International Journal of Innovative
Computing, Information and Control
Volume **7**, Number **8**, August **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 4635–4652

A CHAOS-BASED MULTIPLE SECURITY ENCRYPTION SYSTEM FOR COMPRESSED VIDEO

Shun-Cheng Hong[1], Chi-Huang Kuo[1], Hsi-Kuan Chen[2]
and Chin-Hsing Chen[1]

[1]Institute of Computer and Communication
National Cheng Kung University
No. 1, Ta-Hsueh Rd., Tainan 701, Taiwan
{ n2893129; q3695145 }@mail.ncku.edu.tw; chench@eembox.ncku.edu.tw

[2]Department of Electrical Engineering
Nan Jeon Institute of Technology
No. 178, Chaoqin Rd., Yanshui Dist., Tainan 73746, Taiwan
chen_da@mail.njtc.edu.tw

Received March 2010; revised October 2010

Abstract. *This paper presents a modified chaos-based encryption scheme on the basis of the REC/RPB encryption scheme proposed by D. Xie and C. C. J. Kuo, where the Zhu's chaos-based stream cipher is used to replace the 128-bit MD5 hash function as the secret key. The reason is that the Zhu's chaos-based stream cipher could output keystream of arbitrary length. We encrypted the extracted video compressed stream with various combination according to the demands. Therefore, a multiple security encryption scheme could be obtained. Experimental security analysis showed that it is of high security and able to withstand the attacks of ciphertext only, known plaintext and chosen plaintext. Besides, the compression performance and the computation time comparison among the selective encryption, all entropy encoder output encryption, and the original compressed bitstream without encryption were also examined.*

Keywords: Chaos-based, Multiple security encryption

1. **Introduction.** Image and video encryptions play an important role in network security owing to the rapid growth of communication and information transmission on the Internet. To meet the challenge, a great number of intensive research activities in the study of cryptography have been proposed [1]. As compared to a watermark system [2], which embeds the goal image into another image whose visual configuration is unchanged at the same time, the chaotic encryption directly and as thoroughly as possible destroys the visual configuration of the goal image to avoid its information caught illegally. Many properties of chaotic systems have their corresponding counterparts in the traditional cryptosystems, and the tight relationship between chaos theory and cryptography has been noticed and pointed out by some researchers since 1990s [3,4]. The chaotic systems have received much attention recently due to some of their dynamic property of significance in favor of the information security [5,6], such as pseudo-randomness, i.e., random-like, behavior, ergodicity where the output has the same distribution with respect to arbitrary input, structure complexity where a simple process is of a very high complexity, mixing property where a small deviation in the local area can cause a large change in the whole space, extreme sensitivity to the initial value and control parameter where a small deviation in the local area can cause a dramatic change in the output. There are numerous chaotic encryption employed in ciphers, and chaos becomes a novel rich source of cryptography.