ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

Hardware Implementation of Watermarking – Importance and Survey

Swathi S[1], Shobhana S[1], Lakshmi H R[2]

U.G. Student, Department of ECE, K. S. Institute of Technology, Raghuvanahalli, Bengaluru, India

Assistant Professor, Department of ECE, K. S. Institute of Technology Bengaluru, India

ABSTRACT: The increasing amount of applications using digital multimedia technologies has accelerated 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, to achieve low-power, high performance, real-time, reliable and secure watermarking system. Through this paper we will survey some digital image watermarking schemes which have been implemented based on hardware techniques. Also the study shows the similarities and differences between different watermarking techniques. Hardware can be realized using FPGA (Field Programmable Gate Array), DSP (Digital Signal Processors) or custom VLSI architecture.

KEYWORDS: Real Time Implementation, Reversible Watermarking, Hardware vs Software.

I. INTRODUCTION

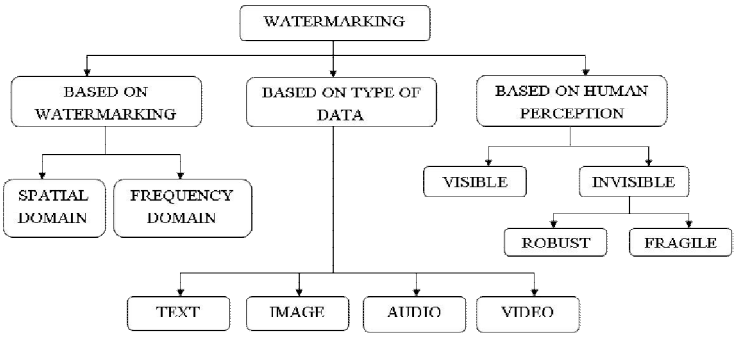

Fig. 1. Digital Watermarking Classification

Watermark is a secret message that is embedded into a message [1]. Digital watermarking is the method of hiding information in multimedia data i.e. video, audio or images, for the purposes of content protection or authentication. In digital image watermarking, the secret information i.e. the watermark is embedded into a cover image, in such a way that distortion of the cover image because of watermarking is almost perceptually negligible.

1. *Spatial and Frequency Domain Watermarking:* Spatial domain watermark algorithms insert watermark data directly into pixels of an image. Spatial domain interleaving is susceptible to noise. The image is transformed to the frequency domain and then the low frequency components are modified to contain the text or signal in frequency domain watermarking. As the watermarks applied to the frequency domain will be dispersed entirely over the spatial image upon inverse transformation, this method is not as susceptible to cropping as the spatial technique. However, there is more a tradeoff here between invisibility and decodability [4].Watermark techniques can be divided into four groups according to the type of data to be watermarked viz Text watermarking, Image watermarking, Video watermarking and Audio watermarking.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

2. *Visible and Invisible Watermarking:* Visibility is associated with perception of the human eye so that if the watermark is embedded in the data and can be seen without extraction, we call the watermark to be visible. Examples of visible watermarks are logos that are used in images and video. Invisible watermarking cannot be seen by the human eye. It is embedded in the data without affecting the content and can be extracted by the person who has right over it. Example of invisible watermarks is the images distributed over the internet [2].

3. *Robust watermarking:* Robustness is one of the properties of digital watermarking. A watermark algorithm is said to be robust if it can survive after common signal processing operations such as loss compression and filtering.

4. *Fragile watermarking:* A fragile watermark should be able to detect after there is any change in the signal and also possible to identify the signal before modification. This watermark is used for the authenticity or verification of original content [18].

5. *Reversible watermarking:* Reversible watermarking is a special kind of digital water marking. It not only assures the ownership of the original image but also completely recovers the original image from the watermarked image without any distortion. This feature is applicable in various areas such as medical as well as military images [19].

Reversible watermarking has to be robust against the intentional or non-intentional attacks. It should be imperceptible to avoid the attacks. Reversible data embedding is also called as lossless data hiding. It is a fragile technique in which the embedded data will mostly be destroyed by small distortions of the watermarked image. Reversible data embedding allows embedding a relatively large amount of data into an image in a way that the original image can be reconstructed from the watermarked image.

Section II discusses about the characteristics of watermarking. Importance of hardware implementation has been discussed in section III. The various hardware digital watermarking schemes are discussed in section IV. The comparison of various watermarking schemes has been discussed in section V.

II. CHARACTERISTICS OF WATERMARKING

These are the following important characteristics of Watermarking [4]:

1. *Transparency:* It is the perceptual similarity between the Watermarked image and the original image. The watermark should be imperceptible and it should not degrade the quality of the content. Sometimes the watermark is embedded to data in a way that can be seen without extraction. This is called as visible watermark. Examples of visible watermark are logos.
2. *Robustness:* A watermark algorithm is said to be robust if it can survive after common signal processing operations. This means that, it is detectable after common signal processing operations such as lossy compression, spatial filtering, translation, and rotation operations.
3. *Capacity:* A watermarking system must allow for a useful amount of information to be embedded into an image. The amount of information that can be embedded in a watermarked image is called data payload. Data payload means the number of bits encoded with the image.

4. *Security:* The watermark must withstand the attacks, aimed directly at the embedded information. It must not be possible for an attacker to delete the watermark. It must not be possible to retrieve or even modify the watermark without the knowledge of the secret watermark key.

III. IMPORTANCE OF HARDWARE IMPLEMENTATION

A watermarking system can be implemented using either software or hardware. The software implementation of watermarking algorithms is significantly large, whereas the hardware implementation of the algorithms is lacking [7]. In a software implementation, the algorithms operations are performed as code running on a microprocessor [8]. This code should be stored in a memory and require a dedicated processor that consumes significantly more power,

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

occupies more area, and may still not perform adequately fast. [8] software-based watermarking provides the following: (i) Availability of software tools for various data operations. (ii) Limited means of improving time complexity (speed) of the implementation and improving area. Although it might be faster to implement an algorithm in software, there are a few reasons for a move towards the hardware implementation. In hardware implementation the algorithm's operations are implemented in custom-designed circuitry. This provides advantages such as reduce hardware scheme area, increase speed of performance and decrease power consumption [7-10]. Therefore a hardware watermarking solution is more economical.

IV. HARDWARE DIGITAL IMAGE WATERMARKING SCHEMES

Digital watermarking scheme requires two algorithms namely embedding algorithm and extraction algorithm. Embedding algorithm acts as an encoder in hardware applications, while extraction algorithm represents a decoder.
In this paper, several watermarking algorithms have been proposed for securing digital image.

A. *Neighbour Mean Interpolation*

Sakthivel S.M et al [9] discuss the implementation of neighbour mean image interpolation technique for data hiding in grayscale images using a new VLSI architecture, as this mechanism will have a minimum computation complexity. In this data hiding process, the secret digital signature is hidden in the host image and analysed with the PSNR value and Payload capacity. The technique provides good visual quality with higher resolution at the cost of higher complexity (i.e. more number of neighbor pixels).
The proposed algorithm provides a robust, invisible, and real time high speed hardware implementation with the capability of resolving the privacy and piracy issues. Sakthivel S.M et al [9] propose FPGA implementation of data hiding (watermarking) and extraction algorithm in real time with its VLSI architecture. This algorithm does not create any changes in the host image and the watermark is invisible. The watermark can be extracted by reversing the embedding and interpolation mechanism.

B. *Difference Expansion using FPGA*

For the retrieval of the cover image at the decoder, it is necessary for lossless watermarking system. This can be solved using hardware implementation. Sudip Ghosh et al [10] focus mainly on the digital design with pipelined architecture of reversible watermarking algorithm based on Difference Expansion (DE). The three different digital architectures proposed are dataflow architecture, optimized dataflow architecture using pipelining and the modified architecture using pipelining. These designs are implemented on Xilinx based FPGA. To the best of our knowledge this is the first digital design and pipelined architecture for reversible watermarking using difference expansion.

C. *Reversible contrast mapping (RCM)*

Sudip Ghosh et al [11] discuss the implementation of reversible contrast mapping (RCM) based image watermarking algorithm using a fast FPGA (Field Programmable Gate Array) based architecture. The advantage of this architecture is fast clock-less encoder design and implementation which makes the design faster. The encoder module response time is independent of clock frequency, and thus the embedding of the watermark is possible as soon as the input is fetched. The schematic based design and implementation of the VLSI architecture has been done with Xilinx 14.1 on Spartan 3E FPGA family. This architecture provides low cost, high speed real time use of the proposed VLSI architecture. FPGA is used because of its advantages like reconfigurability, low cost and simpler design process is used for the hardware implementation.
It is used in real-time applications like digital cameras, medical and military applications. The hardware complexity of the decoder module is higher compared to the encoder module. The maximum clock frequency of the decoder is 45 MHz. The design is low cost, fast and easily implementable for real time watermarking.

D. *Rhombus Interpolation by Difference Expansion*

Santi P Maity et al [12] discuss the implementation of VLSI architecture of rhombus interpolation based reversible watermarking by difference expansion. This architecture has been implemented and tested on Xilinx Virtex-7 FPGA, Zynq SoC (System On Chip) and ultra-scale FPGA platforms. The system is used to embed and extract the copyright

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

protection for medical and military imaging applications. This is the first FPGA, SoC and Ultra-scale based watermarking VLSI architecture for improved rhombus interpolation by difference expansion method. This chip can be easily integrated in any existing JPEG encoder to watermark images with different FPGA, SoC and Ultra-scale FPGA families. Implementation on Xilinx FPGA gives very compatible and suitable result of the reversible watermarking system on chip. The drawback of this technique is the high power utilization. Thus low-power VLSI features, such as multiple supply voltages, dynamic clocking and clock gating must be used to reduce the power utilization. The results show the viability of low cost, high speed and real-time use of the proposed VLSI architecture.

E. *Weighted Median Prediction*

Sakthivel et al [13] propose a new VLSI architecture for watermarking greyscale images using weighted median prediction operation. This mechanism will have a minimum computation complexity. In this VLSI based data hiding process the secret digital signature is hidden in the host image, PSNR value and Payload capacity are analysed. The area, speed and power optimization is not possible in software implementation unlike hardware based watermarking [11]. The Effectiveness of the watermarking process is evaluated based on its imperceptible nature and payload capacity. This algorithm provides an invisible, robust and real time high speed hardware implementation.

F. *Discrete Fast Walsh Hadamard Transform (DFWHT)*

Sudip Ghosh et al [15] focus on the design of an improved Discrete Fast Walsh Hadamard Transform (DFWHT) domain digital image watermarking algorithm and its low complexity as well as fast hardware architecture implementation on Xilinx based (version 14.7 Virtex-7 series) FPGA.This is the first architecture for the corresponding algorithm. Both encoding and extraction algorithm have been verified using MATLAB R2013a.Greyscale and binary watermarks are used and only grayscale cover image of maximum size (256 x 256) is used. This algorithm and the architecture is applicable for both gray scale and binary watermarks. Hadamard and Hartley transforms provide higher resiliency at low quality compression compared to DCT and Wavelet transforms.
Walsh Hadamard transform for watermark shows better robustness for both JPEG and JPEG 2000 images. This algorithm provides the design of a new invisible, blind and robust (with respect to sharpening and scaling) image watermarking algorithm in DFWHT (Discrete Fast Walsh Hadamard Transform) domain along with its FPGA based implementation. The VLSI architecture for the implementation of the algorithm is simple and applicable for both binary and grayscale images. Thus the watermarking scheme is quite effective than the other architecture which are mostly applicable for binary image watermarking.

G. *Discrete Cosine transform*

Archana Aniyan et al [16] discuss the implementation of a discrete cosine transform (DCT) based blind watermarking method for digital images and its hardware implementation using Beagle Board. The results show that the developed method is robust against various attacks and potentially compatible with JPEG compression. For implementation, Beagle Board is used as the hardware with the support of OpenCV which is open source with a strong focus on real time applications. Implementation on Beagle Board makes the system cost effective with high performance. The DCT watermarking method can be tested for various attacks like filtering, sharpening, cropping, intensity value adjustment.

H. *Felics algorithm*

Priyadharshini J. et al [17] discuss the hardware implementation of a digital watermarking system that can insert invisible and visible watermark information into compressed image in real time application. Discrete cosine transform domain proposed so far are not robust to all possible attacks and multimedia data processing operations. Felics algorithm is a new watermarking and Fast Efficient Lossless JPEG Image Compression scheme that is proposed to optimize security. The proposed system was suitable for implementation using an FPGA and can be used as a part of an ASIC. In the current implementation, FPGA was the simple. It is used for real-time image data protection for example surveillance cameras.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

V. COMPARISON

Table. 1. Comparison of proposed scheme

Proposed scheme	Domain	Visibility	Human perception	Hardware technology	Hardware features
[9]	Spatial	Invisible	Robust	FPGA	High Visual Quality and Resolution
[10]	Spatial	Invisible	Robust	FPGA	Low cost, High Embedding Capacity, Simple Design
[11]	Spatial	Invisible	Robust	Xilinx 14.1 on Spartan 3E FPGA	Reconfigurable, Low Cost, Simple Design
[12]	Spatial	Invisible	Robust	Xilinx Virtex-7 FPGA	Low Cost, High Speed
[13]	Spatial	Invisible	Robust	FPGA	Minimum Computational Complexity
[15]	Spatial	Invisible	Robust	Xilinx(version 14.7 Virtex -7 series) FPGA	Simple Design
[16]	DCT	Invisible	Robust/Fragile	Beagle Board	Cost Effective and High Performance
[17]	Spatial	Invisible/Visible	Robust	FPGA and can be used as a part of an ASIC	Simple Design

VI. CONCLUSION

This survey paper shows that it is possible to have digital image watermarking in real time using hardware implementation. Hardware implementation has occupied a valuable range of applications due to its economical features, in spite of the flexibility features of software implementation. Though there are many hardware implementation schemes available, an optimal solution is yet to be formulated keeping the area, power and performance tradeoffs to a minimum.

REFERENCES

[1] B. Surekha, Lakshmi HR, "Asynchronous Implementation of Reversible Image Watermarking Using Mousetrap Pipelining", 6th IEEE International Advance Computing Conference (IACC - 2016), S R K R Engineering College, Bhimavaram, Andhra Pradesh, India, 27-28 February 2016.

[2] B. Surekha, P. Ravi Babu, G.N. Swamy, "Security analysis of a novel copyright protection scheme using visual cryptography, IEEE International conference on computing and communication technologies, Osmania University, Hyderabad, Dec. 11-13, 2014, pp.1-5.

[3] Mustafa Osman Ali , and Rameshwar Rao ,"An Overview of Hardware Implementation for Digital Image" ,2011 International Conference on Signal, Image Processing and Applications With workshop of ICEEA, pp. 90-95, 2011.

[4] Gaurav Gupta, Kanika Sharma, "Image watermarking and its hardware realization: a survey international journal of electrical and electronics engineering" IJEEE, Volume 2, Issue 4, pp. 20-31, 2015.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

[5] Nayak et al., "Simultaneous storage of medical images in the spatial and frequency domain: A comparative study", published in Bio Medical Engineering on Line, 2004, 3:17 [available online] http://www.biomedical-engineering- online.com/content/3/1/17 (as on 15/02/2015).
[6] Fabien AP, Petitcolas, Anderson Ross A, Kuhn Marcus G, "Information hiding: A Survey", Proceedings of the IEEE, pp. 1062-1077, 1999.
[7] Knopp R , Robert A, "Detection Theory and Digital Watermarking", Proceedings of SPIE, pp. 14-23, 2000.
[8] Langelaar G, Setyawan I, Lagendijk R, "Watermarking digital image and video data: a state-of-art overview", IEEE Signal Processing Magazine, Vol. 17, pp. 20-46, 2000.
[9] Sakthivel. S.M, Ravi Sankar, "A FPGA Implementation of Data Hiding in Grayscale Images using Neighbour Mean Interpolation", IEEE sponsored 2nd international conference on electronics and communication system , pp1124 – 1127, 2015
[10] Sudip Ghosh, Nachiketa Das, Subhajit Das, Santi P. Maity and Hafizur Rahaman, "Digital Design and Pipelined Architecture for Reversible Watermarking Based on Difference Expansion using FPGA", 2014 13th International Conference on Information Technology(ICIT) IEEE, pp. 123-128 ,2014.
[11] Sudip Ghosh, Bijoy Kundu, Debopam Datta, Santi P Maity and Hafizur Rahaman, "Design and Implementation of Fast FPGA Based Architecture for Reversible Watermarking", 2013 International Conference on Electrical Information and Communication Technology (EICT), pp. 1-6, 2013.
[12] Santi P Maity and Hafizur Rahaman Sudip Ghosh, Nachiketa Das, Subhajit Das, "FPGA and SoC Based VLSI Architecture of Reversible Watermarking Using Rhombus Interpolation By Difference Expansion",2014 Annual IEEE India Conference (INDICON) ,pp. 1-6,2014.
[13] Sakthivel, S.M. Ravi Sankar, "A VLSI Architecture for Watermarking of Grayscale Images using Weighted Median Prediction", IEEE sponsored 2 nd international conferences on electronics and communication system (ICECS 2015) ,pp. 1128-1131, 2015.
[14] P.Karthigaikumar, K.Baskaran, "FPGA and ASIC implementation of robust invisible binary image watermarking algorithm using connectivity preserving criteria", Microelectronics Journal 42, pp. 82-88, 2011.
[15] Sudip Ghosh, Arijit Biswas, Santi P Maity, Hafizur Rahaman, "Design of A Low Complexity and Fast Hardware Architecture for Digital Image Watermarking in FWHT Domain on FPGA",2014 Fifth International Symposium on Electronic System Design(ISED), IEEE 2012. Pp. 68-72, 2012.
[16] Archana Aniyan, Deepa .J, " Hardware Implementation of a Robust Watermarking Technique for Digital Images", 2013 IEEE Recent Advances in Intelligent Computational Systems (RAICS),pp. 293-298,2013.
[17] Priyadharshini J, R. S. Sabeenian, " Hardware Implementation of a Robust Watermarking Technique for Digital Images",2013 IEEE Recent Advances in Intelligent Computational Systems (RAICS) Electronics and Communication Systems (ICECS), 2014 International Conference ,pp. 1 – 4,2014.
[18] B.Surekha, Dr.G.N.Swamy, "Visual Secret Sharing Based Digital Image Watermarking", International Journal of Computer Science Issues, Vol. 9, Issue 3, No 2, pp.312-317, May 2012.
[19] G. N. Swamy, B. Surekha, "Lossless Watermarking Technique for Copyright Protection of High Resolution Images", IEEE TENSYMP'2014, Kaula Lumpur, Malaysia, April 14-16, pp. 73-78, 2014.
[20] B.Surekha, Dr.G.N.Swamy, "Digital image Ownership Verification based on Spatial Correlation of Colors," IET Conference on Image Processing University of Westminster, London, UK, July 3-4, pp. 1-5, 2012.