An Effective Selective Encryption Scheme for H.264 Video based on Chaotic Qi System

Fei Peng, School of Information Science and Engineering, Hunan University, Changsha, China
Xiao-wen Zhu, School of Information Science and Engineering, Hunan University, Changsha, China
Min Long, College of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha, China

ABSTRACT

With the wide use of H.264 in Internet and wireless network, many concerns have been made to the security of it. Aiming at providing an effective content protection method for H.264 video, a novel selective encryption scheme based on chaotic Qi system is proposed in this paper. The unpredictability of chaotic system is implemented to construct a pseudo-random number generator based on the 3-dimensional chaotic Qi system, and then some key data such as intra-prediction modes, residual coefficients and MVD are encrypted by the generated key stream. Experimental results and analysis show that the proposed scheme can achieve a good encryption result, a low computational complexity, little impact on compression ratio, and good format compatibility. It has a great potential to be applied in some real-time applications.

Keywords: Chaotic Encryption, H.264, Qi System, Selective Encryption, Video Encryption

INTRODUCTION

H.264 is a video coding standard jointly developed by ITU and ISO/IEC (JVT, 2005). It can provide a higher compression performance than H.263 and MPEG-4, and save about 30%~50% bitrate meanwhile guarantee the quality of image coding. It plays an important role in digital television broadcasting, real-time video communication, and network streaming media delivery due to its significant compression performance. However, the vulnerability of the network increases the risk of the disclosure of some sensitive content of H.264 video, which

DOI: 10.4018/jdcf.2013040103
 Encryption of video content is proved to be an effective way to protect videos. Due to the bulk data and real-time requirement, traditional encryption algorithms such as DES, AES or RSA cannot be applied to H.264 video directly (Stutz T. & Uhl A., 2012). To maintain the compression performance and avoid the computational overhead, many researchers have paid much attention to selective video encryption, which only some important parts are encrypted (Wu & Kuo, 2001; Ahn, Shim, Jeon, & Choi, 2004). At the same time, format (or syntax) compliance also attracts researchers’ attentions because the encrypted video can be decoded correctly with no destroy in syntax, which can achieve many advantages, such as maintaining synchronization and error resiliency. However, most of the existing video encryption methods are proposed for MPEG standard, and cannot achieve a good balance between security and compression performance, which is difficult to meet the requirements of real application (Stutz & Uhl, 2012). Therefore, it still needs more works to be done for the protection of the content of H.264 video.

In this paper, an effective selective encryption scheme for H.264 video based on chaotic Qi system is proposed. Firstly, a pseudo-random number generator is designed based on a 3-dimensional chaotic Qi system, and then some key data such as intra-prediction mode, residual coefficients and MVD are encrypted by the generated key stream. Experimental results and analysis show that the proposed scheme can obtain a good balance between security, computational complexity, and compression ratio. At the same time, it can maintain the format-compliance to the H.264 standard decoder.

The remaining content of this paper is organized as follows: the related work is introduced in the second section; the preliminary knowledge about chaos and H.264 is presented in the third section; the selective video encryption scheme is described in the fourth section in details; experiments and analysis are performed in the fifth section; finally, some conclusions are drawn in the last section.

RELATED WORKS

Encryption is a basic mean for the protection of the content of video data. The existed methods can be classified into the following two categories according to the range of the content to be encrypted:

1. **Full encryption of video data:** Full encryption of video data can achieve the highest security. The video data is simply regarded as a binary sequence and is encrypted as a whole with traditional encryption algorithms, such as DES, AES and RSA. VEA (Video Encryption Algorithm) is proposed to encrypt video data (Qiao & Nahrstedt, 1997). It divides plaintext block into odd-numbered bytes and even-numbered bytes to form two new byte streams called as odd list and even list. One part of cipher-text is achieved by encrypting the odd list with DES, and the other is the XOR results between the even list and the encrypted odd list. The cryptographic complexity is reduced to almost half of the original one. The complexity is further reduced to one fourth of the original one by re-dividing the odd list into two parts (Tosun & Feng, 2001). This kind of encryption methods takes advantage of high security of the traditional cryptography, but it is not format-compliance, and the computational efficiency is low, which cannot be applied in some real-time applications (Stutz & Uhl, 2012).

2. **Selective encryption of video data:** The characteristics of the video data and the requirements of video compression standard are considered in selective encryption of video data, and only some key data in the video are selected for encryption. An encryption scheme for MPEG-1 named as SECMPEG is proposed (Meyer & Gade-
Related Content

A Methodology for UICC-Based Security Services in Pervasive Fixed Mobile Convergence Systems
www.irma-international.org/chapter/methodology-uicc-based-security-services/60958/

A Policy-Based Security Framework for Privacy-Enhancing Data Access and Usage Control in Grids
www.irma-international.org/chapter/policy-based-security-framework-privacy/60954/

A Forensic Tool for Investigating Image Forgeries
www.irma-international.org/article/a-forensic-tool-for-investigating-image-forgeries/103935/

Multimedia Forensic Techniques for Acquisition Device Identification and Digital Image Authentication
www.irma-international.org/chapter/multimedia-forensic-techniques-acquisition-device/39216/

Progressive Scrambling for Social Media
www.irma-international.org/article/progressive-scrambling-for-social-media/201536/