ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 8, Issue 2, August 2018

FPGA- Based Video Watermarking using LSB

Suleiman Abdulbary R., Hamid Amena Ghanim

Abstract*— Digital video watermarking techniques can achieve copyright protection, data authentication, tamper detection, fingerprinting, and broadcast monitoring for multimedia data networking security. This paper will fundamentally concentrates on invisible and robust digital video watermark schemes based on identical frame extraction. N-significant bit technique is used to embeda logo (image) inMP4video as (a multimedia data) without diminishing its perceptual quality. In case of any argument, the watermarked logo can be discovered or removed from the video and used as a proof of regality*. Normalized Cross-Correlation *(NCC) and Peak Signal-To-Noise Ratio (PSNR), Mean Squared Error (MSE)* can be used to measure the *robustness of the watermarking scheme. In our experiments, performance evaluation is given for no attack case and for four type of attacks. The Results verified the robustness of the watermarking system. Matlab R2017b software is used to implement the technique and evaluate the results.HDL codes are generated using the Matlab and these codes are used to achieve hardware implementationforour watermarking scheme in Xilinx Spartan 6 FPGA (*Field Programmable Gate Arrays*).FPGA implementation results are obtained which show that the proposed scheme can be applied in real-time.

***Keywords*—Digital video watermarking, FPGA, LSB algorithm, NCC, PSNR.**

I. INTRODUCTION

With rapid the growth of the communication multimedia technology, persons can facilely use digital equipment to process, product and store media information such as text, image, audio and video. At the same time, digital network announcement is speedily developing, which makes the transmission and distribution of information achieved "digitized" and "networked".

Internet becomes the most excellent spreading technology for digital media because it is not only cheap, but also needs no warehouse to store, and can send in real time, therefore, digital media can be easily copied, processed, transmitted, and distributed via the use of the Internet [1].Watermark inserting method is used to safeguard digital video against reformation and allotment illegally. The root of watermarking as an information hiding technique can be traced in ancient Greece as Steganography [2].In recent years the watermarking science was developed organization. It is recognized by inserting data that is not sensitive for the human visual system. The data should be inserted in secure and efficient manner such that most attackers cannot remove it. A watermark can be inserted in such method that it stays watchable with the quality of the digital information remains almost at an appropriate level. In public, any watermarking scheme involves the following portions: Watermark, Carrier, Inserter, and detector. A field-programmable gate array (FPGA) is an integrated circuit designed to be configured by a user (i.e. designer) after manufacturing and therefore called field software.

The hardware description language (HDL) is used for configuration of FPGA, similarly as used for an application-specific integrated circuit (ASIC),RAM blocks, logic gates, and FPGAs have large resources of Look up tables (LUTs) to implement any complex digital computations. The most applications of image or video processing may use FPGA hardware [3].

II. GENERAL VIDEO WATERMARKING PROCESS

In watermarking process the watermark pixel is embedding in to original video for getting video watermarking that is still unobserved (for invisible watermarking system) while in the same time, it has a protection by which only authorized persons can detect it. Figure (1) shows the inserting watermarking scheme. On the other hand the extracting watermarking scheme is process to detect watermark pixels from the watermarked video as illustrated in Figure (2) [4].

A watermark can be a sequence number, text, image, or video.

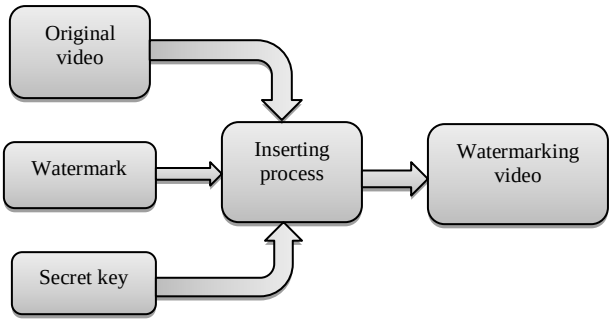


Fig 1 Watermarking inserting scheme

Watermarking inserting scheme are required for inputs the following original video, watermark and may using the key, that it is used to strength protection in watermarking process.

The extracting process requires watermarked video and/or key and/or original video. Inserting scheme produces

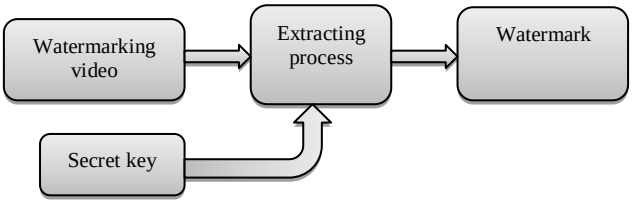


Fig 2 Watermarking extracting scheme

watermarked video as an output. [3].

The blind watermarking algorithm that is presented in this paper is based only on watermarked video without using the original video for extraction process. While non-blind

Manuscript received: 17 July 2018
Manuscript received in revised form: 16 August 2018
Manuscript accepted: 01 September 2018
Manuscript Available online: 10 September 2018

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 8, Issue 2, August 2018

watermarking need the original video and watermarked video [4].

III. WATER MARKING APPLICATIONS

The designated type of applications determines the requisites of the watermarking technique that have to be interrogated with accredits of the designated type. Digital watermarking is using in a massively of applications, as listing below [5].

A. Copy Protection

There has permanently been a problem in given the identity of the proprietor of an object, therefore the data owner need to insert the watermark in the data for the purpose of protecting the prominent data. So if there's an expropriation on the proprietorship of data, then watermark is used to extract the identity of the owner [6].

B. Broadcast Monitoring

From application is used to tracking illegal broadcast in location is called Broadcast Monitoring. It is authenticate in whether the data is actually aired or not. It also refers to the technique of cross-attesting whether the data that was intended to be aired has actually been aired or not. To solve broadcast monitoring problem watermarking system is used [7]. The major applications are advertisement broadcasting where the entity wants to monitor whether his advertisement was actually broadcasted at the desired time and for the desired duration.

C. Digital Fingerprinting

Each finger printing and serial number area like existing on any product. A dissimilar watermark can be inserted for every spread multimedia copy [8]. The idea of fingerprinting can used to define the true possessor of digital data, and then single identity is given for each shopper of digital data as fingerprint [9].

D. Tamper Detection

Tamper detection is used fragile watermarks. If the watermark is damaged or modified, digital content cannot be trusted because it indicates existence of tampering. Digital data can be discovered for manipulation by inserting fragile watermarks. If the fragile watermark is damaged, then, digital data may indicate the presence of tampering in order not to be trusted. Tamper detection is very necessary for some applications, including very sensitive data similar to medical images or satellite images. Digital images can also be used to determine the legal instrument where it is also beneficial to tamper the federal court if tamping the images or not [7].

E. Data Authentication

Content authentication can be realized during the use of semi-fragile or fragile watermark because it is able to discover any difference in digital content, then which has small strength to modification in an image. So, the images can be categorized with its content and can be used in search machines [7].

IV. PROPOSED METHOD

The watermarking algorithm processed in this work is based on LSB technique. For security purpose the watermark (logo) is embedded in first, second, and third LSB of the data.

Most grayscale watermarking embedding in the blue components and green components of original video because of less sensitivity of human eye to both colors and a few of grayscale watermark embedding in the red components. Figure 3 shows the structure of the process.

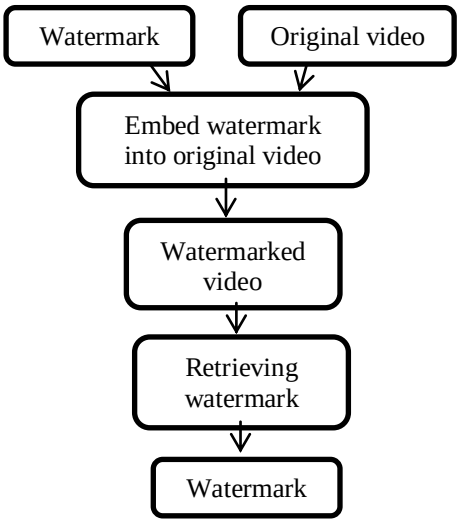


Fig 3 The watermarking structure

In this algorithm the watermark must be binary data represent a logo or seal of a company. The size of watermark is proportional to size of the frame of video (there are several other parameters limit this point). As another defending wall; the embedding process is depended on human virtual system.

A. Watermark inserting

The watermark inserting scheme is proposed as shown in Figure 4. The watermark image is a binary image in which the frame of the original video is 8 bit for each color of the frame. The watermark is inserted in different percentages in the frame of original video according to the sensitivity of the human eye. So that the largest quantity of watermark is embedded in blue because it is less sensitive to the human eye. The binary watermark Wm of size 64*64pixels is used to protect a frame of original color video (MP3) of size 240*360 pixels. The inserting method is demonstrated as follows:

1. The original video is changed to form frames and each frame is decomposed into R, G, and B components
2. The positions of inserting the watermark is determined by private key. Each I-frame is divided into n*n block and entropy is calculated.
3. Depending on entropy the watermark W is inserted in the Red, Blue, and Green component:

$$Fr' = AND(Fr, 252) + AND(W, 3) \ldots\ldots (1)$$

$$Fg' = AND(Fg, 248) + SHR(AND(W, 28), \ldots\ldots (2)$$

$$Fb' = AND(Fb, 248) + SHR(AND(W, 224), \ldots. (3)$$

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 8, Issue 2, August 2018

Where Fr', Fg', and Fb' are modified red frame, green

4. The block of pixels is restructured, then set in its original position of the frame and then stepes 3 and 4 is frequent until all watermark bits W'' are inserted.
5. The watermarked video is obtained.

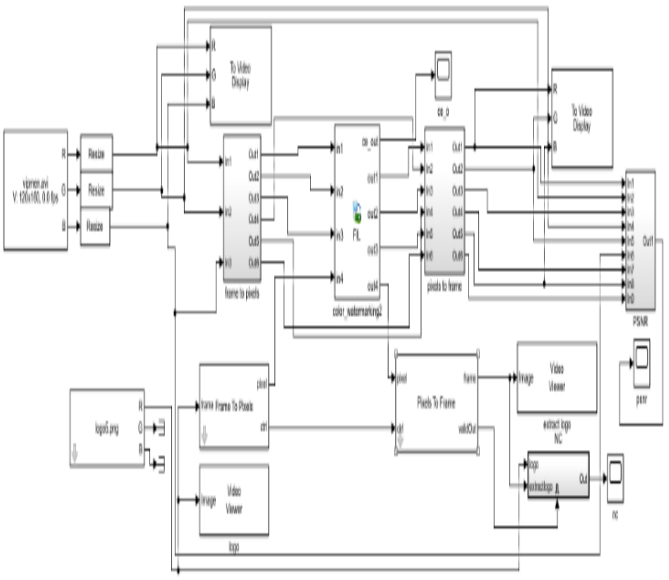


Fig 4 Block diagram of video watermarking implementation

B. Watermark Extraction

The watermark extraction steps are the same as the inserting steps but in the inverse direction. As follows

1- Watermarked video is partitioned into frames.

2- The following relations are applied on Red, Green, and Blue frames to extract the watermark :

w1 = AND (Fr', 3) . ……. (4)

w2= SHL (AND (Fg', 28),2). ……. (5)

w3=SHL (AND (Fb',224),5). ……. (6)

W'=w1+w2+w3 ……. (7)

Where: W' is extracted watermark

3- The extracted watermark is compared with the original watermark as follows:

4- $$NCC = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(Wm(i,j)\cdot Wmv(i,j))}{\sum_{i=1}^{N}\sum_{j=1}^{M}(Wm(i,j)\cdot Wm(i,j))} \quad \ldots(8)$$

This is Normalized Cross-Correlation (NCC)(normalized by the reference watermark energy) giving unity as the peak correlation [8]. This measure is used to assess performance scheme

V. SIMULINK BASED IMPLEMENTATION

FPGA-in-the-Loop (FIL) accelerates a video processing simulation using Simulink and FPGA [10]. The FIL process consists of three steps. The first step, the design is simulated using Matlab Simulink.. Then, co-simulation based ModelSim is generated, Third step is the verification of the co-simulation model in which the hardware is implemented and simulated on the FPGA. The co-simulation model includes a co-simulation block which is EDA (Electric Design Automation) Simulink gateway to ModelSim that provides on the fly hardware signals. The hardware signals timing can be verified and investigated for timing and functional correctness.

HDL Verifier works with Simulink, HDL Coder, and the FPGA development environment to automatically generate HDL Codes for implementation on FPGA. To perform FIL simulation the following steps are followed:

1. Dragging the FIL block into Simulink model connecting all inputs and outputs.
2. Setting the output sample times, data types, and frame size.
3. Attaching the FPGA development board to host computer (FPGA programming cable and Gigabit Ethernet cable).
4. Setting the host IP address.
5. Downloading FPGA programming file.

FIL simulation allows running a Simulink with FPGA board strictly synchronized with the software. This process allows getting a real time operation for the design while speeding up the simulation with the speed of the FPGA as shown in Figure 5.

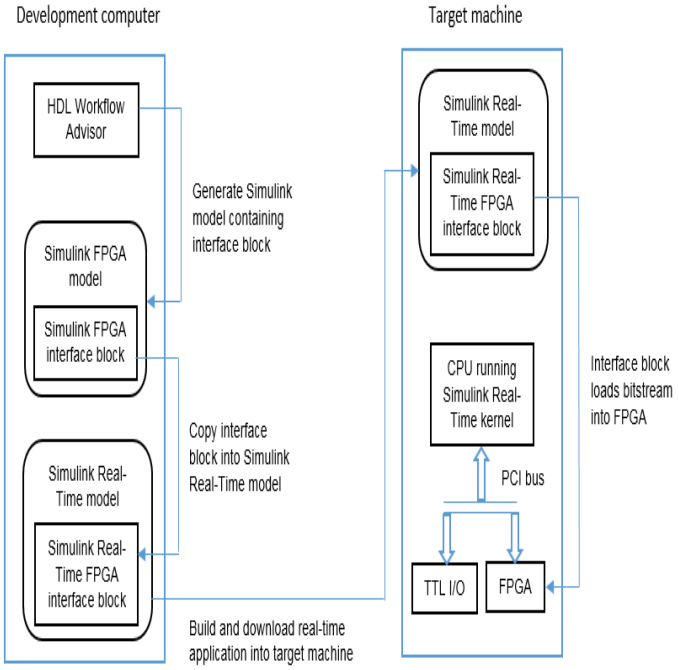


Fig 5 Hardware and Software FPGA Simulink Real-Time interface subsystem model

VI. RESULTS AND DISCUSSION

Our model in figure (4) is applied on the video sequence and the performance of algorithm is measured with respect of its imperceptibility and adjustment, Histogram equalization and so. The watermarking scheme is tested against Frame Gaussian noise, Frame Histogram equalization, Frames hear, and Frame Median filters. Peak Signal to Noise Ratio (PSNR) is used to evaluate the performance of any watermarking system, as a general measure of the visual quality of the watermarking scheme robustness against the possible attacks. The Peak-Signal-To-Noise Ratio (PSNR) is used to measure deviation of the

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 8, Issue 2, August 2018

watermarked and attacked frames from the original video frames and is defined in equation (9):

$$PSNR = 10log10\,(\max\,(fr, fb, fg)/MS..(9)$$

Where:

$$mser = \sum_{i=1}^{m}\sum_{j=1}^{m} fr(i,j) - fr'(i,j))\,\hat{}\,2$$

$$mseg = \sum_{i=1}^{m}\sum_{j=1}^{m} (fg(i,j) - fg'(i,j))\,\hat{}\,2$$

$$\text{MSE}= \frac{\text{mser+mseg+m:}}{3}$$

Table1: Values of PSNR, NC, and MSE for video frames

Typical Attack	PSNR(all frame)	NC (all frame)	MSE (all frame)
No attack	**43-38dB**	**1**	**9.5%~10%**
Gaussian Noise(35db)	**30-24dB**	**0.94~0.81**	**21.9%~18.13%**
Histogram Equalization	**26-24.dB**	**0.95-0.72**	**42.32%~30.4%**
Shear	**32-28dB**	**0.92~0.71**	**25.6%~23.8%**
Median filter	**36-32dB**	**0.96~0.80**	**23.45%~22.3%**

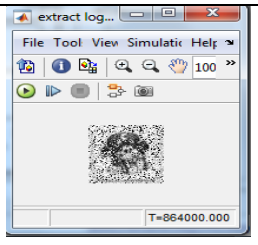
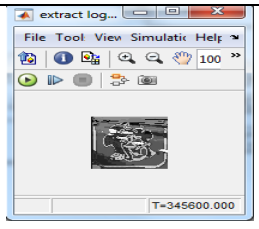
Table2: Device Utilization Summary of Xilinx Spartan 6 FPGA

Slice logical utilization	Used	Available	Utilization
Number of Slice Registers	1,863	18,224	10%
Number of Slice LUTs	2,922	9,112	32%
Number of LUT Flip Flop pairs used	1,496	3,144	46%
Number of bonded IOBs	30	232	12%
Number of BUFG/BUFGMUXs	1	30	3%
Number of DCM/DCM_CLKGENs	1	4	24%

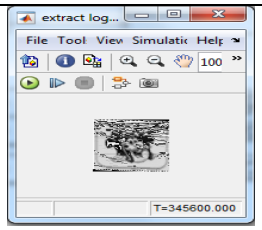
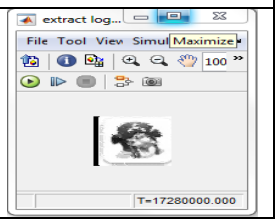
$$mseb = \sum_{i=1}^{m}\sum_{j=1}^{m} (fb(i,j) - fb'(i,j))\,\hat{}\,2$$

The NCC is used to evaluate the range similarity between the original watermark and extracted watermark from the attacked image as defined in the equation (8). These results are shown in table 1.

Table 3:- Performance evaluation of LSB technique for different number of video frames

Case	Frame 10	Frame 33	Frame 105	watermark (logo)
No attack				
Gaussian Noise(35db)				
Histogram Equalization				

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 8, Issue 2, August 2018

Shear				
Median filter				

VI. CONCLUSION

Experienced results show that the base of the algorithm is robust to most attacks such as Gaussian noise, Histogram equalization, Shear, Median filter, etc. Moreover at receiver it isn't need any information in extraction process while other techniques may need some information such as original video or watermark (logo). Matlab Vision HDL Toolbox provides a design environment that support video and image processing in HDL architecture.

Normalized cross-correlation (NCC), peak signal to Noise Ratio (PSNR), and mean squared error (MSE) measures are used to evaluate the performance of the watermarking scheme. Hardware implementation is done using *Xilinx Spartan 6 FPGA* from which the results approve the real-time operation of the video watermarking algorithm.

REFERENCES

[1] Qingtang Su, Ludong and Walter de Gruyter, "Color Image Watermarking: Algorithms and Technologies", University, Shandong, China, GmbH & Co KG, 2017.

[2] Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T.: Digital Watermarking and Steganography, 2Nd Ed. ISBN: 978-0123725851.

[3] Hartung F, Kutter M. "Multimedia watermarking techniques". Proceedings of the IEEE. 1999; 87(7):1079–107.

[4] Gunjal BL, Manthalkar RR. An overview of transform domain robust digital image watermarking algorithms. Journal of Emerging Trends in Computing and Information Sciences. 2010; 2(1):37–42

[5] Abdullah Mohamud Hassan, "A Robust digital image watermarking using repetition against common attacks", February 2015.

[6] Namita Tiwari1 and Sharmila" Digital Watermarking Applications, Parameter Measures and Techniques", IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.3, March 2017.

[7] Er.Sandeed kaur, Er.Jaspreet kaur, and Er.inderpreet kaur, 'Technicalities of Digital Watermarking: Review', International Research Journal of Engineering and Technology, volume: 03 Issue: 20 –Feb-2016.

[8] Dr. Vipula Singh, "Digital Watermarking: A Tutorial", Geethanjali College of Engineering and Technology, Hyderabad India (2011).

[9] Anupma Yadav, Anju Yadav, "Comparison of SVD-Watermarking and LSB-Watermarking Techniques", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May- 2014, pg. 495-499.

[10] Pik-Wah Chan and Michael R. Lyu1 "A DWT-based Digital Video Watermarking Scheme with Error Correcting Code" , ,Department of Computer Science and Engineering, The Chinese University of Hong Kong, Shatin , Hong Kong.