2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS) | 979-8-3503-1706-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCAMS60113.2023.10526035

VLSI Implantation of Image Watermarking using TIWT with Hybrid Accumulation

Ujjelli Rakesh Reddy
PG Scholar, Deparment of ECE
Mallareddy Engineering College
Maisammaguda, Hyderabad, India
rakeshreddyujjelli@gmail.com

Shankaranand Jha
Associate Professor, Department of ECE
Mallareddy Engineering College
Maisammaguda, Hyderabad, India
shankaranand@mrec.ac.in

***Abstract*— The VLSI implementation of digital watermarking system must meet the low area (look up tables, slices, registers, memory elements), delays (path, logical) delays. However, the conventional discrete wavelet transforms (DWT) based VLSI watermarking systems suffers with higher consumption of these attributes due to down sampler. So, this work is focused on implementation of translation invariant wavelet transform (TIWT) based watermarking system using VLSI fundamentals. The grayscale image is decomposed into several frequency bands using the TIWT algorithm. This results in a set of coefficients representing the image in each frequency band. A subset of low coefficients is selected from one or more of the frequency bands for embedding the watermark. The selected coefficients are modified to embed the watermark. The modification is performed using a pseudo-random sequence, which is generated using a secret key. The sequence determines the locations and values of the watermark bits that will be embedded in the selected coefficients. Here, embedding operation is implemented using VLSI based adders and multipliers, such as hybrid accumulation. Finally, the modified coefficients are used to reconstruct the watermarked image using the inverse TIWT algorithm. The simulation results show that, the proposed TIWT system resulted in reduced hardware resource utilization, and improved watermarking robustness as compared to existing methods.**

***Keywords*—** *VLSI implementation, Digital watermarking, Low area, Low delays, Look-up tables, Slices, Registers, Memory elements, discrete wavelet transform, Translation Invariant Wavelet Transform.*

I. INTRODUCTION

Embedding digital information into an image is the essence of digital image watermarking, also known as DIW. The digital information that may be embedded into an image includes a digital picture, a digital signature, or a random series of binary integers. The process can be classified as either visible watermarking or invisible watermarking, depending on whether the embedded information is apparent [1]. It is also possible to classify it as either robust or fragile watermarking, depending on the durability level of the watermark. Recently, reversible watermarking (RIW) has gained popularity in various fields such as e-healthcare (telemedicine, telesurgery, and remote patient monitoring), the military, and the legal sector. Unlike traditional watermarking methods, RIW ensures that the embedded watermark is detected without any errors and fully recovers the original data from the watermarked data. In most cases, a reversible technique will perform some kind of lossless compression operation on the host media to create space for hiding the compressed data [2]. Message authentication codes (MAC), including hashes, signatures, or other properties extracted from the media, are then used as watermarks.

RIW aims for minimal visual distortion even at a high embedding rate, blind decoding, and simple procedures with a low computing cost, making it suitable for hardware implementation [3]. The ease with which digital content can be duplicated has led to a demand for efficient copyright protection technologies [4]. One method to enhance digital file security is by embedding sensitive information or data within a digital object, such as applying a watermark to an item. This watermark may contain information that validates the owner's intellectual property rights over the item. This process of protecting a multimedia asset by inserting a watermark into it is known as watermarking [5]. There are different categories of digital watermarks, including visible watermarks and invisible watermarks [6]. A visible watermark can be seen as a secondary translucent image overlaid on the original image when examined closely. In contrast, an invisible (robust) watermark is encoded into the image in a way that changes to pixel values are imperceptible to the human eye, and the watermark can only be retrieved using the correct decoding process. While various watermarking algorithms are found in the literature, there are few documented hardware designs [7]. Custom VLSI hardware designs can aim for better performance, reduced power consumption, and high reliability [8]. In this note, the authors present a VLSI architecture capable of performing both invisible and visible watermarking simultaneously. The chip's architecture was developed using dual voltages, dual frequency, and clock gating concepts [9]. Additionally, pipelining and parallelism were incorporated into the design to achieve excellent performance with low power consumption [10]. The design aims to facilitate the implementation of the aforementioned low-power and high-performance qualities..

The remaining portions of the article are structured as follows: The literature review, along with criticisms is found in section 2. Section 3 contains a detailed analysis of the proposed system model. Section 4 contains the simulation information regarding the proposed system model. The article is finished with section 5.

II. LITERATURE SURVEY

Sonam et al. [11] proposed the use of a hyperchaotic oscillator based on memristors as the foundation for a secure digital photo watermarking system. To simulate the human