Technological Institute of Crete

School of Technological Appliances
Informatics Engineering Department

Cryptography of processed image on embedded systems.

Kalliopi Vazakopoulou, Dimitrios Bakoyannis, Othonas Tomoutzoglou,
Ioannis Christoforakis & George Kornaros

AMIES 2015.

Overview

- Introduction
  - The proposed technique description
  - Motivation & Aims
- Implementations of the Proposed Methodology
- Related Work
- Methodology & System Analysis on FPGA
  - Image processing
    - MATLAB® vs. FPGA
  - Encryption- Decryption
- Measurements – Results
- Conclusion
- Future Work

Introduction

The proposed technique description

- A system designed by two microblaze processors
  - 1 rst : processing the selected image by applying the Sobel edge detection algorithm.
  - 2nd : encryption - decryption via TEA, Present, Blowfish and AES algorithms.
- Results verification of the processed image, to the corresponding exported by MATLAB ® for the same image.
- Efficiency Measurements and Optimization of different cipher algorithm.
- Implementation on ml405 of Xilinx with FPGA Virtex4.

Motivation & Aims

- Encryption implementation of a real application on FPGA platform.
- Implementation and comparison of cipher algorithms on FPGA development platform
- Verifying results of FPGA with those of MATLAB®.
- Encryption-decryption evaluation by differently data format

Implementations of the Proposed Methodology

- Personal Convenience
  - Mobile phones
  - Personal Digital Assistant (PDA)
- Telecommunications
  - Digital telephone exchanges
  - Network equipment (routers, switches, etc.)
- Computers & Peripherals
  - Wireless Networks (routers and Wi-Fi cards, etc.)
- Services
  - Systems of automated teller machine (ATM), credit card transactions

Related Work

- Xilinx FPGA implementation of a pixel processor for object detection applications, Peter Mc Curry, Fearghal Morgan, Liam Kilmartin.
  - Implementation of TEA at Sensors
- EMBEDDED IMAGE PROCESSING SYSTEM ON FPGA, Vo Ky Chau and Truong Quang Vinh, Viet Nam
  - Image processing on Embedded Systems on FPGA
- A Digital Image Copyright Protection Scheme Based on Visual Cryptography, Ren-Junn Hwang, *TamKang y Tamsui, Taipei Hsien, 251, Taiwan, R.O.C.*
  - Watermarking
- A brief experience on journey through hardware developments for image processing and it's applications on Cryptography, Sangeet Saha, Chandrajit pal, Rourab paul, Satyabrata Maity , Suman Sau
  - Secure image transmission on multiple FPGA

Methodology & System Analysis on FPGA

- Image processing (Sobel) - Comparison of MATLAB® with FPGA
- Implementation of Sobel detector on 'cameraman.bmp' image on MATLAB ® so as to find the edges.
- Comparison of the initial image's results (having undergone Sobel mask) in MATLAB ®, as those of the dual core system on FPGA.

'cameraman.bmp'

Results of MATLAB®

Sobel Horizontal Edges

Sobel Vertical Edges

7

MATLAB® vs. FPGA

Initial Image

'cameraman.bmp'

- **MATLAB® processing**

Cropped Image

Width: 29 Height: 30

cropped

Processed Image

Results of MATLAB®

- **FPGA processing**

Pixels of cropped image after Sobel processing on FPGA, from minicom

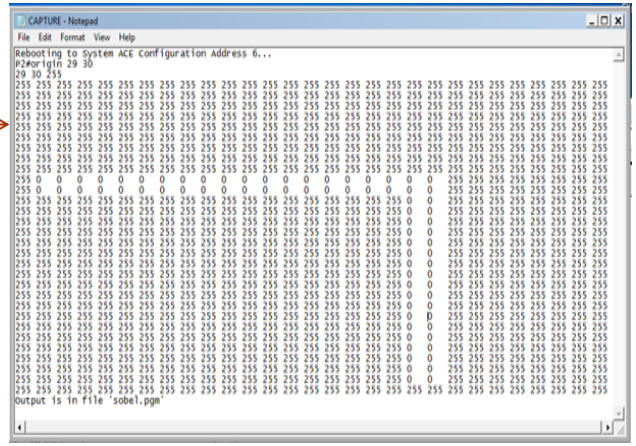
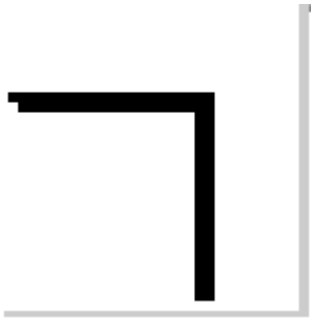


Image after Sobel processing on FPGA

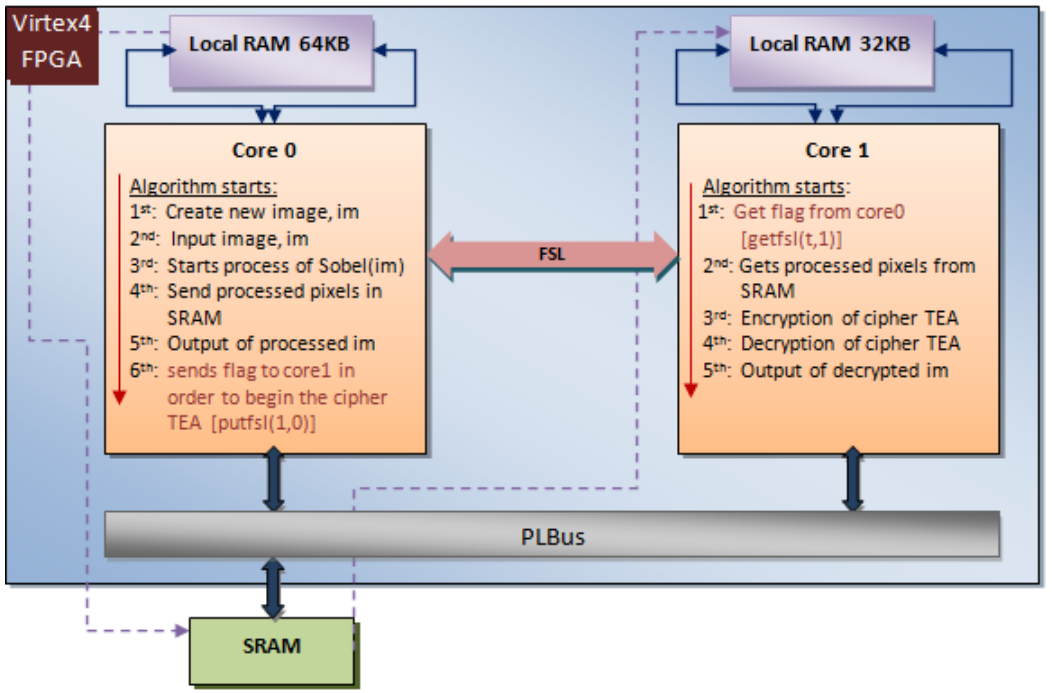
Results on FPGA



8

Methodology & System Analysis on FPGA

- Processors operation and the subsystem's architecture
  - FSL: Processors communication
  - Core 0 : Sobel, flag = "true"
  - Core 1 : flag= "true", TEA
  - SRAM : Storage of processed Pixels
  - PLBus : Communication of processors with peripherals.



9

Methodology & System Analysis on FPGA

Image processing - Sobel

- Creation - Insert Image
  - The image is a 2D table, 30x29 which is stored in the local memory of the first core
- Transfer of processed pixels in SRAM
  - Sobel sends the processed pixels making use of a pointer which is placed in the SRAM
- Output of processed image
  - By the use of a function the user is capable to view the processed image
- Trigger among cores
  - The first core triggers the second through the fsl in order to launch the last one.

1rst : microblaze

Sobel

Core 0

Algorithm starts:

1st: Create new image, im
2nd: Input image, im
3rd: Starts process of Sobel(im)
4th: Send processed pixels in SRAM
5th: Output of processed im
6th: Sends flag to core1 in order to begin the cipher TEA [putfsl(1,0)]

Methodology & System Analysis on FPGA

Encryption of Processed Image - TEA

- Launching TEA
  - The encryption begins as soon as the second core is triggered by the proper flag.
- Extraction of processed pixels from SRAM
  - The second core reads the processed image from the SRAM
- Insert image per 2 pixel of the processed image - input the encryption algorithm
  - Storage of the pixels in a 1D table in order to be encrypted

2nd : microblaze

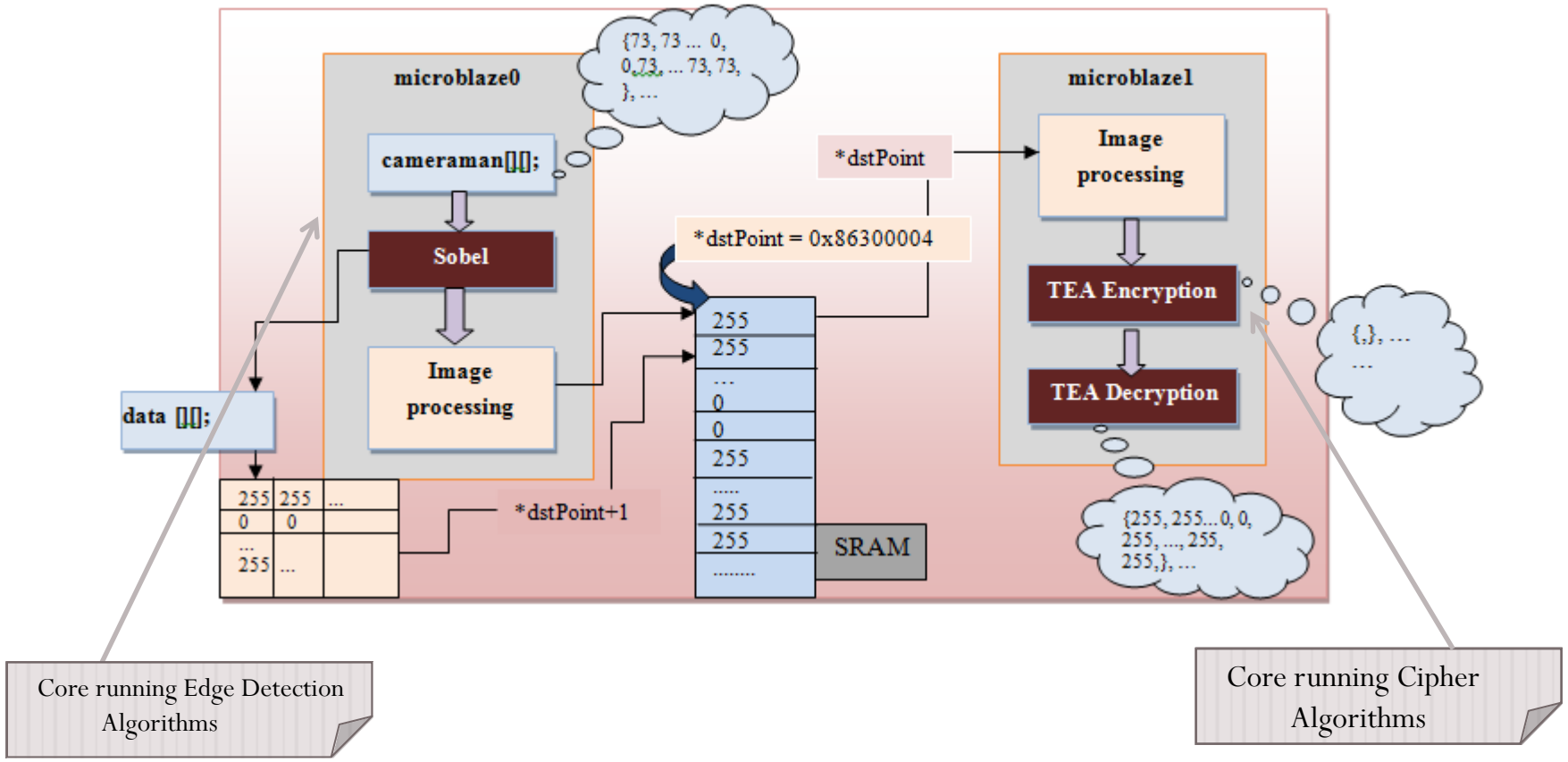
Cipher

Core 1

Algorithm starts:

1st: Get flag from core0 [getfsl(t,1)]
2nd: Gets processed pixels from SRAM
3rd: Encryption of cipher TEA
4th: Decryption of cipher TEA
5th: Output of decrypted im

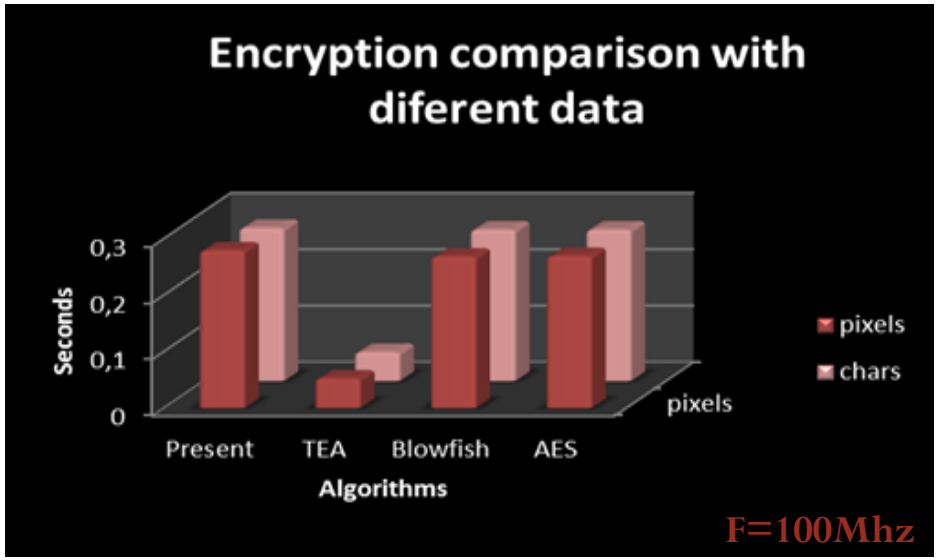
Methodology & System Analysis on FPGA



Measurements – Results

- Comparison of encryption algorithms

Encryption		
	seconds	
	pixels	chars
Present	0,279	0,271
TEA	5,21E-02	5,12E-02
Blowfish	0,268	0,268
AES	0,269	0,268

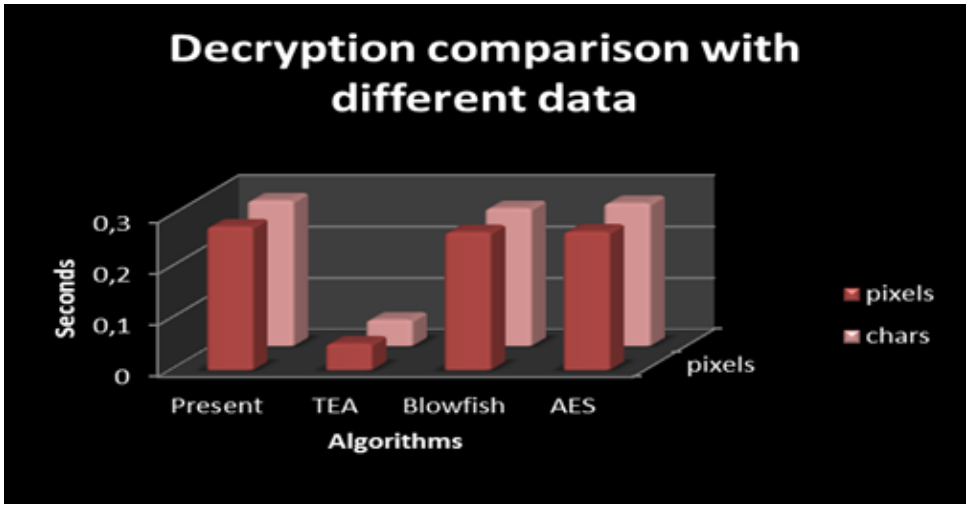


- **Apparent difference of TEA regarding the other algorithms!**

Measurements – Results

- Comparison of decryption algorithms

Decryption		
	seconds	
	pixels	chars
Present	0,279	0,283
TEA	5,12E-02	5,11E-02
Blowfish	0,268	0,268
AES	0,269	0,278

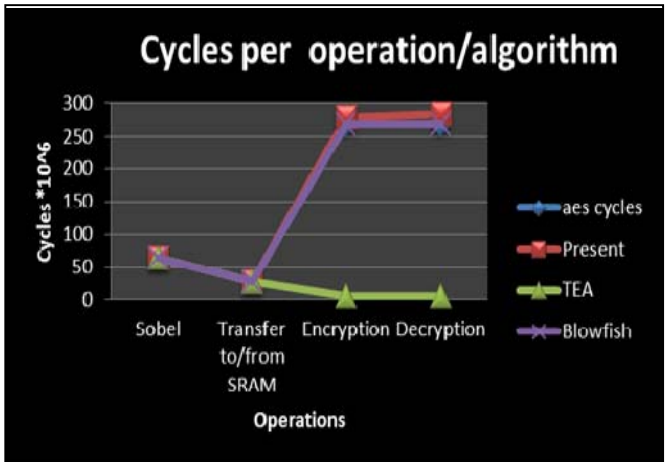


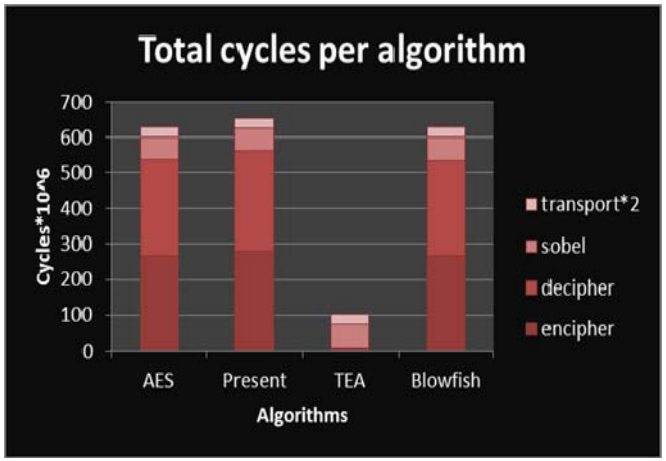
- **Either with input data pixels, or chars, came out similar results!**

Measurements – Results

- Required cycles for each process

Total Cycles / Algorithm				
	AES	Present	TEA	Blowfish
encipher	268	279	5	268
decipher	269	283	5	268
sobel	63,9	63,9	63,9	63,9
transport*2	2,80E+01	28	28	28
Total(*10^6)	**628,9**	**653,9**	**101,9**	**627,9**





- **TEA is almost six times more rapid than the Present, AES and Blowfish!**

Conclusion

- The TEA algorithm extracts the same results on less time than the Present, AES and Blowfish.
- The data entered as input on cipher algorithms do not significantly affect the overall operation.
- The image processing performed has the same effects as those of functions on MATLAB®.
- The encryption of the real implementation is implemented rapidly, by selecting the appropriate cipher algorithm.

Future Work

- A comparison with other subsystems and methodologies so as to export more comprehensive conclusions.
- Comparison of the algorithms with a higher range of data.
- Creating a HW Block in order to undertake the encryption and decryption process of memory data, by implementing the TEA.

Thank you! ☺