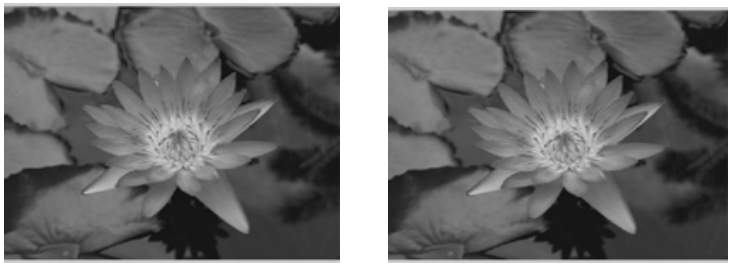

Fig. 7: Original image and recovered image, α=0.1.

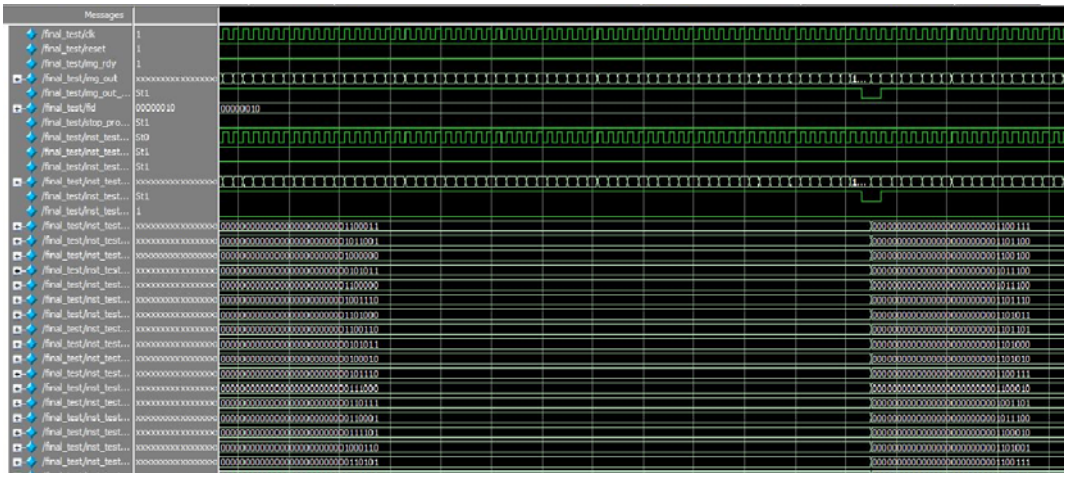

Fig. 8: DCT for v1.

Then, a different watermark is inserted to the watermarked image using different order sequences. The recovered watermark using the second order sequences presents a similarity of 1.216 with respect to the first watermark and a similarity of 29.79 with respect to the second watermark. The encoder block of the watermark system can be simulated in MATLAB and it is simulated using Xilinx software. The simulation waveform is shown in fig.7-10.

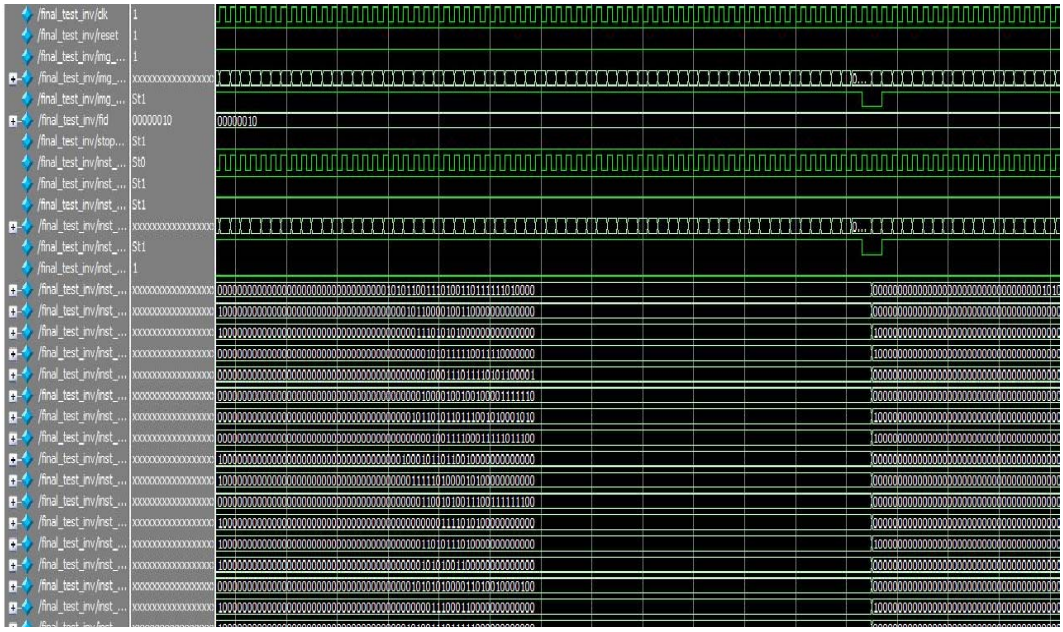

Fig. 9: DCT for V1.

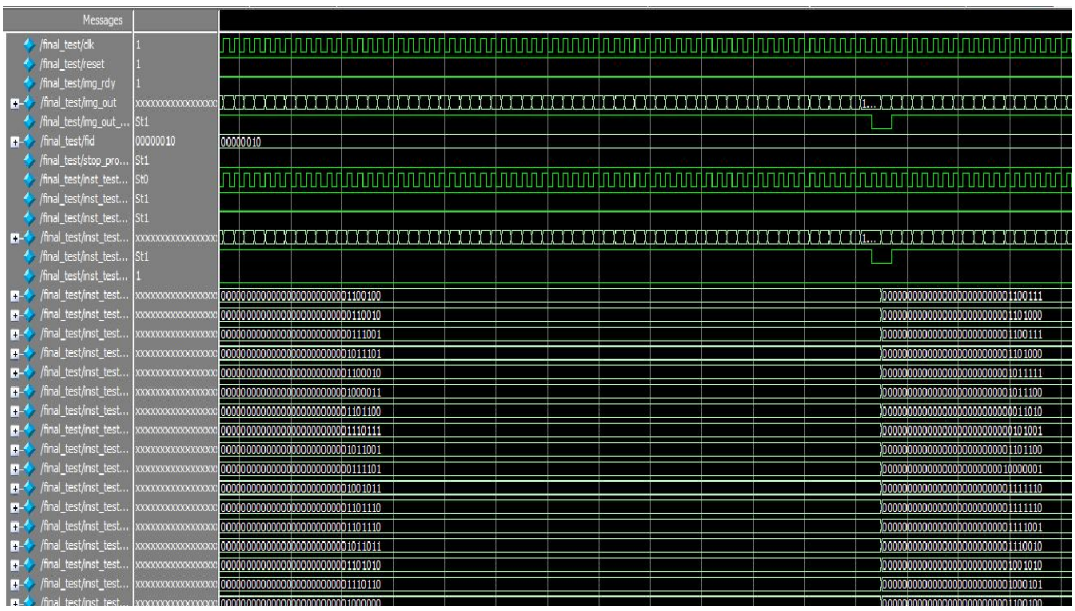

Fig. 10: Reconstruction for V1.

4. Synthesis Report

Table 1: Summary of synthesis report.

Units(Overall Encoder)	Utilisation	Cell usage
Number of Slices	32492	1327%
Flip flops	249	5%
Input LUTs	62482	1267%
Bonded IOBs	2117	1230%
Number of	4	33%
MULT18X18SIOs	1	4%
Number of GCLKs		

LUTs: Look Up Table, IOBs: Input/output blocks

Minimum utilisation indicates the minimum no. of devices which has been utilized in the design. The cell usage indicates all the logical cells that are basic elements of the technology.

5. Conclusion

In this proposed watermarking scheme the presence of the original image is not required for watermark recovery. It is achieved by inserting a watermark sample to one pair of DCT coefficients, with each perturbed differently. For watermark extraction, it is indispensable to have knowledge of the two order sequences. Thus, even though an attacker knows all details of the algorithm, it is unlikely that he/she will be able to extract with no knowledge of the exact order sequences. The encoder of the watermarking system is implemented in the hardware Xilinx Spartan FPGA board. It is concentrated on making the method more practical by hardware based FPGA implementation. The objective is to develop low power, real time, reliable and secure watermarking systems, which can be achieved through hardware implementations. Its low power high performance implementation is currently under progress. There is scope for a lot of optimization that can be done to achieve a clear image for recovering for the decoder part in the future.

References

[1] Cox, J. Kilian, F. Leighton, and T. Shamoon, "**Secure Spread Spectrum Watermarking for Multimedia**," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[2] L. Liu, **"A survey on digital watermarking technologies"**, Technical Report, Stony Brook University, New York, USA, 2005.

[3] I.Podilchuk and E. J. Delp, "**Digital Watermarking: Algorithms and Applications**", *IEEE Signal Processing Magazine,* pp.33-46, July 2001.

[4] M. Kutter and F. A. P. Petitcolas, "**A fair benchmark for image watermarking systems**," in *Proc. Security and Watermarking of Multimedia Contents*, Jan. 1999, pp. 226–239.

[5] Y. J. Zhang, T. Chen, and J. Li, "**Embedding watermarks into both DC and AC components of DCT**," in *Proc. SPIE Security and Watermarking of Multimedia Contents III*, Jan. 2001, pp. 424–435.

[6] A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "**DCT-Based watermark recovering without restoring to the uncorrupted original image**", in *IEEE ICIP*, 1997.

[7] R. Dugad, K. Ratakonda, and N. Ahuja, "**A new wavelet-based scheme for watermarking images**," *in IEEE ICIP*, 1998.

[8] Wai C. Chu, "**DCT-Based Image Watermarking Using Subsampling"**, *IEEE Transaction on Multimedia*, vol. 5, no.1, March 2003.(P-15).