International Journal of Innovative Computing, Information and Control
Volume **6**, Number **1**, January **2010**

ICIC International ©2010 ISSN 1349-4198
pp. 315–322

VIDEO COMPRESSION AND ENCRYPTION BASED-ON MULTIPLE CHAOTIC SYSTEMS

Qinchun Qian, Zengqiang Chen and Zhuzhi Yuan

Department of Automation
Nankai University
Tianjin, 300071, P. R. China
qqczyf@mail.nankai.edu.cn; chenzq@nankai.edu.cn

Received October 2008; revised March 2009

Abstract. *Different from most of recent studies or researches on chaos-based encryption algorithms, the paper schemes out multiple chaotic systems which deal with both video streams being compressed and compressed video streams. The so-called multiple chaotic system actually consists of three chaotic or hyperchaotic maps, namely Logistics Map [1], 2-D Baker Map and a 4-D hyperchaotic Map [2]. The three secret key functions are carried out as partial encryption when compressing the video data, as block permutation and confusion after the video compression respectively. The implemented software fully substantiates the favorable efficiency of the proposed scheme in terms of speedy compression and encryption, overall high security and small size preservation.*

Keywords: Partial encryption, Block permutation, Confusion, Multiple chaotic systems

1. Introduction.

In the last decade, the development of multimedia over open networks, especially the Internet, has been dramatically advanced by ongoing and emerging development of image and video compression and transmission technologies. Accordingly, to ensure the multimedia security, particularly video data security, more and more cryptographic methods have been introduced in many related realms. Basically, the existing image and video encryption algorithms are roughly divided into two categories: encrypting the compressed video streams and encrypting the source streams. In fact, encrypting the compressed video data can actually exterminate the statistical correlation within video frames and images; furthermore, this method may satisfy the requirement of high compression ratio. However, many traditional cryptosystems such as DES are generally considered not to be suitable for video encryption because of the relative slow speed. On the contrary, partial encryption, among many other existing encryption algorithms, just encrypts a part of image data. For example, Cheng and Li [3] provided several partial encryption algorithms.

Besides, chaos theory and its applications have attracted many researchers' attention. For example, Yasuda [10] newly introduced a class of nonlinear discrete system with invariant density. As to chaos-based encryption and watermarking, many novel algorithms such as [8] have been designed and published in literatures. Generally speaking, MPEG-based partial encryption has become a prevailing selective encryption method. Shi and Bhargava [4] designed an encryption scheme using stream ciphers to encrypt sign bits of DCT coefficients or those of motion vectors for MPEG video streams. Furthermore, Fridrich [5] schemed out 2-dimensional image encryption scheme for block permutation using Baker Map and Cat Map respectively. However, many researchers have pointed out the weaknesses of these methods such as low compression ratio and insecurity.