International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 3, Issue 9, September 2014

Hardware Implementation of a Digital Watermarking System Using 3D DCT

Ms. Ann Varghese, M.Tech Student, Ms. Haripriya P, Assistant Professor,
Dept. of Electronics & Communication Engineering, SNGCE, Kadayiruppu, Ernakulam, Kerala.

***Abstract*—This paper presents a hardware implementation of a digital watermarking system that can insert invisible watermark information into compressed video streams in 3D DCT. The watermark embedding and video compression is processed in the discrete cosine transform domain. The compression is performed using 3D DCT instead of using the motion compensation algorithms. Hardware implementation is performed using field programmable gate array. Results show that hardware-based video authentication system using this watermarking technique features minimum video quality degradation. Furthermore, the proposed hardware based watermarking system features low power consumption, high processing speed, and reliability.**

***Index Terms*—Digital video watermarking, hardware implementation, 3D DCT, very large scale integration(VLSI), video authentication.**

I. INTRODUCTION

With the advancement in technology and the rapid growth of techniques for multimedia processing, the distribution of video data is much easier and faster [2]–[4]. Since digital video sequences can be easily manipulated, concerns regarding authentication of the digital video are increasing. In situations where the video data should be credible, that is when it needs to be used as evidence, this issue becomes serious. So we need authentication techniques to maintain authenticity, integrity, and security of digital video content. Digital watermarking is one of the key authentication methods [5], [6]. Digital watermarking is the process of embedding an additional, identifying information within a host multimedia object, such as text, audio, image, or video. By adding a transparent watermark to the multimedia content, we can verify the ownership of the digital media.

Digital video WM techniques have wide applications [3]–[8]. Watermarking can ensure the authenticity of original content. Current digital Watermarking techniques have focused on multimedia data having video contents. Video WM applications has new challenges to overcome compared to image watermarking techniques. Shoshan *et al.* [5] and Li *et al.* [6] presented an overview of the various existing video WM techniques and showed their features and specific requirements, possible applications, benefits, and drawbacks.

The main objective of this paper is to describe a hardware-based digital video WM system, which inserts invisible watermarking in 3D DCT compressed video streams. Both watermarking and compression is performed in discrete cosine transform (DCT) domain. The proposed system achieves performance that matches complex software algorithms [11] with a simple hardware implementation. This design is suitable to fit easily in devices like surveillance cameras. The proposed system is implemented using the Verilog hardware description language (HDL) and synthesized into a field programming gate array (FPGA).

The remainder of this paper is organized as follows. A survey on the previous related work on video WM technologies is given in Section II. Section III describes the procedure for the digital video watermarking system. The hardware architecture design of the proposed system is provided in Section IV. Section V gives experimental results. Conclusions are presented in Section VI.

II. RELATED WORK ON VIDEO WATERMARKING SYSTEMS

A. Robustness level of wm for video authentication

The level of robustness of the WM can be categorized into three main divisions: fragile, semi fragile, and robust. A watermark is called fragile if it fails to be detectable after the slightest modification. A watermark is called robust if it resists a designated class of transformations. A semi fragile watermark is the one that is able to withstand certain legitimate modifications, but cannot resist malicious transformations [18], [21].

A semifragile invisible watermark rejects malicious changes like segment removal but withstands alterations like compression, mild geometric changes etc. Frequency domain processing of semifragile watermarking is generally followed. Frequency-domain WM methods are more robust than the spatial-domain techniques [7]. Video sequences are generally compressed and then stored or transmitted. Compression is usually done by transforming it from spatial to frequency domain. Thus, a watermark that is inserted directly

in the compressed video can reduce computational demands.

B. Watermark implementations- Hardware vs. Software

Implementations can be done in software or hardware or a mixture of both. In software , we just need a computer and some tools which runs the codes to perform watermarking of different levels of complexity. Thus software has the advantage of flexibility but it cannot be easily modified for video signals or for use in portable devices. Thus hardware-based implementations are more suitable for real-time WM of video streams [9]. It has advantages like low power consumption, reduced area, and reliability. Also, it enables portability by adding tiny, fast and cheap watermark embedder as part of multimedia devices, where the data are watermarked at the origin. Both computational and design complexity need to be flexible for hardware implementations.

C. Past research on video watermarking

In the past few years, research effort has been focused on efficient WM systems implementation using hardware platforms. For example, Strycker *et al.* [9] proposed a well known video WM scheme, called just another watermarking system (JAWS), for TV broadcast monitoring. A new real-time WM very large scale integration (VLSI) architecture for spatial and transform domain was presented by Tsai and Wu [10]. Mohanty *et al.* [19] presented a concept of secure digital camera with a built-in invisible-robust watermarking and encryption facility. Also, another watermarking algorithm and corresponding VLSI architecture that inserts a broadcasters logo (a visible watermark) into video streams in real time was presented [20] by the same group.

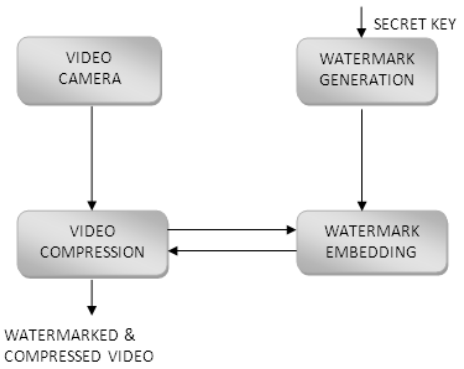


Fig. 1. The proposed video WM system.

In this paper we present the hardware implementation of the invisible semifragile watermarking system for video authentication. Here we are trying to combine the watermarking system with a video camera ,which compresses the data, for real-time watermarking.

III. PROCEDURE FOR THE DIGITAL VIDEO WATERMARKING SYSTEM

The proposed digital video WM system is described here. Fig. 1 gives the general block diagram of the proposed system. It consists of a video compression unit, watermark generation, and watermark embedding units.

The watermark embedding process is performed in the DCT domain.DCT is used in almost all the video compression formats, including JPEG, MPEG, H.26x. Thus we can combine watermarking and compression into a single system. Compression consists of 3 stages: DCT transformation, quantization, and Huffman encoding. Inserting the watermark after compression makes the watermark robust. In video compression the frames are first divided into 8 × 8 blocks.Better robustness is achieved by inserting watermark specifically into each 8X8 block [15].

Each of the video frames undergoes 3Dimensional DCT and quantization. Then, they are passed to the watermark embedding module. Using some secret keys, specific watermark data is generated, which will then be inserted into each of the video frames. The watermark embedding module inserts the watermark data into the quantized DCT coefficients for each video frame. Finally, watermarked DCT coefficients of each video frame are encoded by the video compression unit which outputs the compressed frame with embedded authentication watermark data.

A. Video compression

There can be two types of redundancies in video frames: temporal redundancy and spatial redundancy. These redundancies need to be reduced in order to compress the images. In general video compression methods, spatial redundancy is done by DCT and temporal redundancy by motion estimation and compensation techniques. In this paper we are performing the video compression using the 3 Dimensional DCT. The three-dimensional Discrete Cosine Transform (3D DCT) is used for video compression where the main principle is the correlation between points inside a group of frames (GOF). The 3D DCT extends the energy compaction properties of conventional 2D DCT to integral 3D images/videos. Three-dimensional (3-D) transform coding is an alternative approach to the motion compensation transform coding (using 2D DCT plus motion estimation and compensation) technique used in today's video coding standards.

In video coding the application of the Discrete Cosine Transform along the temporal axis is advantageous over motion compensation prediction schemes because 3 dimensional discrete cosine transform coding reduces the inter frame redundancy among a number of consecutive frames, while the motion compensation technique can reduce the redundancy of at most two frames.

B. Watermark generation

The watermark data should be encoded so as to prevent it from being susceptible to attack. This makes sure that the watermark data before it is inserted into the video frame cannot be cracked. The WM generator combines the watermark sequence and secret keys to produce a secure watermark sequence.

According to the recommendation by Dittman *et al.* in [12] for the feature of a video watermark, a primitive watermark pattern can be defined as a meaningful identifying sequence for each video frame. The watermark data consists of time, date, camera ID, and frame serial number (that is related to its creation) [Fig. 2]. Any alteration can be detected by the specific watermark. The binary value of the pattern[64 bit] is taken and will be used as primitive watermark sequence. This would generate a different watermark for every frame (time-varying) because of the instantaneously changing serial number and time. The block diagram of the watermark generator is depicted in Fig. 3. Scrambling and modulation are performed for obtaining a secure watermark. Two keys are generally used. Scrambling and modulation are simple XOR operations. Key 1 is used for scrambling and Key 2 is used for the random number generator (RNG) module that generates a pseudorandom sequence. A buffer is used for storing the watermark sequence. Key 1 initiates the scrambling process by specifying two different addresses (*Add1* and *Add2*) of the buffer for having the XOR operation in between them. Scrambling adds complexity and encryption in the watermark structure. The scrambled sequence, is modulated by a binary pseudorandom sequence to generate the secured watermark sequence. Due to the random nature of the pseudorandom sequence, modulation makes the watermark sequence a pseudorandom sequence and thus difficult to detect, locate, and manipulate. A secure pseudorandom sequence used for the modulation can be generated by an RNG structure using the *Key 2*. RNG is based on a Gollmann cascade of filtered feedback with carry shift register (F-FCSR) cores, presented by Li *etal.* [13], [17].

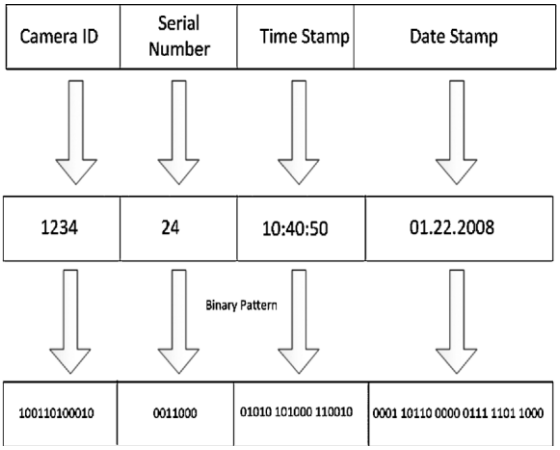


Fig. 2. Structure of the primitive watermark.

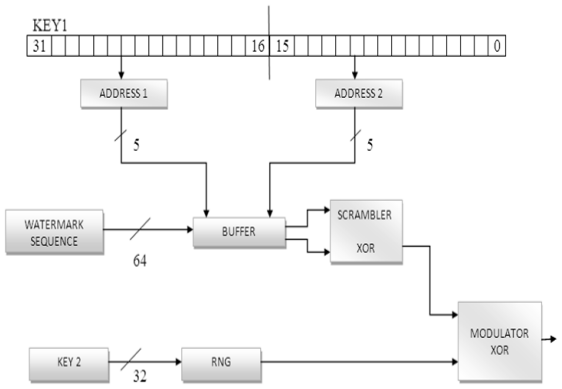


Fig. 3. Block diagram of the proposed watermark generator.

C. Watermark embedding

Watermark embedding is done on the quantized frames. The watermarking algorithm should be hardware friendly in a way that it can be implemented in hardware with high throughput. The watermark embedding approach used in this paper was originally developed by Nelson *et al.* [14] and Shoshan *et al.* [15]. This WM algorithm, capable of inserting a semifragile invisible watermark in a compressed image in the DCT frequency

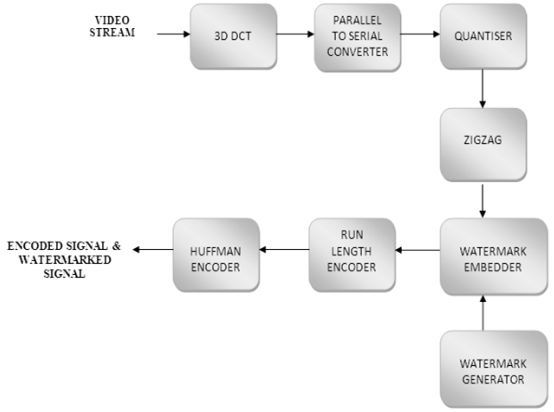


Fig. 4. Dataflow of the proposed WM algorithm.

domain, was modified and then applied in watermarking of a video stream. In general, for

each DCT block of a video frame, *N* cells need to be identified as "watermarkable" and modulated by the watermark sequence.
The chosen cells contain nonzero DCT coefficient values and are found in the mid-frequency range. This algorithm was detailed by Shoshan *et al.* [15]. The proposed WM algorithm along with MJPEG video encoding standard is presented as a flow chart in Fig. 4. This can be described as follows.
1) Split incoming video frame and watermark data into 8 × 8 blocks
2) For each 8×8 block, perform DCT, quantization, and zig–zag scan to generate quantized DCT coefficients.
3) Identify *N* watermarkable cells for each block and calculate the modification value for each selected cell.
4) Modify the identified watermarkable DCT coefficients according to the modification values.
5) Perform entropy coding for the blocks of the different frames.
6) Generate compressed and watermark embedded video steam.

IV. HARDWARE ARCHITECTURE DESIGN

All the processing in the implementation is assumed to be done on a block basis (such as 8 × 8 pixels). First, the captured video frame is temporarily stored in a memory buffer, and then each block of the frame data is continuously processed by the video compressor unit using DCT and quantization cores. The watermark embedder block inserts an identifying message, generated using the watermark generator unit, in the selected block data within the video frame. Finally it is encoded using the entropy encoder section.

A. Video compressor

For hardware implementation of the video compressor module, the MJPEG video encoding technique was chosen as because it offers several significant advantages for hardware implementation [16]. Even though MJPEG provides less compression, it is easy to implement in hardware with relatively low computational complexity and low power dissipation. Moreover, it is available for free usage and modification, and it is now supported by many video data players.

B. Watermark generator

Fig. 5 describes the hardware architecture of the novel watermark generator. Scrambling is done by using the secret digital key *Key1*, which has two parts. The two different parts initiate two different counters. At each state of the counters two readings (addressed by *Add1* and *Add2*) from the buffer occur for having the XOR operation between them. Thus, the scrambled watermark sequence, c_i, is generated. Furthermore, different digital keys can make the counters start running with different states and generate different corresponding addresses so that we can get different patterns of c_i. A secure pseudorandom sequence p_i, generated by the proposed Gollman cascade filtered feedback with carry shift register RNG [13], seeded with secret key *Key2*, is used to modulate the expanded and scrambled watermark sequence c_i. Finally, the generated secure watermark data w_i is embedded into the video stream by the watermark embedder.

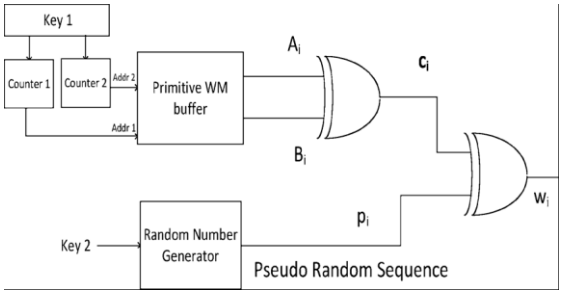


Fig. 5. Hardware architecture of the watermark generator

C. Watermark embedder

A schematic view of the hardware architecture for the watermark embedder unit is presented in Fig. 6.

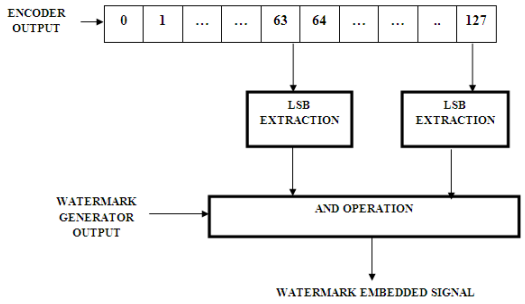


Fig. 6. Hardware architecture of the watermark embedder module designed by Shoshan *et al.* [25]

D. FPGA-based prototyping

Each module in the proposed digital video WM system, including the MJPEG compressor, watermark generator and watermark embedder has been implemented and tested individually, and then integrated together to obtain the final system architecture. The proposed architecture was first modeled in Verilog HDL using Xilinx ISE Design Suite 14.2 and the functional simulation of the HDL design was performed using the Xilinx ISim tool. Finally, the system design was synthesized to Xilinx Spartan6 FPGA device with speed grade of -2.

V. EXPERIMENTAL RESULTS

A. Performance analysis

The performance of the overall FPGA implementation was evaluated in terms of memory usage and processing speed. The data of each frame are processed macroblock (8×8) wise. Each macro-block first passes through the DCT module, and

then through the WM embedder. Timing Analysis shows that the proposed system reduces the time required for outputting the encoded and watermarked image. The memory usage also got reduced from 78% to 22%.The logic utilization of slice registers got reduced from 18% to 11%.

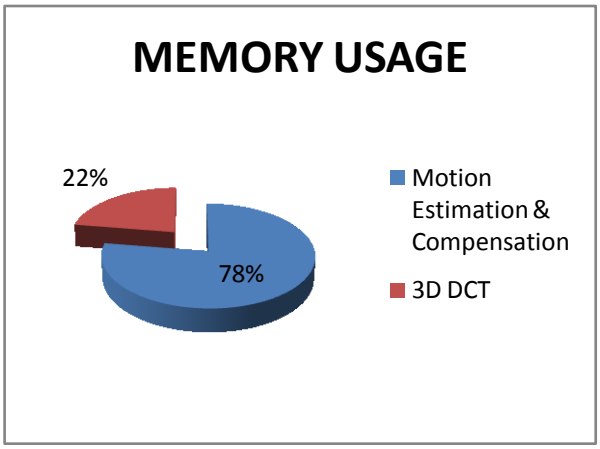


Fig7. Memory Usage Analysis

B. Comparison with existing research

The proposed hardware-based video WM authentication features minimum video frame quality degradation with no visually perceptible artifacts. Moreover, the results are comparable to that generated by software-based algorithms. However, the complexity of the proposed algorithm is lower since 3D DCT is employed. Furthermore, the watermark embedding that is designed to be performed directly in the compressed video streams minimizes computationally demanding operations.

VI. CONCLUSION

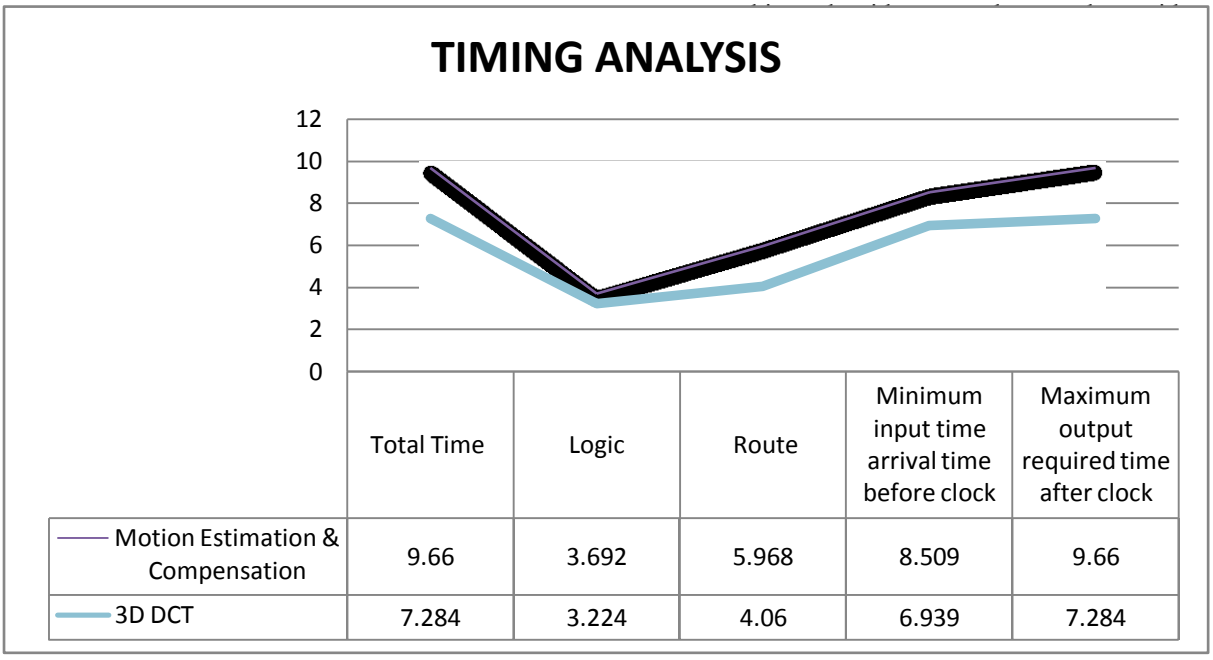
A. Summary and conclusion

Design of the hardware architecture of a digital video watermarking system to authenticate video stream in real time was presented in this paper. The proposed system was suitable for implementation using an FPGA and can be used as a part of an ASIC. In the current implementation, FPGA was the simple and available way of the proof-of concept. The implementation made integration to peripheral video (such as surveillance cameras) to achieve real-time image data protection. The aim of this paper was to achieve three objectives.

First, to propose a new HW architecture of a digital watermarking system for video authentication and making it suitable for VLSI implementation. Second, to make the watermarking system suitable for a real time video, this can be easily adapted with commonly used digital video compression standards with minor video frame degradation. The proposed watermark system was capable of watermarking video streams in the DCT domain in real time.

B. Future research

Future research should concentrate on applying the



	Total Time	Logic	Route	Minimum input time arrival time before clock	Maximum output required time after clock
Motion Estimation & Compensation	9.66	3.692	5.968	8.509	9.66
3D DCT	7.284	3.224	4.06	6.939	7.284

Fig8 Timing Analysis

that it can be utilized in various commercial applications as well. Embedding the watermark information within high resolution video streams in real time is another challenge.

References

[1] Sonjoy Deb Roy, Xin Li, Yonatan Shoshan, Alexander Fish, and Orly Yadid-Pecht "Hardware Implementation of a Digital Watermarking System for Video Authentication "IEEE Transactions On Circuits And Systems For Video Technology, February 2013

[2] V. M. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques," in *Proc. IEEE Int. Conf. Ind. Informatics*, Aug. 2005, pp. 709–716.

[3] A. D. Gwenael and J. L. Dugelay, "A guide tour of video watermarking," *Signal Process. Image Commun.*, vol. 18, no. 4, pp. 263–282, Apr. 2003.

[4] A. Piva, F. Bartolini, and M. Barni, "Managing copyright in open networks," *IEEE Trans. Internet Comput.*, vol. 6, no. 3, pp. 18–26, May– Jun. 2002.

[5] Y. Shoshan, A. Fish, X. Li, G. A. Jullien, and O. Yadid-Pecht, "VLSI watermark implementations and applications," *Int. J. Information Technol. Knowl.*, vol. 2, no. 4 pp. 379–386, Jun. 2008.

[6] X. Li, Y. Shoshan, A. Fish, G. A. Jullien, and O. Yadid-Pecht, "Hardware implementations of video watermarking," in *International Book Series on Information Science and Computing*, no. 5. Sofia, Bulgaria: Inst. Inform. Theories Applicat. FOI ITHEA, Jun. 2008, pp. 9–16 (supplement to the *Int. J. Inform. Technol. Knowledge*, vol. 2, 2008).

[7] 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.

[8] S. P. Mohanty. (1999). *Digital Watermarking: A TutorialReview* [Online]. Available: http://www.linkpdf.com/download/dl/digital-watermarking-a-tutorial-review-.pdf

[9] L. D. Strycker, P. Termont, J. Vandewege, J. Haitsma, A. Kalker,M. Maes, and G. Depovere, "Implementation of a real-time digital watermarking process for broadcast monitoring on Trimedia VLIW processor," *Proc. Inst. Elect. Eng. Vision, Image Signal Process.*, vol. 147, no. 4, pp. 371–376, Aug. 2000.

[10] T. H. Tsai and C. Y. Wu, "An implementation of configurable digital watermarking systems in MPEG video encoder," in *Proc. Int. Conf.Consumer Electron.*, Jun. 2003, pp. 216–217.

[11] X. Wu, J. Hu, Z. Gu, and J. Huang "A secure semifragile watermarking for image authentication based on integer wavelet transform with parameters," in *Proc. Australian Workshop Grid Comput. E-Research*, vol. 44. 2005, pp. 75–80.

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

[13] X. Li, Y. Shoshan, A. Fish, and G. A. Jullien, "A simplified approach for designing secure random number generators in HW," in *Proc. IEEE Int. Conf. Electron. Circuits Syst.*, Aug. 2008, pp. 372–375.

[14] G. R. Nelson, G. A. Jullien, and O. Yadid-Pecht, "CMOS image sensor with watermarking capabilities," in *Proc. IEEE Int. Symp. Circuits Syst.* vol. 5. May 2005, pp. 5326–5329.

[15] 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.

[16] A. Filippov, "Encoding high-resolution Ogg/Theora video with reconfigurable FPGAs," *Xcell J.* (Plugging into High-Volume Consumer Products), no. 53, pp. 19–21, 2005 [Online]. Available: http://www.xilinx.com/publications/archives/xcell/Xcell53.pdf

[17] (2012, Jan. 13) [Online]. Available: http://wiki.xiph.org/index.php/TheoraSoftwarePlayers

[18] (2012, Jul. 28) [Online]. Available: http://en.wikipedia.org/wiki/Digital–watermarking

[19] S. P. Mohanty, "A secure digital camera architecture for integrated realtime digital rights management," *J. Syst. Architecture*, vol. 55, nos. 10– 12, pp. 468–480, Oct.–Dec. 2009.

[20] S. P. Mohanty and E. Kougianos, "Real-time perceptual watermarking architectures for video broadcasting," *J. Syst. Softw.*, vol. 84, no. 5, pp. 724–738, May 2011.

[21] S. Saha, D. Bhattacharyya, and S. K. Bandyopadhyay, "Security on fragile and semifragile watermarks authentication," *Int. J. Comput.Applicat.*, vol. 3, no. 4, pp. 23–27, Jun. 2

Ms. Ann Varghese received her Btech from SCMS School of Engineering & Technology, Kerala. She is currently pursuing her Mtech in VLSI & Embedded Systems from Sree Narayana Gurukulam College of Engineering & Technology, Kerala. Her field of interest is in VLSI.

Ms. Haripriya P received her Btech from Sree Narayana Gurukulam College of Engineering & Technology, Kerala. She did her Mtech in VLSI & Embedded Systems from Viswajyothi College of Engineering & Technology, Kerala. She is currently working as Assistant Professor at Sree Narayana Gurukulam College of Engineering & Technology, Kerala. Her fields of interest are Digital Signal Processing and Wireless Communication

