

Implementing an Efficient Encryption Block for MPEG Video Streams

M. N. Bojnordi, M. R. Hashemi, S. O. Fatemi

Multimedia Processing Laboratory

Department of Electrical and Computer Engineering, University of Tehran, Tehran, Iran.

Email: m.bojnordi@ece.ut.ac.ir, hashemi@comnete.com, omid@fatemi.net

Abstract – Considering the typically large data size and real time constraints of most multimedia contents, specially video, current encryption algorithms developed to secure text data are not applicable. Several video encryption methods have been proposed in the literature, but most methods are either too complicated for a real time hardware implementation, or are not secure enough. In this paper a new Video Cipher/Decipher scheme for MPEG video streams has been proposed. The proposed architecture has been implemented in VHDL and tested with MPEG-4 streams. Simulation results indicate that the hardware implementation complexity of the proposed stream cipher is just 2% and 13% of the AES and TDES methods respectively. The computational complexity required to break the cipher is in the order of 2^{63} .

Keywords – Video encryption, stream cipher

1. INTRODUCTION

The rapid growth of visual media in many applications has led to a variety of image and video compression standards. Securing this wide spread visual content is an important and imminent necessity and challenge. Encryption is one of the methods for securing video contents. Encrypting a video stream by simply using current data encryption algorithms such as AES, or DES is not efficient as it does not exploit the video characteristics. In addition the resulted encrypted stream does no longer comply with the standard formats.

Several video encryption methods have been proposed in the literature, but most methods are either too complicated for a real time hardware implementation, or are not secure enough. In this paper a new Video Cipher/Decipher scheme for MPEG video streams has been proposed. The proposed design has been implemented in VHDL and tested with MPEG-4 streams. The proposed block uses the E0 stream cipher, where a computational complexity of nearly 2^{63} is required for finding its initial state [1]. This complexity provides the security level required to protect video contents in most applications. The proposed cipher/decipher block is simple and suitable for real time hardware implementations.

The paper is organized as follows. Current video encryption algorithms are reviewed in Section 2. Section 3 describes the proposed scheme. Finally, simulation results are presented in Section 4.

2. EXISTING VIDEO CIPHERS

Several video encryption methods have been proposed in the literature. They are discussed in more detail in this section.

2.1. Full Encryption

The most straight-forward method is to encrypt the entire MPEG stream using standard data encryption methods such as DES and AES for symmetric cryptography, and RSA for asymmetric cryptography. This is called the naive algorithm approach [2]. The Naive algorithm treats the MPEG bitstream as a traditional text data and does not exploit the special MPEG characteristics. With this approach the resulted stream is not a valid MPEG stream and may not be used by streaming servers. Furthermore, this method is computationally intensive and its hardware implementation is complex and requires a large area.

2.2. Zig-Zag Permutation

The basic idea of the Zig-Zag Permutation Algorithm is to use a random permutation list to replace the zigzag order to map the individual 8×8 block to a 1×16 vector within the MPEG compression algorithm [2]. The algorithm achieves the goal of fast encryption because it is much faster to do permutation than to apply a standard encryption algorithm such as DES. However, since the AC coefficients are reordered, the coding efficiency is decreased. In addition the encryption method can not withstand the known-plaintext attack, which reduces its security level.

2.3. SEC MPEG

Meyer and Gadegast [3] have designed a new MPEG like bitstream, called SEC MPEG, which incorporates selective encryption and additional header information, and has high-speed software execution. SEC MPEG can use both standard encryption algorithms DES and RSA and