Chapter 8
Hybrid Approach of Modified AES

Filali Mohamed Amine
Djellali Liabes University, Algeria

Gafour Abdelkader
Djellali Liabes University, Algeria

ABSTRACT

Advanced Encryption Standard is one of the most popular symmetric key encryption algorithms to many works, which have employed to implement modified AES. In this paper, the modification that has been proposed on AES algorithm that has been developed to decrease its time complexity on bulky data and increased security will be included using the image as input data. The modification proposed itself including alteration in the mix column and shift rows transformation of AES encryption algorithm, embedding confusion-diffusion. This work has been implemented on the most recent Xilinx Spartan FPGA.

INTRODUCTION

It is important aspect to protect the confidential multimedia data from unauthorized access. Multimedia content can be text, audio, still images, animation and video. Such contents are protected by multimedia security method. Commonly, this is attained by techniques that are profoundly based on cryptography. These schemes facilitate communication security, piracy and shelter (Chang, 2014).

Large size of images causes certain challenges for encryption. Normally a typical image has a very large size. Using traditional encryption algorithm will make encryption difficult for large volume of multimedia data (Chang et al, 2016). For the encryption of any multimedia data, we need such algorithms that require less computation because of large size of data. Symmetric-key algorithms are fewer computationally serious than any Asymmetric key algorithms. Typically, symmetric key algorithms are thousands of times sooner than those of the asymmetric algorithms. So, the better suitable method to encrypt the multimedia data is, to encrypt it with symmetric key encryption algorithms.

DOI: 10.4018/978-1-7998-1763-5.ch008

Our research is concerned with optimizing the existing standards of cryptography (AES) for the images and data encryption. It is also slanting towards exploiting the huge amount of data, in order to attain preferred speed.in this work proposes a modified version of AES algorithm and demonstrates that executions can accomplish superior and high throughput (Chang, et al., 2016).

STATE OF ART

There are several modified in AES to improve speed the performance, increase the security and addition same complexity on algorithm steps. (Mohammad, et al., 2015) The reason development is appeared many different the implementation on software and hardware. Each implementation has need to modified AES according to the specific proposes.

In (Xu, et al., 2013) a modified AES by used longer key length and data matrix. That extended the data matrix to eight row and variable number of column (6, 8, 12 and 16) the input data block (48, 64, 96 and 128), and extended the key length to (384,512, 768 and 1024). This paper not change the first and fourth stages (substitution byte, Add Round Key), third stage shift row change from shift third row to seventh row shifted left and four stages (mix column) change the static matrix 3x3 to new matrix 8x8, should be calculate inverse static matrix used in Mix column on GF (28). This modification is increase robustness and use a few times for encryption and decryption processing.

In (Kaur, et al., 2014) modified the AES algorithm by reduce the calculation, computation overhead, and reduce the time encryption process. It replaces the mix column stage in AES algorithm into permutation stage (like the permutation table (IP) that used in DES algorithm) because the mix column is take large calculation time and that makes the encryption process are slow. The other stages in AES algorithm don’t change.

Finally, modification used simple S-box for encryption and decryption to reduce the computation amount, the new S-box has some properties, simple generation and same S-box used for encryption and decryption (Rashidi, 2014).

The Advanced Encryption Standard (AES)

The AES is a block cipher that is the standard version of Rijndael. It has a fixed block length of 128bits and variable key lengths. The number of internal rounds of the AES depends on the key size, which is 10, 12 and 14 for the key length 128,192 and 256 respectively. In our design, we consider the case of 128 bits for the key length and 10 rounds. Before the first round, the main key is added to the plaintext. Then, inrounds1–9, all four operations are performed to the state array. In the last round (10th round), the Mix-columns transformation is not used, which makes encryption and decryption symmetric (Daemen et Rijmen, 2001) (see Figure 1).

Sub Bytes

Function performs a non-linear transformation independently on each byte of the input state. This transformation is performed by substituting each byte of the state with a value from substitution box (also termed as S-box). There are 16 parallel S-boxes each with eight inputs and eight outputs. The S-box operation is the only nonlinear transformation of the AES algorithm. It is an invertible operation and can be used for decryption processes too.