SinFra'09 - Singaporean-French IPAL Symposium

18–20 February 2009, Fusionopolis, Singapore

Tutorials

Relevant Singaporean – French common interest fields
related to the present and future activities in IPAL

Title of the course: Protection of Visual Data by Encryption and Watermarking

Professor: William PUECH, Associate Professor

Affiliation: **LIRMM, UMR 5506 CNRS -** University of Montpellier
Head of ICAR team (Image & Interaction)

Short biography: W. Puech was born in December 1967, in France. He received the diploma of Electrical Engineering from the University of Montpellier, France, in 1991 and the Ph.D. Degree in Signal-Image-Speech from the Polytechnic National Institute of Grenoble, France in 1997. He started his research activities in image processing and computer vision. He served as a Visiting Research Associate to the University of Thessaloniki, Greece. From 1997 to 2000, he had been an Assistant Professor in the University of Toulon, France, with research interests including methods of active contours applied to medical images sequences. Since 2000, he is Associate Professor at the University of Montpellier, France. He works now in the LIRMM Laboratory (Laboratory of Computer Science, Robotic and Microelectronic of Montpellier, UMR 5506 CNRS UMII). His current interests are in the areas of protection of visual data (image, video and 3D object) for safe transfer by combining watermarking, data hiding, compression and cryptography. He has applications on medical images, cultural heritage and video surveillance. He is the head of the ICAR team (Image & Interaction).

Objective of the course:
This tutorial presents the problem of protecting the transmission of visual data. The presented algorithms will be applied to images, videos and 3D objects. The main keywords are compression, encryption, watermarking and data hiding.

Summary:

The amount of digital visual data (image, video and 3D object) has increased rapidly on the Internet. Image, video and 3D object security becomes increasingly important for many applications, e.g., confidential transmission, video surveillance, military and medical applications. For example, the necessity of fast and secure diagnosis is vital in the medical world. Nowadays, the transmission of visual data is a daily routine and it is necessary to find an efficient way to transmit them over networks. Two main groups of technologies have been developed for this purpose. The first one is based on content protection through encryption. In this group, proper decryption of data requires a key. The second group bases the protection on digital watermarking or data hiding, aimed at secretly embedding a message into the data. In order to not increase the processing time, these two approaches must be combined with the compression stage. Nowadays, the challenge is to perform simultaneously for example image encryption and compression.
In this tutorial, in a first part, I will recall the standard information of encryption (block cipher, stream cipher, asymmetric and symmetric encryption) and I will show the application of standard algorithms to images. In a second part I will present combination of image encryption and compression. To finish this second part I will talk of selective encryption methods. In this part I will address the problem of simultaneous partial encryption (PE), selective encryption (SE) and image compression. Indeed, in order to visualize on line images in real time, they must be quickly transmitted and the full encryption is not really necessary. To finish this tutorial I will present some watermarking and data hiding algorithms developped by our team applied to visual data.

Selected references:

B. Schneier, *Applied cryptography*, Wiley, New-York, USA, 1995.

A. Uhl and A. Pommer, *Image and Video Encryption: From Digital Rights Management to Secured Personal Communication*, Springer, 2005.

W. Puech and J.M. Rodrigues, *A New Crypto-Watermarking Method for Medical Images Safe Transfer*, Proc. 12th European Signal Processing Conference (EUSIPCO'04), pp. 1481-1484, Vienna, Austria, 2004.

W. Puech, M. Chaumont and O. Strauss, *A Reversible Data Hiding Method for Encrypted Images*, Proc. SPIE, Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, San Jose, CA, USA, vol. 6819, pp. 68191E-1--68191E-9, January 2008.

W. Puech and G. Coatrieux, *Chapter 10: Coding: Encryption-Watermarking-Compression for Medical Information Security*, Compression of Biomedical Images and Signals, A. Naït-Ali and Christine Cavaro-Menard, Digital Signal Processing, ISTE-Wiley, pp. 247-275, 2008.

P. Amat, W. Puech, S. Druon and J-P. Pedeboy, *Lossless Data Hiding Method Based on MST and Topology Changes of 3D Triangular Mesh*, 16th European Signal Processing Conference (EUSIPCO 2008), Lausanne, Switzerland, 2008.

Image Perception, Access & Language Lab

http://ipal.i2r.a-star.edu.sg/

Supported by
CNRS – French National Research Center
UJF – University of Joseph Fourier, France
NUS – National University of Singapore
I2R / A*STAR – Institute for Infocomm Research, Singapore

For more details, please contact IPAL Admin. Assistant, Mrs. Julie FLOCH
Tel: (65) 6408 2542 , Fax: (65) 6779 6958 , e-mail: visjf@i2r.a-star.edu.sg