Encryption/Decryption Using FPGA

Ahmet Kutay Çalışkan

Supervisor
Dr. Barış Yüksekkaya
Electrical and Electronics Engineering, Hacettepe University

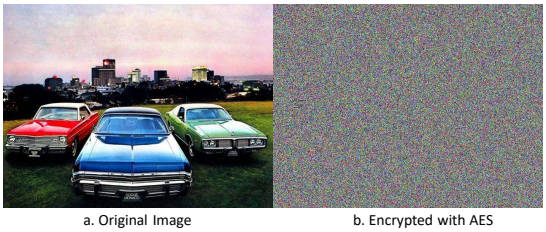
Introduction

- Security always has a very important place for people. Human beings had needed to communicate securely with each other. People produced the cryptography so that their messages could only reach the intended people so unauthorized people could not extract any information.
- The signs in the inscriptions found in Egypt are considered the first example of cryptography. Roman Emperor Julius Caesar used an encryption method, which is known today as his name, in state communications.
- Cryptography algorithms are divided into two main categories which are Classical Techniques and Modern Techniques. Classical Techniques can be calculated with simple operations.

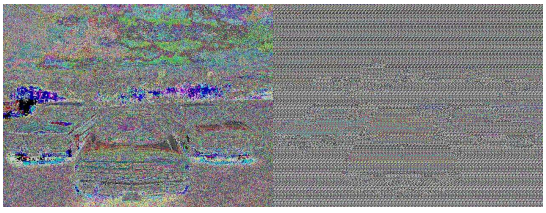
  Modern Techniques are divided into two main categories which are Symmetric Cryptography and Asymmetric Cryptography:
  - In symmetric cryptography algorithms, a secret key is used for encryption and decryption. Key is sent to the receiver and the decryption process is performed.
  - In asymmetric cryptography, public key and private key are used. Public keys is distributed to anyone. The private key is only available to the user to decrypt.

Solution Methodology

- I compared three different cryptography algorithms which are RSA, RC4 and AES. I want to mention comparative analysis that I made. I determined some of specifications to make comparison effective. According to this, speed, time complexity, memory usage and performance under noise are specifications which I compared to get better comparison.

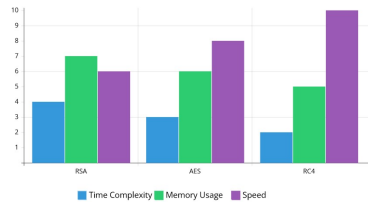


a. Original Image b. Encrypted with AES



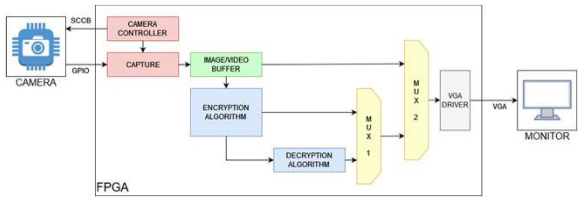
c. Encrypted with RSA d. Encrypted with RC4

Specifications and Design Requirements



Comparison Results

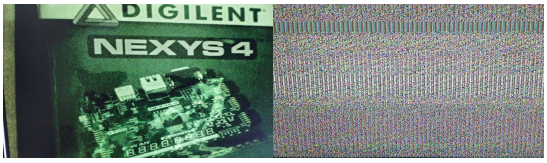
- As a result of comparison, the RC4 algorithm actually has the very first position but the investigation of security condition, the AES algorithm is better a little. So, I decided to use AES algorithm in the project.



Block Diagram

- The block diagram includes camera configuration block, capture block, algorithms for encryption and decryption, and VGA driver block. I also used buffers in my design.
- In this project, I used Nexys 4 development board with Artix-7 FPGA and OV7670 CMOS camera.

Results and Discussion



a. Original Image from Camera b. Encrypted Image

- Since the OV7670 camera sends one pixel with 16 bits (RGB 565) I get a lower quality image than the normal image format (RGB888). Since the VGA port on the development board also works with 12 bits (RGB444), the image quality has decreased again.
- When I converted the 16-bit image from the camera to the format to be used in the VGA port, I used the most significant bit values of the R, G and B channels. Therefore, I used the more significant part of the green channel, and the intensity of the green color appeared in the image from the camera.

Application Areas

- Application areas of cryptography is very wide. Used in a variety of fields in the real world, cryptography uses encryption to hide information in a coded language.
- Some of these areas are: secure communications, end-to-end encryption, storing data, digital currency, military operations…

Acknowledgements

- This project was completed within the context of ELE401-401 Graduation Project courses in Hacettepe University, Faculty of Engineering, Department of Electrical and Electronics Engineering.
- I thank Dr. Barış Yüksekkaya for sharing his knowledge, experience, and time for this Project and for his invaluable contributions.