A Format-Compliant Encryption Framework for JPEG2000 Image Code-Streams in Broadcasting Applications[*]

Jinyong Fang and Jun Sun

Institute of Image Communication and Information Processing, Shanghai Jiaotong
University, Shanghai 200030, China
jyfang@sjtu.edu.cn, sunjun@cdtv.org.cn

Abstract. The increased popularity of multimedia applications such as JPEG2000 places a great demand on efficient data storage and transmission techniques. Unfortunately, traditional encryption techniques have some limits for JPEG2000 images, which are considered only to be common data. In this paper, an efficient secure encryption scheme for JPEG2000 code-streams in broadcasting applications is proposed. The scheme does not introduce superfluous JPEG2000 markers in the protected code-stream and achieves full information protection for data confidentiality. It also deals with the stream data in sequence and is computationally efficient and memory saving.

Keywords: JPEG2000, Format-Compliant encryption, JPSEC, Broadcasting application.

1 Introduction

In the latest still image compression standard JPEG2000, the syntax requires that any two consecutive bytes in the encrypted packet body should be less than 0xFF90 [1]. A JPEG2000 code-stream is composed of markers and data packets. The markers with values restricted to the interval [0xFF90, 0xFFFF] are used to delimit various logical units of the code-stream, facilitate random access, and maintain synchronization in the event of error-prone transmission. The packets carry the content bit-streams whose codewords (any two contiguous bytes) are not in the interval [0xFF90, 0xFFFF]. Since the output of a good cipher appears “random”, straightforward application of a cipher to encrypt code-stream packets is bound to produce encrypted packets, which include superfluous markers. Such markers will cause potentially serious decoding problems (such as loss of code-stream synchronization and erroneous or faulty image transcoding). To overcome the superfluous markers problem, the encryption method must be JPEG2000 code-stream syntax compliant. Such a compliant encryption method does not introduce superfluous markers in the encrypted packets and maintains all the desirable properties of the original code-streams.

[*] This work is supported by Ningbo Industrial Scientific and Technological project (2005-B100003) and Natural science foundation of Ningbo, China. (2005A620002).

Y. Zhuang et al. (Eds.): PCM 2006, LNCS 4261, pp. 64 – 71, 2006.
© Springer-Verlag Berlin Heidelberg 2006

Conan[2] described a technique which selectively encrypt JPEG2000 code-streams in order to generate compliant encrypt JPEG2000. In that scheme, if any byte, says *X*, has a value less then 0xF0, the four LSBs (Least Significant Bits) of *X* are encrypted with a block cipher. Clearly, the security of this scheme is weak. Wu and Ma[3] proposed two packet-level encryption schemes based on stream ciphers and block ciphers respectively. They showed that the two schemes protected most of the code-stream data. However, they are not able to regain synchronization when some transmission error occurs. These algorithms are adopted by on-going JPSEC, which is the part 8 of JPEG2000 and is concerned with all the security aspects of JPEG2000 image codestreams. Later Wu and Deng[4] gave a code-block level compliant scheme. They claimed that this scheme could provide full protection of code-streams. However, this algorithm needs iterative operations to achieve practicable key stream and has a probability of never generating conditional-satisfied encrypted code-stream. Even if it can generate compliant out streams in some cases, its iterative method is computationally inefficient.

In this paper we propose a new scheme to encrypt and decrypt the code-stream in sequence and provide full protection of the information.

2 Brief Description for JPEG2000 Packet Structure

The structure of a JPEG2000 packet is depicted in Fig.1. A packet consists of a packet header followed by a packet body. To note, the Standard ensures that none of the code-stream's delimiting marker codes (these all lie in the range 0xFF90 through 0xFFFF) can appear in the packet-stream except marker segment SOP (start of packet) and marker EPH (end of packet header).

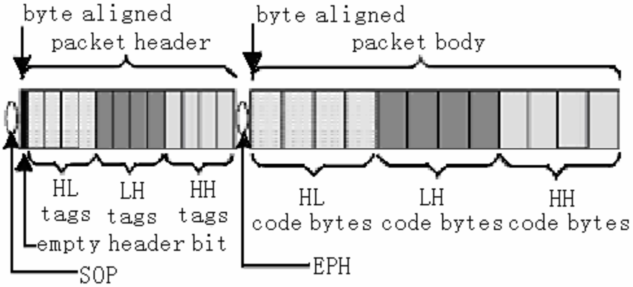

Fig. 1. JPEG2000 packet structure

3 Compliant Code-Stream Encryption Scheme Description

To hold the JPEG2000 structure, the proposed scheme is to encrypt the packet body data. The marker codes (ranging from 0xFF90 to 0xFFFF) will be kept their original values and will not appear in the packet body. Let *M* express a part of packet body, and $M = m_1 || m_2 || \ldots || m_n$, where || denotes concatenation and each m_i depicts one byte in *M*. In the same way, we denote ciphertext as $C = c_1 || c_2 || \ldots || c_n$, where c_i depicts one byte.