



International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Implementation and Performance Analysis of DWT Based Video Watermarking Algorithms on FPGA

Alka N. Potkar*, Prof. Saniya M. Ansari

E&TC department, Savitribai Phule Pune University Maharashtra, India

Abstract—Digital video watermarking was introduced at the end of the last century to provide means of enforcing video copyright protection. Video watermarking involves embedding secret information (data) in the video. This paper proposes Discrete Wavelet Transform (DWT) to authenticate the multimedia image and LSB algorithm to insert the bits of the hidden message or image into the least significant bits of the pixels. This proposed method is developed on Xilinx Spartan3 Field Programmable Gate Array (FPGA) device using embedded development kit (EDK) tools from Xilinx. To check effectiveness of this technique for Imperceptibility and robustness PSNR and NCC parameters are calculated by adding different attacks. To improve performance implemented the propose system with addition of DWT-DCT algorithm using MATLAB software.

Keywords— Digital watermarking, FPGA, LSB algorithm, DWT, DCT, EDK, PSNR, NCC.

I. INTRODUCTION

Watermarking is a method of embedding additional information into the digital contents that is undetectable to listeners. We are investigating its embedding, detecting, and coding techniques. Digital video watermarking involves embedding secret symbols known as watermarks within video data which can be used later for copyright detection purposes. There are three factors (robustness, security, perceptual fidelity) which are necessary for video watermarking system. The watermark can be visible or invisible. In visible watermarking, the information is visible in the video. While in invisible watermarking, information is not visible. It can be detected only by the owner. This paper proposed LSB Information Hiding algorithm which can lift wavelet transform image. The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels. Achieving the purpose of information hiding with the secret bits of information to replace the random noise, using the lowest plane embedding secret information to avoid noise and attacks, making use of redundancy to enhance the sound embedded in the way nature to be addressed. In this paper we propose an invisible video watermarking technique based on LSB & 2-Level DWT [13]. The results showed that the proposed algorithm has a very good hidden invisibility, good security and robustness for a lot of hidden attacks. However, the limitation of capacity has led us to think about an improved approach which can be achieved through hardware implementation systems with the help of a programmable gate array (FPGA) board.

II. PROPOSED METHOD

The use of discrete wavelet transform (DWT) is increased for image coding day by day. That is because of the DWT property which supports features like progressive image transmission (by quality, by resolution), use of compressed image manipulation [6], region of interest coding, etc.

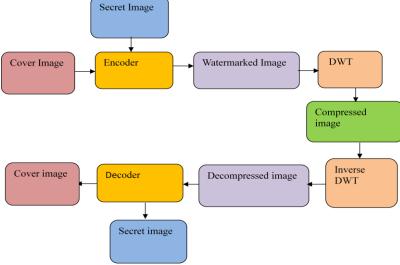


Figure 1Block diagram of proposed method

Potkar et al., International Journal of Advanced Research in Computer Science and Software Engineering 5(2), February - 2015, pp. 683-689

We can use Least Significant Bit (LSB) algorithm [13]. This is technique is the one in which least significant bit of the image is replaced with data bit [13]. As this method is used in image-analysis so as to make it more secure and encrypt the raw data before embedding it in the image. Fig.1 shows the proposed method block diagram [2] which uses LSB algorithm for encoding data or pixel value of image. DWT algorithm is used for compressing the watermarked image.

III. PROPERTIES OF DIGITAL WATERMARKING

An effective digital watermarking algorithm must have number of properties. In this section we describe these properties [23].

A. Imperceptibility

It is normally required to have watermarked image which should perceptually be as close to original image as possible [14]. Otherwise, the distortions caused by watermarking embed-ding process would degrade its aesthetic value. This property is called imperceptibility or transparency of the watermarking system [23]. A watermarking system is of very little use, if it destroys the cover image to the extent of being useless. Theoretically, the watermark should be invisible to human eye, even on the highest quality equipment. To evaluate the imperceptibility, generally, Peak Signal to Noise Ratio (PSNR) is used.

B. Robustness

Robustness refers to the capability of watermark to survive against both legitimate and illegitimate attacks. Legitimate or unintentional attacks are those which do not explicitly aim at removing the watermark or marking it unusable [23]. Illegitimate or intentional attacks precisely aim at damaging the embedded watermark in the cover work. Except fragile watermarking systems, almost all watermarking systems need to be resistant against any legitimate or illegitimate processing of watermarked image.

C. Capacity

Capacity of the watermarking system is defined as the maximum amount of information that can be embedded in the cover work [14]. This property of watermarking technique determines whether a technique can profitably be used in a given context or not [29]. There is always compromise between capacity and other two important properties of watermarking system, imperceptibility and robustness. A higher capacity is always obtained by sacrificing either robustness or imperceptibility (or both), it is thereby necessary that a good tradeoff is found depending on the application on hand [23].

D. Security

A watermark system is said to be secure, if the hacker cannot remove the watermark without having full knowledge of embedding algorithm, detector and composition of watermark. A secure watermarking system can resist many hostile attacks which thwart the watermark's purpose [23]. These attacks can be unauthorized operations that can remove, embed, modify or detect the watermark.

IV. HARDWARE IMPLEMENTATION

1. MicroBlaze Processor Design

FIELD-PROGRAMMABLE GATE ARRAYS (FPGA's) [2] are flexible and reusable high-density circuits that can be easily re-configured by the designer, enabling the VLSI design / validation /simulation cycle to be performed more quickly and less expensive. Increasing device densities have prompted FPGA manufacturers, such as Xilinx and Altera, to incorporate larger embedded components, including multipliers, DSP blocks and even embedded processors. One of the recent architectural enhancements in the Xilinx Spartan, Virtex family architectures is the introduction of the MicroBlaze (Soft IP) and PowerPC405 hard-core embedded processor. The MicroBlaze processor is a 32-bit Harvard Reduced Instruction Set Computer (RISC) architecture optimized for implementation in Xilinx FPGAs with separate 32-bit instruction and data buses running at full speed to execute programs and access data from both on-chip and external memory at the same time.

2. Xilinx Platform Studio

The Xilinx Platform Studio (XPS) [2] is the development environment or GUI used for designing the hardware portion of your embedded processor system. Embedded Development Kit Xilinx Embedded Development Kit (EDK) is an integrated software tool suite for developing embedded systems with Xilinx MicroBlaze and PowerPC CPUs. EDK includes a variety of tools and applications to assist the designer to develop an embedded system right from the hardware creation to final implementation of the system on an FPGA. System design consists of the creation of the hardware and software components of the embedded processor system and the creation of a verification component is optional. A typical embedded system design project involves [13]: hardware platform creation, hardware platform verification (simulation), software platform creation, software application creation, and software verification as shown in fig 2. Base System Builder is the wizard that is used to automatically generate a hardware platform according to the user specifications that is defined by the MHS (Microprocessor Hardware Specification) file.

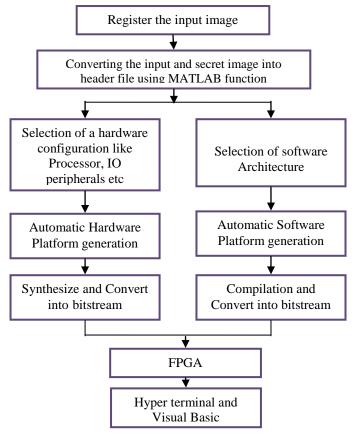


Fig2 Flow chart of FPGA implementation

The MHS file defines the system architecture, peripherals and embedded processors. The Platform Generation tool creates the hardware platform using the MHS file as input.

V. SOFTWARE DEVELOPMENT PROCESS

In this proposed method as shown in fig 4 and fig 5 a digital video watermarking technique based on identical frame extraction in 3-Level Discrete Wavelet Transform (DWT). In the proposed method, first the host video is divided into video shots [32]. Then from each video shot one video frame called identical frame is selected for watermark embedding. Each identical frame is decomposed into 3-level DWT [32]. Our proposed digital video watermarking technique based on 3-level DWT and DCT.

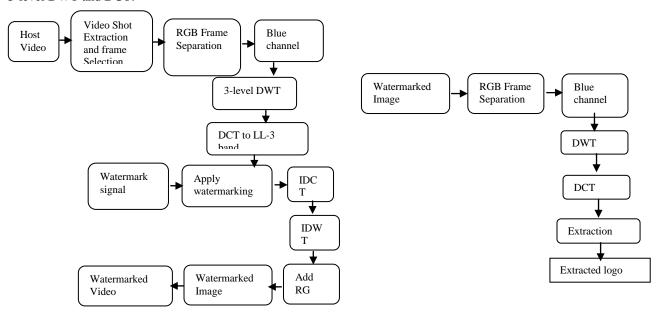


Fig 3. Watermark Embedding Process

Fig 4. Extraction Process

At first, the formation of 3-Level DWT is presented. Then the proposed watermark embedding process, including identical frame extraction technique is used.

VI. **EVALUATION PARAMETERS**

The PSNR and NCC are used as evaluation parameter.

Peak Signal to Noise Ratio (PSNR) [14], is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation.

Let A is the original image & B is the watermarked image of size m x n then MSE (Mean Square Error) & PSNR will be

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (A - B)^{2}$$

PSNR = 10.log10MAX²A/MSE

Normalized Cross Correlation (NCC) is calculated to evaluate the robustness of algorithm. NCC is defined as follows where OW is original watermark and EW is Extracted watermark [14].

$$NCC = \sum_{i=0}^{M-1} \sum_{i=0}^{N-1} (OW * EW) / \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (OW * OW)$$

VII. SIMULATION RESULTS AND ANALYSIS

A. SIMULATION RESULT

To check the efficiency of proposed algorithm different size of images are considered for numerical simulation. MSE, PSNR and NCC value is checked on Hyper Terminal as shown in fig 6.The input, Secret, DWT, IDWT and received secret images are shown in fig 7,8,9,10,11 respectively in Visual Basic 6.0.



Fig 5.output on Hyper Terminal

Fig 6. Input image

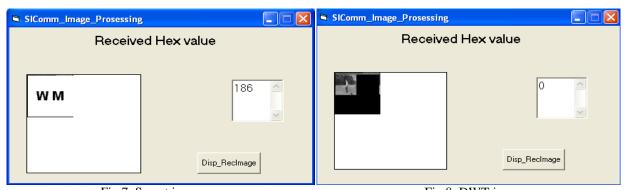


Fig 7. Secret image

Fig 8. DWT image

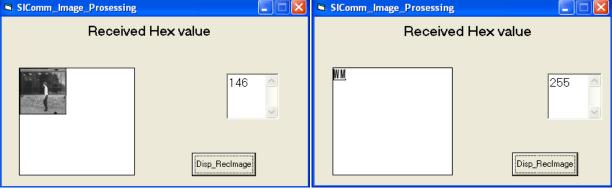


Fig 9. IDWT image

Fig 10. Received secret image

B. Synthesis Report:

This report contains the results from the synthesis run, including area and timing estimation. This report contains a detail study of the FPGA utilization as calculated during the synthesis of the FPGA. Timing report is available after the compile server completes the mapping step of the compilation process. This report contain utilization of the FPGA clocks, as estimated in the process of mapping the FPGA. The following table 1 shows the design summary for entire structure.

TABLE I
HARDWARE RECOURSE UTILIZATION
WATERMARKING CHIPS

Logic	Available	Used	Utilization	
Utilization			(%)	
Number of	1920	1880	97%	
Slices				
Number of	3840	2118	55%	
Slice Flip				
Flops				
Number of 4	3840	2971	77%	
input LUTs				
Number of	97	62	63%	
bonded IOBs				
Number of	12	4	33%	
BRAMs				
Number of	12	3	25%	
MULT18X18s				
Number of	8	4	50%	
GCLKs				
Total memory usage is 186128 kilobytes				

TABLE III COMPARISONS WITH OTHER

Researc	Desig	Type	Medi	Domai	Chip
h	n	of WM	a	n	Feature
Works	Type				s
Mohant	FPGA	Visible	Image	Spatial	3.3V,
y et					292MHz
al.[50]					
Sonjoy	FPGA	Semi	Video	DCT	40MHz
Deb		fragile			takes 7
Roy et					ms
al.[16]					
Petitjea	FPGA	Invisibl	Image	Fractal	50MHz
n et	Board	e-			takes 6
al.[52]		Robust			μ s
Mathai	Custo	Invisibl	Video	Wavel	1.8V
et al.	m IC	e		et	
[51]					
This	FPGA	Invisibl	video	Wavel	1.2V, 50
paper		e		et	MHz
					takes
					15ns

C. Performance Analysis

The performance of the overall FPGA implementation was evaluated in terms of memory usage and processing speed as shown in table II.

Table II Comparisons with other watermarking chips

The value of PSNR in proposed method is 48 which give quite enough robustness. To improve efficiency of system implemented software simulation of DWT-DCT combined algorithm using MATLAB

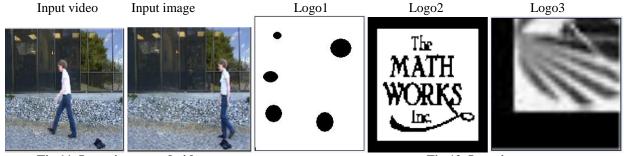


Fig.11. Input image and video

Fig 12. Logo images

Table III
Elapsed time, MSE, PSNR and NCC values for Different attacks.

RESULT	Logo1	Logo2	Logo3
Elapsed time(sec)	3.5364	3.6586	3.8733
MSE	0.005855	0.00310 8	0.00158 1
PSNR	70.4552	73.2055	76.139
NCC	1	1	1

	NCC	NCC	NCC
Brightness Adjustment	4.13542	5.34202	7.24233
Salt pepper	-225.329	- 312.367	- 452.089
Gaussian	-223.357	-310.54	- 449.666
Poisson	-225.329	-310.54	- 450.911
Median filter	0.9226	0.89185	0.84120

VIII. CONCLUSIONS

We have developed a new hardware which is suitable for VLSI implementation. First video is converted into number of frames. These frames are saved as images and from that one image is selected as cover image. Convert that cover image and secret image into header file. Second take those header file in XPS as input and apply LSB and DWT algorithms for watermarking. LSB is used to hide secret data in the least significant bit of the 8 bit data. DWT is used to compress the watermarked image.

Third calculated the evaluation parameters like MSE, PSNR and NCC.As per the result of the proposed video watermarking algorithm implemented on Spartan-3 FPGA kit PSNR is 48 and NCC is 1. Fourth Power requires for our system is very less (1.2-3.3V) and total time require for processing is in nanoseconds i.e.12ns which is compared with other authors as shown in table III. Hence require low cost and less time.

To improve the robustness and imperceptibility of proposed system software simulation of DWT-DCT combined algorithm is implemented in MATLAB. In this software simulation process PSNR maximum value obtained is 76.139 which produce the system to be more robust. On this algorithm we have apply different attacks to check the performance of the system. For Median filter the value of NCC is nearly equal to 1. Hence median filter give better result compare to other attacks. Hence we can prove that our system is robust again various attacks.

In future we will try to implement the proposed system on vertex kit for real time video. Apply the watermarking algorithm to other modern video compression standards, such as MPEG-4/H.264 So that it can be utilizes in various commercial applications.

ACKNOWLEDGMENT

My sincere thanks to my honorable guide Prof. Saniya M.Ansari and others those who have contributed towards the preparation of paper.

REFERENCES

- [1] Muthukumar.J, G.A.Sathish kumar, "Video Authentication using Digital watermarking" 2014 International conference on computation of power, energy, information and communication (ICCPEIC), pp. 899-903, 2014 IEEE
- [2] K.Tamilvanan, R.B.Selvakumar "FPGA IMPLEMENTATION OF DIGITAL WATERMARKING SYSTEM", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, ISSN 2320–088X, pp. 1321-1327, April- 2014
- [3] Waikhom Mona Chanu1, Bitan Chakraborty2 and Diwarkar R Marur, "Implementation of Blind Image Watermark Encoder in FPGA" International Journal of Information and Computation Technology, ISSN 0974-2239 Volume 4, Number 5, pp. 545-552, 2014
- [4] G.Sujitha Rajeswari, S.Vani, S.Visithra, R.Radeep Krishna, "Implementation of FPGA based Image Identification using modified Watermarking Algorithm" International Journal of Digital Communication and Networks (IJDCN) Volume 1, Issue 3, pp.15-18, September 2014
- [5] Rohollah Mazrae Khoshki, Sami Oweis, Shumei Wang, George Pappas, Subramaniam Ganesan, "FPGA Hardware Based Implementation of an Image Watermarking System" International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 5, ISSN (Online): 2278-1021, ISSN (Print): 2319-5940, pp.6400-6405, May 2014
- [6] S.Sivasankari, "FPGA Implementation of Invisible Video Watermarking using DWT Technique" International Journal of Innovations in Scientific and Engineering Research (IJISER), Vol. 1 Issue 1, ISSN: 2347-971X (online), Jan 2014
- [7] Meena Kumari , Dr. Pankaj Kumar Verma," A Digital Video Watermarking Technique Based on Frame Extraction in 5-Level DWT", INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, ISSN: 2277-9655, pp.163-168, June, 2014
- [8] Sunil Sharma, Mahendra Kumar Rai and Tanvi Sharma, "An Enhance LSB Watermark Approach for Robustness and Security in uncompressed AVI Video", International Journal of Emerging Trends &

- Technology in Computer Science (IJETTCS), Volume 3, Issue 1, ISSN 2278-6856,pp.181-185, January February 2014
- [9] Prof. R.V.Babar, Mr. Akshay. A.Jadhav, "LSB & DWT BASED DIGITAL WATERMARKING SYSTEM FOR VIDEO AUTHENTICATION" International Journal of Technical Research and Applications e-ISSN: 2320-8163, Volume 2, Issue 3, PP. 80-83, (May-June 2014)
- [10] Nidhi Divecha and Dr. N. N. Jani, "Implementation and performance analysis of DCT-DWT-SVD based watermarking algorithms for color images" 2013 International Conference on Intelligent Systems and Signal Processing (ISSP), pp.204-208,IEEE-2013
- [11] Anumol T J, Binson V A and Soumya Rasheed, "FPGA Implementation of Low Power, High Speed, Area Efficient Invisible Image Watermarking Algorithm for Images "International journal of scientific & engineering research volume 4, issue 8, ISSN 2229-5518, August-2013
- [12] Sanjoy Deb Roy, Xin Li, Yonatan Shoshan, Alexander Fish, Member IEEE and Orly Yadid-Pecht, Fellow IEEE, "HARDWARE IMPLEMENTATION OF A DIGITAL WATERMARKING FOR VIDEO AUTHENTICATION", IEEE Transactions on circuits and systems for video technology, Vol no.23, no.2,pp.289-301, Feb-2013
- [13] Rakesh Kumar, Savita Chaudhary, "Video Watermarking Using Wavelet Transformation", International Journal of Computer Trends and Technology (IJCTT) volume4 Issue5, ISSN: 2231-2803,pp.1154-1157, May 2013
- [14] Prabhishek Singh, R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, pp.165-175, March 2013
- [15] Gopika V Mane, G. G. Chiddarwar "Review Paper on Video Watermarking Techniques" International Journal of Scientific and Research Publications, Volume 3, Issue 4, ISSN 2250-3153 pp.1-5, April 2013
- [16] Mr. Ashish S. Bhaisare, Prof. A. H. Karode and Prof. S. R. Suralkar "Significance Research Review on Real Time Digital Video Watermarking System for Video Authentication", Proc. of the Second Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering -- CEEE 2013, ISBN: 978-981-07-6260-5,pp.161-166, 2013
- [17] Prof. N. R. Bamane, Dr. Mrs. S. B. Patil "Comparison & Performance Analysis of different Digital Video Watermarking Techniques" International Journal of Scientific & Engineering Research Volume 4, Issue 1, ISSN 2229-5518 pp.1-6, January-2013
- [18] L.Agilandeeswari, K.Muralibabu "A Novel Block based Video in Video Watermarking Algorithm using Discrete Wavelet Transform and Singular Value Decomposition" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, ISSN: 2277 128X, pp. 878-886, April 2013
- [19] Keta Raval and Sameena Zafar, "Digital Watermarking with Copyright Authentication for Image Communication" 2013 International Conference on Intelligent Systems and Signal Processing (ISSP) ©2013 IEEE, pp. 111-116, 2013
- [20] Harleen Kaur, "Study on audio and video watermarking" International Journal of Communication Network Security ISSN: 2231 1882, Volume-2, Issue-1, pp. 34-38, 2013
- [21] Tamanna Tabassum, S.M. Mohidul Islam "A Digital Video Watermarking Technique Based on Identical Frame Extraction in 3-Level DWT", IEEE, 2012
- [22] Aditi Agarwal, Ruchika Bhadana and Satishkumar Chavan," A Robust Video Watermarking Scheme using DWT and DCT", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4), ISSN.0975-9646, pp.1711-1716, 2011
- [23] Rini T Paul, "Review of Robust Video Watermarking Techniques" IJCA Special Issue on "Computational Science New Dimensions & Perspectives" NCCSE,pp. 90-95, 2011
- [24] Xin Li, Yonatan Shoshan, Alexander Fish, Graham Jullien, Orly Yadid-Pecht, "HARDWARE IMPLEMENTATIONS OF VIDEO WATERMARKING" Sixth International Conference on Information Research and Applications i.Tech 2008, Varna, Bulgaria, pp. 9-16, June-July 2008
- [25] Vidyasagar M. Potdar, Song Han and Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques" 3rd International Conference on Industrial Informatics(INDIN 2005) ©2005 IEEE
- [26] Mohanty, S.P., Rangnathan, N., Namballa, R.K.: VLSI Implementation of Visible Watermarking for a Secure Digital Still Camera Design. In: Proceedings of the 17th International Conference on VLSI Design. (2004) 1063–1068
- [27] Mathai, N.J., Sheikholeslami, A., Kundur, D.: VLSI Implementation of a Real-Time Video Watermark Embedder and Detector. In: Proceedings of the IEEE International Symposisum on Circuits and Systems (Vol. 2). (2003) 772–775
- [28] Petitjean, G., Dugelay, J.L., Gabriele, S., Rey, C., Nicolai, J.: Towards Real-time Video Watermarking for Systems-On-Chip. In: Proceedings of the IEEE International Conference on Multimedia and Expo (Vol. 1). (2002) 597–600