IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. IV (May-Jun. 2014), PP 59-64
www.iosrjournals.org

Design and Simulation of Dct Chip In Vhdl and Application in Watermark Extraction

[1]Nirabh Agarwal, [2]Arpit Jain, [3]Prof. Sanjeev Sharma
[1]M.Tech Scholar, Department of Computer Science & Engineering, Teerthankar Mahaveer University, Moradabad, U.P. India
[2]Assistant Professor,Department of Computer Science & Engineering, Teerthankar Mahaveer University, Moradabad, U.P. India
[3]Dean & HOD of CS, IT and MCA, JPIET Meerut UP, India

Abstract: *The paper presented the design, modeling and chip implementation of 2D Discrete Cosine Transform (DCT) domain for copyright protection of images, as digital watermarking chip. Recent improvement in computational world and the proliferation of the Internet have facilitated and demanded the production and distribution of unauthorized copies of copyrighted digital contents. The research work involved simulations and synthesis of VHDL code utilizing recent FPGA families of Xilinx, SPARTEN 3E. It is achieving the most demanding real-time requirements of some standardized frame resolutions and rates. The simulation and Synthesis results for 8-point DCT implementations indicate operating frequencies of 50 MHz, and 60 MHz for Xilinx ISE Environment and functional check using Modelsim 10.1 b software.*

I. Introduction

Digital watermarking [1, 4] is the process of computer-aided information hiding in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing the watermarks for copyrights and for banktone authentication. Digital watermarks [2] are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible [1, 3] anytime else. If a digital watermark distorts the carrier signal in a way that it gets perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. A digital watermark does not change the size of the carrier signal [5], unlike metadata that is added to the carrier signal. The needed properties of a digital watermark depend on the use case, in which it is applied. For marking media files with copyright information [7, 9], a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied.

Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool [2, 3]. It just marks data, but does not degrade it nor controls access to the data. One application of digital watermarking is source tracking [3]. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies. It is difficult to model the distortions introduced by common signal processing transformations, which either intentionally or unintentionally affect the watermark detection or identification capabilities[1, 7]. Although very nice work exists in trying to understand the fundamental limitations of watermark embedding and detection, attack channels such as geometrical distortions cannot be described by these models. Other areas have not been resolved as well. Besides the obvious caveat of whether watermarking technology will be effective in a court of law, other questions remain.

II. Applications and Phases of Digital Watermarking

Digital watermarking may be used for a wide range of applications, such as Copyright protection, Source tracking for different recipients get differently watermarked content, Broadcast monitoring for television news often contains watermarked video from international agencies.

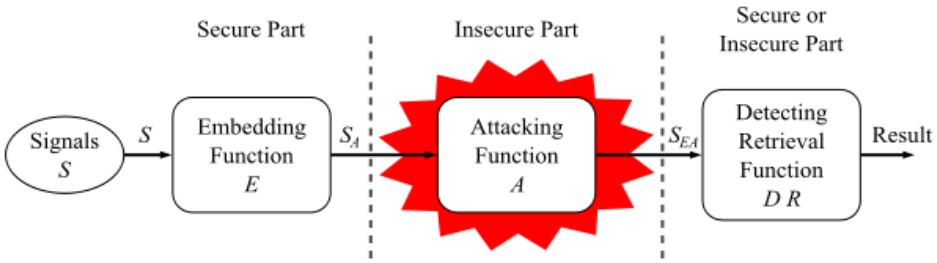

Fig. 1 Phases of Digital Watermarking Life Cycle

General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions. The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video or intentionally adding noise.

Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal.

III. Classification of Digital Watermark

A digital watermark is called robust with respect to transformations if the embedded information may be detected reliably from the marked signal, even if degraded by any number of transformations. Typical image degradations are JPEG compression, rotation, cropping, additive noise, and quantization. For video content, temporal modifications and MPEG compression often are added to this list. A digital watermark is called imperceptible if the watermarked content is perceptually equivalent to the original, unwatermarked content. In general, it is easy to create robust watermarks or imperceptible watermarks, but the creation of robust **and** imperceptible watermarks has proven to be quite challenging. Robust imperceptible watermarks have been proposed as tool for the protection of digital content, for example as an embedded no-copy-allowed flag in professional video content. Digital watermarking techniques may be classified in several ways.

3.1 Robustness

A digital watermark is called fragile if it fails to be detectable after the slightest modification. Fragile watermarks are commonly used for tamper detection (integrity proof). Modifications to an original work that clearly are noticeable commonly are not referred to as watermarks, but as generalized barcodes. A digital watermark is called semi-fragile if it resists benign transformations, but fails detection after malignant transformations. Semi-fragile watermarks commonly are used to detect malignant transformations. A digital watermark is called robust if it resists a designated class of transformations. Robust watermarks may be used in copy protection applications to carry copy and no access control information.

3.2 Perceptibility

A digital watermark is called imperceptible if the original cover signal and the marked signal are perceptually indistinguishable. A digital watermark is called perceptible if its presence in the marked signal is noticeable. A digital watermark that is perceptual, on the other hand, is imperceptible. It works context-sensitive/adaptive.

3.3 Capacity

The length of the embedded message determines two different main classes of digital watermarking schemes. The message is conceptually zero-bit long and the system is designed in order to detect the presence or the absence of the watermark in the marked object. This kind of watermarking scheme is usually referred to as zero-bit or presence watermarking schemes. Sometimes, this type of watermarking scheme is called 1-bit watermark, because a 1 denotes the presence (and a 0 the absence) of a watermark. The message is a n-bit-long

stream ($m = m_1 \dots \dots m_n, n \in N$) with $n = |m|$ or $M = \{0,1\}^n$ and is modulated in the watermark. These kinds of schemes usually are referred to as multiple-bit watermarking or non-zero-bit watermarking schemes.

3.4 Embedding method

A digital watermarking method is referred to as spread-spectrum if the marked signal is obtained by an additive modification. Spread-spectrum watermarks are known to be modestly robust, but also to have a low information capacity due to host interference. A digital watermarking method is said to be of quantization type if the marked signal is obtained by quantization. Quantization watermarks suffer from low robustness, but have a high information capacity due to rejection of host interference. A digital watermarking method is referred to as amplitude modulation if the marked signal is embedded by additive modification which is similar to spread spectrum method, but is particularly embedded in the spatial domain. The evaluation of digital watermarking schemes may provide detailed information for a watermark designer or for end-users, therefore, different evaluation strategies exist. Often used by a watermark designer is the evaluation of single properties to show, for example, an improvement. Mostly, end-users are not interested in detailed information. They want to know if a given digital watermarking algorithm may be used for their application scenario, and if so, which parameter sets seems to be the best.

- **Digital Cameras and Watermarking**

Epson and Kodak have produced cameras with security features such as the Epson Photo PC 3000Z and the Kodak DC-290. Both cameras added irremovable features to the pictures which distorted the original image, making them unacceptable for some applications such as forensic evidence in court. According to Blythe and Fridrich, "[n]either camera can provide an undisputable proof of the image origin or its author". A secure digital camera (SDC) was proposed by Mohanty, et al. in 2003 and published in January 2004. This was not the first time this was proposed. Blythe and Fridrich also have worked on SDC in 2004 for a digital camera that would use lossless watermarking to embed a biometric identifier together with a cryptographic hash.

- **Reversible Data Hiding in Watermarking**

Reversible data hiding is a technique which enables images to be authenticated and then restored to their original form by removing the digital watermark and replacing the image data that had been overwritten. This would make the images acceptable for legal purposes. The U.S. Army also is interested in this technique for authentication of reconnaissance images.

- **Watermarking for Relational Databases**

Digital watermarking for relational databases emerged as a candidate solution to provide copyright protection, tamper detection, traitor tracing, and maintaining integrity of relational data. Many watermarking techniques have been proposed in the literature to address these purposes. A survey of the current state-of-the-art and a classification of the different techniques according to their intent, the way they express the watermark, the cover type, the granularity level, and their verifiability.

IV. Discrete Cosine Transform

The mathematical model equation for a (8 x 8) point 2D DCT [7, 9] is shown below, in which the transformed outputs are represented as Y (k, m). Where k, m = 0,1,...,7, and the two dimensional input sequence, represents the image pixel values) by x(i, j), where i, j = 0,1,...,7.

$$Y(k,m) = \frac{2C_k C_m}{N} \sum_{i=0}^{7} \sum_{j=0}^{7} x(i,j) \cos\left[\frac{(2i+1)k\pi}{2N}\right] \cos\left[\frac{(2i+1)m\pi}{2N}\right] \qquad (1)$$

and C_0=1/□2 else C_k, C_m =1. Using matrix notation, the (8 x 8) point 2D DCT [7] can be expressed as a matrix vector computation equation (2), where C represents the DCT coefficient matrix.

$$[Y] = [C_{8\times 8}].[x] \qquad (2)$$

With the help of row column decomposition, the algorithm can be rewritten using two, 1D DCTs and a matrix transpose, as shown in Equation (3).

$$[Y] = [C].[x].[C^t] \qquad (3)$$

With row column decomposition, the 8 point 1D DCT is applied to each row of the input matrix, and each (8 x 8) block of "semi-transformed" values is transposed and has a further 1D DCT applied to it. The expanded matrix representation for the 8 point 1D DCT is given below.

$$\begin{bmatrix} Y(0) \\ Y(1) \\ Y(2) \\ Y(3) \\ Y(4) \\ Y(5) \\ Y(6) \\ Y(7) \end{bmatrix} = \frac{1}{2} \begin{bmatrix} C_4 & C_4 & C_4 & C_4 & C_4 & C_4 & C_4 & C_4 \\ C_1 & C_3 & C_5 & C_7 & -C_7 & -C_5 & -C_3 & -C_1 \\ C_2 & C_6 & -C_6 & -C_2 & -C_2 & -C_6 & C_6 & C_2 \\ C_3 & -C_7 & -C_1 & -C_5 & -C_5 & C_1 & C_7 & -C_3 \\ C_4 & -C_4 & -C_4 & C_4 & C_4 & -C_4 & -C_4 & C_4 \\ C_5 & -C_1 & C_7 & C_3 & -C_3 & -C_7 & C_1 & -C_5 \\ C_6 & -C_2 & C_2 & -C_6 & -C_6 & C_2 & -C_2 & C_6 \\ C_7 & -C_5 & C_3 & -C_1 & C_1 & -C_3 & C_5 & -C_7 \end{bmatrix} \begin{bmatrix} x(0) \\ x(1) \\ x(2) \\ x(3) \\ x(4) \\ x(5) \\ x(6) \\ x(7) \end{bmatrix}$$

Here $C_x = \cos(x\pi/16)$. In the direct implementation of the above equation, there is the requirement of 64 multiplications and 56 additions. With the help of symmetrical approach, the above can be rewritten, which reduces computations and the hardware in terms of multiplications, which are 32 and 8 adders / subtractors.

$$\begin{bmatrix} Y(0) \\ Y(2) \\ Y(4) \\ Y(6) \\ Y(1) \\ Y(3) \\ Y(5) \\ Y(7) \end{bmatrix} = \frac{1}{2} \begin{bmatrix} C_4 & C_4 & C_4 & C_4 & 0 & 0 & 0 & 0 \\ C_2 & C_6 & -C_6 & -C_2 & 0 & 0 & 0 & 0 \\ C_4 & -C_4 & -C_4 & C_4 & 0 & 0 & 0 & 0 \\ C_6 & -C_2 & C_2 & -C_6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & C_1 & C_3 & C_5 & C_7 \\ 0 & 0 & 0 & 0 & C_3 & -C_7 & -C_1 & -C_5 \\ 0 & 0 & 0 & 0 & C_5 & -C_1 & C_7 & C_3 \\ 0 & 0 & 0 & 0 & C_7 & -C_5 & C_3 & -C_1 \end{bmatrix} \begin{bmatrix} x(0)+x(7) \\ x(1)+x(6) \\ x(2)+x(5) \\ x(3)+x(4) \\ x(0)-x(7) \\ x(1)-x(6) \\ x(2)-x(5) \\ x(3)-x(4) \end{bmatrix}$$

The simplifications of the above can be done as following with the assumption of

$$\begin{bmatrix} Y(0) \\ Y(2) \\ Y(4) \\ Y(6) \\ Y(1) \\ Y(3) \\ Y(5) \\ Y(7) \end{bmatrix} = \frac{1}{2} \begin{bmatrix} C_4 & C_4 & C_4 & C_4 & 0 & 0 & 0 & 0 \\ C_2 & C_6 & -C_6 & -C_2 & 0 & 0 & 0 & 0 \\ C_4 & -C_4 & -C_4 & C_4 & 0 & 0 & 0 & 0 \\ C_6 & -C_2 & C_2 & -C_6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & C_1 & C_3 & C_5 & C_7 \\ 0 & 0 & 0 & 0 & C_3 & -C_7 & -C_1 & -C_5 \\ 0 & 0 & 0 & 0 & C_5 & -C_1 & C_7 & C_3 \\ 0 & 0 & 0 & 0 & C_7 & -C_5 & C_3 & -C_1 \end{bmatrix} \begin{bmatrix} K(1) \\ K(2) \\ K(3) \\ K(4) \\ K(5) \\ K(6) \\ K(7) \\ K(8) \end{bmatrix}$$

Where,

$C_1 = \cos \pi/16 = 0.9808$ $\quad K_1 = x(0) + x(7)$

$C_2 = \cos 2\pi/16 = 0.9239$ $\quad K_2 = x(1) + x(6)$

$C_3 = \cos 3\pi/16 = 0.8315$ $\quad K_3 = x(2) + x(5)$

$C_4 = \cos 4\pi/16 = 0.7071$ $\quad K_4 = x(3) + x(4)$

$C_5 = \cos 5\pi/16 = 0.5556$ $\quad K_5 = x(0) - x(7)$

$C_6 = \cos 6\pi/16 = 0.3827$ $\quad K_6 = x(1) - x(6)$

$C_7 = \cos 7\pi/16 = 0.1951$ $\quad K_7 = x(2) - x(5)$

$K_8 = x(3) - x(4)$

After solving the above matrix the output equations can be written in simplified form

$Y(0) = C_4 (K_1 + K_2 + K_3 + K_4)$

$Y(2) = C_2 (K_1 - K_4) + C_6 (K_2 - K_3)$

$Y(4) = C_4 [(K_1 + K_4) – (K_2 + K_3)]$
$Y(6) = C_6 (K_1 – K_4) – C_2 (K_2 – K_3)$
$Y(1) = C_1K_5 + C_3K_6 + C_5K_7 + C_7K_8$
$Y(3) = (C_3K_5 – C_7K_6) – (C_1K_7 + C_5K_8)$
$Y(5) = (C_5K_5 – C_1K_6) + (C_7K_7 + C_1K_8)$
$Y(7) = (C_7K_5 + C_3K_7) – (C_5K_6 + C_5K_8)$

V. Results and Discussion

The RTL view of the developed DCT chip is shown in figure 1 and internal schematic of the chip is shown in figure 2. The functional simulation of the developed chip is shown in waveform of Modelsim simulator in figure 3. The size of the watermark can be of 'N' bits. The watermark is extracted in ASCII code format. In the chip X_0, X_1, X_2, X_3, X_4, X_5, X_6 and X_7 are the input of the watermark and Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6, and Y_7 are the outputs of DCT.

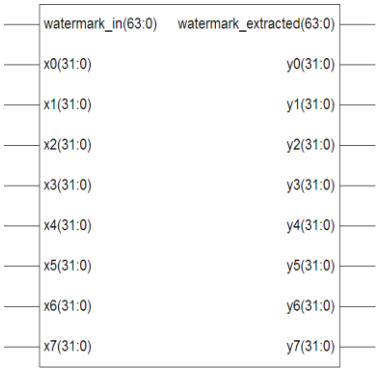

Fig.2 RTL View of DCT with Watermark Chip

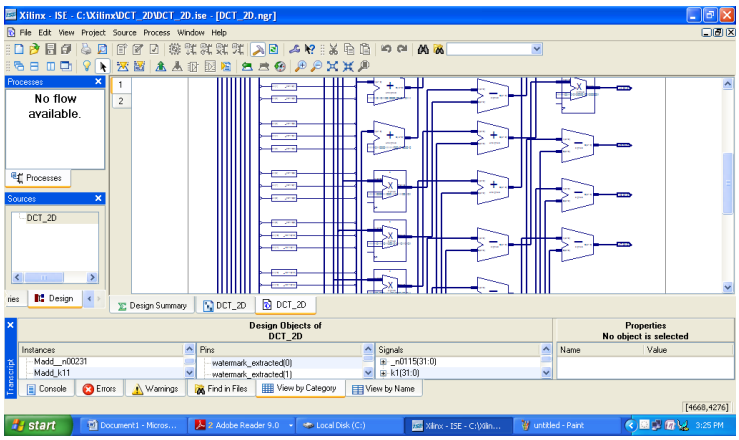

Fig.3 Internal Schematic of the Chip

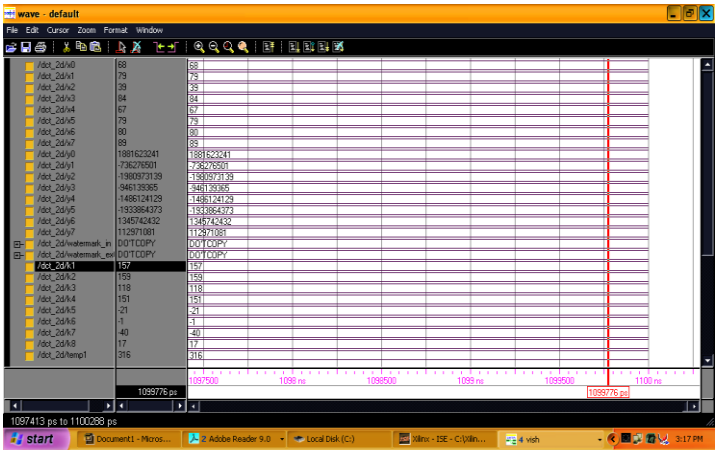

Fig. 3 Modelsim Simulation of the developed Chip

VI. Conclusion

The chip can be easily integrated in any existing JPEG encoder to watermark images right at the source end. The implementation of a low-power, high-performance version is currently in progress, Low-power VLSI features, such as multiple supply voltages, dynamic clocking, and clock gating will be considered. High performance architectural implementations, such as pipeline or parallelism, are under research. The disadvantage of the watermarking algorithms implemented is that the processing needs to be performed pixel by pixel. The watermarks are tested with block by clock extraction with different test cases.

References

[1] A. M. Eskiciogluand E. J. Delp, "An Overview of Multimedia Content Protection in Consumer Electronics Devices," Elsevier Signal Processing: Image Communication, vol.1 6, pp.681–699, 2001.

[2] D.W. Trainor J.P. Heron* and R.F. Woods, White paper on "IMPLEMENTATION OF THE 2D DCT USING A XILINX XC6264 FPGA", Department of Electrical Integrated Silicon Systems Ltd and Electronic Engineering Chlorine Gdn's The Queen's University of Belfast N. Ireland(Page 9)

[3] H. Berghel, "Watermarking Cyber space," Communications of the ACM, vol.40, no.11, pp.19–24, November1997.

[4] IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010 ISSN (Online): 1694-0784 ISSN (Print): 1694-0814 Watermarking of Digital Video Stream for Source Authentication Kesavan Gopal, Dr. M. Madhavi Latha, Team Leader, Infotech Enterprises Limited Bangalore, Karnataka, India (Page 1,6)

[5] I.J.Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, vol.6, no.12, pp.1673–1687, Dec1997.

[6] N. M. Kosaraju, M. Varanasi, and S.P. Mohanty, "A High Performance VLSI Architecture for Advanced Encryption Standard (AES) Algorithm, "in Proceedings of 19th IEEE International Conference on VLSI Design, 2006,pp .481–484.

[7] N. Memonand P.W. Wong, "Protecting Digital Media Content," Communications of the ACM, vol. 41, no.7, pp.35–43, July 1998.

[8] S. Katzen beisser and F.A.P. Petitcolas, Information Hiding techniques for steganography and digital watermarking, Artech House, Inc.,MA, USA, 2000.

[9] S.P.Mohanty, "Digital Watamerking of Images," M.S. thesis, Department of Electrical Engineering, Indian Institute of Science, Bangalore, India,1999.