Informació i Seguretat 2012/2013

Code: 42236
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	O	1	0

Contact

Name: Jordi Herrera Joancomarti

Email: Jordi.Herrera@uab.cat

Use of languages

Principal working language: anglès (eng)

Prerequisites

There are no pre-requirements.

Objectives and Contextualisation

The objective of this module consists of providing an introduction to information processing, emphasizing the mathematical theory of information and its treatment, the data compression and/or images coding, the encoding for error correction, techniques and cryptographic encoding for the security of the information, applications to communications networks, and the design of applications.

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

1. To formulate methods for codification to forward error correction.
2. To formulate methods for the compression of data, with particular emphasis in images.
3. To decide what is the most convenient type of compression, depending on the characteristics of the images and of the transmission channel.
4. To gain some basic knowledge on cryptography.
5. To analyze and to evaluate the implementation requirements of security algorithms.

Skills

- Analyse, synthesise, organise and plan projects related to information theory, security and high performance computing.
- Apply the functions and operations of Internet, new generation network technologies and protocols, component models, intermediate software and services to systems design.
- 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.
- 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.

- 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 the reliability of a communication channel using different information coding systems
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. Decide which is the most appropriate type of compression depending on the characteristics of images and the transmission channel
5. Develop different information codification mechanisms to improve the channel's performance
6. Distinguish between data compression methods and those for the correction of errors occurring during transmission
7. Evaluate the security of network protocols on the basis of the cryptographic components used
8. Innovate in the search for new spaces / areas in one's field of work
9. 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
10. 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 work of the student, the presentation of working papers throughout the course, and the oral and public dissertation about a specific subject previously approved.

Distribution of the tasks:

Attended 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, 3, 4, 5, 6, 7, 8, 9, 10
Type: Autonomous			
Study	60	2.4	1, 2, 3, 4, 5, 6, 7, 8, 9, 10

Evaluation

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

1.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%.

2.Class activities will be proposed. Some home-works will be compulsory, others will be optional. Mark: 40%

3.Oral presentation of a particular subject. Presentation in English is strongly advised. Mark: 40%.

Evaluation activities

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