

Informació i Seguretat Avançada

2012/2013

Code: 42237
ECTS Credits: 6

Degree	Syllabus	Type	Year	Semester
4313133 Còmput d'Altes Prestacions, Teoria de la Informació i Seguretat / High Performance Computing, Information Theory and Security	1094 Còmput d'Altes Prestacions, Teoria de la Informació i Seguretat / High Performance Computing, Information Theory and Security	P	1	0

Contact

Name: Mercè Villanueva Gay

Email: Merce.Villanueva@uab.cat

Use of languages

Principal working language: anglès (eng)

Prerequisites

Objectives and Contextualisation

The objective of this module consists of providing advanced techniques for the data compression and/or images coding, the encoding for error correction, and the information security.

After completeness of the module, the student will be able:

1. To formulate methods for the compression of data, with particular emphasis in images.
2. To decide what is the most convenient type of compression, depending on the characteristics of the images and of the transmission channel.
3. To analyse and to evaluate the implementation requirements for lossy, progressive lossy-to-lossless, and pure lossless compression.
4. To know different advanced methods for codification to forward error correction.
5. To decide what type of codification is depending on the structure of the channel.
6. To understand and know recent steganographic techniques and schemes.
7. To gain knowledge and expertise in image/audio watermarking and coding theory based fingerprinting.
8. To be acquainted with image forensics.

Skills

- Analyse, synthesise, organise and plan projects related to information theory, security and high performance computing.
- Apply the methodology of research, techniques and specific resources for investigating and producing innovative results in a certain specialised field.
- Assure, guarantee, manage, certify and investigate the quality of advanced computing developments, processes, systems and products.
- Design solutions for complex information theory problems, analysing different technical and technological solutions and backing up these decisions with efficient criteria.
- Direct innovation and research projects and work teams in the area of information theory, security and high performance computing.
- Innovate in the search for new spaces / areas in one's field of work.
- Investigate new methods for certification and warranty of security in the treatment of and access to information in local or distributed processing systems, which guarantee a higher level of security, more efficient treatment and more effective access to the information.

- Possess and comprehend knowledge that offers the basis and opportunity to be original in the development and/or application of ideas, frequently in a research context.
- Recognise the human, economic, legal and ethical dimensions of professional exercise.
- Show responsibility in the handling of information and knowledge, and in the management of multidisciplinary groups and/or projects.
- Students must possess learning abilities to enable them to continue studying in a way that will to a large extent have to be self-managed and autonomous.

Learning outcomes

1. Analyse and evaluate information labelling schemes to guarantee the security and integrity of digital documents.
2. Analyse and evaluate the requirements for compression with loss, without loss and progressively from loss to without loss.
3. Analyse, synthesise, organise and plan projects related with information theory, security and high performance computing
4. Apply the methodology of specific research, techniques and resources for investigating and producing innovative results in a certain specialised field
5. Decide which is the most appropriate type of compression depending on the characteristics of images and the transmission channel
6. Devise codification mechanisms to obtain robust fingerprinting schemes for use in digital content protection mechanisms
7. Establish data codification policies in the area of control systems
8. Formulate methods for data compression and for the correction of errors produced during transmission
9. Innovate in the search for new spaces / areas in one's field of work
10. Plan and develop research projects with content related to data compression and the correction of errors produced during transmission
11. Possess and comprehend knowledge that offers the basis and opportunity to be original in the development and/or application of ideas, frequently in a research context
12. Recognise the human, economic, legal and ethical dimensions of professional exercise
13. Show responsibility in the handling of information and knowledge, and in the management of multidisciplinary groups and/or projects
14. Students must possess learning abilities to enable them to continue studying in a way that will to a large extent have to be self-managed and autonomous

Content

1. Compression
 - Lossless remote sensing compression
 - No-Data coding and future image coding
 - Image coding applications I (Kakadu, BOI, CADI, TER, GCOMP)
 - Image coding applications II (Kakadu, BOI, CADI, TER, GCOMP)
 - Conclusions of image coding
2. Advanced error correcting codes
 - Finite fields
 - Linear and cyclic codes over finite fields
 - Algebraic codes: Reed-Solomon codes
 - Algebraic codes: BCH codes
 - Decoding Reed-Solomon and BCH codes
3. Security and Information hiding
 - Steganographic scheme properties
 - Practical steganographic techniques
 - Watermarking schemes (image/audio)

- Coding theory for fingerprinting
- Image forensics

Methodology

The methodology applied to the student work will combine the attended lectures, the laboratories, the independent and assisted work of the students, and the presentation of working papers throughout the course, and a short public talk about a specific subject previously approved.

Distribution of the tasks:

Attending lectures and activities: 30%

Guided learning activities (outside classroom): 40%

Learning self-activities (outside classroom): 30% presented/displayed.

Activities

Title	Hours	ECTS	Learning outcomes
Type: Directed			
Lectures	30	1.2	1, 2, 5, 6, 7, 8, 10
Type: Autonomous			
Study	60	2.4	1, 2, 5, 6, 7, 8, 10, 11, 14

Evaluation

The final evaluation will take into account the portfolio delivered by the students, the attendance and participation in class, and the oral presentation.

- Attendance and active participation are compulsory. At least an 80% of the lectures shall be attended. Absences might be compensated with a home-work after agreement with the teacher. Mark: 20%
- Class activities will be proposed. Some home-works will be compulsory, others will be optional. Also, short oral talks or a particular subject will be scheduled. Mark: 80%

Evaluation activities

Title	Weighting	Hours	ECTS	Learning outcomes
Attendance	20	0	0	1, 2, 5, 6, 7, 8, 10
Oral presentations	40	30	1.2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13
Reports and exercises	40	30	1.2	1, 2, 5, 6, 7, 8, 10

Bibliography

BOOKS

- D.S. Taubman and M.W. Marcellin (2002). *JPEG 2000*. Kluwer Academic Publishers.
- David Salomon (2006, 4th Edition). *Data Compression: The Complete Reference* (Hardcover), Springer.

- Thomas M. Cover and Joy A. Thomas, *Elements of Information Theory*, John Wiley & Sons, Inc, 1991.
- Robert J. McEliece, *The Theory of Information and Coding*, Addison-Wesley Publishing Co., 1977.
- Josep Rifà and Llorenç Huguet, *Comunicación Digital*, Masson Ed., 1991.
- F. J. Mcwilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, Amstardam-N.Y.-Oxford, 1978-1996.
- Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, *Digital watermarking and Steganography*, (2nd Edition) Morgan Kaufmann, 2008.