

Fast and Secure Image Processing applications

Parole chiave	SECURITY, HARDWARE DESIGN, FPGA-BASE DESIGN, IMAGE PROCESSING, EMBEDDED SYSTEMS, DIGITAL SYSTEM DESIGN, SYSTEM LEVEL DESIGN & TEST , OPEN-SOURCE
Riferimenti	Paolo PRINETTO
Riferimenti esterni	Pascal TROTTA (PhD student), Giuseppe AIRO' FARULLA (PhD Student)
Gruppi di ricerca	TESTGROUP - TESTGROUP
Tipo tesi	EXPERIMENTAL

Motivations:

Nowadays, many services and applications need to be secured in order to guarantee the users' privacy as well as the commercial and legal issues related to security threats and to safeguard the business stakeholders. While several standards, protocols and algorithms exist for handling the basic primitives for security (i.e., confidentiality, authentication, privacy), their implementation in real objects may require very high expertise and efforts.

The development of the Advanced Open-source Security Platform *SEcube*TM (Secure Environment Cube) tries to fill this gap providing heterogeneous security-oriented hardware, coupled with an open-source modular software architecture. In the Platform, all the functional blocks are isolated and well documented in order to deliver to developers an easy-way to build, understand, modify, and rewrite the whole system if wanted.

The *SEcube*TM hardware consists of a single System-on-Chip (SoC) composed of three main blocks: (i) a low-power ARM Cortex-M4 processor, (ii) a flexible and fast Field-Programmable-Gate-Array (FPGA), and (iii) an EAL5+ certified embedded SmartCard.

Descrizione	<p>All these features make the <i>SEcube</i>TM platform perfectly suitable for a wide range of applications where security is a major concern, including, among the others, Telecommunications, Internet of Things, and Home Automation.</p> <p>Within the aforementioned applications fields, the <i>SEcube</i>TM platform can be effectively employed to implement custom fast image processing algorithms (exploiting the embedded FPGA module) while, at the same time, providing security features with the aim of protecting processed images and information, that eventually will be sent or received through a network.</p>
-------------	--

Goal of the thesis:

- Definition of a reference use case in the field of secure image processing.
- Hardware implementation (VHDL or Verilog) of selected secure image processing algorithms on the FPGA module embedded in the *SEcube*TM platform.
- Implementation of software drivers to allow the *SEcube*TM platform processor to access the hardware modules implemented in the FPGA and send/receive their input/output data.

Learning outcomes:

The student will improve her/its VHDL/Verilog coding skills and digital systems design knowledge. Moreover, she/he will understand the entire design flow of FPGA-based hardware modules, starting from requirements definition to logic simulation and synthesis with state-of-the-art EDA tools.

Finally, she/he will be able to test and debug designed modules on actual hardware (i.e., SEcube™ or other commercial FPGA development boards).

External/Industrial cooperations:

The thesis will be carried out in collaboration with:

- *Blu5* View Pte. Ltd. (Singapore)
- *CINI CyberSecurity National Lab*, Nodo di Torino (Torino, Italy)
- *Lero*, the Irish Software Research Centre (Limerick, Ireland)
- *LIRMM* (Montpellier, France)

Conoscenze richieste	Programming Languages: VHDL / Verilog, C / C++ Digital System design methodologies, Computer Architecture, FPGA
Note	Number of required Students: 1 or 2
Scadenza validita proposta	31/12/2016

PROPONI LA TUA CANDIDATURA