4

Real Time Implementation of Digital Watermarking Algorithm for Image and Video Application

Amit Joshi[1], Vivekanand Mishra[1]
and R. M. Patrikar[2]
[1]*Sardar Vallabhbhai National Institute of Technology*
Surat
[2]*Visvesvaraya National Institute of Technology*
Nagpur
India

1. Introduction

Watermarking is the process of hiding a predefined pattern or logo into multimedia like image, audio or video in a way that quality and imperceptibility of media is preserved. Predefined pattern or logo represents identity of an author or rights. In recent years, rapid growth in digital multimedia has been noticed. Digital data (image, audio, and video) is sent through World Wide Web (www) without much effort and money. But security is the main issue in digital multimedia. In the face of these dramatic changes, the entertainment industry has scrambled to adopt a slew of technologies that allow it to retain the copyright controls provided by the law and harness the new world to increase the industry size and enhance the consumer experience.

In recent years, the research community has seen much activity in the area of digital watermarking as an additional tool in protecting digital content and many excellent papers have appeared over the years (Arun Kejariwal,2003). Digital watermarking attempts to copyright the digital data that is freely available on the World Wide Web to protect the owner's rights. As opposed to traditional, printed watermarks, digital watermarks are transparent signatures. They are integrated within digital files as noise, or random information that already exists in the file. Thus, the detection and removal of the watermark becomes more difficult. Typically, watermarks are dispersed throughout the entire digital file such that the manipulation of one portion of the file does not alter the underlying watermark. To provide copy protection and copyright protection for digital image and video data, two complementary techniques are being developed known as Encryption and Watermarking. One more method for data hiding is which is closely correlated with watermarking known as Steganography.Steganography was basically a way of transmitting hidden (secret) messages between allies. There are various data hiding techqniques are available for security. The deatils of each data hiding techniques are presented in next section.

2. Data hiding techniques

Cryptography: It scrambles a message into a code to obscure its meaning. Scrambling of message is done with help of secret key. Scrambling message called as encrypted and it is again decrypted with that secret key only. Cryptography provides security to message. **Steganography:** With Steganography, the sender would hide the message in a host file. The host file or cover message, is the file that anyone can see. When people use this techique, they often hide the true intent for communicating in a more common place communication scenario. In steganography, usually the message itself is of value and must be protected through clever hiding techniques and the "vessel" for hiding the message is worthless.

Watermarking: It is the direct embedding of additional information into the original content or host signal. Ideally, there should be no perceptible difference between the watermarked and original signal and the watermark should be difficult to remove or alter without damaging the host signal. In watermarking, the effective coupling of message to the vessel which is the digital content is of value and the protection of the content is crucial.

In case of steganography, where the method of hiding the message may be secret and the message itself is kept secret; but in watermarking, typically the watermark embedding process is known and the message (except for the use of a secret key) does not have to be secret.Most of the people find difficulty to differentiate term digital watermarking and steognography. Let us take a simple example to understand this difference. If someone gives me a beautiful birthday gift with his name on wraper. Now if I am interested in steagnography approch, I am more willing to see what is inside the wraper so I will open gift without any care of wrapper. While being digital watermarking person, I am interested in wrapper rather then gift provided to me, which gives me a clear indication of the provider. The conecpt of cryptography is totally different then these approaches of data security. Digital content is encrypted at transmitter using a key and can be decrypted at receiver if and only if the correct key is available. Cryptography gives advantage only through the channel. Once encrypted content is decrypted using a key at receiver, no means of security is available for protecting digital content from copyright. Therefore, encryption must be replaced by some method which protects digital content after decryption and there concept of watermarking comes. Another difference between cryptography and watermarking is: cryptography maps the data such that it is unreadable without decryption while, watermarking embeds data maintaining multimedia in its original form.

3. Digital watermarking

These are the parameters important for digital watermarking.

a. Transparency
b. Security
c. Ease of embedding and retrieval
d. Robustness
e. Effect on bandwidth
f. Interoperability

a. Transparency: The most fundamental requirement for any Watermarking method shall be such that it is transparent to the end user. The watermarked content should be consumable

at the intended user device without giving annoyance to the user. Watermark only shows up a watermark-detector device.

b. Security: Watermarked information shall only be accessible to only authorized parties. They only have the right to alter the Watermark content. Encryption can be used to prevent unauthorized access of the watermarked data.

c. Ease of embedding and retrieval: Ideally, Watermarking on digital media should be possible to be performed on the fly. The computation needed for the selected algorithm should be least.

d. Robustness: Watermarking must be robust enough to withstand all kinds for signal processing operations attacks or unauthorized access. Any attempt, whether intentionaly or unintentionaly, that has a potential to alter the data content is considered as an attack. Robustness against attack is a key requirement for Watermarking and the success of this technology for copyright protection depends on its stability against attacks.

e. Effect on bandwidth: Watermarking should be done in such a way that it does not increase the bandwidth required for transmission. If Watermarking becomes a burden for the available bandwidth, the method fails.

f. Interoperability: Digitally watermarked content shall still be interoperable so that it can be seamlessly accessed through heterogeneous networks and can be played on various plays out devices that may be aware or unaware of watermarking techniques.

4. Need of hardware implementation

The implementation of watermarking could be on many platforms such as software, hardware, embedded controller, DSP, etc. System performance is a major parameter while designing complex systems. The standard DSP which has Von Neumann style of fetch-operate-write back computation fails to exploit the inherent parallelism in the algorithm. For example, a 30 tap FIR filter implemented on a DSP microprocessor would require 30 MAC (Multiply Accumulate) cycles for advancing one unit of real-time. Further, each MAC operation may consist of more than one cycle as it involves a memory fetch, the multiply accumulate operation, and the memory write back. In contrast, a hardware implementation can store the data in registers and perform the 30 MAC operations in parallel over a single cycle. Thus, high throughput requirements of real-time digital systems often dictate hardware intensive solutions.

FPGAs provide a rapid prototyping platform. They can be reprogrammed to achieve different functionalities without incurring the non-recurring engineering costs typically associated with custom IC fabrication. For commercial applications like movie production, video recording,real on-spot video surveillance,where a real-time response is always required, so a software solution is not recommended due to its long time delay. Since the goal of this research is a high performance encoding watermarking unit in an integrated circuit (IC) for commercial applications, and since FPGAs (field programmable gate arrays) have advantages in both fast processing speed and field programmability, it was determined that an FPGA is the best approach to build a fast prototyping module for verifying design concepts and performance.

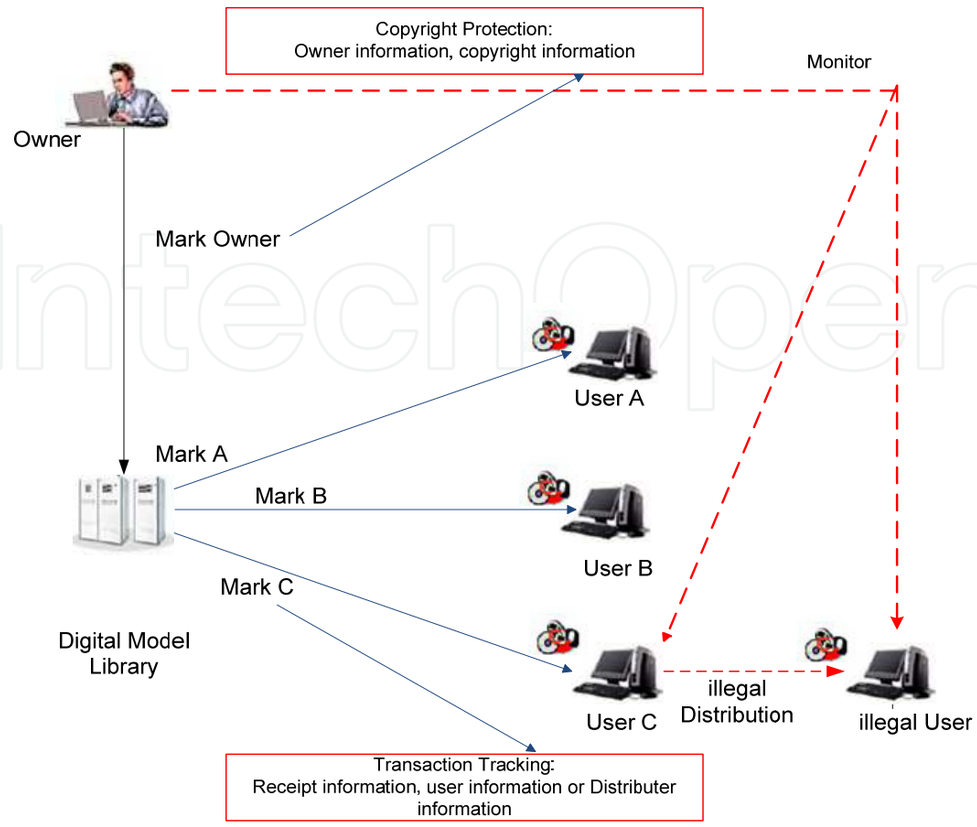


Fig. 1. Copyright Protection service (MarkAny ,2010).

Several software implementations of the watermarking algorithms are available, but very few attempts have been made for hardware implementations. Software implementation of watermarking has been implemented because of their ease of use and flexibility. Mostly software based watermarking works on offline where images are captured through camera and stored on computer and the software for watermarking runs and embeds the watermark and then the images are distributed. This approach has the drawback of certain amount of delay, once images are captured and then watermark is embedded. If attackers would attacks the image before the watermark embedded then it creates issues for ownership of the originator.So there is a need of real-time watermarking where watermark embedding unit reside inside the device (as digital camera) and embedding done directly when image is captured. The hardware implementation of watermarking has advantages in terms of reliability and high performance for area, power and speed. This is very much crucial in some applications like real-time broad casting, video authentication and secure camera system for courtroom evidence. The hardware implementation can have advantage of parallel processin. Since watermarking process deals with processing of watermark and pre-processin of original content before embedding watermark. These two processes are independent and can work in parallel to achieve parallelism to achieve high speed for real-time application.

5. Application of digital watermarking

The digital watermarking technology can be applied to various fields such as copyright protection, transaction tracing, broadcast monitoring and tamper proofing etc.

5.1 Copy-right protection

It is the most common application especially in multimedia object where user inserts copyright information as a watermark or never-copy watermark in a digital content. This watermark can prove his ownership in court when someone has infringed on his copyrights Also number of duplications, manipulations and distribution of digital content can be controlled which are the main sources of illegal process. It is also possible to encode the identity of the original buyer along with the identity of the copyright holder, which allows tracing of any unauthorized copies.

5.2 Transaction tracing fingerprinting

Fingerprint is treated as a transactional watermark. It applies to trace the source of illegal copying of digital content. The owner can embed different unique watermarks for different customers. To trace the source of illegal copies, the owner can use a fingerprinting technique. In this case, the owner can embed different watermarks in the copies of the data that are supplied to different customers. Fingerprinting can be compared to embedding a serial number that is related to the customer's identity in data. It enables the intellectual property owner to identify customers who have broken their license agreement by supplying the data to third party. If misuse of digital content takes place, it is easy to trace out the responsible customer.

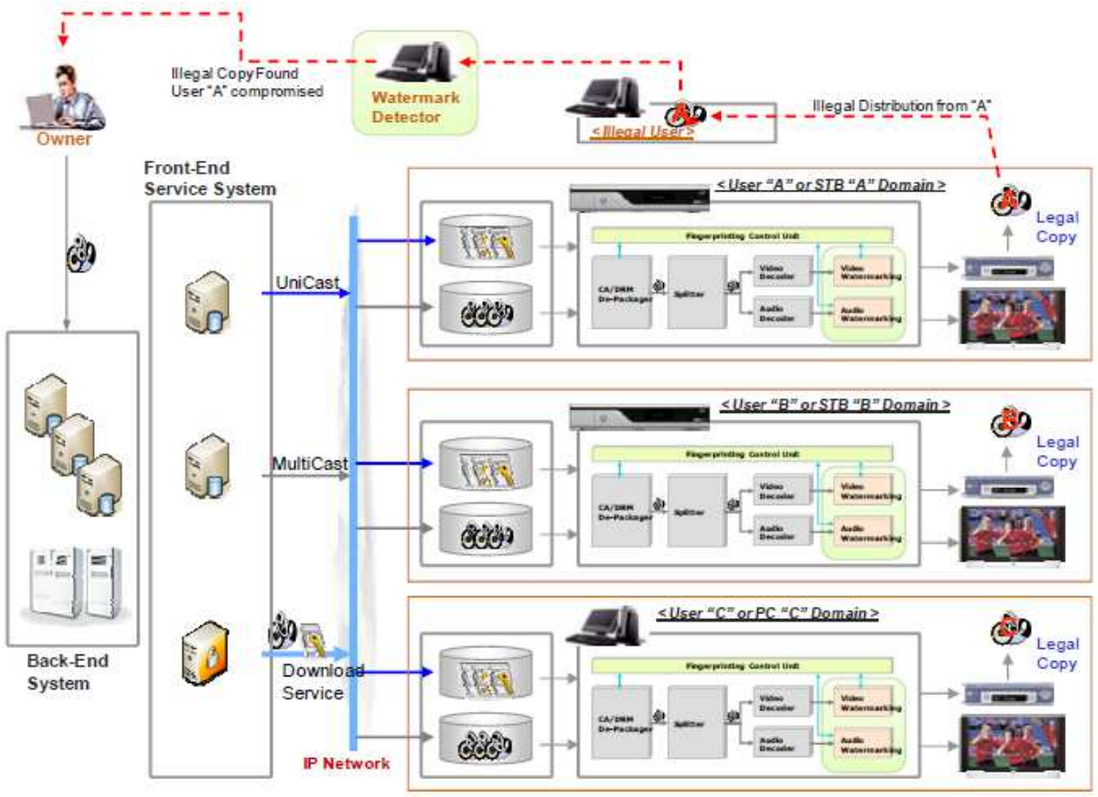


Fig. 2. Video Tracking and finger-printing service (MarkAny, 2010)

5.3 Broadcast monitoring

This application is used by advertisers to broadcast the watermarked information at a specific time and location. Watermarking finds its application to monitor or track the digital content being broadcast, time and location of broadcasting. Specialized equipments are used to track the broadcast channels or radio channels. Upon reception, watermark is detected; content is verified and reported to the broadcasters for true reach of content. It is also useful in finding illegal rebroadcast of copyright information. By embedding watermarks in commercial advertisements an automated monitoring system can verify whether advertisements are broadcasted as contracted. A broadcast surveillance system can check all broadcast channels and charge the TV stations according to their findings. Owners of copyrighted videos want to get their royalties each time their property is broadcasted.

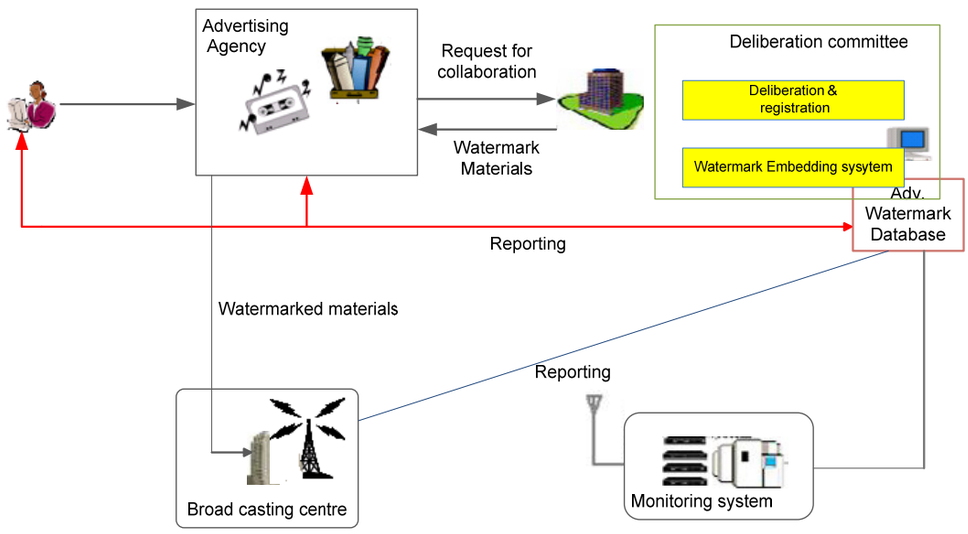


Fig. 3. Broadcast monitoring system (MarkAny, 2010)

5.4 Tamper – proofing

This can be applied to detect existence forgery when contents are forged evil-mindedly and intentionally by embedding watermark information easily damaged by micro-operation. For example, security equipment such as CCTV has been already converted from an analogue system into a digital system, but the data saved by these systems are saved all digitally. However the weakness of digital data that even general users who have personal system can easily operate moving pictures and sound source data which causes a reliability problem for the digital data. A means of judging existence of forgery is necessary to utilize the moving picture data recorded at a digital depository through CCTV as proof data at a court. This can be utilized for a DVR (Digital Video Recorder)/NVR (Network Video Recorder) system, digital camera, camcorder, etc.

6. Implementation of image watermarking

First DCT based semi fragile watermarking algorithm for digital camera with FPGA implementation was developed in paper (Hyum Lim et al,2003). In paper, (Saraju P. Mohanty

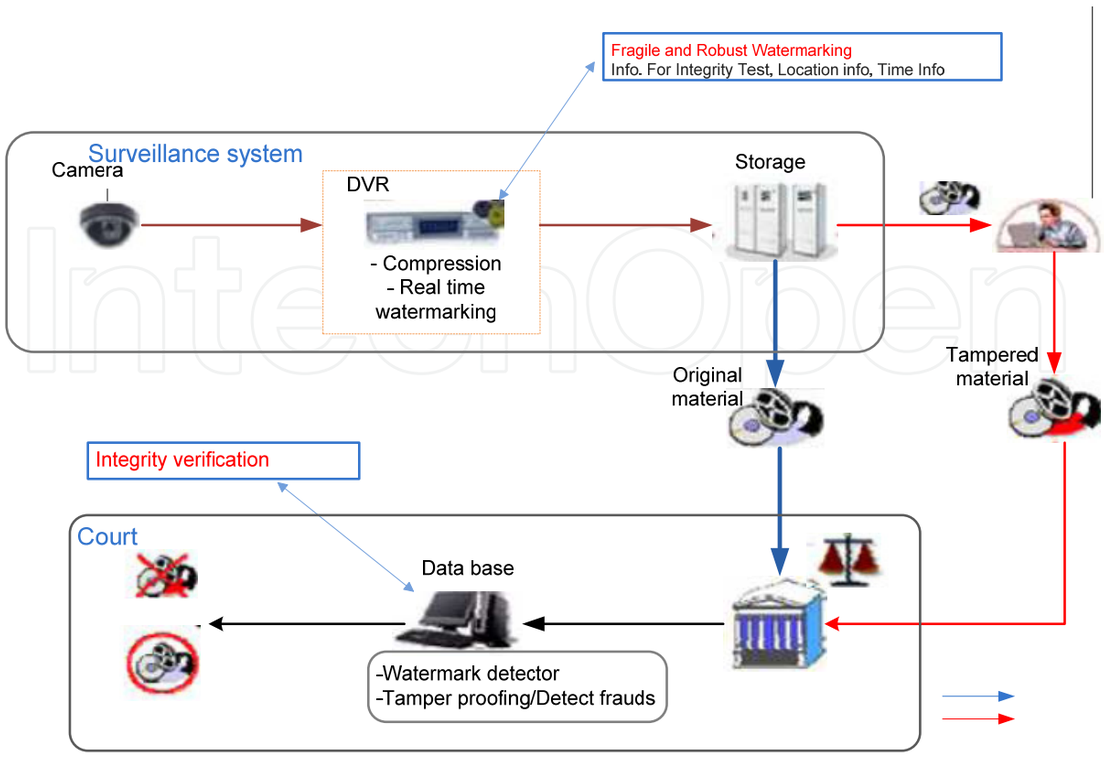


Fig. 4. Tamper proofing Service flow (MarkAny, 2010)

& N. Raganathan 2004) had also developed visible watermarking scheme on DCT. After that algorithms for wavelet based approach were developed to adapt JPEG2000 new millennium standard and to explore multiresolution property of wavelet (Victor V. Hernandez Guzman & Mariko Nankano,2004; Jianyog Huang & Changsheng Yang,2004). In 2005 later part, the proposed watermark (Sammy H. M. Hawk & Edumund Y. Lam, 2002) implementation technique in digital photography with DWT approach for software based implementation. After that next year, development of (Lei Tian, Heng-Ming Tai,2006) secure images captured by digital camera for DWT based approach has been proposed. Another spread spectrum watermarking techniques provides better perceptual transparency and watermark robustness (I.J.Cox et al,1995,1997). This can also developed for secure digital camera application. The watermarking scheme with random binary sequence was developed in paper (A. Lumini & D. Maio,2000). Another watermarking algorithm based on threshold based scheme presnted in paper (Yong-Gang Fu & Hui -Rong Wang,2008). The novel watermarking scheme for block processing method with differential expansion was developed in the paper(Hsien-Wen Tseng & Chin-Chen Chang ,2008). The first attemp to develop simple and efficient watermark technique for JPEG2000 Codec with scattered matrix watermark was presnted in paper (Tung Shou Chen et al,2004). There are many software based implemntation of image watermarking algorithms but very few attempt has been made for hardware implemntation. This will cover in section 6.1 withy detail explanation.

The input image for watermarking algorithm can be either monochrome (black and white) or color image. As with traditional color processing, we first convert a color image from

an RGB color space to the YCbCr color space. Then only the Y component of the image is down-sampled to form a grayscale image of resolution of 1 M pixels (assuming the original is between 2 M and 8 M pixels, true for most digital cameras today). Afterwards, a watermark is embedded in the image by quantizing the coefficients of the n^{th} sub band level for DWT of the image. Finally, the Y image plane is converted back to spatial domain by IDWT and a watermark image is formed by up sampling the image and adding it with the original Y, Cb and Cr color components. For extraction process, the user has access to watermark (w), the coefficient selection key (c key) (A.J. Menezes et al,1996; B. Sehneier,1996) and the original image incase of non blind watermarking. Since only the user knows the secret key for the watermarking therefor security against forgery is guaranteed.

As stated earlier, only luminance component Y is down sampled to embed the watermark. The down sampling is a lossy process and thus down sampling of chroma signals (Cb and Cr) are lost that can not be retrieved by reverse process of up sampling at receving end. The complete process of down and up sampling of Lena 256 x 256 color image is shown in this section. First color images which comprises of RGB components are converted to YcbCr, where Y contains luminance information and Cb and Cr contains the chrominance information of the image. Then Y signal is down sampled at factor two to obtain down sample image. This image is used for wavelet processing and to embed the watermark. This image is again up sampled with factor two to obtain recover Y component. The complete process shown in Fig. 5.

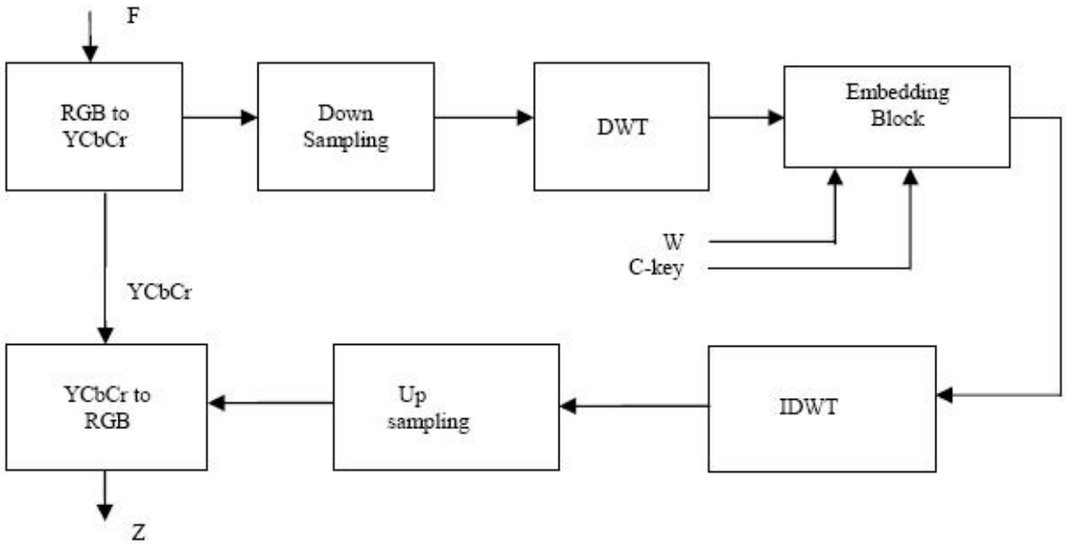


Fig. 5. Watermark Embedding Process

The problem with process that up sampling adds zero's to the images, so the image after up sampling is distorted (recovered Y component) as shown in above Fig 6. To over come this problem, we simply add the original Y component value to the zero paddied values as shown in below in Fig. 7.

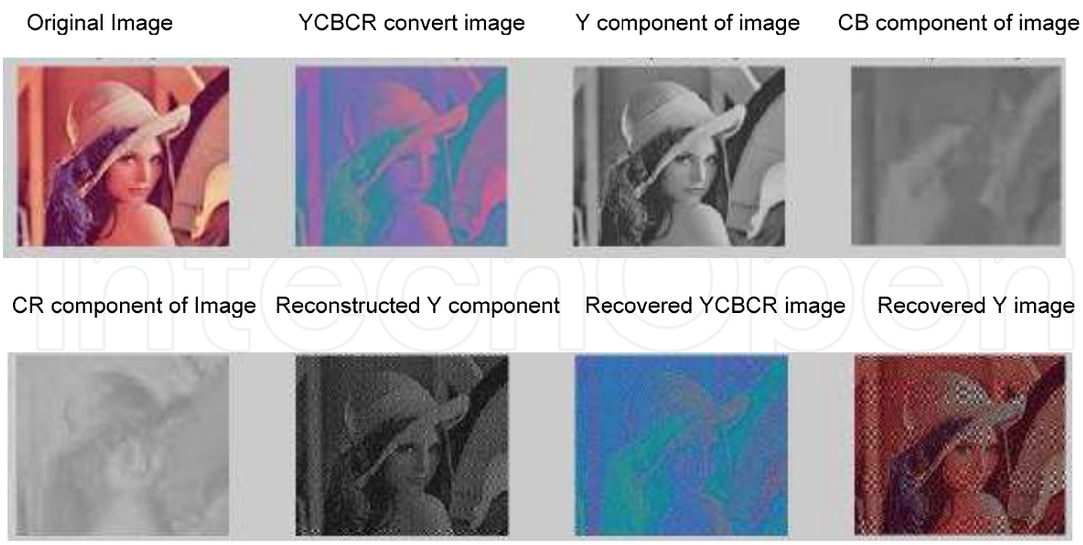


Fig. 6. Down sampling and up sampling process of Y component

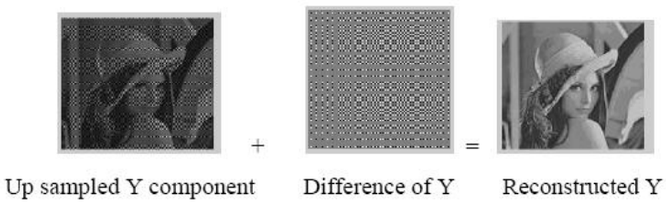


Fig. 7. Reconstructed Y plane after up sampling

The complete modified process is shown in below Fig 8.

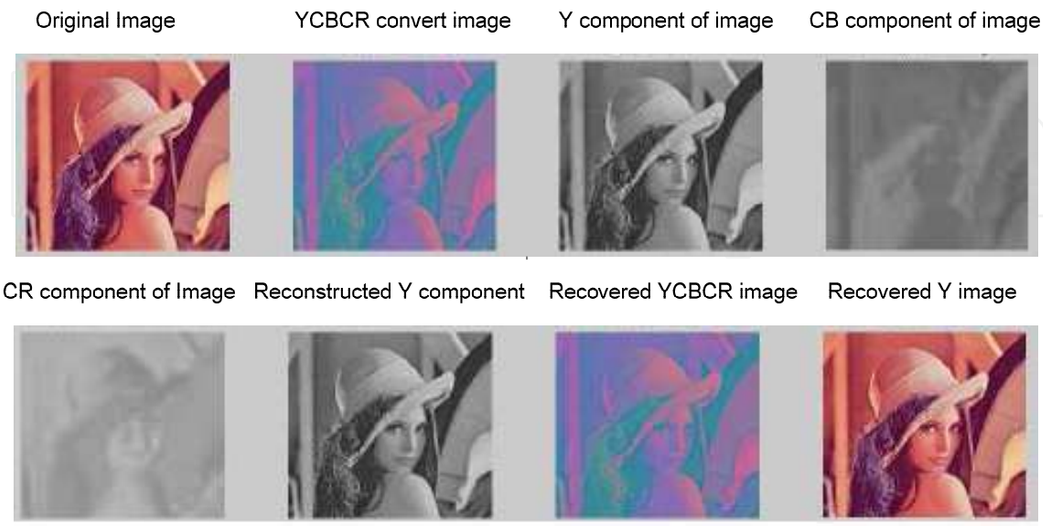


Fig. 8. Modified Down-Up sampling process with proper reconstruction of Image

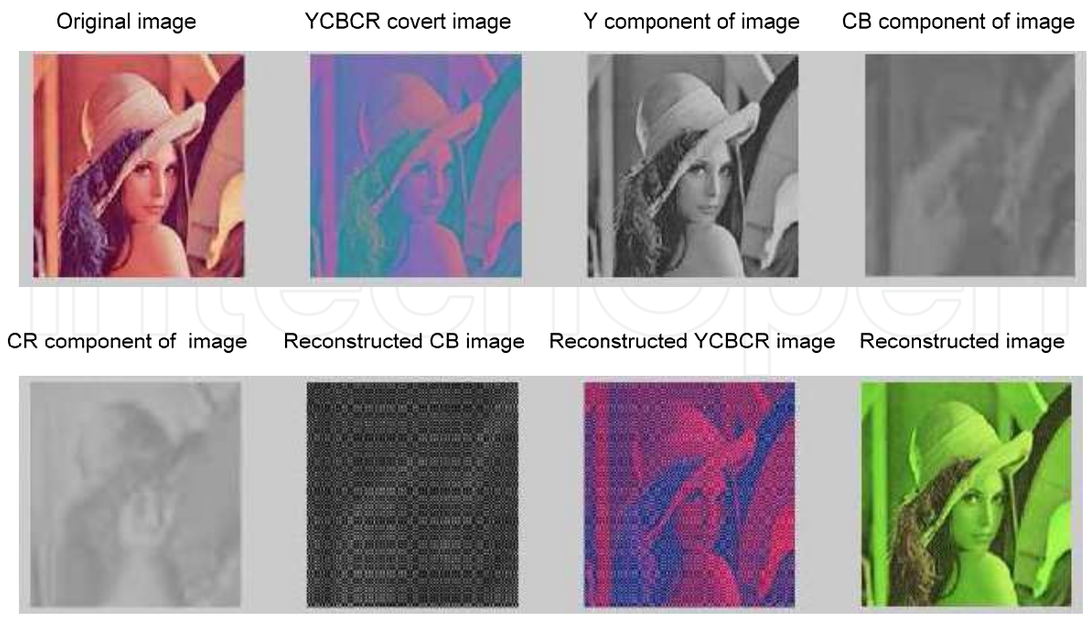


Fig. 9. Down sampling and up sampling process for Cb component

The chrominance signal can also be down sampled as shown in Fig 9 for Cb component and Fig 10 for Cr component. We can see the difference between original and recovered up sampled image in Fig 9 and Fig 10. As we can see, luminance component Y signal down/up sampling process provides better results compare to chrominance signal Cb and Cr down/up sampling.

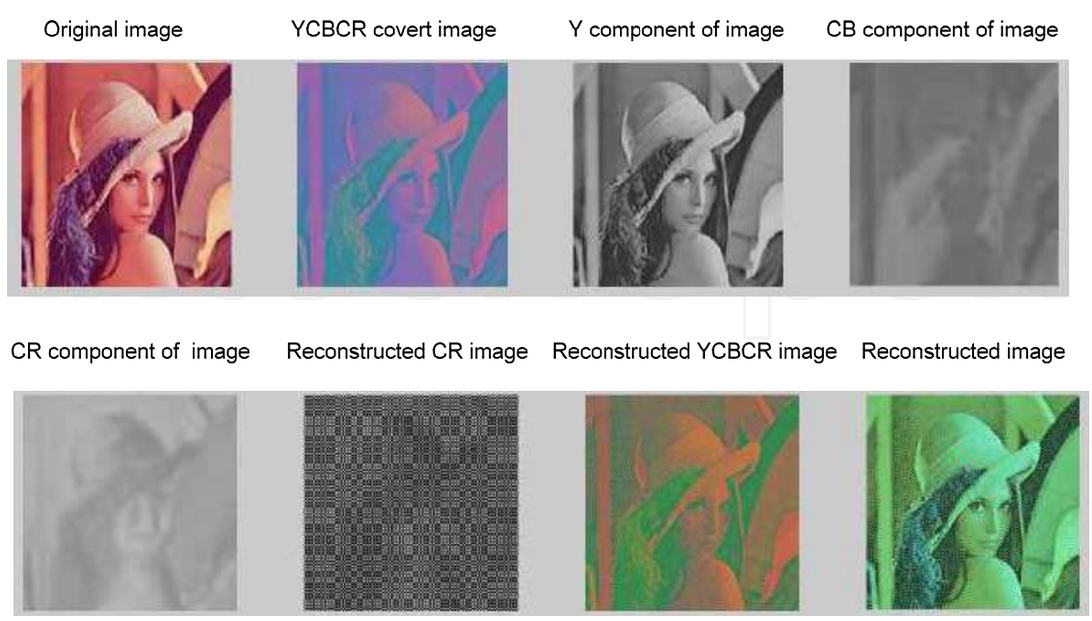


Fig. 10. Down sampling and up sampling process for Cr component

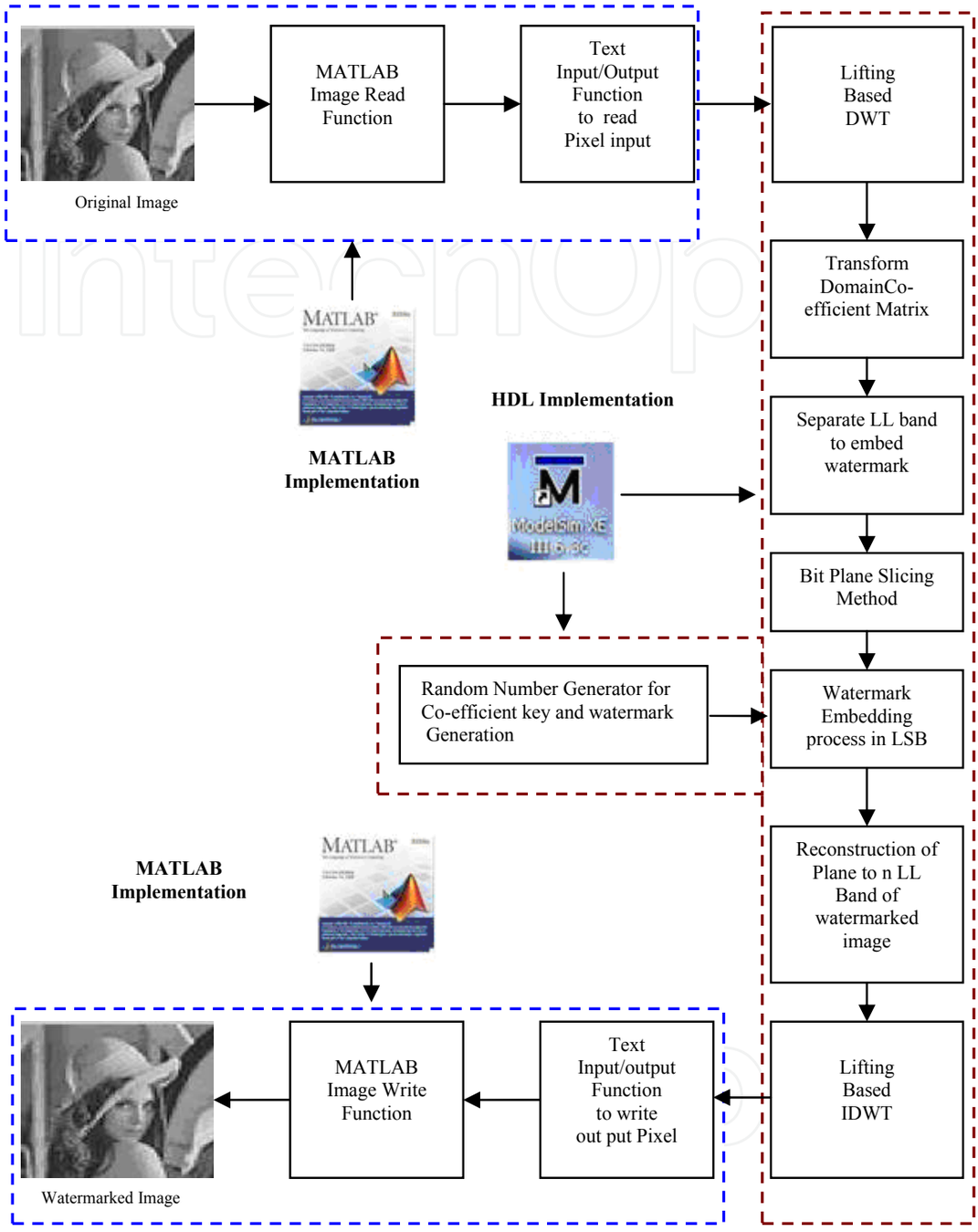


Fig. 11. Embedding scheme for watermarking

6.1 Proposed algorithm

Spatial-domain digital watermarking methods are generally considered as having poor performance after geometric distortion (such as cropping and scaling), common signal processing (such as JPEG and filtering). It is efficient in terms of less computational cost due to their easy operation.On the other hand, frequency-domain watermark techniques,

have their high computation complexity, and provide great robustness to different attack. To increase the robustness, we have to increase number of sub band level which require more computational cost. However, we have adopted the combined approach with spatial-frequency domain approach which has advantages of both domains. The frequency domain transformation is done with lifting based wavelet scheme and spatial domain transformation done with bit plane slicing. The steps of algorithms have been described in paper (Amit joshi,2009). The implementation flow for proposed scheme is shown in Fig 11. The image is read through MATLAB and pixel is stored in datain.txt file. With help of text I/O package, the datain.txt file has been read in VHDL and Legall 5/3 based Lifting wavelet applied to obtain transform domain co-efficient matrix. LL band coefficient stored in separate memory to embed watermark. The RTL code of bit Plane slicing has been developed to separate different planes from LSB to MSB. To the selected co-efficient generated by random number generator, then watermark has been added to them. Then all planes are reconstructed with bit plane slicing RTL code to obtain LL band of watermarked image. Then lifting based legall 5/3 IDWT has been applied to obtain pixel values. The MATLAB function is used to construct watermarked image.

6.1.1 Hardware implementation of wavelet

For implementation of hardware efficient DWT based scheme, lifting based scheme obviously far better than traditional convolution scheme. Lifting based wavelet scheme used in various approaches like Daubechies 9/7 and Le Gall 5/3. But Le Gall 5/3 is proven more hardware efficient due to its simplicity and lossless implementation. The odd and even samples values can be calculated by following equations (1) and (2) are

$$y(2n+1) = x(2n+1) - [\frac{x(2n) + x(2n+2)}{2}] \tag{1}$$

$$y(2n) = x(2n) + [\frac{y(2n-1) + y(2n+1) + 2}{4}] \tag{2}$$

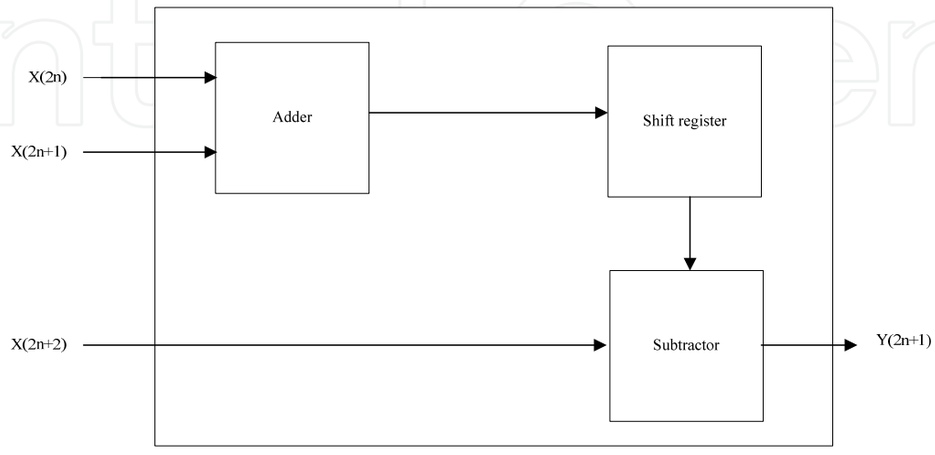


Fig. 12. Predict Phase

To implement this algorithm, the equations stated earlier are utilized. In lifting scheme this algorithm is divided in two phases: predict phase and update phase. In order to find the value for predict phase, simultaneously three inputs are required as per eq. (1). Similarly in the update phase only one even input and two values obtained form predict phase are required as per eq. (2). The 8 bit-gray scale image of LENA is used for performance of Legal 5/3 DWT. The architecture module of predict phase and update phase are shown in Fig. 12 and Fig. 13 respectively.

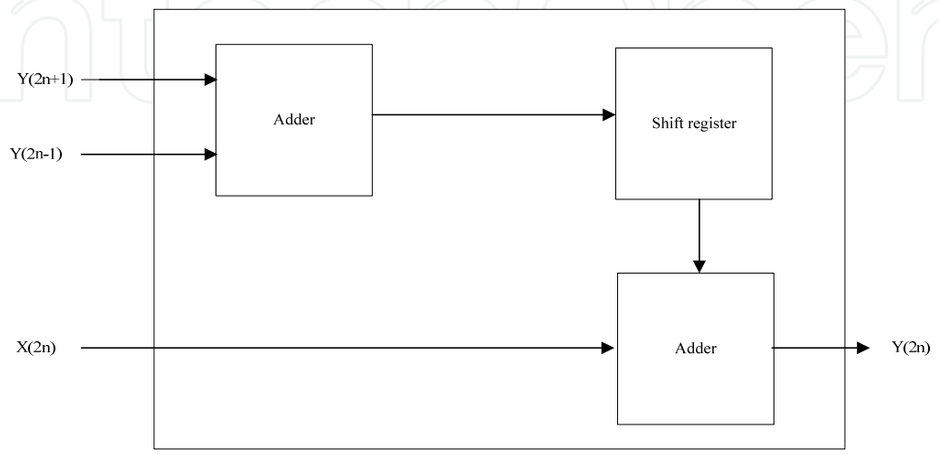


Fig. 13. Update Phase

6.1.2 Memory management

As suggested, to obtain the forward wavelet transform, initially we need to read the three input data. And from these we are get two coefficients detail (high) and approximate (low). One needs to manipulate the co-efficient of the image to obtain the correct output. In VHDL, two dimensional matrixes are not synthesizable. So if we are interested in reading the image having size n X n, then total n^2 memory location are required to store each input pixels. For this, 64 X 64 gray scale image are utilized in the wavelet transform, data is processed row wise and then after columnwise. The memory orgnization is as shown in Fig. 14.

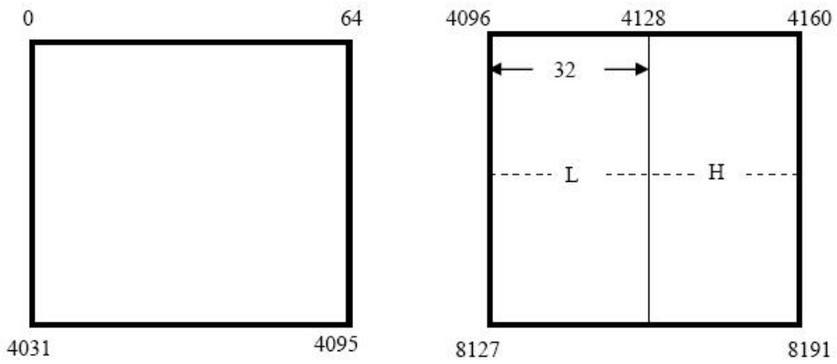


Fig. 14. Memory Management of Wavelet transforms

6.1.3 Watermarking embedding hardware implementation

There are two basic blocks required for watermark embedding process.

a. Bit Plane Slicing scheme implementation
b. Random Number Generator for key selection and watermark generation.

a. Bit Plane Slicing Implementation: It is the spatial domain techniques. In Spatial domain scheme, watermark is directly embedded in the pixel values. Algorithm splits the image

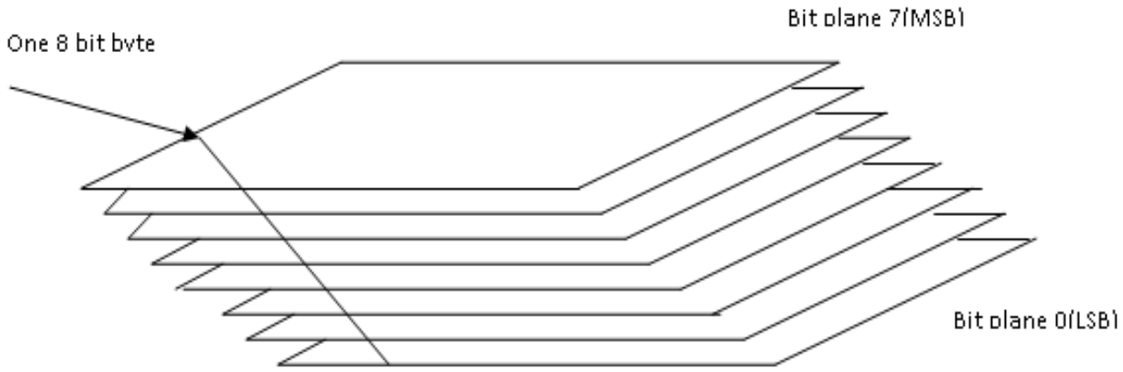


Fig. 15. Bit planes of a Image

into 8 planes from MSB to LSB. The whole concept is explained in details as shown in Fig. 15. Suppose pixel values in binary foramt read from memory as shown here:

01111001 01100101 01001010 00100110 10000100 10000110 10001001 10001101

The values read from memory are taken one by one in temp variable.

To separate out the values in different planes, we will xor the temp values with standard values as follows. Here first value read from memory and stored in temp is **01111001.**

- LSB plane : 01111001 and 00000001 : The resultant values is 0000000**1**.
- Seventh plane: 01111001 and 00000010 : The resultant values is 0000000.
- Sixth plane : 01111001 and 00000100 : The resultant values is 00000**0**0.
- Fifth plane : 01111001 and 00001000 : The resultant values is 0000**1**000.
- Fourth plane : 01111001 and 00010000 : The resultant values is 000**1**0000.
- Third plane : 01111001 and 00100000 : The resultant values is 00**1**00000.
- Second plane : 01111001 and 01000000 : The resultant values is 0**1**000000.
- MSB plane : 01111001 and 10000000 : The resultant values is **0**0000000.

Next time another value of pixel read from memory and stored in temp as 01100101 and same procedure is followed as above. In this way all LSB plane co-efficient are obtained. The reconstruction of the planes are also very simple. Finally we have to just add all the resultant values planes to obtain original value. With addition of all plane values we obtain:

00000001 + 00000000 + 00000000 + 00001000 + 00010000 + 00100000 + 01000000 + 00000000 = 01111001.

b. Random Number Generator: It is one of the important blocks of watermarking process. Basically its role is to generate the coefficient selection key and embed watermark to original content. As shown in Fig 16, it has 8 bit D-flip flop which are used so that the maximum number of co-efficient selection key from random number generator is 255. The watermark is added according to key generated at the output. The random number generator is started with secret key provided as its initial state. We have used 10101101 as key that serves as the initial seed to start random number generation. The same key has been used with same random number at the detection side which generate same pseudo sequence to retrieve the watermark.

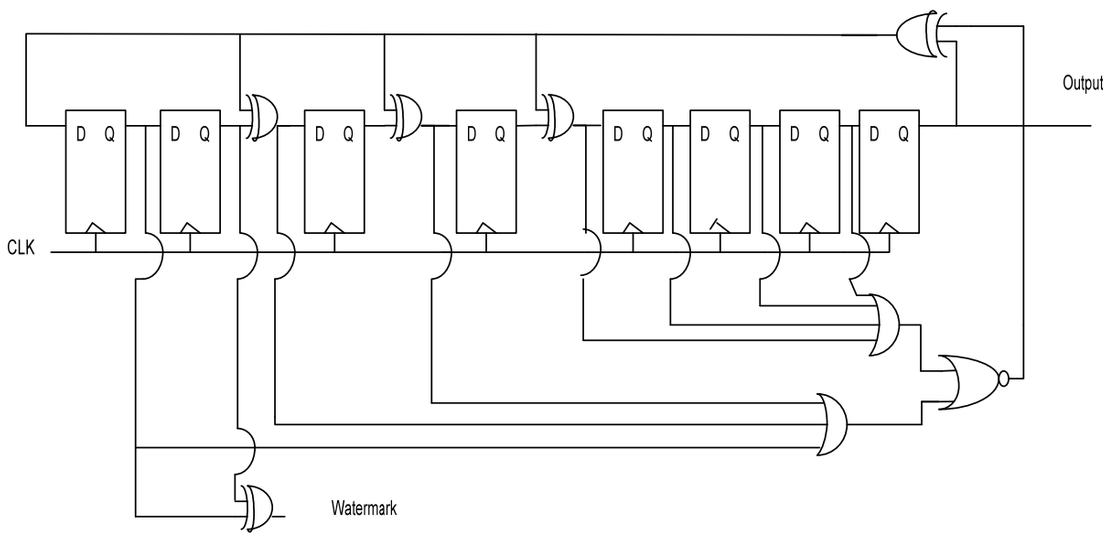


Fig. 16. Random Number Generator

6.1.4 VLSI architecture of image watermarking algorithm

The architecture design proposed for scheme is defined as shown in Fig 17. The main memory comprises the memory space which is twice the size of original image size as it has to store original values and watermarked value. For example, the size of image be 256 x 256, the main memory requirement is 2*256*256=1, 31,072. Now the memory is divided into two parts as RAM1 for original image and second for RAM2 for watermarked image. At the time of detection for non blind scheme, the values in RAM1 are considered as original pixels values and RAM2 are watermarked values. As explained earlier in section 6.1, wavelet scheme based on lifting based legal 5/3 method requires three values to read from RAM1.

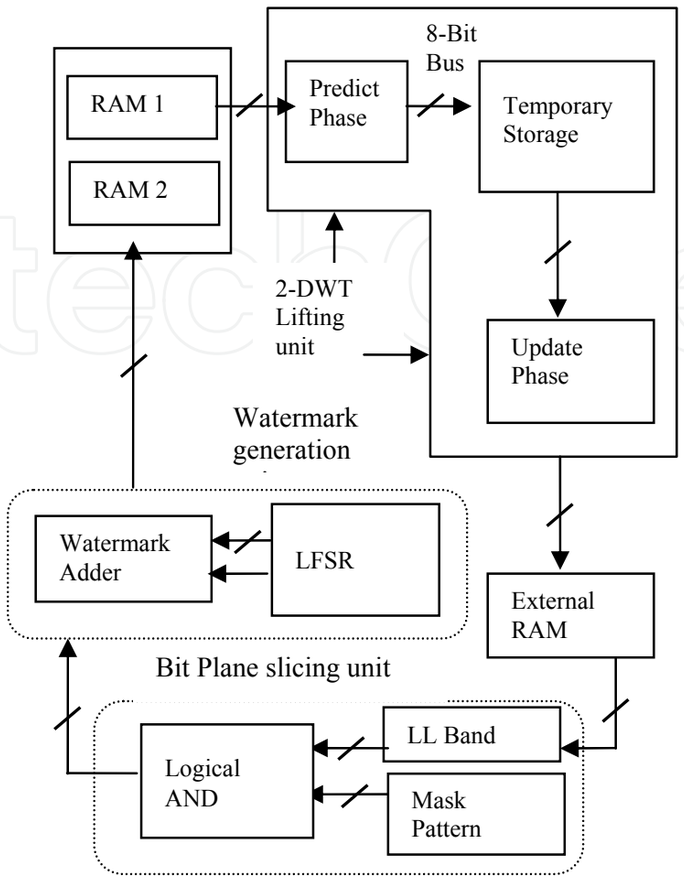


Fig. 17. VLSI Architecture of proposed algorithm

6.1.5 Pin diagram

The pin diagram for wavelet based spatial domain watermarking chip is shown in the Fig. 18. The functional description of each pin is:

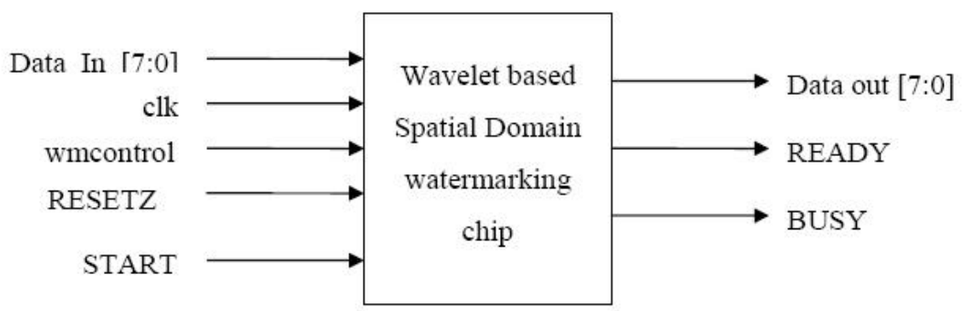


Fig. 18. Pin Diagram

Data In [7:0]: DATA Input bus. Original pixel values which were stored will be input on this bus for operation.

CLK: Clock signal to chip.

Wmcontrol: Enables during embedding the watermark.

RESETZ: It is active low signal to reset the chip

START: It is an active low handshake signal to initiate data transfer operation on Data In bus on every clock edge.

Data out [7:0]: DATA output bus. Watermarked pixel values are output on this bus.

READY: It is active high signal will be activated for one CLK cycle after the completion of watermark embedding operation. It indicates Data out bus has valid out on bus.

BUSY: It is a active high signal. It indicates Watermarking is in progress. When external signal is high which indicates, external access to RAM1's are isolated. The data on data bus out is not valid.

6.2 Hardware implementation results

The simulation results for Legall 5/3 is as shown in Fig. 19.

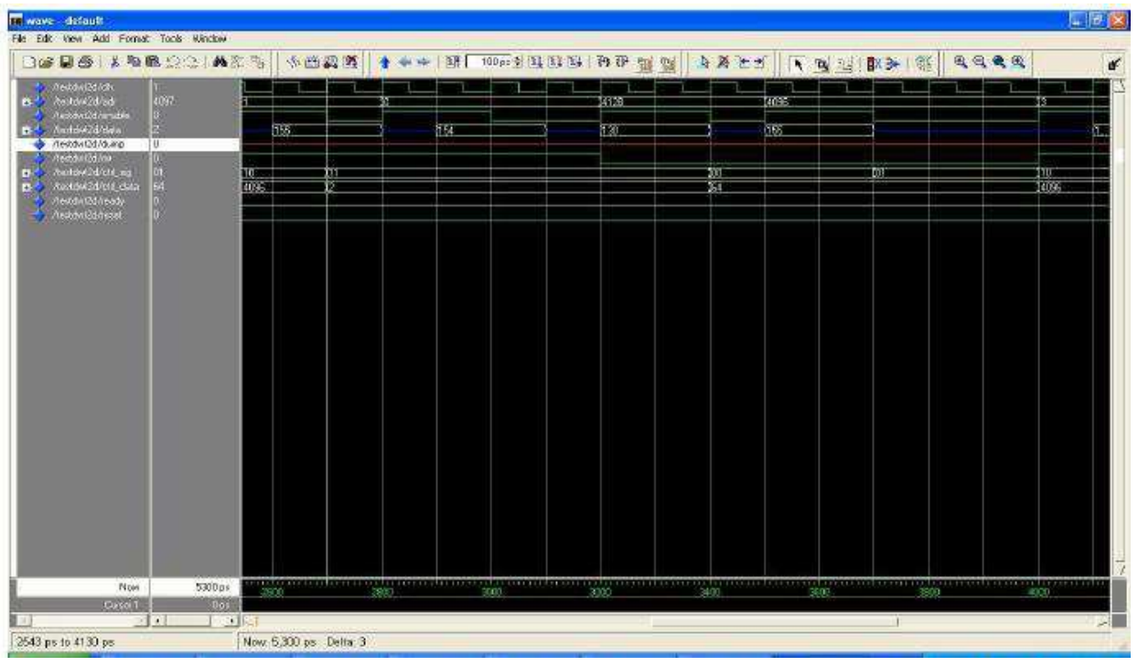


Fig. 19. Simulation of Legal 5/3 wavelet

6.2.1 FPGA results

Synthesis was performed with help of Xilinx project navigator ISE 9.1 software EDA tool. During simulation, textio library was utilized to read the gray scale image (lena 256 x 256) file. After processing, results are stored in text file. This text file is read through

MATLAB to generate image. Synthesis report and device utilization reports for proposed DWT, IDWT and Watermarking Processor is shown in Table 1 and Table 2 respectively. The results are obtained for Xc3s500e-4fg320-SPARTAN 3E FPGA using ISE 9.1 from Xilinx Tool.

Resources	DWT Processor	Watermarking Processor	IDWT Processor
RAM/ROM	3	2	4
Adders/Subtractor	16	2	14
Latches	12	5	10
Muxs	4	3	4
Counters	3	2	3
Registers/Flip Flop	469	62	542

Tt

Table 1. Synthesis Report for Proposed DWT,IDWT and Watermarking Processor

Resources	DWT Processor	Watermarking Processor	IDWT Processor
Slices	(535/4656)	(153/4656)	(570/4656)
Slices FFs	(395/9312)	(117/9312)	(410/9312)
LUTs	982	335	925
I/O	70	25	70
GCLKs	3	1	3

Table 2. Device Utilization Report for Proposed DWT, IDWT and Watermarking Processor

6.2.2 ASIC results

The proposed scheme requires three major blocks to embed the watermark as DWT, IDWT and Watermark process. We have calculated area and power with Design compiler using standard cell library of Farady 0.18 um technology as shown in Table 3. In Table 4, It also has been compared with other existing scheme.

Block	Type	Area (um*um)	Dynamic Power
DWT	1 Dimensional	12196	2.0592 mW
DWT	2 Dimensional	15770	8.6813 m W
IDWT	1 Dimensional	13237	2.8531 mW
IDWT	2 Dimensional	18106	9.3752 mW
Watermarking Processor	Bit Plane Slice	192	23 uW
Watermarking Processor	Binary Number Generator	322	48 uW

yy

Table 3. Area and dynamic power results for proposed scheme

Research Work	Watermarking Type	Processing Domain	Technology	Power	Execution Time
Tsai and Lu,2001	Invisible robust	DCT	0.35 um	107.6 uW	1.494 ms
Garimella et Al,2003	Invisible Fragile	Spatial	0.13um	82 uW	1.3059 ms
Saraju P. Mohanty et Al,2005	Visible	Spatial	0.35um	72uW	0.914ms
Saraju P. Mohanty et al,2006	Invisible Robust	DCT	0.35um	90 uW	1.125ms
Proposed Scheme	Invisible Robust	Wavelet	0.18um	69uW	0.893ms

Table 4. Summary of Watermark Custom IC Hardware Description in the literature of Watermarking

7. Video watermarking

In today's multimedia technology, the most widely used object is a video. Therefor maximum occurrences of copyright infringement and abuse happen for video media content. Video is sequence of frames and each frame is considered as a still image. But the challenges for video watermarking are as follows:

a. Video media is susceptible to increased attacks than any other media.
b. Video content are sensitive to subjective quality and Watermarking may degrade the quality.
c. Video compression algorithms are computationally intensive and hence there is less headroom for Watermarking computation.
d. Video is bandwidth hungry and that is why it is mostly carried in compressed domain. Therefore, Watermarking algorithm shall be adaptable for compress domain processing.
e. For low-bit rate video, Watermarking poses additional challenges, as there is less room for watermark data.
f. During video transmission, frame drops are very usual. If watermark data spreads over many frames, in that case watermark data may become irretrievable. Watermarking should be robust enough against this phenomenon.

The easiest way to embed the watermark in video is consider each of frame of video as still image and apply image watermarking algorithm. So algorithm which described in section 6.1 still holds quite comparable results when applied to video. One algorithm developed for video is presented in paper for wavelet domain (Amit Joshi & Vivekanand Mishra,2011). But with this approach, we are not utilizing the temporal dimension of video. Same way, many algorithms for developing watermarks on images are extended for videos. Some points need to be considered during the extensions. First one is between the frames there exists a huge amount of intrinsically redundant data. So we can explore that before embedding the watermark. Second is there must be a strong balance between the motion and the motionless regions. And another one is strong concern must be put forth on real time and streaming

video applications. Video Watermarking mainly done in uncompressed (raw data) domain or in compressed domain. The raw watermarking is classical approach of video watermarking scheme. In this classical approach, to apply a watermark, firstly the compressed video stream is to decompress. Use a spatial domain or transform- domain watermarking technique to apply the watermark, and then recompress the watermarked video. The disadvantages of classical approach is that watermark embedded has no knowledge of how the video will be recompressed and cannot make informed decisions based on the compression parameters. This approach treats the video compression process as a removal attack and requires the watermark to be inserted with excessive strength, which can adversely impact watermark perceptibility. Another issue with classical approach is that compression step is likely to add compression noise, degrading the video quality further. The main drawback is that fully decompressing and recompressing the video stream can be computationally expensive. A faster and more flexible approach to apply watermarking on compressed video is well know as compressed-domain watermarking. In compressed-domain watermarking, the original compressed video is partially decoded to expose the syntactic elements of the compressed bit stream for watermarking (such as encoded transform coefficients). Then, watermark is embedded in the partially decoded bit stream and again reassembled to form the compressed watermarked video. The watermark insertion process ensures that all modifications to the compressed bit stream will produce a syntactically valid bit stream that can be decoded by a standard decoder. The watermark embed process has access to information contained in the compressed bit stream, such as prediction and quantization parameters, and can adjust the watermark embedding accordingly to improve robustness, capacity, and visual quality.

Similar to image watermark implementations, the video watermark system can be implemented in either software or hardware, each having advantages and drawbacks. In software, the watermark scheme can simply be implemented in a PC environment. The watermark algorithm's operations can be performed as scripts written for a symbolic interpreter running on a workstation or machine code software running on an embedded processor. By programming the code and making use of available software tools, it can be easy for the designer to implement any watermark algorithm at any level of complexity. However, such an implementation is relatively slow and therefore not suitable for real time applications. In practical, video storage and distribution systems, video sequences are stored and transmitted in a compressed format. Thus, a watermark that is embedded and detected directly in the compressed video stream which can minimize computational demanding operations. Furthermore, frequency domain watermark methods are more robust than the spatial domain techniques(Xian Li,2008). Therefore, working on compressed rather than uncompressed video is important for practical watermark applications. There are few standards for video compression. All current popular standards for video compression, namely MPEG-x (ISO standard) and H.26x formats (ITU-T standard), are hybrid coding schemes and are DCT based compression methods. Such schemes are based on the principles of motion compensated prediction and block-based transform coding. Currently, researchers are given more focus on recently developed H.264 based video watermarking standard for low bit rate video application.

7.1 Compressed domain video watermarking

H.264/MPEG4-AVC is the latest video coding standard of ITU-T Video CodingExperts Group(VCEG) and the ISO/IEC Moving Picture Expert Group(MPEG). H.264/MPEG4-AVC has recently become the most widely accepted video coding standard since the deployment of MPEG2 at the drawn of digital television, and it may soon overtake MPEG2 in common use. It covers all common video application ranging from mobile services and video conferencing IPTV,HDTV and HD video storage. The H.264 standard has a number of advantages that distinguish it from existing standards, while at the same time, sharing common features with other existing standards like up to 50 % of bandwidth sharing, high quality video and error resilience.

The paper (Frank Hartung, Bernod Girod, 1998) presented spread spectrum based watermark embedding method for additive digital watermarks into video sequences in uncompressed and compressed video sequences. It adds pseudo-noise signal to the video with invisible and robust against manipulations. For practical applications, watermarking schemes operating on compressed video are desirable. The watermark is processes through discrete cosine transform (DCT) and embedded into the MPEG-2 bit-stream without increasing the bit-rate. The watermark can be retrieved from the decoded video and without knowledge of the original video.

The authors (Karima Ait Saadi et al.,2008) proposes a new block based DCT selection and a robust video watermarking algorithm to hide copyright information in the compressed domain of the emerging video coding standard H.264/AVC. The watermark is first quantized and securely inserted. To achieve invisibility and robustness, the high entropy DCT 4x4 blocks within the macro blocks are elected to minimize the distortion caused by the embedded watermark and then scrambled using Linear Congruential Generator (LCG) technique. This approach provides good robustness against some attacks such as re-compression by the H.264 codec, transcoding and scaling.

The authors (Jing Zhang and Anthony T. S. Ho ,2005) presents a byte replacement watermarking for direct stream marking of H.264/AVC streams. This paper describes a method for applying a watermark directly to an entropy coded H.264/AVC stream. This method can be applied when the stream, or at least the I-frames, is entropy coded with CAVLC. The embedding process involves replacing each identified segment with one of the alternative values from encode VLC table. The choice of alternative is informed by the payload to be embedded.

In this method (Dekun Zou, Jeffrey A. Bloom,2008), a grayscale watermark pre-processing is adapted for H.264/AVC. 2-D 8-bit watermarks such as detailed company trademarks or logos can be used as inconvertible watermark for copyright protection. A grayscale watermark pattern is first modified to accommodate the H.264/AVC computational constraints, and then embedded into video data in the compressed domain. With the proposed method, the video watermarking scheme can achieve high robustness and good visual quality without increasing the overall bit-rate.

They (Jing Zhang.2007) proposes robust MPEG-2 video watermarking techniques , focusing on commonly used typical geometric processing for bit-rate reduction, cropping, removal of any rows, arbitrary-ratio downscaling, and frame dropping. Both the embedding and the extraction of watermarks are done in the compressed domain, so the computational cost is

low. Moreover, the watermark extraction is blind. The presented technique is applicable not only to MPEG-2 video, but also to other DCT-based coding videos.

The author (Satyen Biswas,2005) propose a new adaptive compressed video watermarking scheme uses scene-based multiple gray-level watermark that provides more perceptual information. The concept of human vision system (HVS) is employed to find a suitable set of DCT coefficients for watermark embedding. The developed method embeds several binary images, decomposed from a single watermark image, into different scenes of a video sequence. The spatial spread spectrum watermark is embedded directly into the compressed bit streams by modifying discrete cosine transform (DCT) coefficients. The proposed watermarking scheme is substantially more effective and robust against spatial attacks such as scaling, rotation, frame averaging, and filtering, besides temporal attacks like frame dropping and temporal shifting.

7.1.1 Watermarking embedding hardware implementation

a. Integer DCT Transform based watermarking:

The discrete cosine transform (DCT) is a very promising technique used for video/image coding, and widely adopted by most image and video compression standards including latest H.264 standard. Since increasing applications apply these standards to portable systems like hand-held videophone and multimedia terminals, it becomes imperative to develop a high speed and low complexity DCT chip as one key component for such applications. To support low power applications, it is necessary to minimize the computational complexity as much as possible. For the high speed of operation and low delays pipelining structure is used, which also reduces the resource utilization. H.264 supports Integer based DCT for low complexity and high speed. The 2-D integer DCT is obtained on columns and row processor of 1-D DCT.The detailed architecture is shown below in Fig. 20. First input pixels are read from Memory and then 1-D DCT for column processing is done which stores in transpose memory. In transpose memory, transposing of values are done. The values of column DCT is written on horizontal manner while reading of values are read on vertical basis and then applied to 1-D DCT for row processor.

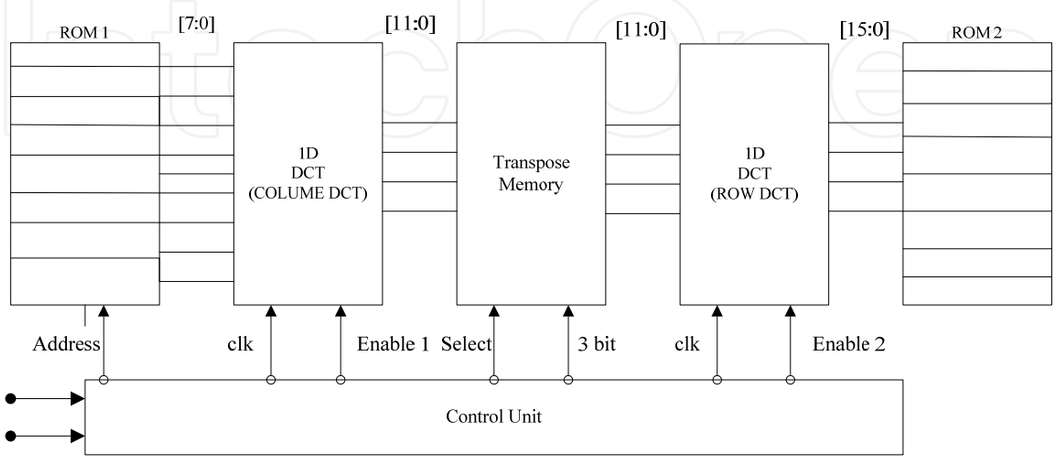


Fig. 20. VLSI Architecture for 2-D DCT.

b. Watermarking Embedding Hardware Implementation

The algorithm presented (Yulin Wang, Alan Pearmain, 2004) is blind watermarking based on scene detection. The algorithm is adapted on hardware where Integer DCT is utilized. The steps for hardware implementation shown in Fig. 21. This algorithm is implemented with simple multiplier, shifter and adder/sub tractor.

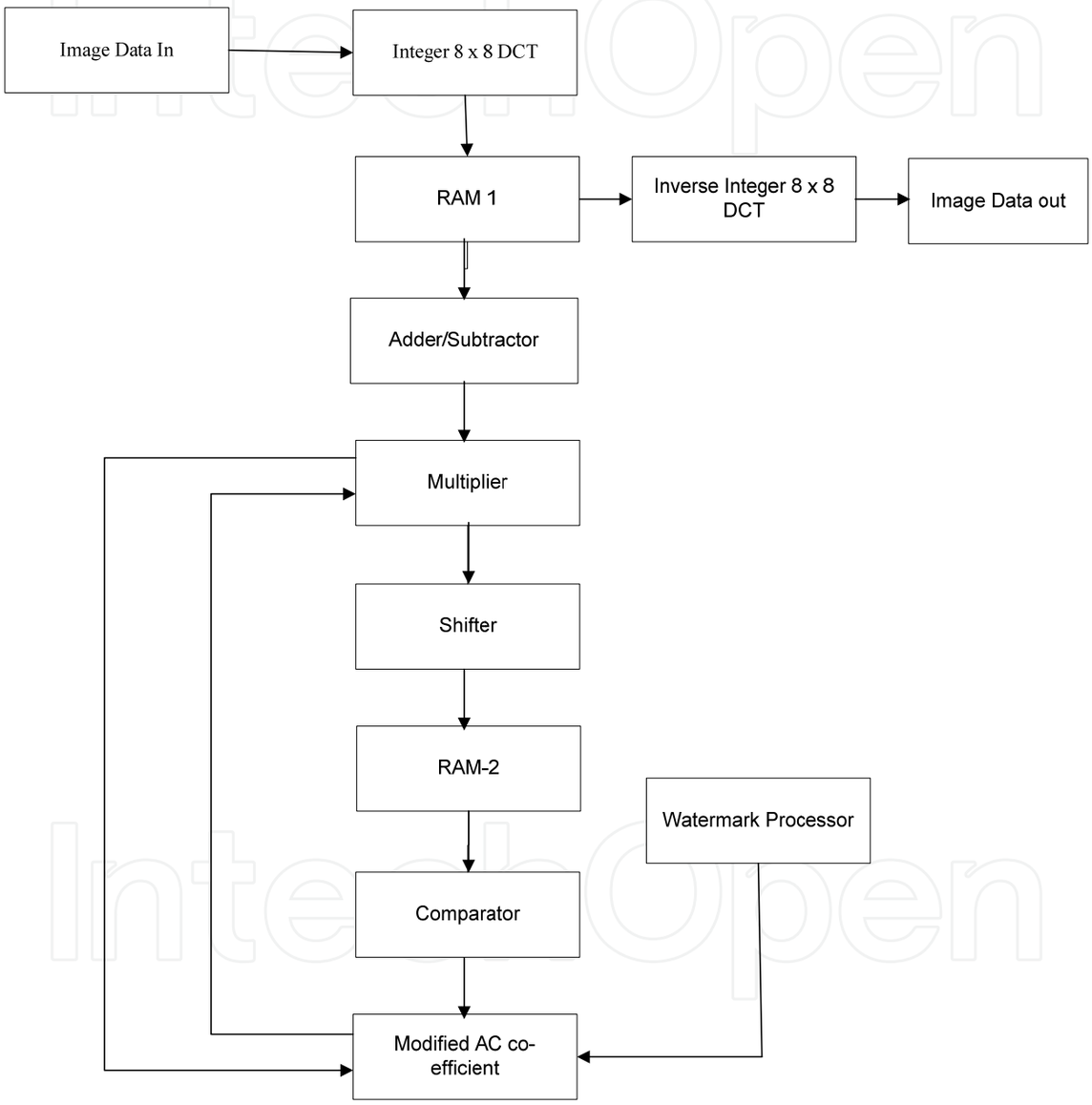


Fig. 21. VLSI Architecture for Integer DCT based watermarking

The input values coming from video capturing devices such as digital camera coming and stored in memory and our DCT column processor run on that stores transformed values in transpose memory and transposing values are given again to row processor. The schematic of video watermarking is as shown in Fig. 22.

Fig. 22. Schematic Design of Integer based DCT watermarking

The device utilization of above algorithm is as shown in following Table 5.

Resources	Number of Utilization	Percentage of utilization
Number of Slices	70 out of 4656	1 %
Number of Slices Flip Flops	105 out of 9312	1%
Number of 4 input LUTs	129 out of 9312	1%
Number of IOBS	40 out of 158	24%
Number of GCLKS	1 out of 24	4%

Table 5. Synthesis Report of Video watermarking algorithm

8. Conclusion

The proposed algorithm is applicable for image and video application. It has combined approaches of spatial and frequency domain. From Table 1-3, it has been conclude that proposed scheme is suitable for real-time application due to its simplicity. It has overcome the problem of block artifacts of DCT and advantage of both domain properties. It has also lesser computational complexity compare to other algorithms because we embed watermark in Legal 5/3 Integer wavelet transform. From Table 4 of ASIC results taken from design vision from Synopsis also shown that proposed scheme has comparable results for speed and power compare to other existing schemes. From Table 5, it has been verified that propose video watermarking algorithm provides hardware efficient algorithm.

9. Acknowledgment

I am thankful to Prof. Anand Darji who provides me guidance to complete this chapter. would also like to thanks all my friends who directly and indirectly helping me every bit. I

am obliged to the in hand support that has been given to me by the my collegaues and especially to the "SMDP Project Lab", which has provided me with the platform like ISE (Xilinx Tool), Modelsim (Mentor Graphics), MATLAB, Design Vision (Synopsys Tool) which could navigate me through the sea of experiments and help me too get the desired level of work satisfaction.. Also quite thankful to SMDP Lab for providing me 180 nm CMOS Standard Cell Library for post synthesis of my design.

10. References

A.J. Menezes, P.V. Oorcscot and S.A. Vanstone (1996), *Handbook of Applied cryptography*, CRC press, Boca Raton.

A. Lumini and D. Maio (2000), A Wavelet-Based Image Watermarking Scheme, *The International Conference on Information Technology: Coding and Computing*, Las Vages, NV, pp. 122-127.

Amit Joshi, Vivekanand Mishra (2011), Blind video watermarking of wavelet domain for copy right protection ,*International Journal of Computing*, Vol 1, Issue 3,pp 291-295.

Amit Joshi, Prof.A.D.Darji (2009), Efficient Dual Domain Watermarking for secure images, *An International Conference on dvances in Recent Technologies in Communication and Computing, 2009. ARTCom '09, pp. 909-914.*

Arun Kejariwal (2003), Watermarking, *IEEE Potential*, October/November, 2003.pp 37-40.

B. Sehneier (1996), *Applied Cryptography: Protocols, Algorithms and Source Code in C*, second edition, John Wiley & Sons, New York.

Dekun Zou, Jeffrey A. Bloom(2008): H.264/AVC stream replacement technique for video watermarking. *ICASSP* 2008: 1749-1752

Frank Hartung, Bernod Girod(1998),"Watermarking of uncompressed and compressed domain Video",*Elseiver,*Vol 66,no. 3,May 1998,pp 283-301

Garimella, A., Satyanarayan, M.V.V., Kumar, R.S., Murugesh, P.S., Niranjan (2003) ,VLSI Implementation of Online Digital Watermarking Techniques with Difference Encoding for the 8-bit Gray Scale Images *In: Proc. of the Intl. Conf.on VLSI Design*.,pp 283–288

Hyun Lim, Soon-Young Park and Seong jun Kang (2003), FPGA Implementation of Image Watermarking Algorithm for a Digital camera, *IEEE Pacific Rim Conference on Communications, Computers and signal Processing, 2003. PACRIM. 2003*, pp.1000-1003.

Hsien-Wen Tseng , Chin-Chen Chang (2008), An extended difference expansion algorithm for reversible watermarking ,*Elsiver, Image and vision computing*, pp 1148-1308

I .J. Cox, J. Kilian, T. Leighton and T. Shanon (1995), Secure spread spectrum for Multimedia, *NEC research institute*, prinecton, NJ, technical report pp. 95-10.

I.J.Cox,J. Kilian, F.T. Leighton, and T. Shamoon (1997), Secure Spread Spectrum Watermarking for Multimedia, *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687

Jianyog Huang and Changsheng Yang (2004),"Image Digital Watermarking algorithm Using Multiresolution wavelet Transform", *IEEE International conference on systems, man and Cybernetics*, pp. 2977-2982.

Jing Zhang,Anthony T.S.Ho, Gang Qiu.Robust(2007), "Video Watermarking of H.264/AVC[J]". *IEEE Transactions on circuits and systems-Ti:express briefs*,vol.54,no.2,February 2007.

Jing Zhang and Anthony T. S. Ho(2005), "Efficient robust watermarking of compressed 2-D grayscale patterns for H.264/AVC," *Proc. of IEEE Workshop on Multimedia Signal Processing*, pp. 1-4, 2005.

Karima Ait Saadi, Ahmed Bouridane, H. Meraoubi(2008):"Secure and Robust Copyright Protection for H.264/AVC based on Selected Blocks DCT". *SIGMAP 2008,*pp 351-355

Lei Tian and Heng-Ming Tai (2006), Secure Image Captured by Digital Camera, *International Conference on Consumer Electronics, 2006. ICCE '06*, pp.341-342

MarkAny (2010), Watermarking Technology, *Whitepaper*,2010.

Sammy H. M. Kwok, Edmund Y. Lam (2002), Watermarking Implementation in digital photography", *Proceeding of International Symposium on Intelligent Signal Processing and Communication System*. Hall

Saraju P. Mohanty, N. Raganathan (2004), VLSI Implementation of Visible Watermarking for a secure Digital Camera Design, *Proceeding of 17th International Conference on VLSI design*

Saraju P. Mohanty, N. Raganathan and R.K. Namballa (2005) ,A VLSI architecture for visible watermarking in a secure still digital camera (S2DC) design, *IEEE Transaction on VLSI*, vol 13., pp 1002-1012.

Saraju P. Mohanty, N. Raganathan and K. Balakrishna (2006), A Dual Voltage- Frequency VLSI chip for Image Watermarking in DCT Domain , IEEE *Transaction on circuits and systems II(TCAS-II),* vol. 53,pp 394-398.

Satyen Biswas, Sunil R. Das, Emil M. Petriu, (2005),"An Adaptive Compressed MPEG-2 Video Watermarking Scheme", IEEE *transaction on instrumentation and measurement*, vol. 54, no. 5, October-2005

Tsai, T.H., Lu, C.Y (2001),A Systems Level Design for Embedded Watermark Technique using DSC Systems, *presented at the IEEE Int. Workshop Intelligent Signal Processing Communication System*, Nashville, TN, pp 20-23

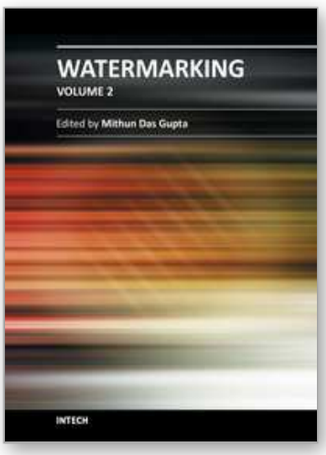
Tung-Shou Chen, Jeanne Chen, Jian –Guo Chen(2004) , A Simple and efficient watermark technique based on JPEG2000 Codec*, Springer, Multi media systems*, pp 16-26.

Victor V. Hernandez Guzman, Mariko Nankano (2004), Analysis of a Wavelet based watermarking Algorithm, Proceeding *of the 14th International Conference on Electronics, Communication and Computers*, pp 283-287.

Xian Li, Yonatan shoshan,Alexander Fish,Graham Jullian,Orly Yadid-Pecht(2010) ,Hardware Implementation of video watermarking , *Information science and computing*, pp-9-16

Yong-Gang Fu and Hui-Rong Wang (2008), A Novel Discrete Wavelet Transform Based Digital Watermarking Scheme, *2nd International Conference on Anticounterfeiting, Security and Identification* ,pp 55-58.

Yulin Wang, Alan Pearmain(2004),"Blind image data hiding based on self reference", *Pattern Recongnition, Elsevier*, 2004, pp. 1681-1689.



Watermarking - Volume 2

Edited by Dr. Mithun Das Gupta

ISBN 978-953-51-0619-7
Hard cover, 276 pages
Publisher InTech
Published online 16, May, 2012
Published in print edition May, 2012

This collection of books brings some of the latest developments in the field of watermarking. Researchers from varied background and expertise propose a remarkable collection of chapters to render this work an important piece of scientific research. The chapters deal with a gamut of fields where watermarking can be used to encode copyright information. The work also presents a wide array of algorithms ranging from intelligent bit replacement to more traditional methods like ICA. The current work is split into two books. Book one is more traditional in its approach dealing mostly with image watermarking applications. Book two deals with audio watermarking and describes an array of chapters on performance analysis of algorithms.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Amit Joshi, Vivekanand Mishra and R. M. Patrikar (2012). Real Time Implementation of Digital Watermarking Algorithm for Image and Video Application, Watermarking - Volume 2, Dr. Mithun Das Gupta (Ed.), ISBN: 978-953-51-0619-7, InTech, Available from: http://www.intechopen.com/books/watermarking-volume-2/real-time-implementation-of-digital-watermarking-algorithm-for-image-and-video-application

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen