*2011 International Conference on Signal, Image Processing and Applications*
*With workshop of ICEEA 2011*
*IPCSIT vol.21 (2011) © (2011) IACSIT Press, Singapore*

# An Overview of Hardware Implementation for Digital Image Watermarking

Mustafa Osman Ali [1] and Rameshwar Rao [2]

Department of Electronics and Communication Engineering, College of Engineering, Osmania University, Hyderabad, India

[1] E-mail: elexman93@gmail.com , [2] E-mail: Rameshwar_rao@hotmail.com

**Abstract.** The increasing amount of applications using digital multimedia technologies has accentuated the need to provide copyright protection to multimedia data. This paper reviews watermarking techniques, by focusing on the hardware based implementation of digital image watermarking. Digital watermarking is an authentication method that has received a lot of attention in the past few years. Through this paper we will survey some digital image watermarking schemes which have been implemented by using hardware techniques. Also the study shows the similarities and differences between different types and then assesses the benefits gained from the use of this technology.

**Keywords:** base-image, DCT, DWT, fragile, invisible, robust, spatial domain, visible, watermark.

## 1. Introduction

Within the fast increasing developments of the internet in the recent years, a parallel developments in the need to create, copy, transmit, and distribute digital data especially multimedia (images, audio, and video) has also increased. Therefore authors are worried to distribute their work in fear that it may be used illegally through proliferation of the *World Wide Web* (WWW). Consequently, this has led to a strong demand for reliable and secure copyright protection techniques for digital data.

There are three basic methods of secure communication available, namely, cryptography, Steganography and watermarking [1]. Among these three, the first one, cryptography, deals with the development of techniques for converting information between intelligible and unintelligible forms during information exchange that deals with the content confidentiality and access control. By using cryptography, only authorized parties holding decryption keys can access the content (text or image). It provides the tools to secure sensitive information. Steganography, on the other hand, is a technique for hiding and extracting information to be conveyed using a carrier signal. The third one, watermarking is a means of developing proper techniques for hiding proprietary information in the perceptual data.

## 2. Digital Watermarking

Digital watermarking is applied for copyright protection, content authentication, detection of illegal duplication and alteration, feature tagging and secret communication. Digital watermarking is used in the hiding of a secret message or information within an ordinary message and its extraction at its destination. The secret message embedded as watermark can be almost anything, for example: a serial number, plain text, image, etc. In general, digital watermarking involves two major operations: (i) Watermark embedding, and (ii) Watermark extraction. For both operations a secret key is needed to secure the watermark [1-5]. The keys in watermarking algorithms can be applied in the cryptographic mechanisms to provide more secure services to copy right protection.

The most important properties of any digital watermarking techniques are robustness, security, imperceptibility, complexity, and verification [1-4]. Robustness is defined as if the watermark can be detected after media operations such as filtering, lossy compression, color correction, or geometric

modifications. Security means that the embedded watermark can't be removed beyond reliable detection by targeted attacks. Imperceptibility means that the watermark is not seen by the human visual system. Complexity is described as the effort and time required for watermark embedding and retrieval. Lastly, verification is a procedure whereby is used as a private key or public key function. Each of these properties must be taken into consideration when applying a certain digital watermarking technique [3].

Watermarking techniques can be classified according to the nature of data (text, image, audio or video), or according to the working (spatial or frequency) domain, also they can be classified according to the human perception (robust or fragile) [4]. In images, the watermarking techniques can be broadly classified into three types: (i) Visible watermark, (ii) Invisible fragile watermark and (iii) Invisible robust watermark [3,4], which has wider currency and use. However all these mentioned classes can be applied by using software, hardware or both together.

## 3. Hardware Versus Software

A watermarking system can be implemented with either software or hardware. The software implementation of the watermarking algorithms is significantly large, whereas the hardware implementation of the algorithms is lacking [6]. In a software implementation, the algorithm's operations are performed as code running on a microprocessor [7]. This code should be stored in a memory e.g. RAM and require a dedicated processor that occupies more area, consumes significantly more power, and may still not perform adequately fast. The authors of [7] believe that software-based watermarking provides the following:

- Abstraction of the implementation from any hardware details.
- Availability of software tools to aid in realizing various data operations.
- Limited means of improving area and improving time complexity (speed) of the implementation.

Although it might be faster to implement an algorithm in software, there are a few compelling reasons for a move toward hardware implementation. In a hardware implementation the algorithm's operations are fully implemented in custom-designed circuitry. This investigates great advantages such as reduce hardware scheme area, decrease power consumption and increase speed of performance [6-9]. Therefore a hardware watermarking solution are often more economical.

## 4. Spatial Domain Versus Frequency Domain

A watermarking scheme can be implemented in either spatial domain or frequency domain. The most straightforward fundamental schemes for the fields of digital watermarking are watermarking in the spatial domain. This technique has started long time ago by designing the embedding and extraction algorithms to modify the luminance values of the pixels in the spatial domain. The most common simplest watermarking technique in the spatial domain is done by manipulating the *Least Significant Bit* (LSB) overall pixels. The watermark to be embedded is placed in the LSB of the base-image. Spatial domain is less complex as no transform is used, but isn't robust against attacks [3-5].

For better imperceptibility as well as robustness, the insertion of the watermark is done in a frequency domain. Many transform formats are available; mainly *Discrete Cosine Transform* (DCT) and *Discrete Wavelet Transform* (DWT) are widely used. In this technique (Frequency Domain) the watermark actually spread throughout the image, not just operating on an individual pixel. Wavelet-based watermarking methods exploit the frequency information and spatial information of the transformed data in multiple resolutions to gain robustness. DWT is closer to the *Human Visual System* (HVS) since it splits the input image into several frequency bands that can be processed independently. It's a multi-resolution transform that permits to locate image features such as smooth areas, edges or textured areas [3,4]. DWT based implementation needs to store results at each level of computation, so the memory requirement increases. This is one of the reasons for higher area requirement compared to DCT based approaches [10].

Generally, hardware watermarking scheme can be done by using each of the domains (spatial or frequency). But due to the simplicity of spatial domain computational overhead and its easiness for its application if compared to the frequency domain, the spatial domain is usually preferred for hardware implementation [5, 6, 8, 9].

## 5. Hardware Digital Image Watermarking Schemes

Any digital watermarking scheme requires two algorithms; embedding algorithm and extraction algorithm. Embedding algorithm acts as an *encoder* in hardware applications, while extraction algorithm represents a *decoder*. All the authors who were mentioned through this survey highlighted the (embedding and/or extraction) algorithms in the beginning of their works with full details due to the importance of these algorithms in which they are the backbones of their works. Most of the authors have taken ready algorithms made by others to be converted to hardware schemes. However, few authors have recommended their own algorithms and then converted to the hardware applications. Since the interest of this survey is in digital image watermarking hardware implementation, browsing of authors' works through it will be classified into:

- Chip implementation.
- Digital camera implementation.

### 5.1. Chip Implementation

Several watermarking algorithms have been proposed for securing digital image in the current literature. Here is a brief browsing of chips implementation to execute secure watermarking algorithms. Authors of [5, 6, 8,11] have implemented chips capable to execute successfully watermarking in spatial domain of the original image.

In [6,11] authors have gently laid out full designs for digital image watermarking algorithms built on VLSI chips such as shown in figure (1). These designs have been implemented and tested by using different VLSI technologies. Design of the [6] developed hardware system that can insert both robust and fragile invisible watermark in the image. This design is built by depending on three algorithms taken from different authors [12-14]. The [12,13] are invisible-robust algorithms proposed by A. Tefas and I. Pitas, where the third one proposed by Mohanty and his work team in [14] for invisible-fragile algorithm. The results of [6] confirmed that the designed chip can perform invisible robust, invisible fragile watermarking and combination of both in spatial domain, and the chip can easily be integrated in any existing *Joint Photographic Experts Group* (JPEG) encoder to watermark the images right at the source end. The same authors have modified their works by using different algorithms for implementing two different visible watermarking schemes for images. These modifications are presented clearly in [15].

The chip which is designed in [11] implemented an *Application Specific Integrated Circuit* (ASIC) for digital color image watermarking. Here the RGB color image is transformed to YUV and intensity values of luminance are modified in spatial domain and transformed back to RGB. This operation has been implemented as a hardware scheme by converting a watermarking algorithm proposed in [16] by the same authors of [11]. This design has implemented in 0.13μm CMOS 6-metal technology.

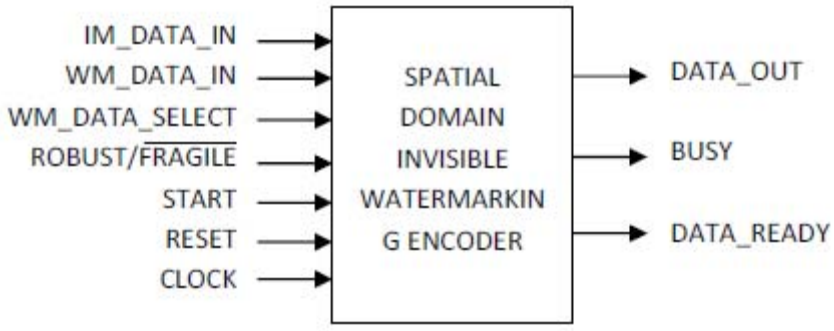


Fig. 1: Pin diagram for proposed watermarking chip in [6].

A new technology used in [5] called *Single Electron Tunneling* (SET) devices, where device size is very small and have ultra low power dissipation capabilities. Through [5] authors gave clear illustration for their algorithm and its implementation details. They have described SET based circuit operation and then illustrated the SET device based architecture for each unit. The results of that work denoted the low cost data embedding algorithm can conceal watermark into original image coming from a sensor much faster than software implementation and the embedded image is easily transmitted to PC by using proper interface.

Most popular and useful technology for implementing hardware designs is *Field Programmable Gate Array* (FPGA)[1],Work of [8] has applied and tested successfully in FPGA (Xilinx ISE 10.1i) model. Full design for spatial domain watermark encoder and decoder has implemented in [8], whereby authors approved reliability of digital image hardware watermarking versus software one.

Challenge of hardware digital image watermarking also includes frequency domain watermarking, such as the experiments which have done into [17] and [18]. For [17], authors presented the VLSI architecture of a watermarking chip and its implementation using TSMC 0.25- m CMOS technology. The chip is capable to insert both visible and invisible watermarks into an image. Dual-voltage, clock gating and dual-frequency techniques were used in that design for low power optimization along with a certain degree of pipelining and parallelism. The [17] authors believe that their design is the first hardware design with the capability to perform both visible and invisible watermarking in the DCT domain (at that time).

Authors of [18] proposed a hardware/software co-design approach for the implementation of a DCT-based visible watermarking algorithm. They have designed their work by implementing the processes that demand high performance in hardware, while those that are not computationally expensive are implemented in software. As a result, power consumption is reduced since only portion of the algorithm is implemented in hardware. Their system was implemented on the Xilinx Virtex-II Pro Board, using the *Xilinx Platform Studio* (XPS). The design allows tradeoff between hardware and software implementation which is not present when a pure software or hardware is used.

## 5.2. Digital camera implementation

A digital camera is a portable device to capture an image frame from scene and store it on the flash memory. An authentication digital camera is a camera with built-in copyright protection and security mechanism for images produced by it. [10,19,20] have presented various secure digital camera models.

Hyun Lim and his team in [19] have proposed an FPGA implementation of a watermarking-based authentication algorithm for a digital camera to authenticate the captured image frame. Their experimental results showed that the FPGA implemented watermarking algorithm could embed the watermark into the captured image coming from a sensor much faster than the software-based implementation and the quality of an embedded image was also comparable to the one implemented by the software algorithm. This scheme consists of three main parts: image capture and LCD controller, watermark imbedding part, and camera control unit. Figure (2) shows the FPGA implementation block diagram of the proposed scheme.

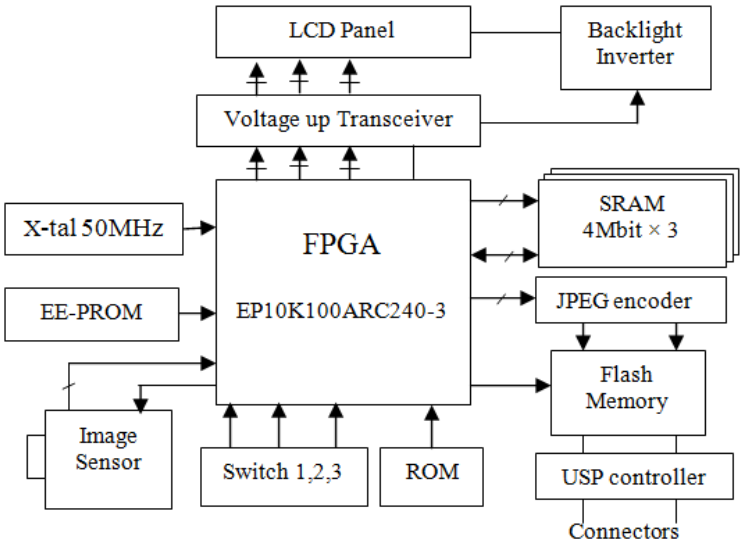


Fig. 2: The block diagram of an FPGA implementation for a secure digital camera in [19]

[1] (FPGAs) are digital integrated circuits (ICs) that contain configurable blocks of logic along with configurable interconnects between these blocks. Design engineers can configure such devices to perform a tremendous variety of tasks [8].

In [20] a prototype of a secure digital camera implementation for DCT based visible watermarking algorithm has proposed. This prototype consists of image sensor, A/D convertor, temporary memory, watermarking unit, controller unit, flash memory, and LCD panel. The authors in [20] focused their efforts to design and implement watermarking unit while the rest of the units of the camera are being carried out in their on-going research.

In [10] DWT based implementation is used to develop a feasible and invisible watermark embedding hardware for the secure digital camera. The proposed scheme of the secure watermarking has described using Verilog HDL, and synthesized using 0.18µm technology UMS standard cell library for VLSI implementation. Authors have suggested a bind watermarking algorithm and then tested it using MATLAB before synthesis for hardware implementation. The algorithm has been evaluated under the various attacks like JPEG compression, noise, scaling and rotation to verify robustness and invisibility properties.

## 6. Analysis and Discussion

Investigation of this survey proves that it is possible to have digital image watermarking in real time using hardware implementation. Also hardware implementation has occupied a valuable range of applications due to its economical features, in spite of the flexibility features of software implementation. Table (1) gives a summary of the proposed schemes which have been browsed in this survey. The first column recognizes the sequence of the schemes as mentioned during this paper and the symbol (-) indicates missing information which hasn't mentioned by the authors in the specified scheme.

## 7. Conclusion

Different hardware architectures for implementing secure watermarking algorithms proposed by different authors has discussed through this paper. These architectures have implemented by using different tools of VLSI technologies and they have achieved positive results. Great advantages are gained due to using hardware based implementation of watermarking algorithms, such as reduce hardware scheme area, decrease power consumption and increase speed of performance. Therefore a hardware watermarking solution is often more reliable and economical.

Table 1: A Summarize of the Proposed Schemes.

| Proposed Scheme | Domain | Visibility | Human Perception | Chip/Camera | Hardware Technology | Hardware Features |
|---|---|---|---|---|---|---|
| [6] | *Spatial* | *Invisible* | *Robust/Fragile* | *Chip* | *0.35µmCMOS* | -Low power<br>-High performance |
| [15] | *Spatial* | *Visible* | - | *Chip* | *Hardware Simulation* | -High performance |
| [11] | *Spatial* | - | *Fragile* | *Chip* | *0.13µmCmos 6 metal DSM* | -Low power<br>-High performance<br>-Small area |
| [5] | *Spatial* | *Invisible* | *Robust* | *Chip* | *SET devices* | -Low power<br>-Small area<br>-Low cost |
| [8] | *Spatial* | *Invisible* | *Robust* | *Chip* | *Xilinx Spartan (2s50tq144-6)* | -Low power<br>-Reliability<br>-Real time |
| [17] | *DCT* | *Visible/ Invisible* | - | *Chip* | *TSMC 0.25µm CMOS* | -Low power |
| [18] | *DCT* | - | *Robust* | *Chip* | *Xilinx Vertix-II* | -Low power |
| [19] | *DCT* | - | - | *Camera* | *EP10K100ARC240-3* | -Low power<br>-Small area |
| [20] | *DCT* | *Visible* | - | *Camera* | *Xilinx ISE 8.1i* | -Low power<br>-High performance<br>-Small area |
| [10] | *DWT* | *Invisible* | *Robust* | *Chip* | *0.18µm UMC* | -Low power<br>-High performance<br>-Small area |

## 8. References

[1] N. S. Kulkarni, I. Gupta, and S. N. Kulkarni. A Robust Image Encryption Technique based on Random Vector. In IEEE Computer Society. *proc. of IEEE 1st International conference on Emerging Trends in Engineering and*

*Technology*. 2008. pp.15-19.

[2] C. Rey, and Jean-Luc Dugelay. A Survey of Watermarking Algorithms for Image Authentication. *In EURASIP Journal on Applied Signal Processing*. 2002. pp. 613–621.

[3] J. Pan, H. C. Huang, and L. C. Jain. Intelligent Watermarking Techniques. World Scientific, 2004.

[4] S. Jayaraman, S. Esakkirajan, and T. Veerakumar. Digital Image Processing. McGraw-Hill, 2009.

[5] D. Samanta, A. Basu, T. S. Das, V. H. Mankar, A. Ghosh, M. Das, and S. K Sarkar. SET Based Logic Realization of a Robust Spatial Domain Image Watermarking. In IEEE(ICECE ). *proc. of 5th International Conference on Electrical and Computer Engineering*. Dhaka, Bangladesh. 2008. pp. 986-993.

[6] S. P. Mohanty, N. Ranganathan, and R. K. Namballa, "VLSI Implementation of Invisible Digital Watermarking algorithms Towards the Developement of a Secure JPEG Encoder," in Proc. of the IEEE Workshop on Signal Processing Systems, 2003, pp. 183-188.

[7] N. J. Mathai, D. Kundur, and A. Sheikholeslami. Hardware Implementation Perspectives of Digital Video Watermarking Algorithms. In MATHAI et al.: Hardware Implementation Perspictives of Digital Video Watermarking Algorithms. *Proc of IEEE Transaction on Signal Processing*. 2003, 51(4): pp. 925-938.

[8] A. Basu, T. S. Das, S. Maiti, N. Islam, and S. K. Sarkar. FPGA Based Implementation of Robust Spatial Domain Image Watermarking Algorithm. *Proc. in International Conference on Computers and Devices for Communication.* 2009.

[9] A. Basu, T. Das, S. Sarkar, A. Roy and N. Islam. FPGA Prototype of Visual Information Hiding. IEEE. 2010.

[10] A. Darji, A.N.Chandorkar, S.N. Merchant, and V. Mistry. VLSI Architecture of DWT based Watermark Encoder for Secure Still Digital Camera Design. In IEEE Computer Society. *proc. of Third International Conference on Emerging Trends in Engineering and Technology*. 2010.pp. 760-764.

[11] A. Garimella, M. V. V. Satyanarayana, P.S. Murugesh, and U.C. Niranjan. ASIC for Digital Color Image Watermarking. *proc. of IEEE 11th Digital Signal Processing Workshop and IEEE Signal Processing Education Workshop.* 2004. pp. 292-296.

[12] A. Tefas and 1. Pitas. Robust Spatial Image Watermarking Using Progressive Detection. *proc. of lEEE International Conference on Acoustics, Speech. and Signal Processing*. 2001.(vol. 3). pp. 1973-1976.

[13] M. Barni F. Bartolini, A. Tefas and I. Pitas. Image authentication techniques for surveillance applications. *proc. of IEEE*. 2001, 89(10): pp. 1403-1418.

[14] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli. A Dual Watermarking Technique for Images. *In proc. of 7th ACM International Multimedia Coifereiice (ACM-MM99) (part-2).* 1999. pp. 49-51.

[15] S.P. Mohanty, N. Ranganathan, and R.K. Namballa. A VLSI Architecture for Visible Watermarking in a Secure Still Digital Camera Design. *proc. of IEEE Trans. on VLSI Systems*. 2005. 13(8): pp.1-10.

[16] A. Garimella, M.V.V. Satyanarayana, R.S. Kumar, P.S. Murugesh, and U.C. Niranjan, VLSI Implementation of Online Digital Watermarking Technique with Difference Encoding for 8-Bit Gray Scale Images. *In Proc. IEEE 16th International Conference on VLSI Design*. New Delhi, India. 2003. pp.283-288.

[17] S.P. Mohanty, N. Ranganathan, and K. Balakrishnan. A dual Voltage-Frequency VLSI Chip for Image Processing in DCT Domain. proc. of IEEE Trans. on Circuits and Systems. 2006. 53(5): pp. 394-398.

[18] Y. Morita, E. Ayeh, O.B. Adamo, and P. Guturu. Hardware/Software Co-design Approach for a DCT-Based Watermarking Algorithm. proc. of IEEE. 2009. pp. 683-686.

[19] Hyun Lim, Soon-Young Park , Seong-Jun Kang, and Wan-Hyun Cho. FPGA implementation of Image Watermarking Algorithm for a Digital Camera. *proc. of IEEE*. 2003. pp. 1000-1003.

[20] O. Adamo, S. P. Mohanty, and E. Kougianos. VLSI Architecture and FPGA Prototyping of a Digital Camera for Image Security and Authentication. *proc. of IEEE*. 2006. pp. 154-158.