DESIGNING SYS-GENERATOR MODEL FOR DIGITAL VIDEO WATERMARKING USING DFT ALGORITHM

*** Neha Rawat and ** Rachna Manchanda**

*M.Tech Scholar, Department of Electronics & Communication, Chandigarh Engineering College, Landran, Mohali, Punjab, India.
** Asistant Profesor, Department of Electronics & Communication, Chandigarh Engineering College, Landran, Mohali, Punjab, India.

ABSTRACT-This paper basically describes about the process of implanting a digital watermark on videos and also extracting the watermark. This is done by applying DFT algorithm. Since, DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions Thus, objective of this scheme is to develop low power, durable, resilient and reliable watermarking system for authentication of video. The system is initially simulated and tested for various attacks in MATLAB/ Simulink® R2011a(7.12.0) and then by using Xilinx System Generator, HDL code has been developed to prototype on FPGA by using Xilinx ISE 14.1. The watermarked video is same as that of original video having Peak-Signal-to-Noise Ratio (PSNR) of 40.95 dB.

***Key words*:** Digital video watermarking, Discrete Fourier Transform, Binary watermark, video authentication, Xilinx System-Generator.

1. INTRODUCTION

A digital watermark is defined as a sequence of bits inserted into a multimedia element such as a digital image, an audio or video file. The name comes from the barely visible text or graphics imprinted on stationery that identifies the manufacturer of the stationery. There are several proposed or actual watermarking applications [20]: broadcast monitoring, owner identification, proof of ownership, transaction tracking, content authentication, copy control, and device control. In particular, watermarking appears to be useful in plugging the analog hole in consumer electronics devices [5]. In applications such as owner identification, copy control, and device control, the most important properties of a watermarking system are robustness, invisibility, data capacity, and security.

Watermark embedding in a video can be of two types frame based or stream based including AVI, MPEG-2 and MPEG-4 video frames/streams. In frame based embedding the watermark bits are embedded in the video by means of complete frame or tiles of the frame. In stream based watermark embedding technique, only the lines of the video frame are embedded. MPEG-4 has increasingly become one of the established exchangeable video formats in the Internet today because it has high and flexible compression rate, low bit rate, and higher effectiveness while providing surpassing visual quality. This paper include following:

1. Design of Invisible robust video watermarking algorithms.

2. Design of MATLAB/Simulink® prototyping of the watermarking modules.

3. Generation of HDL Code with Xilinx System Generator.

4. Final implementation on Xilinx ISE 14.1.

2. DISCRETE FOURIER TRANSFORM

The DFT/FFT is a computationally productive algorithm, used for computing a Discrete Fourier Transform (DFT) of sample sizes which are a positive integer power of 2. The DFT $X(k), k = 0, \ldots, N-1$ of a sequence $x(n), n = 0, \ldots, N-1$ is defined as

$$X(k) = \sum_{n=0}^{N-1} x(n) e^{-\frac{jnk\,2\pi}{N}} \qquad k = 0, \ldots, N-1$$

Where N is the transform size and $j = \sqrt{-1}$. The inverse DFT (IDFT) is given by

$$x(n) = \frac{1}{N} \sum_{k=0}^{N-1} X(k) e^{\frac{jnk\,2\pi}{N}} \qquad n = 0, \ldots, N-1$$

Algorithm

The FFT core comprises of the Radix-4 and Radix-2 decompositions for computing the DFT. For Burst I/O architectures, the decimation-in-time (DIT) method is used, while the decimation-in-frequency (DIF) method is applied for the Pipelined, Streaming I/O architecture. When using Radix-4 decomposition, the *N*-point FFT consists of log4 *(N)* stages, with each stage containing *N/4* Radix-4 butterflies. Point sizes that are not a power of 4 need an extra Radix-2 stage for combining data. An *N*-point FFT which is using Radix-2 decomposition has log*2* (*N)* stages, with each stage containing *N/2* Radix-2 butterflies.

The inverse FFT (IFFT) is quantified by conjugating the phase factors of the corresponding forward FFT.

DFT DOMAIN WATERMARKING

DFT domain has been traversed by researches because it offers robustness against geometric attacks like rotation, scaling, cropping, translation etc.

A. Characteristics of DFT

1) DFT of a video is basically complex valued, which results in the phase and magnitude representation of a video.

2) DFT shows translation invariance. Circular shifts in the spatial domain don't affect the magnitude of the Fourier transform [11].

3) DFT is also resistant to cropping because effect of cropping leads to the blurring of spectrum. If the watermarks are embedded in the magnitude, which are normalized coordinates, there is no need of any synchronization [18].

4) The strongest components of the DFT are the central components which contain the low frequencies.

5) Scaling of video results in amplification of extracted signal and can be detected by correlation coefficient. Translation of image has no result on extracted signal.

6) Rotation of multimedia results in cyclic shifts of extracted signal and can be detected by exhaustive search [11]

7) Scaling in the spatial domain causes inverse scaling in the frequency domain. Rotation in the spatial domain causes the same rotation in the frequency domain [15].

B. Coefficient Selection Criteria

1) Modification to the low frequency coefficients can cause visible artifacts in the spatial domain [11, 15]. Hence, low frequency coefficients should be avoided

2) High frequency coefficients are not suitable because they are removed during JPEG compression [11, 15].

3) The best location to embed the watermark is the mid frequency [11, 15].

3. WATERMARKING PROCESS

A. Watermark Embedding Process

Step 1: Select the video and convert it into Binary File.

Step 2: “Binary File” Block should also be connected to a “Video Viewer” block so that the original video can be viewed simultaneously along with the watermarked video.

Step 3: Using the “Selector” block define the parameters to match the matrices.

Step 4: Divide each selected sub-bands with N/2$\times$ N/2 dimension into $n \times n$ non-overlapping parts $i.e.,(8 \times 8),(16 \times 16), etc$ ... and applying the 2D- FFT algorithm in the Sub-system of the “Block Processing” block.

Step 5: Repeat Steps 1-3 for the image used as a watermark and also apply FFT to convert the image in frequency transform domain.

Step 6: Connect the outputs of the “Block Processing” blocks from the previous step and from step (4) to a “netsum” block. The parameters for list of signs and sample time to ++ and -1, respectively.

Step 7: The output port of the above “netsum” block should feed into a new “Block Processing” block. The parameters for this block should again match those values listed in step (4). However, the

subsystem changes. Click on the “Open Subsystem” button and within it add a “2-D IFFT” block

Step 8: The output obtained is now the required watermarked video that is being sought. Connect this output to a “Video Viewer” block to view the results.

Issue 4 volume 4, July-August 2014
ISSN 2249-9954

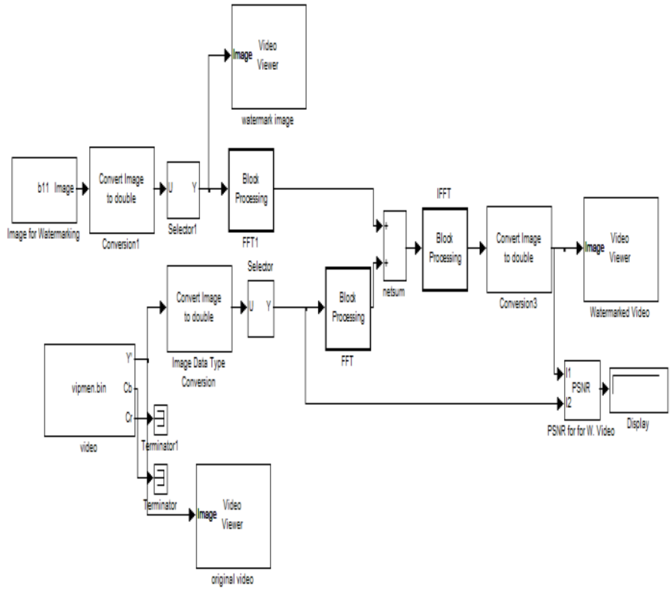

Figure1. SIMULINK model for embedding system

SIMULINK is defined as a block diagram environment and Model-Based Design, which basically supports system-level design, simulation, automatic code creation, and verification and validation of embedded systems. It also provides a graphical editor, customizable block libraries for modelling and simulating dynamic systems. It facilitates to integrate MATLAB algorithms into models and transmit simulation results to MATLAB for further assay. Resultant Simulink models are as shown in figure1.

B. Watermark extraction process

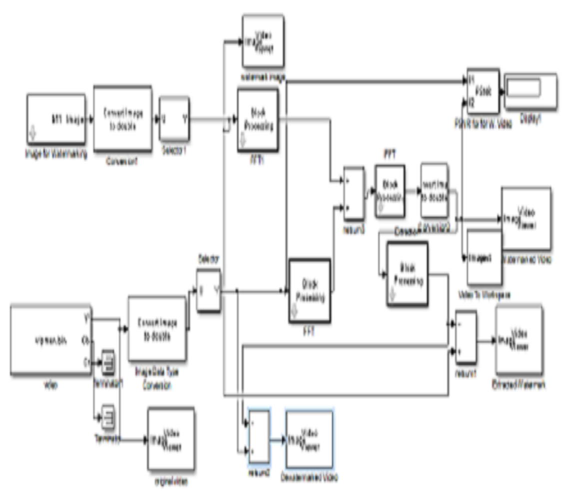

Figure.2: SIMULINK model for extracting system

4. RESULTS & DICUSSIONS

A. MATLAB Simulation Results

Fig. Shows a video sequence 'Vipmen.avi' of speed 25 frames/second and resolution 120*160. Using watermark image Fig. 'CGC logo of size 112*160 is imposed on the video. Thus, using simolink model of extracted watermark original watermark is extracted from watermarked video frame.

Figure 3: Original Video Vipmen.avi [120*160]

Figure 4: Watermark Image CGC logo.jpg [120*160]

Results of embedding and extraction process are shown in below figures. Fig. Shows watermarked video frame having PSNR 40.95 dB. Here, watermarked frame appears exactly same as original video frame.

Figure 5: Watermarked Video Frame [PSNR=40.95 dB]

Results of different Attacks

ATTACK	PSNR
Histogram Equalization 	PSNR=13.96

Gamma Correction by factor 2.2 	PSNR=33.58
Median Filtering 	PSNR=35.26
Gaussian Noise by value of 0.025 	PSNR=15.67

Result of Synthesis Process

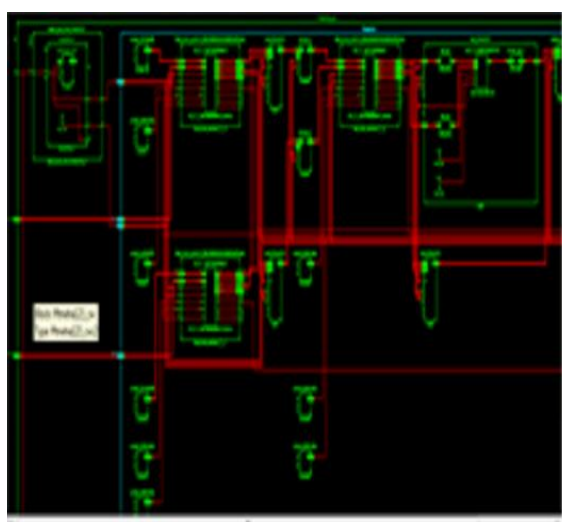

Figure 6: Hierarchical RTL schematic of watermarking process

5. CONCLUSIONS

By observing the synthesis process results it proves that watermarking algorithm can work successfully for grayscale video sequence. After application of different attacks quality of watermarked video frame is unchanged so system is imperceptible and robust against common video processing attacks. As simulink is used Verilog code is automatically generated. Device utilization summary shows that amount of resources required are relatively small. This watermarking based authentication provides a solution for fingerprinting and copy right protection and real time authentication. Also, the PSNR value is 40.95 dB which when compared is in the range of 30 dB to 50 dB of PSNR for video compression for 8 bit.

6. REFERENCES

[1] Emir Ganic, S.D.Dexter and A.M.Eskicioglu "Embedding Multiple Watermarks in the DFT Domain using Low and High Frequency Bands"IJCA International Journal of Computer Applications, Vol 3,Issue 3, No 2, June,2013.

[2] Sonjoy Deb Roy, Xin Li, Yonatan Shoshan, Alexander Fish, Member, and Orly Yadid-Pecht."Hardware Implemen-tation of a Digital Watermarking System for Video Authentication," in IEEE Transactions on Circuits & Systems for Video Tech , vol. 23, no. 2, Feb. 2013.

[3] (2012, Jul. 28) [Online].Available: http://en.wikipedia.org/wiki/ Digital watermarking.

[4] Kesavan Gopal, Dr. M. MadhaviLatha "Watermarking of Digital Video Stream for Source Authentication" IJCSI International Journal of Computer Science Issues,Vol. 7,Issue 4, No 1, July 2010.

[5] Salwa A.K Mostafa, A. S. Tolba, F. M. Abdelkader, Hisham M. Elhindy, „"Video Watermarking Scheme Based on Principal Component Analysis and Wavelet Transform"" IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[6] Mandeep Singh Saini, VenkataKranthi B, Gursharanjeet Singh Kalra., "Comparative Analysis of Digital Image Watermarking Techniques in Frequency Domain using MATLAB SIMULINK", International Journal of Engineering Research and Applications (IJERA)ISSN: 2248-9622 Vol. 2, Issue 4, May-Jun 2012.

[7] Mrs Neeta Deshpande, Dr. Archana rajurkar , Dr. R. manthalkar ,"Review of Robust Video Watermarking Algorithms" International Journal of Computer Science and Information Security, March 2010.

[8] Xu guo-jaun, Wang Rang-ding, "A Blind Video Watermarking Algorithm Resisting to Rotation Attack", International Conference on Computer and Communications Rotation Security, ICCCS, 2009, pp. 111-114.

[9] Y. Shoshan, A. Fish, G. A. Jullien, and O. Yadid-Pecht, "Hardware implementation of a DCT watermark for CMOS image sensors," in Proc. IEEE Int. Conf. Electron. Circuits Syst., Aug. 2008, pp. 368-371.

[10] Y.-J. Jeong, K.-S. Moon, and J.-N. Kim, "Implementation of real time video watermark embedder based on Haar wavelet transform using FPGA," in Proc. 2nd Int. Conf. Future Generation Commun. Networking Symp., 2008, pp. 63–66.

[11] Shoemaker C. , Hidden bits: "A survey of Techniques for Digital Watermarking", Independent Study, EER 290, Prof Rudko, Spring, 2002.

[12] Pereira, S. , Pun, T. , "Robust Template Matching for Affine Resistant Image Water--marks," in IEEE Transactions on Image Processing, vol. 9, no. 6, pp. 1123-1129, June 2000'.

[13] J. Dittmann, T. Fiebig, R. Steinmetz, S. Fischer, and I. Rimac, " Combined video and audio watermarking: Embedding content information in multimedia data," in Proc. SPIE Security Watermarking Multimedia Contents II, vol. 3971. Jan. 2000, pp. 455–464.

[14] Brigitte Jellinek, "Invisible Watermarking of Digital Images for Copyright Protection" submitted at University Salzburg, pp. 9 – 17, Jan 2000.

[15] Frank Hartung, Martin Kutter, "Multimedia Watermarking Techniques", Proceedings of The IEEE, Vol. 87, No. 7, pp. 1085 – 1103, July 1999.

[16] F. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding: A survey," Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, 1999.

[17] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, " Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[18] J. J. K. O. Ruanaidh, W. J. Dowling, F.M. Boland, "Watermarking Digital Images for Copyright Protection", in IEE ProcVis. Image Signal Process., Vol. 143, No. 4, pp 250 – 254. August 1996.

[19] Feig, E., "A fast scaled DCT algorithm", in Proc. SPIE Image Processing Algorithms anid Techniques, vol. 1224, pp. 2-13, Feb. 1990.

[20] "Digital Watermarking" available at http://en.wikipedia.org/wiki/Digital_watermarking.