HARDWARE IMPLEMENTATIONS OF VIDEO WATERMARKING

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

Abstract: Various digital watermarking (WM) techniques for still imaging have been studied in the last several years. Recently, many new WM schemes have been proposed for other types of digital multimedia data, such as text, audio and video. This paper presents a brief overview of existing digital video WM. We classify WM techniques and discuss the properties of video WM. Since each WM application has its own specific requirements, WM design must take the intended application into consideration. Video WM applications are also discussed in the paper. The features of video WM implementations in software and hardware and their differences are presented through the description of four examples of existing work.

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

ACM Classification Keywords: B.0 Hardware - Conference proceedings

Conference: The paper is selected from Sixth International Conference on Information Research and Applications – i.Tech 2008, Varna, Bulgaria, June-July 2008

1. Introduction

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 and integrity of video content. Till date, there have been various such techniques [2], of which digital watermarking (WM) is one of the most popular. Digital WM is a technique that embeds a secret, unnoticeable signal (called watermark) into the original multimedia object, like audio, image and video. The watermark can be detected or extracted later to claim the authenticity of the media content.

Several researchers have investigated digital WM with different contributions, implemented both on software and hardware platforms [3]-[11]. 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.

Although it might be easier to implement a WM algorithm on a software platform, there is a strong motivation for a move toward a hardware implementation [8]. The hardware implementation offers several distinct advantages over the software implementation in terms of low power consumption, less area usage and reliability. It features real time capabilities and compact implementations. 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. Recently, a few hardware specific algorithms have been presented in the literature [7]-[11].

The objective of this paper is to provide an overall review of existing digital video WM solutions and applications. Background on video WM, such as different watermark classifications, applications and specifications are introduced. Following that, existing WM software and hardware implementations are also described.

The rest of the paper is organized as follows. Section II reviews the background on video WM. The WM software and hardware implementations are presented in section III. Conclusions are summarized in section IV.

2. Background on Video WM

2.1 Watermarks Classification

WM techniques can be divided into different categories according to various criterions [12]. The general classification of the currently available watermarks is shown in Figure 1. In [13] 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 video if the individual frames are treated as images [14]. However, contradictory to still image WM techniques, the video WM methods usually require that the WM encoding and decoding are processed in real time.

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 a simple addition of a small amplitude pseudo-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. The frequency domain methods are more robust than the spatial domain techniques [15].

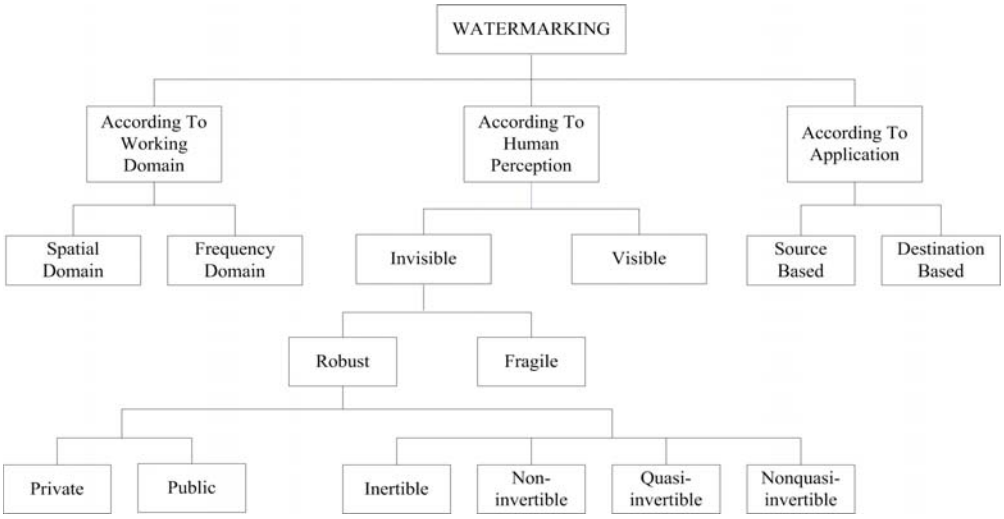

Figure 1 General classification of existing watermarking.

WM techniques can also be divided into three different types: visible, invisible robust and invisible fragile, according to human perception. Different applications have different requirements. Sometimes a certain application requires a WM to be visible, so that the embedded watermark appears visible to a casual viewer. Invisible robust WMs are primarily used in applications such as copyright protection, which require the algorithm to be as robust as possible so that severe modifications and degradations cannot remove the watermark. Conversely, invisible fragile is designed to reflect even slightest manipulation or modification of the media data, since the embedded watermark can easily become altered or destroyed after common attacks, such as lossy compression, cropping and spatial filtering. This WM method is a practical technique for content authentication.

From the application point of view, digital WM could be source based or destination based [12]. 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 watermarking applications are considered in the open literature and as commercial applications [16]. The reader is referred to [16]-[18] for a more thorough investigation. The applications presented have been gathered 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.

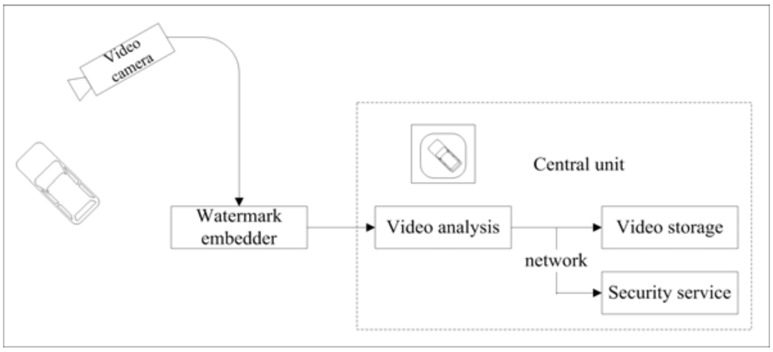

Figure 2 WM-based authentication for automatic VS.

In Figure 2, a sketch of a simple video surveillance (VS) system, in which WM is used to authenticate VS data, is given [17], [18]. 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.

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 3.

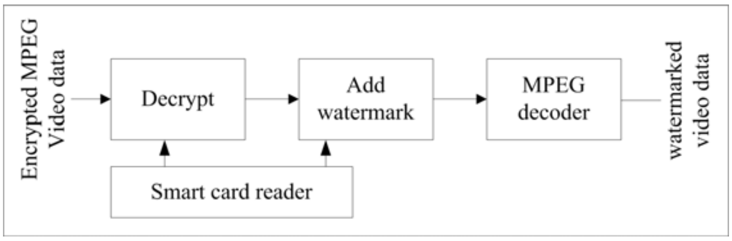

Figure 3 Set-top box with WM capabilities.

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 the copy protection scheme using WM techniques shown in Figure 4, consumers can make copies of any original source, but they cannot make copies of copies.

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.

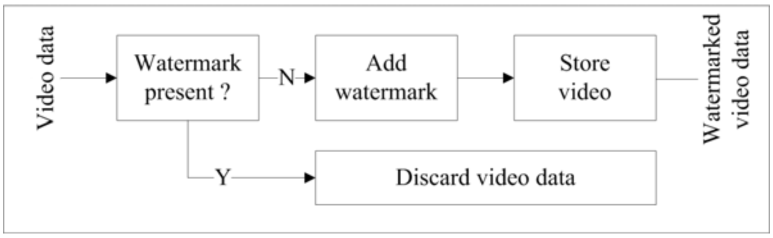

Figure 4 Video recorder with copy protection.

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

Similar to image WM implementations, the video WM system can be implemented in either software or hardware, each having advantages and drawbacks. In software, 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. By 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. However, such an implementation is relatively slow and therefore not suitable for real time applications.

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 can minimize computational demanding operations. Furthermore, frequency domain WM methods are more robust than the spatial domain techniques [15]. Therefore, working on compressed rather than uncompressed video is important for practical WM applications.

Before we describe the video WM techniques, we first briefly review the standards for video compression. 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 [19]. 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.

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.
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 [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 I 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.

3.1 Hardware Implementations

Over the last decade, numerous software WM algorithms have been invented [12]. However, WM implementation in hardware, especially for video stream, is a recent interest in the area. Prior to 1999, no work on video WM implementation in hardware had been shown [8]. However, the watermarking of video streams in real-time applications is mostly suitable for hardware implementations, thus motivating research efforts to that direction.

The implementation of hardware WM is usually done on custom-designed circuitry, i.e. application specific integrated circuits (ASICs) or field programmable gate arrays (FPGAs). The overall advantage of this scheme over the software implementation is in terms of lower power consumption, reduced area and reliability. It may 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.

For example, in 2000, Strycker et al. proposed a real time video WM scheme, called Just Another Watermarking System (JAWS), for television broadcast monitoring [7]. JAWS is a well-known video WM algorithm and because it works on uncompressed real time video data, the author was allowed to concentrate on the watermark process and not on the compression issues. 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 [8], [9]. 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 both spatial and transform domains is presented by Tsai and Wu [10]. In this scheme, the concepts of spread spectrum from the field of communications 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 streams 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. Conclusions

In this paper, background on video WM techniques was provided. Common WM classification criterions and requirements, including general properties and specific constrains for video WM scheme, were presented. Various applications of video WM were discussed. Comparisons between software and hardware implementations have been presented from several points of view: major advantages, drawbacks and differences. Four examples of previous software and hardware WM implementations were also shown.

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] 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.

[8] 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.

[9] 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.

[10] 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

[11] 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.

[12] 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.

[13] 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.

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

[15] 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.

[16] 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.

[17] 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.

[18] 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.

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

Authors' Information

Xin Lin – 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: fish@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, Israel; e-mail: orly@atips.ca