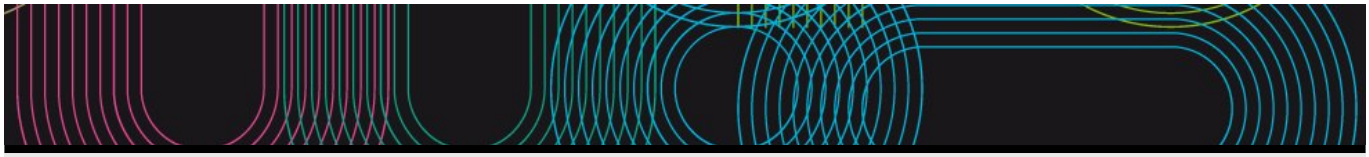
Universidade Vigo

Subject Guide 2020 / 2021



IDENTIFYING DATA				
Multimedia Security				
Subject	Multimedia Security			
Code	V05M145V01318			
Study programme	Telecommunication Engineering			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Optional	2nd	1st
Teaching language	English			
Department				
Coordinator	Pérez González, Fernando			
Lecturers	Pérez González, Fernando			
E-mail	fperez@gts.uvigo.es			
Web	http://faitic.uvigo.es			
General description	Multimedia security is an increasingly important topic as most of the information exchanged nowadays over the Internet is multimedia. Traditional data protection solutions like cryptography only solve the problem partially, because contents, once decrypted, are no longer protected. In addition, there is a rising concern over the integrity of multimedia contents: modern editing tools jeopardize our trust on video, images or audio. Fortunately, a number of research groups and companies have addressed these problems and ingenious solutions exist. This course presents advanced topics in multimedia security, with emphasis on cryptography, watermarking, forensics and signal processing in the encrypted domain. Contents, teaching and exams are in English. Students may participate in classes and answer to exams preferably in English, but Spanish and Galician are also accepted.			

Competencies	
Code	
B4	CG4 Capacity for mathematical modeling, calculation and simulation in technological centers and engineering companies, particularly in research, development and innovation tasks in all areas related to Telecommunication Engineering and associated multidisciplinary fields.
B8	CG8 Ability to apply acquired knowledge and to solve problems in new or unfamiliar environments within broader and multidiscipline contexts, being able to integrate knowledge.
C31	CE37/OP7 Ability to model, operate, manage, and deal with the full cycle and bagging of networks, services and applications considering the quality of service, direct and costs of operation, the plan of implementation, monitoring, security, scaling and maintenance, managing and ensuring the quality of the development process

Learning outcomes	
Expected results from this subject	Training and Learning Results
Handle the most advanced information protection methods.	B4 B8 C31
Understand the potential and limitations of the different methods.	B4 B8 C31
Handle the use of different algorithms in current multimedia communications environments.	B4 B8 C31
Understand technical material in an autonomous way.	B4 B8 C31

Contents

Topic	
Introduction to cryptography.	Application to multimedia systems. Integration with source and channel coding. Block and stream ciphers. Hashing and MAC codes. Specific algorithms.
Conditional access systems.	Requirements. History and state of the art. Design of a conditional access system.
Secret sharing.	Simple secret sharing systems. Visual cryptography.
Data hiding and watermarking.	Basic concepts. Watermarking versus data hiding. Spread-spectrum watermarking. Quantization-based watermarking. Application to images and video.
Forensic signal processing.	Quantization detection and estimation. Filtering detection and identification. Resampling detection and estimation. Source ballistics.
Signal Processing in the Encrypted Domain.	Privacy metrics and notions. Homomorphic encryption. Garbled cicruits. Signal representation and cipher blowup. Applications.

Planning

	Class hours	Hours outside the classroom	Total hours
Lecturing	14	28	42
Laboratory practical	9	42	51
Report of practices, practicum and external practices	0	30	30
Essay questions exam	2	0	2

*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.

Methodologies

	Description
Lecturing	The course is structured in several topics in multimedia security, including cryptography, watermarking, forensics and signal processing in the encrypted domain. Competences: CG4, CG8, CE31
Laboratory practical	Lab practices will cover different aspects of multiple-input data hiding, watermarking and forensics. This will allow students to practically implement and considerably expand some of the concepts seen in the lectures. Competences: CG4, CG8, CE31

Personalized assistance

Methodologies	Description
Lecturing	The teachers will provide individualized and personalized attention to students during the course, solving their doubts and questions. Doubts will be answered during the master session, or during the office hours. Office hours will be given at the beginning of the course and published in the subject's webpage.
Tests	**Description**
Report of practices, practicum and external practices	The teachers will provide individualized and personalized attention to students during the course, solving their doubts and questions. Doubts will be answered during the work review sessions or during the office hours.

Assessment

	Description	Qualification	Training and Learning Results

Report of practices, practicum and external practices	Reports of the practices and additional personal work that employ the techniques seen in the classroom. Quality of the reports and correctness of the results will be evaluated. Reports will be individual or collective, depending on the size of the unit that carried out the practices.	70	B4 B8	C31
Essay questions exam	Final exam with short questions on the contents of the subject.	30	B4 B8	C31

Other comments on the Evaluation

A minimum score of 30% with respect to the maximum possible score in the final exam is required to pass the course.

In those cases in which the student decides not to carry out the continuous evaluation tasks, the final score will be solely based on the exam with questions of the subject. This applies as well to the second call.

In case the student does not achieve the minimum score in the final written exam, his/her global score will be obtained using the formula: 0.35*REP+0.15*TEST, where REP is the score achieved in the reports and TEST is the score achieved in the final exam.

In case of collective reports, the respective contribution of each student must be clearly stated, and the final score will be personalized as a function of such contribution. An interview with the lecturer may be required in order to assess the individual contributions.

Once the student turns in any of the deliverables, he/she will be considered to be following the continuous evaluation track. Any student that chooses the continuous evaluation track will get a final score, regardless of he/she takes the final exam.

Continuous evaluation tasks cannot be redone after their corresponding deadlines, and are only valid for the current year.

In the case that plagiarism is detected in any of the reports/exams done/taken, the final score for the subject will be 'fail' (0) and the teachers will inform the School authorities of the affaire so that they take the appropriate measures. Besides, the teachers will inform the School authorities of any conduct against ethics by the students, the possibility existing that the School authorities take the appropriate measures.

Sources of information

Basic Bibliography

A.J. Menezes, **Handbook of Applied Cryptography**, 1996,

Complementary Bibliography

Cox, Miller, Bloom, Fridrich, Kalker, **Digital Watermarking and Steganography**, 2nd,

Troncoso-Pastoriza, Perez-Gonzalez, **Secure Signal Processing in the Cloud: enabling technologies for privacy-preserving multimedia cloud processing**, Signal Processing Magazine,

A. Piva, **An Overview of Image Forensics**, Signal Processing,

Recommendations

Contingency plan

Description

=== EXCEPTIONAL PLANNING ===
Given the uncertain and unpredictable evolution of the health alert caused by COVID-19, the University of Vigo establishes an extraordinary planning that will be activated when the administrations and the institution itself determine it, considering safety, health and responsibility criteria both in distance and blended learning. These already planned measures guarantee, at the required time, the development of teaching in a more agile and effective way, as it is known in advance (or well in advance) by the students and teachers through the standardized tool.

=== ADAPTATION OF THE METHODOLOGIES ===
In such case, teaching and evaluation will take place fully or partially online.