ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

A Literature review on hybrid watermarking based VLSI schemes for real time authentication

V.Nanammal[1*], BV.Kavetha[2], R.Bhavani[3]
Department of Electronics and Communication Engineering, Jeppiaar Engineering College, Chennai, India
***Corresponding author: E-Mail: sathyajeyamaruthi@gmail.com**,

ABSTRACT

Due to mass development of multimedia content, protection of digital data is needed one always and future research is going everyday on this real time authentication. This paper summarizes the watermarking concepts and hardware suited to this authentication process. In this paper, an extensive review on various watermarking schemes based on several transformations like DFT, DCT, DWT and SVD etc was presented. In addition, the below work also concentrate on the hardware implementation part related to this study for real time audio/video/image protection. FPGA (Field Programmable Gate Arrays) like boards offer high speed, low cost and efficient architecture for incorporating watermarking algorithms in it.

KEY WORDS: Input data, Embedding, Extraction, Watermarking, VLSI boards.

1. INTRODUCTION

In this paper, a comparison on various data hiding schemes like medical image watermarking, basic image to image and image into video watermarking (Nidhi Bisla, 2013) are presented. Based on the comparative analysis and interpretation, my further research area involve the implementation of hardware suited watermarking architectures and testing of critical datas like medical, audio, video conferencing etc. Matlab-simulink blockset commonly used one. For advanced concepts of watermarking based hardware structures, Xilinx-sysgen and cadence EDA tools are preferred.

Different Watermarking and Its Concepts: Commonly steganography, cryptography, watermarking used for hiding data. Digital watermarking is the form of hiding text, logo, image, sign, audio or video thereby maintains the privacy and protects data from illegal users.

First, they transform to frequency domain: DFT will make the watermark chosen as a content dependent and translation invariant. DCT forms JPEG compression algorithms & it will be in frequency of cosines. DWT provides signal analysis and synthesis for time reduction & sub separation of data.

These are important considerations for calculating the image quality:

- Based on pixel differences
- Based on correlation
- Based on edge quality or texture
- Based on spectral distance
- Based on context
- Based on HVS (Human Visual System)

Upon above all metrics, the following key parameters to be calculated for significant performance of watermarking algorithms in both embedding and extraction: Bit Error Rate - BER(%), Signal to Noise Ratio - SNR(dB), Peak Signal to Noise Ratio - PSNR(dB), Mean Square Error - MSE . In general, Embedding is the process in which the watermark is hided into host data and Extraction is the process in which the reconstruction of original data without any loss.

Procedure for Digital watermarking system: The basic classification of watermarking is shown in Fig.1. In any hiding process, there will be two key stages: embedding and extraction. By various analysis studies, transform domain and invisible watermarks very much useful for variety of applications by proving it effectiveness in authentication and suited for high-performance boards. Among LSB, DFT, DCT, DWT and SVD transformations, DCT-SVD and DWT-SVD hybrid transforms (Kaiser, 2015) based invisible watermarking will provide best results in all key considerations of digital data prevention against all kinds of attacks. Meanwhile, the retrieval stage of watermarking has the best PSNR and BER values by maintaining the perceptual quality of the host data (Nirabh Agarwal, 2014).

Study of Various Methodologies: In this section presents the properties of watermarking process such as robustness, imperceptibility, computational cost, hiding capacity, interoperability, CBR (constant bit rate), random detection, blindness, perceptual transparency, data payload, security, effectiveness, effect on bandwidth, ease of embedding and retrieval.

The following attacks and prevention of noises is important for secure watermarking:

Some of the Attacks – Removal and interference, geometric, cryptographic, protocol, physical

Some of the Distortions are: Noise addition: Averaged noise, Multiplicative noise, Salt and Pepper Noise, Gaussian noise, Compression, Erosion, Motion blur, Dilations and shiftings, rotation, cropping, scaling, resizing.

Detailed description of the hardware architecture: To ensure an effective watermarking suited to VLSI hardware boards, various criterias to be satisfied and tested. Chips must be generated for each of the blocks used in embedding and extraction watermarking process.

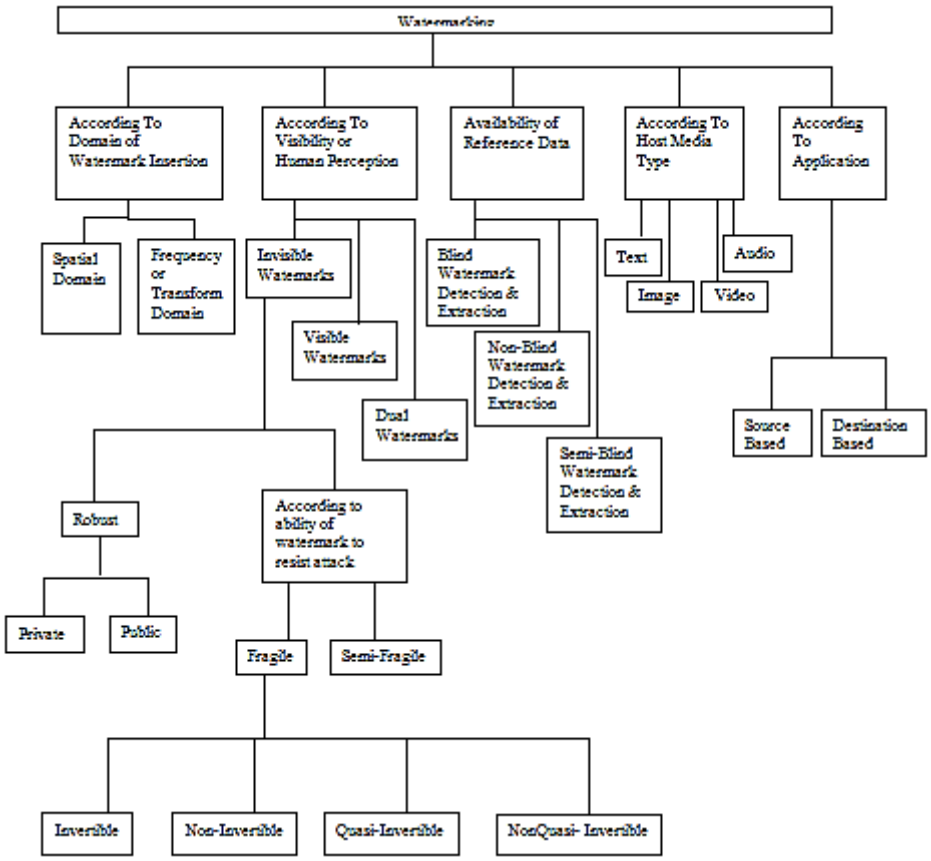


Figure.1. General Block diagram of watermarking system

2. MATERIALS AND METHODS

Verilog or VHDL hardware description languages can be easily targeted to FPGA or ASIC boards (Tamilvanan, 2014). This way of direct mapping works well if sufficient code is generated for the watermarking concept to develop its protection in real-time thereby achieving high speed, low power and cost effective one.

In Matlab, Simulink models are the one which use to generate VHDL codes for synchronizing with FPGA boards. Similarly, Xilinx System Generator (Abhishek Basu, 2012) makes use of xilinx block set for generating the ICs suits for hardware boards. SysGen tools are mostly used and works well for advance technology based watermarking. The latest one is the use of Cadence EDA tool which will be effective for all types of mixed-signal capabilities and for future this will provide best results of watermarking with audio, video, medical modalities in real-time detection.

The above Fig.2 shows the main components present for any VLSI related boards and the chips needed for on-board testing of functionalities of the watermarking algorithms real-time.

Advantages:

- Watermarking should provide high robustness and hiding capacity
- It should prevent unauthorized copying, illegal users hacking, and redistributing multimedia data.
- Additional information should be ready in the event of any error correction
- It must be able to prove the ownership by tracing the malicious user

Applications:

- Annotation
- Authentication and Integrity Verification
- Broadcast monitoring
- Content description/recovery
- Covert communication
- Protection of Copy-rights or Access control
- Defense application
- Transaction tracing Digital fingerprinting or Content labeling

- Multimedia's protection
- Ownership demonstration or source identification
- Tamper-proofing or detection

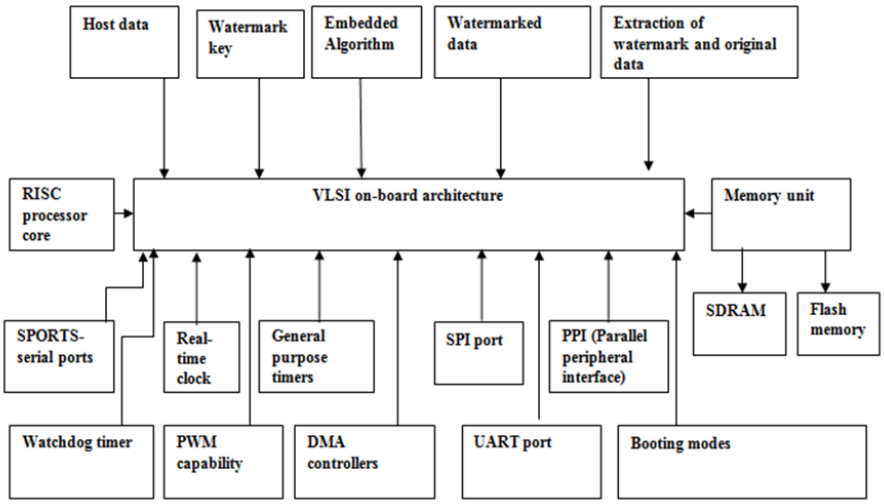


Figure.2. Hardware design of any watermarking concept for real-time protection

3. COMPARASION RESULTS AND DISCUSSIONS

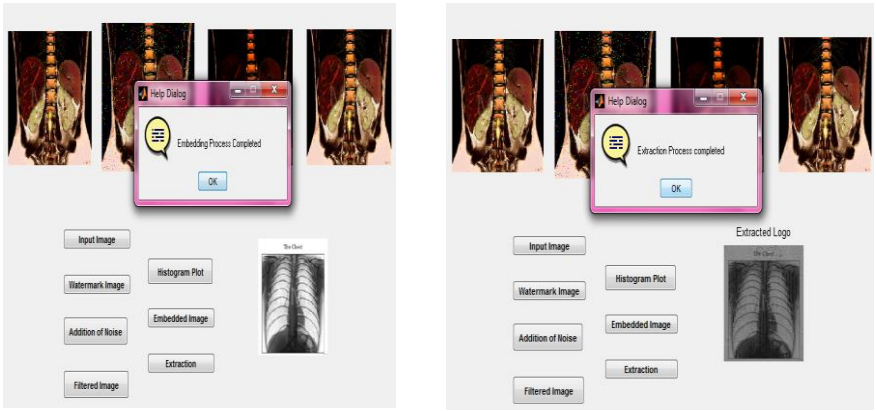
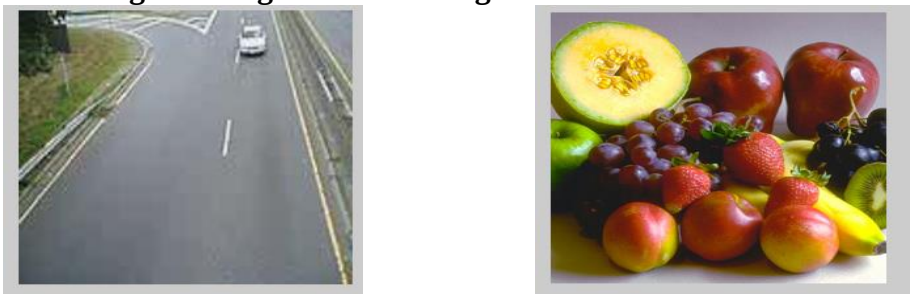


Figure.3. Shows the hiding of medical data with gray scale image.

Fig.3 Basic Embedding and Extraction watermarking process of medical data. Fig.4 shows hiding of image into image. The process involved are: Blue plane separation, DWT and SVD.

Figure.4. Image to Image watermarking based on DWT-SVD transformation



Fiure.5. (a) Cover video 5(b) Watermark image

Figure.6. (a) Watermarked video (b) DWT process

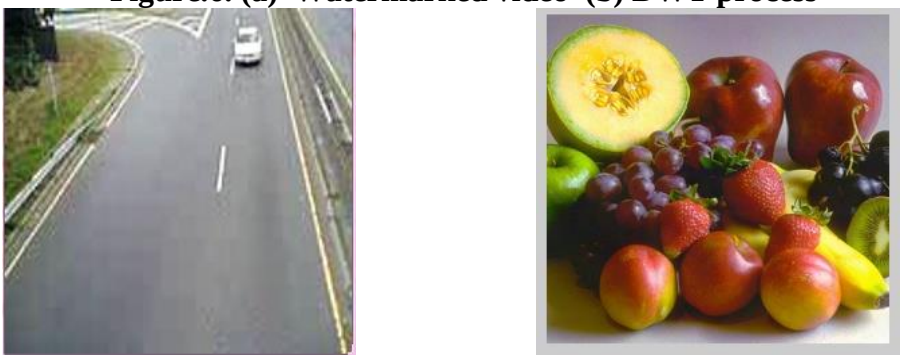


Figure.7. (a) Extraction of original video (b) Extraction of Watermark

Fig. 5 (a) , 5 (b), 6 (a), 6 (b), 7 (a), 7 (b) shows the image into video watermarking. Likewise I have compared several watermarking designs and studied the relative hardware supporting boards for this algorithms.

4. CONCLUSION & FUTURE WORK

Thus, developing FPGA or ASIC prototypes for successful implementation of the watermarking algorithms is the critical task and still research going on these areas. I have concluded by survey all relevant papers regarding hardware assisted watermarking techniques. It should involve good robustness and transparency thereby supporting hardware key goals of high speed and less area, cost-efficient design for real-time authentication of multimedia data.

REFERENCES

Abhishek Basu, Tirtha Sankar Das, Subir Kumar Sarkar, SysGen Architecture for Visual Information Hiding Framework, International Journal of Emerging Technology and Advanced Engineering (IJETAE), 2(3), 2012, 32-40.

Alka N, Potkar, Saniya M, Ansari, Implementation and Performance Analysis of DWT Based Video Watermarking Algorithms on FPGA, International Journal of Advanced Research in Computer Science and Software Enginneering (IJARCSSE), 5(2), 2015, 683-689.

Kaiser J, Giri, Mushtaq Ahmad Peer and Nagabushan P, A Robust Color Image Watermarking Scheme Using Discrete Wavelet Transformation I.J. Image, Graphics and Signal Processing (IJIGSP), 2015, 47-52.

Md. Maklachur Rahman, A DWT, DCT and SVD Based Watermarking Technique To Protect the Image Piracy, International Journal of Managing Public Sector Information and Communication Technologies, 4(2), 2013, 21-32.

Nidhi Bisla, Prachi Chaudhary, Comparative Study of DWT and DWT-SVD Image Watermarking Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, 3(6), 2013, 821-825.

Nirabh Agarwal, Arpit Jain, Sanjeev Sharma, Design and Simulation of Dct Chip In Vhdl and Application in Watermark Extraction, IOSR Journal of Computer Engineering (IOSR-JCE), 16(3), 2014, 59-64.

Rathod Jigisha D, Rachana V, Modi, A Hybrid DWT-SVD Method for Digital Video Watermarking, International Journal of Advanced Research in Computerr and Communication Engineering (IJARCCE), 2(7), 2013, 2771-2775.

Tamilvanan K, Selvakumar RB, FPGA Implementation of Digital Watermarking System, International Journal of Computer Science and Mobile Computing (IJCSMC), 3(4), 2014, 1321-1327.