I T H E A

International Journal

INFORMATION TECHNOLOGIES & KNOWLEDGE

2009 Volume 3 Number 2

International Journal
INFORMATION TECHNOLOGIES & KNOWLEDGE
Volume 3 / 2009, Number 2

IJ ITK is official publisher of the scientific papers of the members of the ITHEA International Scientific Society

IJ ITK rules for preparing the manuscripts are compulsory.
The rules for the papers for IJ ITK as well as the subscription fees are given on *www.ithea.org*
The camera-ready copy of the paper should be received by e-mail: info@foibg.com.
Responsibility for papers published in IJ ITK belongs to authors.

General Sponsor of IJ ITK is the Consortium FOI Bulgaria (www.foibg.com).

International Journal "INFORMATION TECHNOLOGIES & KNOWLEDGE" Vol.3, Number 2, 2009

Edited by the Institute of Information Theories and Applications FOI ITHEA®, Bulgaria,
in collaboration with the V.M.Glushkov Institute of Cybernetics of NAS, Ukraine,
and the Institute of Mathematics and Informatics, BAS, Bulgaria.

Publisher: ITHEA®
Sofia, 1000, P.O.B. 775, Bulgaria. www.ithea.org, e-mail: info@foibg.com
Printed in Bulgaria

ISSN 1313-0455 (printed) ISSN 1313-048X (online) ISSN 1313-0501 (CD/DVD)

HARDWARE IMPLEMENTATIONS OF VIDEO WATERMARKING

Xin Li, Yonatan Shoshan, Alexander Fish, Graham Jullien, Orly Yadid-Pecht

Abstract: Digital watermarking (WM) is the process that embeds an additional, identifying message called a watermark into a host multimedia object, such as audio, image or video for authentication purpose. Recently, digital WM technique, an information hiding technique has been investigated as one of the key authentication methods to maintain authenticity and security of multimedia content. By adding a transparent watermark to the multimedia content, it can be possible to make any malicious alteration detected to verify the integrity and the ownership of the digital media. During the last several years various WM techniques for still image have been extensively invented for software implementations due to the low data rate of these signals. Although the software approach holds an advantage of flexibility, certain computational restrictions may arise when attempting to operate at video rate or in portable devices. The hardware-level design offers several distinct advantages over the software implementation in terms of lower power consumption, reduced area and reliability. Therefore, there is a strong motivation for a move toward the hardware-based implementation for digital video WM system.

In order to give a help for future related research works, this paper presents an up to date overview of digital video WM techniques and discusses the important considerations involving in designing VLSI architecture for a novel WM system in many ways. First of all, it goes through a brief survey on WM theory, laying out common classification criterions, discussing the properties of video WM techniques including the specific requirements as well as the comparison to image WM schemes. Various applications of video WM in practice are discussed. Since each WM application has its own specific requirements, WM design must take the intended application into account. Furthermore, the features of video WM implementations in software and hardware and comparison on those two approaches are presented from several points of view: major advantages, drawbacks and differences through the description of several examples of previous works. In addition, a versatile development methodology for hardware WM implementation including the general scheme of a proposed digital video WM system and testing using the custom breadboard are described.

Keywords: Digital video, watermarking, WM, hardware implementation, security.

ACM Classification Keywords: B.0 Hardware

1. Introduction

Over the past decade, storing and transmitting digital multimedia data has become incredibly available throughout the world, especially with the advent of digital times. This has been a catalyst for the rapid growth of digital video technologies and applications [1]. Nowadays, the expansion of high speed digital computer networks all over the world and the advance of compression technologies have made the distribution of video data and applications much easier and faster. The amount of high quality digital video data is ready available on the internet so that users can conveniently be able to enjoy watching on-line video, transmit and exchange video files. Digital video is also useful in many other applications: surveillance video systems and broadcasting are good examples. However, at the same time a number of security problems have been introduced, since digital video sequences are very susceptible to manipulations and alterations using widely available editing software. This way video content is not reliable anymore.

For example, a video shot from a surveillance camera cannot be used as a piece of evidence in a courtroom because it is not considered trustworthy enough. Therefore, authentication techniques are consequently needed in order to ensure the authenticity, integrity and security of digital video content. So far, there have been various such techniques [2], of which digital watermarking (WM), a data hiding technique, is one of the most popular approaches. Digital WM is a technique that embeds a secret, unnoticeable signal (called watermark) into the original multimedia objects, like audio, image and video for their protection and authentication. The watermark can be detected or extracted later to claim the authenticity and the ownership of the digital media.

During the past few years several researchers have investigated digital WM with different contributions, implemented both on software and hardware platforms [3]-[14]. In 1990, the modern study of steganography and digital WM was started by Tanaka et al. [3]. They suggested hiding information in multi-level dithered images as a form of secured military communications. Following that work, digital image WM arose, and recently the development of video WM algorithms became a growing field of research. A relatively simple WM algorithm, working on raw video data, was presented in [4]. In [5], Wu proposed a method that adds a discrete cosine transform (DCT) transformed pseudo-random sequence (used as watermark) directly to the DC-DCT coefficients of the video frame to achieve better robustness against MPEG lossy compression. A spread spectrum method, described by Shan [6], was applied to watermark color video frames. According to this method, the mid-frequency DCT coefficients of a green component of the color frames were selected to embed the watermark because it was found to be the most robust after compression.

While the software approaches hold advantages of easy implementation and flexibility, certain computational restrictions may arise when attempting to operate at video rate or in portable devices. The hardware implementation offers several distinct advantages over the software implementation in terms of low power consumption, less area usage and reliability. Furthermore, it features real time capabilities and compact implementations. Therefore, there is a strong motivation for a move toward the hardware-based implementation for digital video WM system since real time WM of video streams is too expensive for software [11]. On the other hand, hardware implementations of WM techniques demand the flexibility of implementation both in the computation and design complexity. The algorithm must be carefully designed to minimize any unexpected deficiencies, while still providing the sufficient level of security. In the past few years, a great deal of research efforts has been focused on efficiently implement WM systems using hardware platforms. Those include implementations in custom-designed circuitry or application specific integrated circuits (ASICs), as well as field programmable gate arrays (FPGAs) implementations [10]-[14]. In consumer electronic devices, a hardware WM solution is often more economical because adding the WM component only takes up a small dedicated area of silicon.

In this paper, we aim to achieve two main goals. The first goal is to provide an in-depth overview of previous works on the field of hardware-based video WM through discussing different watermark classifications, new applications and specific requirements. Following that, existing WM software-based and hardware-based implementations and their comparisons are also described. Secondly, to give a help for future related research works, a development methodology for designing and testing hardware-based video WM system has been discussed. In the proposed methodology, VLSI architecture of a prototype chip for real-time video WM design is briefly described.

The remainder of this paper is structured as follows. Section II tries to classify and discuss the digital video WM techniques in various ways in order to give a thorough overview of conventional WM techniques. The software and

hardware implementations of WM algorithms proposed so far are presented in section III. Finally, a design methodology for hardware video WM implementation and conclusions are presented in section IV and V respectively.

2. Background on Video WM

2.1 Watermarks Classification

WM techniques can be divided into different categories according to various criterions [15]. The general classification of the currently available watermarks is shown in Figure 1. In [16] we have presented a decomposition of the variety of existing watermarks for still images and showed their features and possible applications, benefits and drawbacks. Since a video stream is regarded as a three-dimensional signal with two dimensions in space (called m x n frame) and one dimension in time, we can consider a video stream as a succession of still images. Therefore, most image WM techniques are equally applicable to the field of video WM if the individual frames are treated as images [17]. However, contradictory to still image WM techniques, the video WM methods usually require that the WM encoding and decoding are processed in real time.

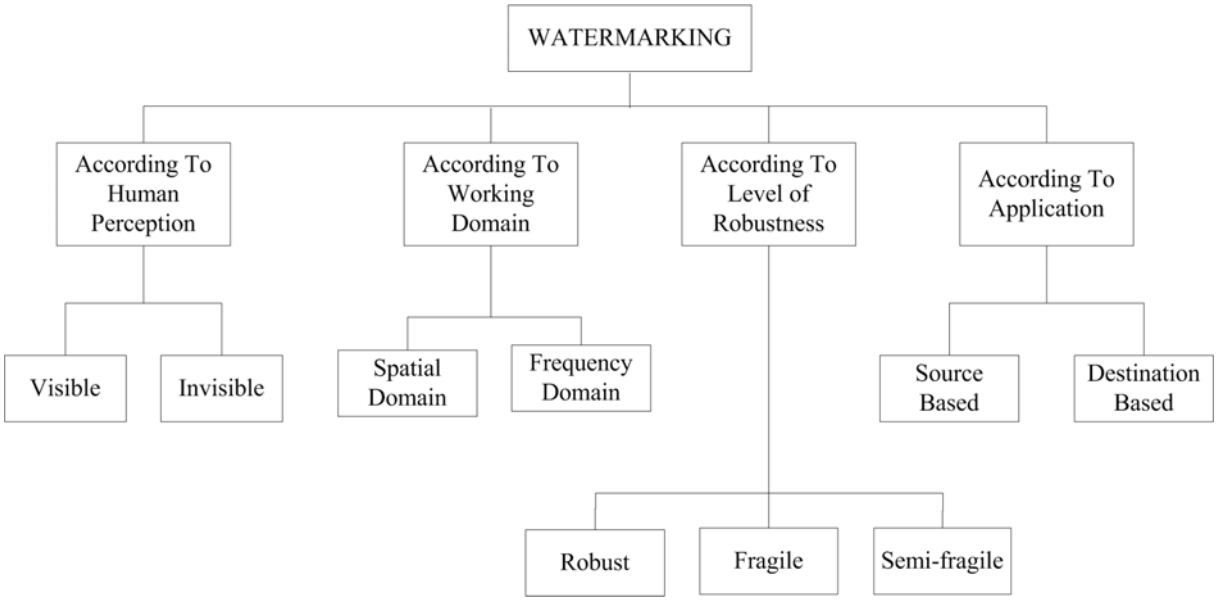

Figure 1. General classification of existing watermarking.

In general, most digital WM techniques proposed can be divided into two different types: visible and invisible watermarks according to human perception [7]. Each of the schemes is equally important due to its unique applications. Sometimes a certain application requires a watermark to be visible, so that the embedded watermark appears visible to a casual viewer. However, the most popular digital WM technique recently used for copyright authentication purposes is the invisible watermark, which marks the more significant digital media object, without perceptually changing it. By extracting the watermark data later with the appropriate decoding mechanism, it can be possible to make any malicious alteration detected to verify the integrity and the ownership of the digital media. The

hidden watermark can be meaningful, like a logo or tag or the information representing the customer identity. A simple example of such techniques can be found in Figure 2.

According to the domain in which video WM is performed, WM processing methods can be classified into two categories: spatial domain and frequency domain. In the spatial domain, directly applying minor changes to the values of the pixels in a minor way is mainly used. This technique makes the embedded information hardly noticeable to the human eye. For example, pseudo-random WM works by simple addition of a small amplitude pseudorandom noise signal to the original media data. In the frequency domain, the object first goes through a certain transformation, DCT or discrete wavelet transforms (DWT), the WM is embedded in the transform coefficients and then it is inversely transformed to receive the watermarked data. However, 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 (frequency domain) can minimize computational demanding operations. Moreover, frequency domain WM methods are more robust than the spatial domain techniques [5]. Therefore, working on compressed rather than uncompressed video is important for practical WM applications.

Figure 2. Example of an invisible watermark.

WM techniques proposed so far for media authentication are usually designed to be robust, fragile and semi-fragile watermarks according to the level of robustness. In copyright protection applications, the robust MW would be detectable even after an image or video frame goes through severe modifications and degradation. For image integrity applications it is efficient to apply a fragile WM which is designed to detect even the slightest change in the image. Most of the fragile WM methods perform the embedding in the spatial domain. Unlike the fragile WM techniques, a semi-fragile algorithm, such as the proposed algorithm, is designed to withstand certain innocuous manipulations but to reject malicious ones. Here, the innocuous manipulations mean the legitimate modifications such as lossy compression performed to the media during storage and distribution. The semi-fragile approaches are generally processed on the frequency domain (such as DCT, DWT), which make it substantially more attractive than the other two WM schemes [5].

From the application point of view, digital WM could be source based or destination based [13]. Source based WM can be used to authenticate whether a received media data has been manipulated and the destination based WM can trace the source of illegal copies.

2.2 Applications of Video WM

This section is consequently dedicated to the presentation of various applications in which digital WM can bring a valuable support in the context of video data. The following main WM applications are considered in the open literatures and as commercial applications [19]. The reader is referred to [19]-[21] for a more detailed investigation. The applications presented have been distilled down in Table 1.

Table 1. Video WM: Applications and Purposes.

Applications	Purpose
Copyright protection	Proof of ownership
Video authentication	Insure that the original content has not been altered
Fingerprinting	Trace back a malicious user
Copy control	Prevent unauthorized copying
Broadcast monitoring	Identify the video item being broadcasted

Copyright protection: For the protection of intellectual property, the video data owner can embed a watermark representing copyright information in his data. This watermark can prove his ownership in court when someone has infringed on his copyrights. For instance, embedding the original video clip by noninvertible WM algorithms during the verification procedure happens to prevent the multiple ownership problems in some cases.

Video authentication: Popular video editing software permit today to easily tamper with video content and therefore it is not reliable anymore. Authentication techniques are consequently needed in order to ensure the authenticity of the content. One solution is the use of digital WM.

In Figure 3, a sketch of a simple video surveillance (VS) system, in which WM is used to authenticate VS data, is given [20], [21]. Timestamp, camera ID and frame serial number are used as a watermark, embedded into every single frame of the video stream. The central unit is in charge of analyzing the watermarked sequences and generating an alarm whenever a suspicious situation is detected, and then may either be sent to the security service or compressed for storage. When needed, the stored video sequence can be used as a proof in front of a court of law. It is possible to reflect any manipulation by detecting the watermarks.

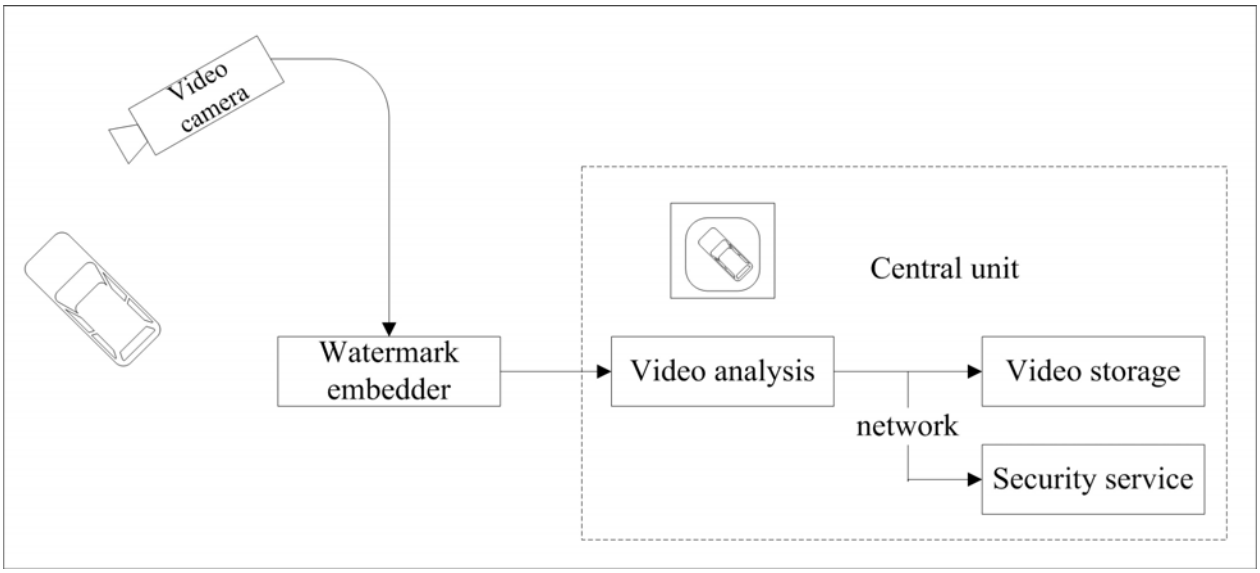

Figure 3. WM-based authentication for automatic VS.

Video fingerprinting: To trace the source of illegal copies, a fingerprinting technique can be used. In this application, the video data 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 the data. It enables the intellectual property owner to identify customers who have broken their license agreement by supplying the data to third parties.

A consumer can receive digital services, like pay TV, by cable using a set-top box and a smart card, which he has to buy and can therefore be related to his identity. To prevent other non-paying consumers from making use of the same service, the provider encrypts the video data and this protects the service during transmission. The set-top box of the consumer, who paid for the service, decrypts the data only if a valid smart card is used. Then, a watermark, representing the identity of the user, is added to the compressed video. The watermarked (fingerprinted) data can now be fed to the internal video decoder to view the video. A set-top box with WM capabilities is depicted in Figure 4.

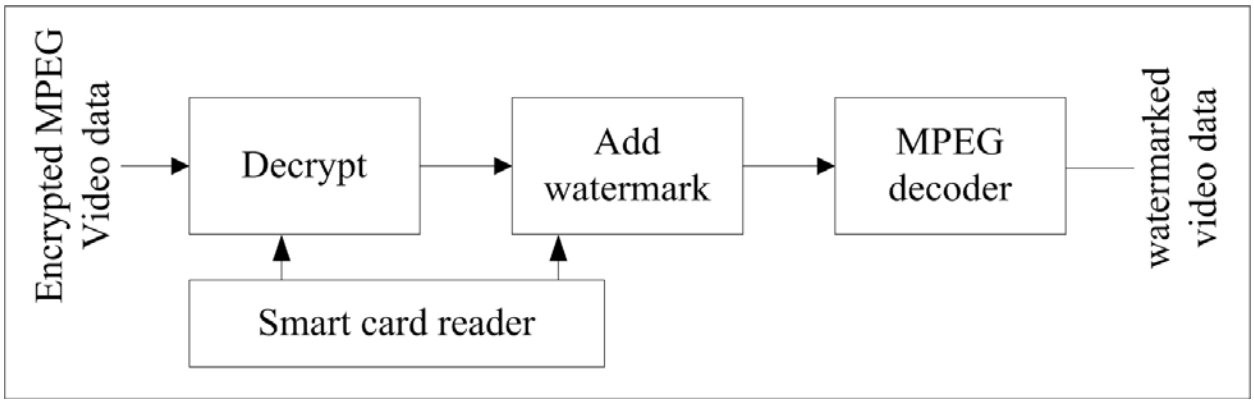

Figure 4. Set-top box with WM capabilities.

Copy control: The information stored in a watermark can directly control digital recording devices for copy protection purposes. In this case, the watermark represents a copy-prohibit bit and watermark detectors in the recorder determine whether the data offered to the recorder may be stored or not.

For example, in a copy protection scheme using WM techniques shown in Figure 5, consumers can make copies of any original source, but they cannot make copies of copies.

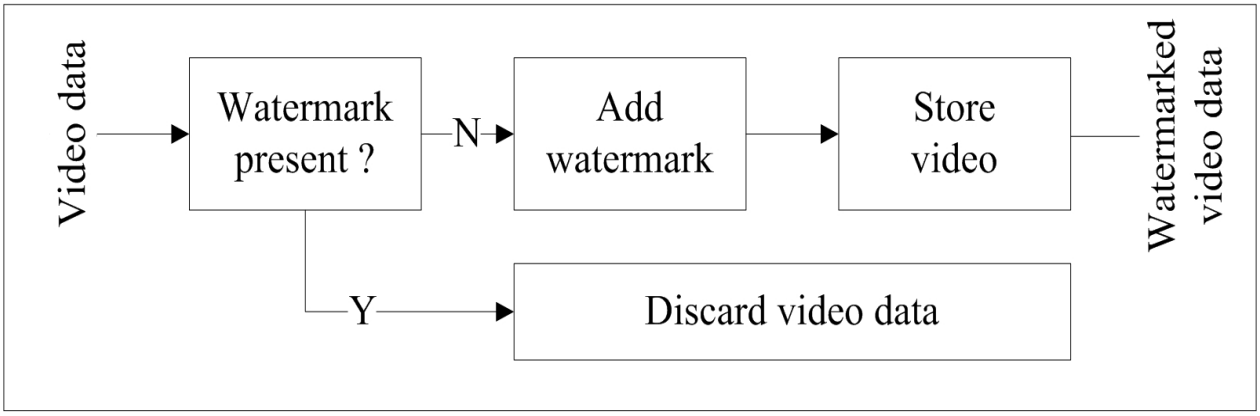

Figure 5. Video recorder with copy protection.

This copy protection system checks all incoming video streams for a predefined copy-prohibit watermark. If such a watermark is found, the incoming video has already been copied before and is therefore refused by the recorder. If the copy-prohibit watermark is not found, the watermark is embedded and the watermarked video is stored. This means that video data stored on this recorder always contains a watermark and cannot be duplicated if the recorder is equipped with such a copy protection system.

Broadcast monitoring: By embedding watermarks in commercial advertisements an automated monitoring system can verify whether advertisements are broadcasted as contracted. Not only commercials but also valuable TV products can be protected by broadcast monitoring. News items can have a value of over 100.000 USD per hour, which makes them very vulnerable to intellectual property rights violation. A broadcast surveillance system can check all broadcast channels and charge the TV stations according to their findings.

2.3 Requirements for Video WM

Different WM applications have specific requirements. Therefore, there is no universal requirement to be satisfied by all WM techniques. Nevertheless, some general directions can be given for most of the applications:

- Invisibility: WM should be imperceptible and invisible to a human observer.
- Transparency: WM embedding does not affect the quality of the underlying host data.
- Robustness: It should be impossible to manipulate the watermark by processing techniques or intentional operations such as filtering, addition of noises and cropping.

- Security: A WM technique is truly secure if knowing the exact algorithms for embedding and extracting the watermark does not help an unauthorized party to detect the presence of the watermark. It is very important, especially in authentication applications, that the watermark cannot be added or removed by an unauthorized user.
- Oblivious: It should be possible to extract watermark information without using the original multimedia data, since most receivers do not have the original data at their disposals.

Even though the requirements for the image and video WMs are very similar, they are not identical. New problems and new challenges have emerged in video WM applications. Apart from the basic requirements mentioned above, a WM technique should meet the following extra specific requirements to qualify as a real time technique for compressed video data:

- Low complexity: WM embedding and extracting should have low complexity, because they are to be processed in real time and if used in consumer products, they should also be inexpensive.
- Compressed domain processing: It should be possible to incorporate the watermark into compressed video (bit-stream).
- Constant bit-rate: WM should not increase the size of the compressed host video data and the bit-rate, at least for constant bit-rate applications where the transmission channel bandwidth has to be obeyed.

3. Video WM Implementations

In practical video storage and distribution systems, digital video sequences are stored and transmitted in a compressed format. Thus, a watermark that is embedded and detected directly in the compressed video stream can minimize computational demanding operations. Furthermore, frequency domain WM methods are more robust than the spatial domain techniques [18]. Therefore, working on compressed rather than uncompressed video is important for practical WM applications. Before we describe the video WM techniques, a briefly description of the video compression standards will be presented in the next flowing subsection.

3.1 Compression Standards

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 [22]-[24]. Such schemes are based on the principles of motion compensated prediction and block-based transform coding. Table 2 resumes the features of commonly used video compression standards. In the following, we refer particularly to description of MPEG-2 video compression technique.

Table 2 Popular Video Compression Standards.

Compression standards	Features
H.261	• Aimed at bit rates from 40 kbps to 2 Mbps. • Typically used in ISDN video conferencing.
MPEG-1	• Aimed for 1.5 Mbps data-rates and 352 x 240 resolutions. • Typically used for VCDs.
MPEG-2	• Outperforms MPEG1 at 3 Mbps • Below 1 Mbps, MPEG2 is similar to MPEG1. • Typically used for DVDs.
MJPEG	• Low bit rate video compression format based on JPEG compression. • Relatively low computational complexity.
H.263	• Aimed at video coding for low bit rates (20 to 30 kbps). • Typically used for web video conferencing.
MPEG-4(H.264)	• 33% improvement over MPEG2. • 4 times frame size of MPEG4 part 2 at a given data rate. •Targeted for all media applications: mobile, internet, standard video, high definition, and full high definition.

In general a video sequence can be divided into multiple group of pictures (GOP), representing sets of video frames which are contiguous in display order as illustrated in Figure 6(a). Each video frame is separated into slices and macro blocks. The block layer is formed by the luminance and chrominance blocks of a macro block. An encoded MPEG video sequence is made up of two frame-encoded pictures: intra-coded frames (I frames) and Inter-coded frames (P or B frames). P-frames are forward prediction frames and B-frames are bidirectional prediction frames. Within a typical sequence of an encoded GOP consisting of ten frames, as shown in Figure 6 (b), P-frames may be 10% the size of I-frames and B-frames 2%.

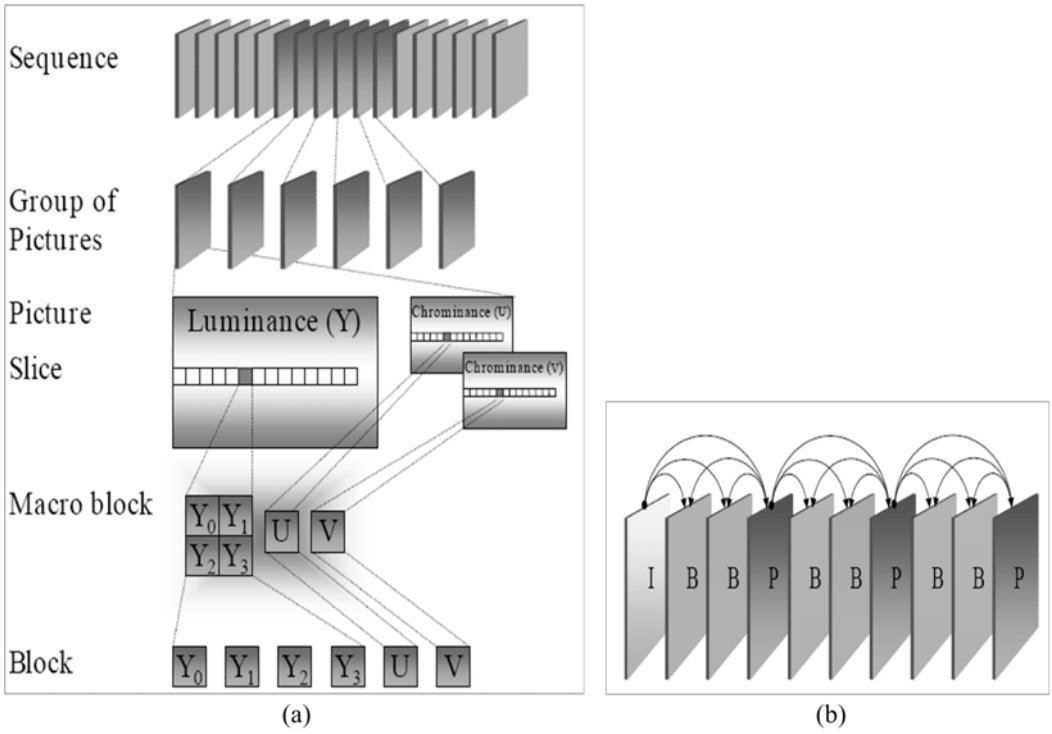

Figure 6. MPEG-2 GOP.

The MPEG-2 video compression algorithm is based on the basic hybrid coding scheme. As can be seen in Figure 7 this scheme combines inter-frame and intra-frame coding to compress the video data [23].

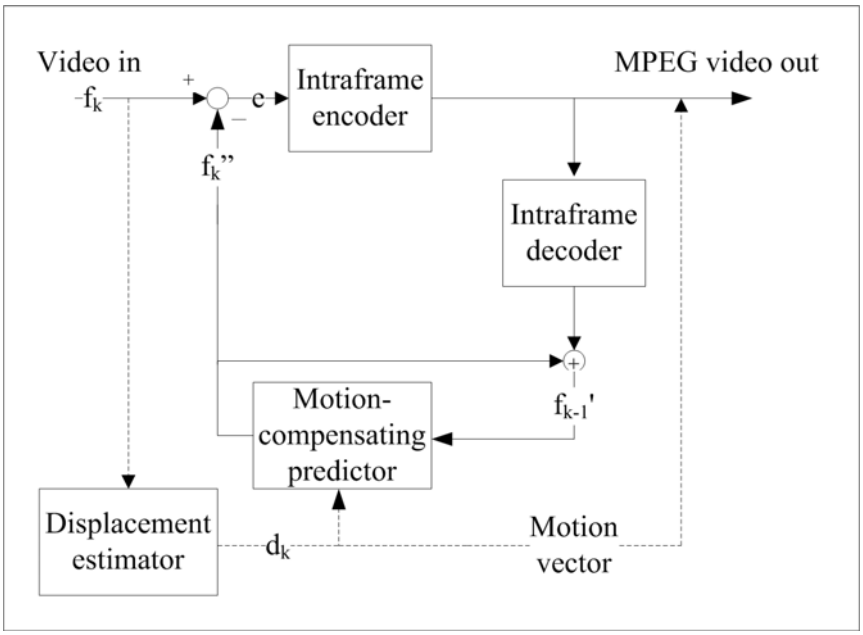

Figure 7. Block diagram of MPEG-2 encoder.

Within a GOP the inter-frames are temporally predicted by other motion compensated frames to reduce the temporal redundancy among the video frames. For each new inter-frame f_k, the motion compensating predictor will generate a prediction frame f_k' based upon the reconstructed previous frame f_{k-1}'' and a displacement estimate d_k that is obtained by an analysis of f_k. Since the original video is not available at the decoder d_k, also called motion vector, has to be transmitted. The prediction error (e), which is called the displaced frame difference, is encoded by the intra-frame encoder. The data flow of the MPEG-2 video encoder is shown in Figure 8.

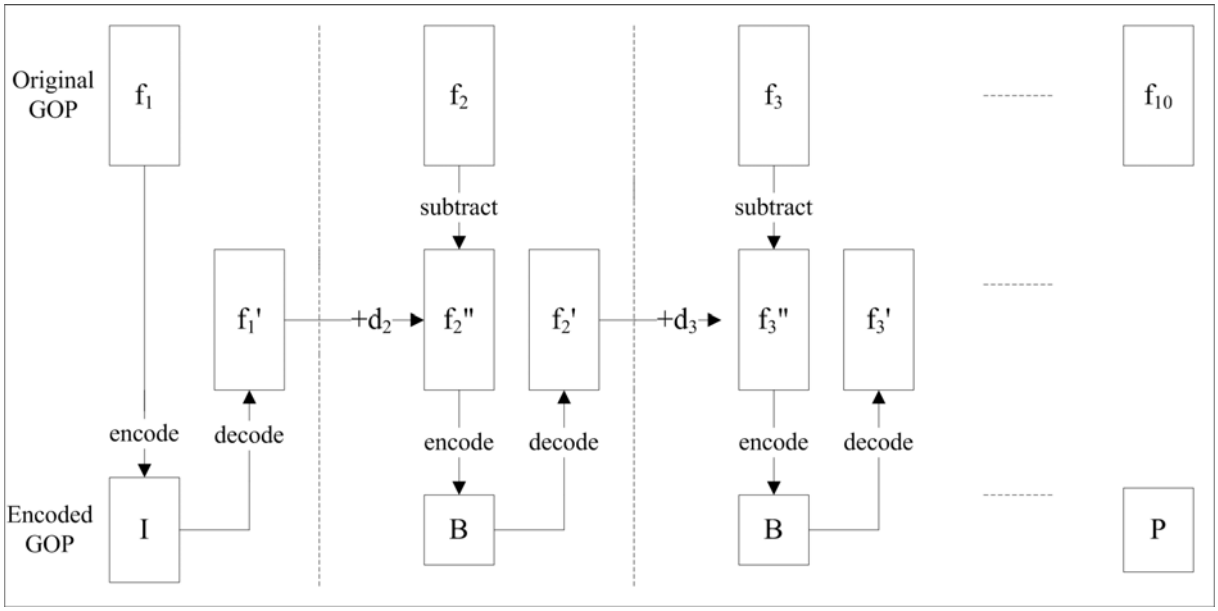

Figure 8. Data flow of MPEG-2 encoder.

The spatial redundancy in the prediction error (e) of the predicted frames and the intra-frames (I-frames) is reduced by the intra-frame encoder using the following operations(just like a JPEG image compression): they are split into blocks of size N × M (8 × 8) pixels which are compressed using the DCT, quantization (Q), zig-zag-scan, run-level-coding (Tuple coding) and entropy coding (VLC). Figure 9 depicts the procedure for the encoding of a single 8×8 block which is, in the bit-stream, represented as a series of Hunffman codewords.

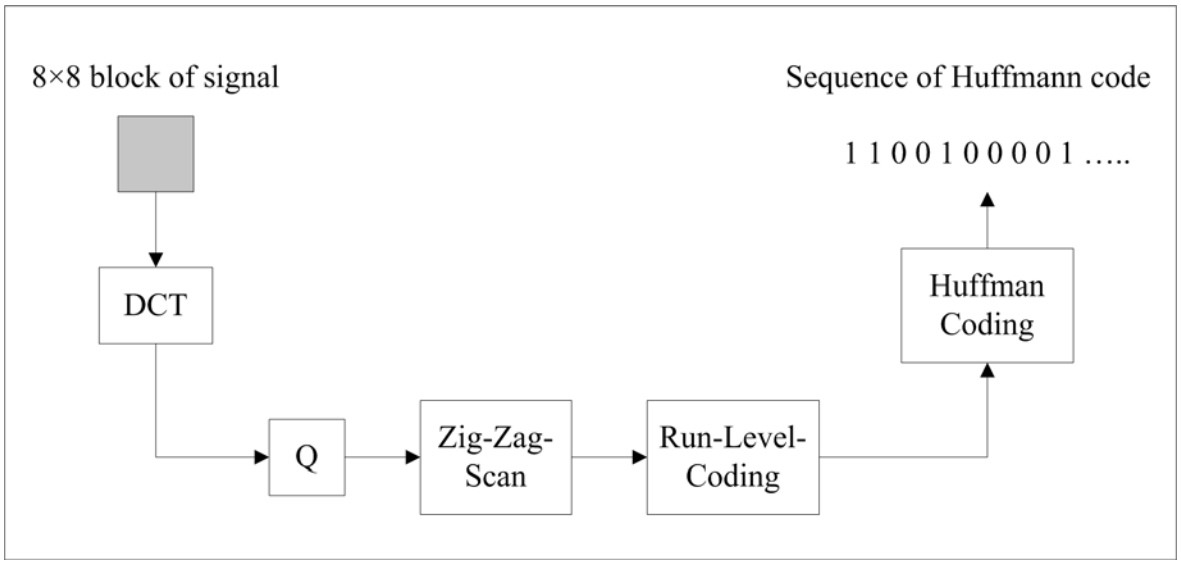

Figure 9. DCT encoding of 8×8 pixel block.

3.2 Software Implementations

Similar to image WM implementations, there exist tow kinds of video WM implementations: software and hardware, each having advantages and drawbacks. In software, the WM approaches hold advantages in terms of easy implementation and flexibility since the WM scheme can simply be implemented in a PC environment. The WM 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. Moreover, programming the code and making use of available software tools, it can be easy for the designer to implement any WM algorithm at any level of complexity.

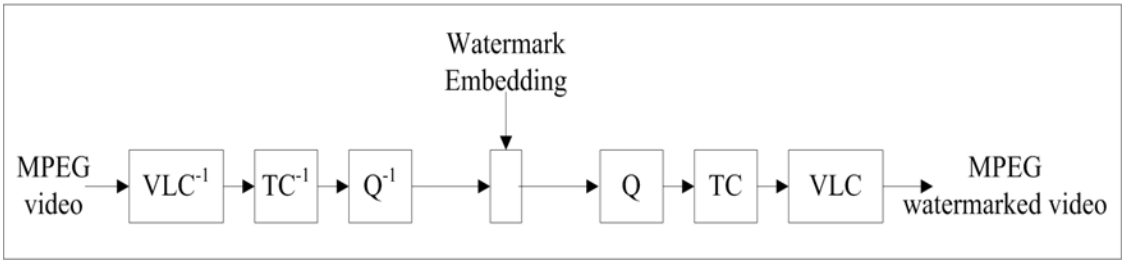

Figure 10. Block diagram of DCT-coefficient domain video WM.

A real-time WM algorithm for MPEG compressed video should closely follow the MPEG compression standard to avoid computationally demanding operations, like DCT and inverse DCT transforms or motion vector calculation.

Therefore, a MPEG compressed video WM algorithm, as shown in Figure 10, which operates on the DCT coefficient domain level only needs to perform VLC coding, tuple coding (TC) and quantization (Q) steps.

The basic idea for this WM algorithm is described as following several steps.

1. Generating a watermark message with the same manner and size as the video frame (to be watermarked).
2. Dividing watermark data into blocks of size N×M (such as 8 × 8) and computing the DCT coefficients for each watermark block.
3. The MPEG video frame is decoded (VLC^{-1} and TC^{-1}) and the resulting quantized DCT coefficients for all blocks then inversely quantized (Q^{-1}) in order to obtain the DCT coefficients.
4. The watermark is embedded into the video frame in DCT domain block-by-block according to certain algorithms and watermarked frame block is obtained.
5. The watermarked DCT coefficients for all blocks are re-encoded and the final result is a compressed watermarked video stream.

A major problem of directly modifying DCT-coefficients in an MPEG encoded video stream is drift or error accumulation. In an MPEG encoded video stream predictions from previous frames are used to reconstruct the actual frame, which itself may serve as a reference for future predictions. The degradations caused by the watermarking process may propagate in time, and may even spatially spread. Since all video frames are watermarked, watermarks from previous frames and from the current frame may accumulate and result in visual artifacts when decoding the MPEG watermarked video. By adding drift compensation signal during watermarking can solve this issue [4].

In [4], Hartung presents a good example of software MPEG compressed video WM solution. The spread spectrum concept of communications is employed to watermark a compressed video stream, where the basic idea is embedding the watermark in the transform domain as represented in the entropy coded DCT coefficients. This is done in an MPEG-2 video signal, which currently is a mature and widely used video compression standard. Although an existing MPEG-2 bit-stream is partly modified, the scheme avoids visible artifacts by adding a drift compensation signal. This signal is needed because the P and B frames on the MPEG-2 compression format rely on information found on the intra frame for encoding and decoding. For the retrieval of the WM, no original signal is needed. The system succeeds in achieving high data rate and a robust watermark scheme against malicious manipulations. Moreover, the computations involved in the embedding process are kept relatively basic, suggesting suitability for future hardware implementation as well.

Wu proposed a method that adds a DCT transformed pseudorandom pattern directly to the DC-DCT coefficients of an MPEG compressed video stream [5]. The WM process only takes the luminance values of the I-frames into account. A spread spectrum method is used to watermark video frames, described by Shan in [6]. In a color frame, the mid-frequency DCT coefficients of a green component of the frame are selected to embed the watermark since it is the most robust after compression. Another research work on DCT coefficient domain WM for MPEG-2 compressed video has been presented in [8]. The proposed WM scheme was designed to be undeletable, perceptually invisible, statistically undetectable, and robust to lossy compression and survives to video manipulation and processing.

3.3 Hardware Implementations

Over the last decade, numerous software-based WM algorithms have been invented [15]. However, WM implementation in hardware, especially for video stream, is a recent interest in the area. Up to 1999, no work on video WM implementation in hardware had been shown [11]. However, the watermarking of video streams in real-time applications is mostly suitable for hardware implementations, thus motivating research efforts to that direction.

The hardware WM implementation is usually implemented in custom-designed circuitry, application specific integrated circuits (ASICs) or field programmable gate arrays (FPGAs). As shown in Table 3, we provide a comparative view of most hardware-based video WM designs developed so far. The overall advantage of this scheme over the software implementation is in terms of lower power consumption, reduced area and reliability. It can be possible to add a small, fast and potentially cheap WM embedder as a part of portable consumer electronic devices, such as a digital camera, camcorder or other multimedia devices, so that the media data are watermarked at the origin. Therefore, it is most suitable for real time applications. On the other hand, hardware implementations of WM techniques demand the flexibility of implementation both in the computation and design complexity. The algorithm must be carefully designed, minimizing any unexpected deficiencies.

Table 3. Hardware-based implementations of Video WM.

Author	Design type	WM	Multimedia	Domain	Chip features
Maes	FPGA/IC	Invisible-robust	Video	Spatial	17/14 kG logics
Mathai	Custom IC	invisible	Video	Wavelet	1.8V
Tsai	Custom IC	Invisible-robust	Video	Spatial	NA

For example, in 2000, Strycker et al. proposed a real time video WM scheme, called Just Another Watermarking System (JAWS), for television broadcast monitoring [10]. JAWS is a well-known video WM algorithm and because it works on uncompressed real time video data, the author is allowed to concentrate on the watermark process and not on the compression issues. Therefore it is more suitable for hardware implementation. In the embedding procedure, a PR sequence is embedded in an uncompressed, real time video stream and the depth of the watermark insertion depends on the luminance value of each frame. The implementation of JAWS is performed on a Trimedia TM-1000 VLIW processor with 4 BOPS (billion operations per second) developed by Philips Semiconductors. The results prove the feasibility of a professional television broadcast monitoring system. Mathai et al., present an ASIC implementation of the JAWS WM algorithm using 1.8V, 0.18μm CMOS technology for real time video stream embedding [11], [12]. The authors claim that their work is the first step toward analyzing the relationship between WM algorithmic features and implementation cost for practical systems. A WM embedder and detector have been demonstrated to process raw digital video streams at a rate of 30 frames/sec and 320×320 pixels/frame. The results

show a chip with a core area of 3.53 mm^2, capable of operating at 75 MHz frequency, processing a peak pixel rate of over 3 Mpixels/sec and only consuming 60 mW of power for the embedder. The hardware employed in this implementation is comprised of video and WM RAM memories, adders/subtractors, registers and multipliers.

A new VLSI architecture of real time WM system for spatial and transform domain is presented by Tsai and Wu [13]. In this scheme, the concepts of spread spectrum from the field of communication and the human visual system (HVS) are applied to create a robust WM system. The proposed design embeds a logo (used as a watermark) in uncompressed and compressed video stream efficiently. Performance is tested under real time conditions, using a video stream with a rate of 6 Mbits/sec and 65 bits/frame watermark sequence. They also claim that it could be combined with an MPEG encoder in a System-On-Chip (SOC) design to achieve real time intellectual property protection on digital video capturing devices.

To conclude, there is still much to be accomplished in the field of video WM hardware implementations. There are many potential applications and still not enough solutions at hand. The existing work is mainly focused on the adaptation of watermarking algorithms that were originally designed for still images software watermarking to the requirements of video and hardware. It is a great opportunity for new innovative watermarking solutions, specifically designed to accommodate the requirements of video applications including compression standards and real time operation.

4. Hardware-based Video WM Design – A Development Methodology

In this section, we present a development methodology to design a hardware-based video WM system. Although our end goal is to implement the whole system monolithically on a single chip, it is expected that more than one prototype will be designed before a final version is issued. Therefore, it is worthwhile to first focus on determining the core elements of the system which include six functionality modules, such as video camera, watermark compressor, watermark generator, watermark embedder, control unit and memory, as well as the interface between them. A top view of a general scheme for the developed solution is depicted in Figure 11.

To improve the overall performance of the design, the expected system architecture should be designed to make most computational operations performed with temporal parallelism (using pipelining) and spatial parallelism (using parallel hardware).

Field-programmable gate array (FPGA) devices can be used to implement any logical function that an application-specific integrated circuit (ASIC) could perform [25]. The basically building blocks of many FPGA architectures are the programmable logic components that can be configured to perform logical functions and memory elements for data storage. Currently, the high density techniques of FPGA devices have been successfully used to build entire system on a single chip [26]. As they provide significant features in terms of high performance, efficient implementation, lower development cost and flexibility, it make them to be a highly attractive solution for hardware implementation of real-time video WM system. Here, a FPGA will be chosen to implement a prototype chip of the proposed video WM system, of which the FPGA implementation parts are shown in shady blocks as shown in Figure 8. Finally, the overall performances of the hardware implementation using FPGA can be evaluated by

performing experiments (offline and real-time with a CMOS image sensor) on the custom versatile breadboard described below.

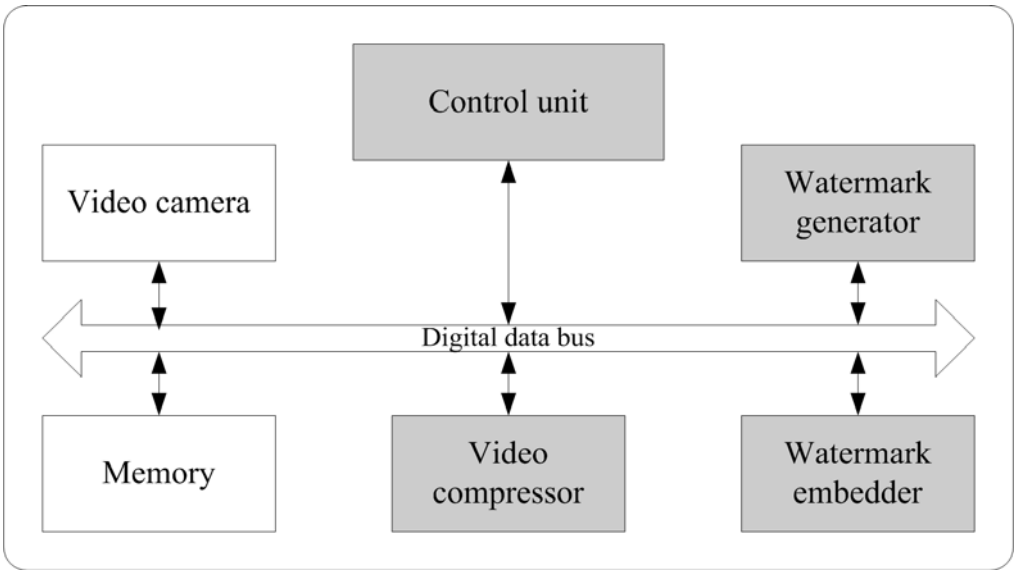

Figure 11. A general scheme of the video WM system.

The specifically designed board emulates a System-On-a-Chip (SoC) platform, allowing the incorporation of custom VLSI designs (such as the image sensor) with peripheral elements and digital logic implemented on an FPGA device. It features low-noise, separated digital and analog power supplies, 12 bit analog voltage and current biasing, 12 and 18 bit A/D converters, an SRAM memory and several I/O ports including LVDS, RS-232 and direct test points for maximum testing flexibility. The designer can choose what part of the system he wants to implement in VLSI and what elements he would use of those available on board. For the discussed digital video WM system implementation a basic imager is first designed, and then the WM modules including video compressor, watermark generator and embedder and control unit are implemented on the FPGA, together with all other required control logic, making use of the A/D converter and SRAM memory to aid the implementation of more complex algorithms. Therefore, the captured video stream can be watermarked at the origin such that the system security is improved as it is certain that the video data entering the system is untouched by any external party. Finally, the compressed watermarked video stream can be sent to SRAM memory for storage or transmitted to the host PC through the frame grabber for performance analysis.

5. Conclusions

In this paper, an in-depth overview of previous works on the field of digital video WM techniques was provided in order to provide help for further research works. Common WM classification criterions and requirements, including

general properties and specific constrains for video WM scheme, has been analyzed. Furthermore, various applications of video WM in practice were discussed, as well as the comparisons between software-based and hardware-based implementations from several points of view: major advantages, drawbacks and differences. Four examples of previous software and hardware WM implementations were also shown. In addition, a development methodology for hardware WM implementations including the general scheme of a proposed digital video WM system and its testing using the custom versatile breadboard were described.

Bibliography

[1] V. M. Potdar, S. Han, E. Chang, "A survey of digital image watermarking techniques", 3rd IEEE International Conference on Industrial Informatics (INDIN '05), Aug. 2005, pp. 709- 716

[2] Piva A. & Barni M., “managing Copyright in Open Networks,” IEEE Internet Computing, MAY-June 2002.

[3] S. P. Mohanty, "Digital Watermarking: A Tutorial Review",
URL: http://www.csee.usf.edu/~smohanty/research/Reports/WMSurvey1999Mohanty.pdf

[4] Frank Hartung, and Bernd Girod. “Watermarking of Uncompressed and Compressed Video,” IEEE Transactions on Signal Processing. Vol. 66, No. 3, May 1998, pp. 283 - 302.

[5] T.L. Wu, S.F. Wu, “Selective encryption and watermarking of MPEG video,” International Conference on Image Science, Systems, and Technology, CISST’97, June 1997.

[6] Ambalanath Shan, and Ezzatollah Salari, “Real-Time Digital Video Watermarking,” 2002 Digest of Technical Papers: International Conference on Consumer Electronics, June 2002, pp.12 – 13.

[7] F. Mintzer, G. Braudaway, and M. Yeung, “Effective and ineffective digital watermarks,” in proc. IEEE Int. Conf. Image Process., vol. 3, 1997, pp. 9-12.

[8] Chiou-Ting Hsu, and Ja-Ling Wu, “Digital Watermarking for Video,” 13th International Conference on Digital Signal Processing Proceedings, DSP 97. Vol. 1, July 1997 pp. 217 – 220.

[9] Christoph Busch, Wolfgang Funk, and Stephen Wolthusen, “Digital Watermarking: From Concepts to Real-Time Video Applications”. IEEE Computer Graphics and Applications. Vol. 19, Issue 1, Jan.-Feb. 1999. pp. 25 – 35.

[10] 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,” IEE Proc. Vision, Image Signal Processing, vol. 147, no. 4, pp. 371–376, Aug. 2000.

[11] Nebu John Mathai, Ali Sheikholesami, and Deepa Kundur, “Hardware Implementation Perspectives of Digital Video Watermarking Algorithms”, IEEE Transactions on Signal Processing. Vol. 51, Issue 4, April 2003. pp. 925 - 938.

[12] Nebu John Mathai, Ali Sheikholesami, and Deepa Kundur, “VLSI Implementation of a Real-Time Video Watermark Embedder and Detector”. Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS '03. Vol. 2, May 2003 pp. II772 - II775.

[13] Tsai, T.H., Wu, C.Y, “An Implementation of Configurable Digital Watermarking Systems in MPEG Video Encoder,” In: Proc. of Intl. Conf. on Consumer Electronics. (2003) 216–21

[14] Maes, M., Kalker, T., Linnartz, J.P.M.G., Talstra, J., Depovere, G.F.G., Haitsma, J, “Digital Watamarking for DVD Video Copyright Protection,” IEEE Signal Processing Magazine 17 (2000) 47–57.

[15] Sin-Joo Lee, and Sung-Hwan Jung, "A survey of watermarking techniques applied to multimedia". IEEE International Symposium on Industrial Electronics, Korea, June 2001. Vol. 1, pp. 272 – 277.

[16] Y. Shoshan, A. Fish, X. Li, G. A. Jullien, O. Yadid-Pecht, "VLSI Watermark Implementations and Applications," IJ Information and Knowledge Technologies, Vol.2, 2008.

[17] Watermarking World, http://www.watermarkingworld.org.

[18] 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.

[19] G. Doërr and J.-L. Dugelay, "A guide tour of video watermarking," Signal Processing: Image Commun., vol. 18, no. 4, pp. 263–282, Apr. 2003.

[20] M. Barni, F. Bartolini, J. Fridrich, M. Goljan, and A. Piva, "Digital watermarking for the authentication of AVS data," in EUSIPCO00, 10th Eur. Signal Processing Conf., Tampere, Finland, Sept. 2000.

[21] F. Bartolini, A. Tefas, M. Barni, and I. Pitas, "Image authentication techniques for surveillance applications," Proc. IEEE, vol. 89, no. 10, pp. 1403–1418, Oct. 2001.

[22] ISO/IEC 13818-2:1996(E), "Information Technology – Generic Coding of Moving Pictures and Associated Audio Information" , Video International Standard, 1996.

[23] K, Jack, "Video Demystified: a handbook for the digital engineer," 2rd ed., LLH Technology Publishing, Eagle Rock, VA 24085, 2001.

[24] Andrey Filippov, "Encoding High-Resolution Ogg/Theora Video with Reconfigurable FPGAs," in Xcell Journal. Second Quarter 2005.

[25] B. Shackleford, G. Snider, R. J. Carter, E. Okushi, M. Yasuda, K. Seo, and H. Yasuura, "A high-performance, pipelined, FPGAbased genetic algorithm machine," Genetic Programming and Evolvable Machines, vol. 2, no. 1, pp. 33–60, March 2001.

[26] S. O. Memik, A. K. Katsaggelos, and M. Sarrafzadeh. "Analysis and FFGA Implementation of Image Restoration Under Resource Constrain," IEEE Trans. on Computers, VoL52. N0.3, Mar. 2003.

Authors' Information

Xin Li – ISL lab, ATIPS lab, ECE Department, University of Calgary, Calgary AB, Canada; e-mail: xinli@atips.ca

Yonatan Shoshan – ISL lab, ATIPS lab, ECE Department, University of Calgary, Calgary AB, Canada; e-mail: shoshayi@atips.ca

Alexander Fish – ISL lab, ATIPS lab, ECE Department, University of Calgary, Calgary AB, Canada; e-mail: fishi@atips.ca

Graham Jullien – ISL lab, ATIPS lab, ECE Department, University of Calgary, Calgary AB, Canada; e-mail: jullein@atips.ca

Orly Yadid-Pecht – ISL lab, ATIPS lab, ECE Department, University of Calgary, Calgary AB, Canada;

The VLSI Systems Center, Ben-Gurion University, Beer-Sheva, Isreal; e-mail: orly@atips.ca