VLSI ARCHITECTURE OF AN INVISIBLE WATERMARKING UNIT FOR A BIOMETRIC-BASED SECURITY SYSTEM IN A DIGITAL CAMERA

Saraju P. Mohanty
Email: smohanty@cse.unt.edu
Computer Science and Engineering
University of North Texas, TX 76203.

O. B. Adamo
Email: oba0002@unt.edu
Computer Science and Engineering
Univ of North Texas, TX 76203.

Elias Kougianos
Email: eliask@unt.edu
Electrical Engineering Technology
Univ of North Texas, TX 76203.

***Abstract*— Due to the need for increased border security, we present a novel system in the form of a digital camera that embeds biometric data into an image. The embedding process is performed using an invisible watermarking algorithm that allows for verification of the image as well as the identity of the carrier. This paper presents an area efficient and high performance VLSI architecture implementing the invisible watermarking algorithm towards the development of the camera.**

I. Introduction

In order to improve document and border security, it is proposed to include biometric data such as fingerprints, signatures, etc., in the electronic passport [1]. The key objectives of the passport are to identify the owner, authenticate the document, and copyright the passport. However, there are continuous risks of unauthorized access and modification to the data contained within the passport. We propose that an effective solution to combating unauthorized access such as "skimming" and "eavesdropping" is the *judicious use of watermarking [2] and encryption [3]*.

We have introduced the concept of a secure digital camera (SDC) that has both watermarking and encryption capabilities in [2]. In this paper we present a novel architecture of an invisible watermarking unit which will be integrated in our previous SDC work. We employed the use of parallelism and resource-sharing to meet the timing and area constraints. The FPGA prototype version of the proposed architecture is estimated to be operating at $256MHz$. Earlier in [4] a *software* based biometric system were presented and cameras, such as the PhotoPC 3000Z/800Z, with watermarking capabilities were commercially produced (but discontinued.)

II. Secure Biometric Data Processing in Our SDC

The passport image is watermarked with biometric data during the "enrollment process" as shown in Fig. 1. When an individual applies for a passport or ID card, our proposed SDC is used to invisibly watermark the individual's binary biometric data into the applicant's image captured by it.

The "verification process" is needed during the authentication of the individual's identity and picture. At the checkpoint, the image is acquired by scanning the passport and the encrypted compound biometric data is extracted from the acquired image and decrypted using the original key that was earlier stored in a secure external storage, as shown Fig. 2. The biometric data is then authenticated with the biometric data of the passport's owner through invisible watermarking.

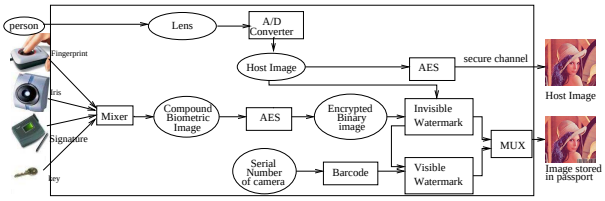


Fig. 1. The Enrollment Process

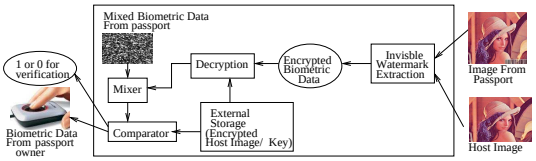


Fig. 2. The Verification Process

III. Secure Invisible Watermarking Algorithm

As presented in Fig. 3, the algorithm inserts a binary image as a watermark into the host image (passport photo). The watermark is inserted in the perceptually significant components so that the watermarked image is robust with respect to common attacks. After the preprocessing phase, the host image I is divided into 8×8 blocks and the DCT (discrete cosine transform) of each block is calculated. For the insertion phase, the DC component c_{00} and the three low frequency components c_{00}, c_{10}, and c_{11} are considered for insertion. The watermark (biometric image) is partitioned to the same number of blocks as the host image (passport photo) with a block size of 2×2. If the watermark's binary value in block k is $w_{ij}(k)$ the insertion process is carried out as, $\forall i, j,\ and\ k$ [5],

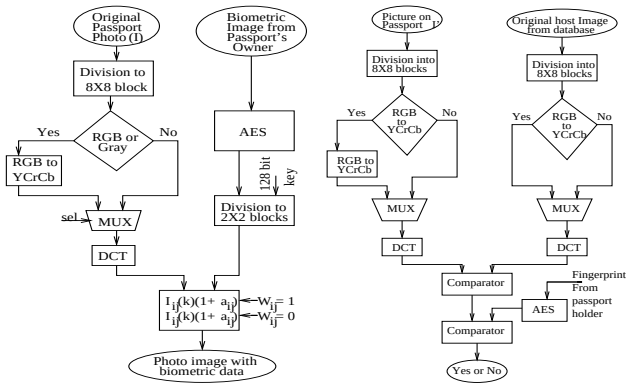
$$c'_{ij}(k) = \begin{cases} c_{ij}(k)(1+\alpha_{ij}) & if \quad w_{ij}(k) = 1, \\ c_{ij}(k)(1-\alpha_{ij}) & if \quad w_{ij}(k) = 0. \end{cases}$$

A value of 0.1 is used for α_{ac} and 0.02 for α_{dc}.

IV. Our Proposed VLSI Architecture

The architecture of the invisible watermarking chip consists of 3 distinct modules: insertion module, extraction module, and controller module. The structures of the extraction and insertion modules are very similar, so due to lack of space we will present the insertion module only.

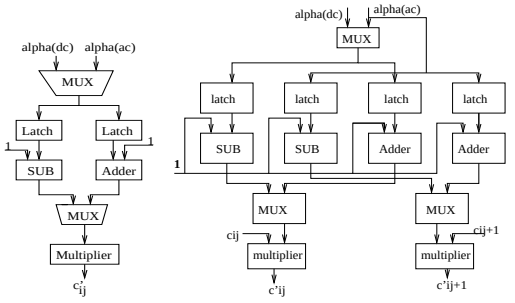
The insertion module performs the watermarking insertion process. The architecture of this module is shown Fig. 4(a),



(a) Insertion (b) Extraction

Fig. 3. Flowchart of Invisible Watermarking

and uses minimal number of resources. The architecture consists of one multiplier, two multiplexers, one adder, one subtractor and two latches. The insertion unit takes the DC DCT component (c_{00}), the first (c_{01}), second (c_{10}) and third (c_{11}) AC components of each 8×8 block for watermarking. The top multiplexer (MUX) is used to choose between the watermarking strength factors, α_{ac} and α_{dc}. The lower multiplexer helps in selecting an additive or subtractive process of watermarking insertion. To improve the performance of this architecture we also developed a parallel version using more resources in parallel as shown in Fig. 4(b). This parallel architecture provides the capability to watermark a DCT block in two clock cycles instead of four. This improves the performance of our system, however, there is a trade-off between the performance and the area used. We used latches in the insertion module for temporary buffering.



(a) Low Area (b) High Performance

Fig. 4. Datapath of the Insertion Architecture

One of the most computational intensive units needed in the datapath architecture is the DCT module (not shown in Fig. 4 due to lack of space). The DCT module consists of two 1D DCT sub-modules and was implemented following the same approach as our previous work in [2]. Buffer circuitry is used to assist in finding the transpose. It also serves as temporary storage for the first 1D DCT coefficient. In order to reduce the latency, we use a multiplexer between the buffer and the second 1D DCT submodule. We used registers as opposed to RAM cells, typically used to design the transpose buffer in order to reduce the latency and to increase performance. The DCT module does not have a separate controller, i. e. it is controlled by the main controller.

The controller is modeled as a finite state machine with seven states (init, S0 $\rightarrow$ S6). Transition from the initial state (init) to S0 occurs when the start signal is high. The pixels (I_{ij}) are read from storage to the input register for their DCT coefficients to be calculated. The first DCT operation is carried as a pipelined operation. If the DCT coefficient of all the coefficients of a block is not completed, there is a transition from state S2 to state S0. Transition is made to state S3 for the second DCT operation after the completion of the 1D DCT operation on the original image pixel (I) of the block. Due to the use of transpose buffer and the multiplexer, as discussed in the previous section, the input to the second DCT is done in a parallel fashion. The 2-D DCT coefficients (c_{ij}) of the original image are obtained in state S4. The watermarking process is performed on (c_{ij}) in state S5 and then written to RAM or displayed in state S5. If all the coefficients of the block are watermarked, a transition occurs to the initial state.

V. Implementation Results and Conclusion

The prototype was implemented in VHDL and synthesized using Xilinx Vertex II technology with an xc2v500-6fg256 target device. A multiplication unit was shared between the DCT module and the insertion module by using two multiplexers. We also employed the use of registers instead of RAM to increase the performance of our system. The synthesis and timing reports are also presented in Table I. While we presented the architecture of an invisible watermarking unit for biometric applications that will be employed in our SDC, the complete design of the camera is currently being actively conducted in our laboratory.

TABLE I
Invisible Watermarking Unit Synthesis Data

Parameter	Values
Cells Usage (BELs)	218
Maximum Operating Frequency	$256.148MHz$
Critical Path Delay	$2.164ns$
Minimum Time Period	$3.904ns$

VI. Acknowledgment

O. B. Adamo acknowledges help of Murali Varanasi.

References

[1] "U.S Department of State," `http://www.state.gov/r/pa/prs/ps/2006/61538.htm`.

[2] O. B. Adamo, S. P. Mohanty, E. Kougianos, M. Varanasi, and W. Cai, "VLSI Architecture and FPGA Prototyping of a Digital Camera for Image Security and Authentication," in *Proc. of the IEEE Region 5 Technology and Science Conference*, 2006, pp. 154–158.

[3] N. M. Kosaraju, M. Varanasi, and S. P. Mohanty, "A High Performance VLSI Architecture for Advanced Encryption Standard(AES) Algorithm," in *Proc. of 19th IEEE International Conference on VLSI Design*, 2006.

[4] P. Blythe and J. Fridrich, "Secure Digital Camera," in *Proceedings of Digital Forensic Research Workshop (DFRWS)*, Baltimore, August 2004.

[5] S. P. Mohanty, "Digital Watamerking of Images," M.S. thesis, Department of Electrical Engineering, Indian Institute of Science, Bangalore, India, 1999.