



## JORNADAS DE SEGUIMIENTO

# PROYECTOS EN TECNOLOGÍAS DE RADIO, COMUNICACIONES Y TELEMÁTICA

### DESCRIPCIÓN DE RESULTADOS

<b>Referencia del Proyecto:</b>	TIC 2001 – 0633 – C03
<b>Título del Proyecto:</b>	STREAMOBILE: “Streaming de contenidos multimedia hacia dispositivos móviles con retribución por micropago”
<b>Investigador Principal:</b>	Dr. Josep Domingo-Ferrer
<b>Dirección de contacto:</b>	Dpto. Ingeniería Informática y Matemáticas Escuela Técnica Superior de Ingeniería Universidad Rovira i Virgili Av. Països Catalans, 26 43007 Tarragona e-mail: jdomingo@etse.urv.es
<b>Datos del Grupo de Investigación:</b>	Grupo de investigación CRISES (Comercio Electrónico Seguro). Grupo consolidado por la Generalitat de Catalunya (2002 SGR 00170)
<b>¿Se trata de un proyecto coordinado?</b>	Sí
<b>Referencia del Proyecto:</b>	TIC 2001 – 0633 – C03 – subproyecto 1
<b>Investigador responsable:</b>	Dr. Josep Domingo-Ferrer
<b>Dirección de contacto:</b>	jdomingo@etse.urv.es
<b>Referencia del Proyecto:</b>	TIC 2001 – 0633 – C03 – subproyecto 2
<b>Investigador responsable:</b>	Dr. Vicenç Torra Reventós
<b>Dirección de contacto:</b>	vtorra@iia.csic.es
<b>Referencia del Proyecto:</b>	TIC 2001 – 0633 – C03 – subproyecto 3
<b>Investigador responsable:</b>	Dr. Jordi Herrera Joancomartí
<b>Dirección de contacto:</b>	jherreraj@uoc.edu

## **1. OBJETIVOS DEL PROYECTO**

En este primer apartado se introduce el proyecto, se describen sus tareas y objetivos y se muestra el cronograma de tiempos.

### **1.1 El proyecto STREAMOBILE**

Con la llegada de las nuevas generaciones de móviles y la proliferación de ordenadores de mano y teléfonos móviles con prestaciones multimedia surgen grandes oportunidades en la prestación de servicios de banda ancha a dispositivos móviles.

Aprovechar estas oportunidades supone beneficios de mejor servicio para el usuario, así como beneficios económicos para los proveedores de contenido, para las entidades financieras y también para los operadores de telecomunicaciones. El objetivo de STREAMOBILE es poner a punto un prototipo de goteo en tiempo real (streaming) de contenidos multimedia hacia dispositivos móviles.

El usuario móvil paga por los contenidos recibidos mediante un micropago efectuado por cada ranura de tiempo o cada bloque de datos con una tarjeta inteligente insertada en el dispositivo móvil. La propiedad intelectual de los contenidos recibidos se halla protegida por marcas de agua.

### **1.2 Descripción de tareas**

Las tareas descritas en la solicitud del proyecto se detallan a continuación:

#### **PT0: Gestión y explotación del proyecto**

Se pretende asegurar la gestión, seguimiento y coordinación del proyecto.

#### **PT1: Análisis de requisitos**

Un objetivo importante es cuantificar las necesidades concretas de streaming de las empresas vinculadas y de los usuarios de la UOC.

#### **PT2: Desarrollo del primer demostrador**

Se deberá hacer un estudio sobre el hardware y software necesario, así como su adquisición. Sobre este hardware, se deberá implementar el streaming de audio/vídeo en el demostrador, tanto en la parte cliente como en la parte servidor.

#### **PT3: Watermarking / fingerprinting contra ataques múltiples**

Se hará hincapié en el desarrollo de métodos de watermarking / fingerprinting que resistan ataques de distorsión / confabulación combinados.

#### **PT4: Micropagos**

Estudio, desarrollo e implementación de sistemas de micropagos.

#### **PT5: Desarrollo del segundo demostrador**

La principal característica del segundo demostrador es el cambio de la parte cliente del primer demostrador a tecnología móvil UMTS. Por otra parte, se pretende incorporar los métodos de watermarking / fingerprinting robustos ante ataques múltiples al primer demostrador.

#### **PT6: Pruebas de campo**

Las pruebas de campo del segundo demostrador deben permitir el testeo de la aplicación y su ajuste a las expectativas explicitadas en los análisis de requisitos.

### 1.3 Cronograma del proyecto

Actividades / Tareas	Primer año	Segundo año	Tercer año
PT0	■		
PT1	■	■	■
PT2	■	■	■
PT3	■		
PT4	■		
PT5	■	■	■
PT6	■	■	■

## 2. GRADO DE CONSECUCIÓN

### 2.1 Descripción de los resultados obtenidos

En esta sección se enumeran los resultados obtenidos hasta el momento para las tareas descritas anteriormente. Nótese que en algunos casos se han añadido hitos o bien ha habido alguna modificación respecto los objetivos anteriores.

#### 2.1.1 Gestión y explotación del proyecto

##### *Reuniones hasta la fecha*

Se han realizado varias reuniones, la primera de las cuales fue una sesión de introducción. En dicha reunión, celebrada en marzo de 2002, se presentó el proyecto STREAMOBILE a todas las partes participantes y se definieron las primeras líneas de trabajo.

En las reuniones de junio de 2002, noviembre de 2002 y abril de 2003, cada grupo expuso el estado de su subproyecto. Después de un turno de discusión entre todos los miembros del proyecto, se trazaron objetivos a alcanzar para la siguiente reunión. Cabe decir que la relación entre los miembros del proyecto STREAMOBILE es muy fluida, usando el correo electrónico y la videoconferencia como medio habitual de comunicación.

A principios de julio de 2003 tuvo lugar la última reunión hasta la fecha, donde se definieron los ítems descritos en el presente documento. Se debatió cómo debería realizarse la presentación y se realizó un ejercicio de evaluación.

##### *Sitio web STREAMOBILE*

Tal y como se definió en la solicitud del proyecto, se ha realizado una web del proyecto STREAMOBILE. En ella se describen los subproyectos y sus objetivos, y se enumeran publicaciones y actividades realizadas.

La web se encuentra en <http://vneumann.etse.urv.es/streamobile>.

##### *Relación con las empresas*

El análisis de requisitos realizado en el PT1 de STREAMOBILE reveló que existía la necesidad de diseñar nuevos servicios que rentabilizasen el streaming sobre telefonía de 3ª generación o sobre redes inalámbricas locales y/o metropolitanas. Entre estos servicios se identificó el juego electrónico en línea (casinos virtuales) como un nicho de mercado interesante, tanto a nivel económico como a nivel deontológico (la mayoría de casinos virtuales existentes ofrecen muy pocas garantías de equidad al usuario). En colaboración con la empresa tecnológica SCYTL Online World Security S.A. (<http://www.scytl.com>) hemos desarrollado una patente internacional PCT de póquer electrónico en red [Cast02]. Entre los servicios que dará el demostrador final de STREAMOBILE figurará el protocolo de juego electrónico desarrollado, que ofrece garantía de equidad en la elección de carta por parte del usuario del dispositivo móvil.

Nuestros algoritmos de marca de agua para protección del copyright electrónico de contenidos multimedia (desarrollados durante el anterior proyecto TEL98-0699-C02-02 y también durante

STREAMOBILE) han suscitado el interés de Fujitsu España, empresa con la que estamos negociando un acuerdo de colaboración.

La relación con los operadores telefónicos ha sido algo más compleja. En efecto, no hemos conseguido servicio UMTS de ninguno de los operadores contactados (Amena, Telefónica Móviles). Se nos ofrecía servicio GPRS, pero no fue posible llegar en un tiempo razonable a un acuerdo que nos permitiese usar GPRS con fines experimentales a una “tarifa académica”.

Se están realizando contactos con los socios del proyecto de investigación europeo OPIUM – *Open Platform for Integration of UMTS Middleware* (EU IST-2001-36063). Dicho proyecto se centra en el desarrollo e implementación de la OSA/Parlay (*Open Services Architecture*), un middleware diseñado para servicios móviles. Entre los socios de este proyecto está la filial española del operador Vodafone que proporciona su red UMTS que actualmente ya tiene desplegada y en fase de pruebas.

### 2.1.2 Análisis de requisitos

Después de mantener contactos con proveedores de contenidos y de “entertainment”, se llegó a la conclusión de que había dos grandes grupos de servicios que podían justificar el despliegue masivo de infraestructuras móviles avanzadas:

- Streaming de contenidos con retribución por micropago. Dicho streaming puede tener varias finalidades (educación, ocio, etc.).
- Participación en protocolos criptográficos avanzados, tales como juego electrónico seguro, votación electrónica por red.

Para fijar los requisitos de la aplicación de streaming de contenido, nos centramos en el entorno educativo, y tomamos como base de trabajo la biblioteca de la Universitat Oberta de Catalunya. El hecho que el conjunto de la universidad, y en particular parte de su biblioteca, sea virtual y que todos sus estudiantes estén conectados a un campus virtual hace que sea un entorno de pruebas muy idóneo.

El fondo videográfico de la biblioteca comprende distintos vídeos digitalizados que están accesibles para los estudiantes. Si bien la cesión de los volúmenes de la biblioteca es gratuita para los estudiantes de la UOC, el hecho prestar el servicio de streaming de dichos vídeos a través de dispositivos móviles implica una infraestructura de comunicaciones. El volumen de tráfico de dicha infraestructura podría llegar a ser insostenible (puesto que la universidad tiene más de 20.000 alumnos) si todos los alumnos utilizaran de manera indiscriminada dicha utilidad. Por este motivo, la posibilidad de realizar un control de dicho servicio es sumamente importante. De este modo, se sustituye el concepto de micropago (poco aceptado en un entorno universitario) por un concepto de cupón, de modo que la matrícula del alumno va ligada a un número de cupones que permite un cierto cupo de minutos de vídeo. Dicho cupo puede ir en función de las asignaturas de las que el alumno se matricule puesto que puede darse el caso que algunas asignaturas tengan más videografía que otras.

Si bien el requisito de transacción anónima no es especialmente relevante en el caso de streaming de contenidos educativos, puede ser más interesante cuando los contenidos son de otro tipo (ocio, etc.), razón por la cual decidimos mantener el objetivo de realizar transacciones anónimas.

En cuanto a participación en protocolos criptográficos avanzados, nos centramos en juego electrónico seguro y votación electrónica segura. Para ello, nos pusimos en contacto con la empresa tecnológica SCYTL Online World Security (<http://www.scytl.com>), especializada en este tipo de aplicaciones. Aunque en dichos protocolos lo fundamental es que el cliente tenga una cierta capacidad de cálculo, no es menos cierto que se requiere un ancho de banda sustancial y se puede hacer uso del streaming de vídeo si éste se halla disponible. Por todo ello, pareció fácil que el prototipo STREAMOBILE pudiese abarcar tanto el streaming de contenidos como la participación en protocolos criptográficos avanzados.

La funcionalidad de los demostradores se ha ido definiendo en las sucesivas reuniones del proyecto.

### 2.1.3 Desarrollo del primer demostrador

En su momento se decidió implementar el módulo de micropagos para el primer demostrador en lugar del módulo de marca de agua. Esto fue debido a que las implementaciones de algoritmos de marca de agua para vídeo de que disponemos (para formato MPEG-1) no soportan el formato de archivo utilizado en la implementación sobre PDA (formato propietario de Microsoft, *Windows Media Video*).

Así pues, se ha implementado un servicio de vídeo *pay-per-view* con retribución por micropagos. En este sistema, se va pagando una pequeña suma de dinero cada  $n$  segundos, de modo que el usuario paga mientras está viendo el vídeo (*pay-as-you-watch*). La primera versión del prototipo se halla descrita en detalle en [Mart02] y las líneas generales de su diseño se publicaron en [DM02]. El sistema funciona a través de Internet y usa el sistema de micropagos PayWord. Soporta un cliente sobre PC. Posteriormente, el sistema se adaptó al uso de varios clientes de forma concurrente, funcionando sobre un PDA en un entorno de red local inalámbrica. Esta segunda versión del sistema se presentó en las Jornadas Técnicas de Rediris 2002 [DMS03b]. Queda para una tercera versión la incorporación de los protocolos criptográficos avanzados (votación y juego electrónico), así como la posible migración a teléfono móvil (que dependerá de la evolución de la oferta por parte de los operadores).

#### *Adquisición de hardware*

Para la implementación del demostrador se adquirió un punto de acceso de red de área local inalámbrica y un ordenador de bolsillo (PDA) de prestaciones avanzadas. Además de la adquisición de los elementos de red inalámbrica, se está estudiando la compra de teléfonos móviles de última generación para el desarrollo y prueba de prototipos (véase 2.3). De todas formas, el cambio tecnológico que se ha producido desde que se redactara la memoria de solicitud de STREAMOBILE hace que actualmente las redes inalámbricas, tanto locales como metropolitanas, estén mejor posicionadas para la distribución de contenidos hacia dispositivos móviles que la tan esperada telefonía de 3ª generación. Ello se debe a factores de oportunidad (el número y el alcance de las redes inalámbricas implantadas no para de crecer, mientras que la telefonía UMTS todavía no ha llegado al usuario) y de coste (las redes inalámbricas suponen un coste mínimo o nulo para el usuario, a diferencia de la telefonía de 3ª generación).

### **2.1.4 Protección del copyright**

#### *Watermarking robusto*

Se han implementado técnicas de watermarking robustas para la inserción de información en imágenes y secuencias de vídeo. En [MVS02] presentamos un método que introduce la marca en el dominio DCT que resulta especialmente robusto a altos factores de compresión JPEG y a ataques de recorte. Los códigos de inserción fueron los códigos ML. Este método se ha adaptado al sistema DCT por bloques y se han introducido máscaras perceptuales en este dominio que permiten al mismo tiempo que disminuir la perceptibilidad de la marca, aumentar la potencia y por tanto la robustez del sistema [VSV03], [Vent02]. En esta dirección se ha desarrollado también un trabajo en el dominio wavelet cuyas características se asemejan a las del sistema visual humano. En este dominio se consigue robustez a sistemas de compresión wavelet, como el JPEG2000, pero también a los basados en DCT [Mart03b], [MS04]. Finalmente se han desarrollado técnicas robustas basadas en el sistema de compresión de vídeo MPEG2, comparándose distintos códigos para la inserción de la marca [Cama02].

#### *Watermarking contra ataques múltiples*

En el caso particular de imágenes digitales, existe una multitud de propuestas cada una de ellas robusta contra determinado tipo de ataques. Obtener sistemas de watermarking robustos contra más y más ataques es una tarea difícil.

Nuestra propuesta [DS02a] consiste en coger una imagen y marcarla mediante distintos métodos de watermarking. Cada uno de estos sistemas es resistente a un conjunto específico de ataques, con más o menos éxito. A continuación, se mezclan convenientemente las imágenes marcadas, de forma que se obtiene una nueva imagen. Se demuestra que esta imagen resultado es resistente al conjunto de ataques soportados por cada uno de los métodos de marcaje.

Por otro lado, se ha estudiado distintos ataques con algoritmos de compresión de imágenes con pérdidas [HM03] y se han desarrollado esquemas de marcado [MHM03a, HMM03] que ofrecen robustez contra dichos ataques.

#### *Watermarking de audio*

Para obtener un grado elevado de eficiencia en la protección de videos estamos desarrollando técnicas de protección del copyright de audio que complementan las técnicas de protección del

copyright de imágenes que se han desarrollado. Nuestra propuesta [MHM03b] utiliza el algoritmo de compresión de audio MPEG Layer 3 para obtener un esquema de marcado robusto y eficiente.

#### *Watermarking invertible*

La autenticación de contenidos multimedia mediante firma digital presenta el problema de tener que manejar un fichero adjunto con la firma.

En [DS02b] presentamos un estudio sobre la invertibilidad del sistema de watermarking de Hartung y Girod. El estudio demostraba que en el caso concreto de imágenes digitales, este sistema puede ser usado para proporcionar integridad y autenticación transparente sin pérdidas.

#### *Códigos para huella digital seguros contra confabulaciones de hasta tres atacantes*

Los códigos clásicos resistentes a ataques por confabulación (Boneh y Shaw) son extremadamente largos para ser empotrados en un objeto multimedia como una imagen, incluso para tamaños pequeños de confabulación.

En [SD03] se presenta una construcción para códigos para huella digital seguros contra confabulaciones de hasta tres atacantes. La construcción consiste en una composición de dos códigos: un código dual de Hamming como código interno (cuyas propiedades se estudian en [SD02a] y [SD02c]) y un código de dispersión como código externo (publicación en revista [SD02b]). En el trabajo se demuestra que, para el caso particular de confabulaciones de tamaño no superior a tres y para un número de posibles compradores no extremadamente alto, nuestra propuesta obtiene palabras código de longitud más corta que la construcción general de Boneh y Shaw.

#### *Protección del copyright mediante un sistema de fingerprinting asimétrico*

Las propuestas actuales de fingerprinting asimétrico (aquellas que, dado que el vendedor del contenido no tiene conocimiento de cómo queda la copia una vez marcada, proporcionan seguridad al comprador) están basadas en herramientas criptográficas que, o bien son difícilmente implementables (cálculo seguro multiparte y pruebas de conocimiento nulo) o bien su coste de ejecución es extremadamente elevado (transferencia inconsciente).

En [MSDS03] se propone un protocolo seguro, basado en entidades de confianza y criptografía de clave pública. Este protocolo permite implementar sistemas que proporcionan servicios para el marcaje y la detección de copia ilegal, con seguridad y anonimato para el comprador.

#### *Fingerprinting seguro contra confabulaciones en esquemas multicast*

Tras estudiar la propuesta de fingerprinting en multicast basado en encriptación, nos dimos cuenta de que, con la distribución de claves propuesta, no ofrecía seguridad contra confabulaciones.

En [MDS03b] propusimos un sistema de distribución de claves basado en los códigos de Boneh y Shaw, mediante el cual el sistema resulta seguro contra ataques de confabulación.

#### *Testeo de la privacidad de las transacciones*

Tal como se había previsto en el plan de trabajo, las pruebas de campo encaminadas al testeo de la privacidad de las transacciones están previstas para el tercer año del proyecto. La idea es ver hasta qué punto es factible para un intruso confeccionar un perfil de los servicios demandados por un cierto usuario de STREAMOBILE. Se supone que el intruso emplea algoritmos de enlace de registros para construir el perfil del usuario (los registros que enlaza corresponden a la información que intercepta durante el funcionamiento de STREAMOBILE y a la información que puede conseguir por otras vías respecto de un cierto usuario). Durante el 2º año de STREAMOBILE hemos producido un estado de la técnica sobre enlace de registros [TD03] y hemos propuesto un algoritmo de enlace de registros que no requiere compartición de atributos entre las fuentes de información enlazadas [DT03].

### **2.1.5 Retribución por micropagos**

El modelo de comunicación que mejor se adapta a la transmisión de vídeo en directo o casi-bajo-demanda es el multicast (de uno a muchos). Estudiamos la adecuación de los sistemas de micropago existentes a multicast y nos percatamos de que presentan un problema de escalabilidad, al verse el receptor de los pagos inundado por multitud de cupones de pago.

En [DMS02] propusimos un sistema de micropagos escalable orientado a un entorno multicast. En este sistema, los micropagos se van comprobando y agregando en los encaminadores intermedios.

Por otra parte, actualmente estamos estudiando la viabilidad de la implementación de sistemas de micropagos en teléfonos móviles de última generación.

### **2.1.6 Desarrollo del segundo demostrador**

El segundo demostrador se encuentra actualmente en fase de desarrollo.

#### *Diseño del servidor para el segundo demostrador*

La variedad de servicios a ofrecer por los distribuidores, los diferentes tipos de contenido vendidos y la pluralidad de dispositivos finales y redes de comunicación, hacen que se deba diseñar un modelo de servidor específico que además trate los conceptos de pago mediante un módulo de micropagos y protección del copyright mediante watermarking.

En [MDS03a] se especificó el diseño del servidor para un servicio que cumple los requisitos anteriores.

Asimismo, también se ha implementado el sistema de servicio de protección del copyright mediante fingerprinting descrito en [MSDS03] y se ha presentado durante el 2º Simposio Español de Comercio Electrónico [MSD03].

### **2.1.7 Pruebas de campo**

Tal y como se muestra en el cronograma, las pruebas de campo se realizaran en la última anualidad del proyecto cuando ya se encuentre completamente operativo el segundo demostrador. Para la realización de dichas pruebas se está contactando con los socios del proyecto OPIUM (ver apartado 2.3).

## **2.2 Problemas surgidos**

El principal problema surgido hasta la fecha es de índole tecnológico. La llamada 3ª generación de telefonía móvil (UMTS) se está retrasando considerablemente. El problema es debido a la falta de terminales y falta de redes. Pese su existencia en entornos de experimentación relacionados con grandes operadoras de telecomunicaciones, el acceso a estas tecnologías es complicado.

Por otra parte, tecnologías como las redes inalámbricas extendidas (habituales ya en algunas ciudades, aeropuertos, zonas de ocio, etc.) conforman un entorno tecnológico más adecuado que el UMTS para implementar nuestros desarrollos.

## **2.3 Soluciones aportadas**

Dada la dificultad o poca viabilidad de que un servidor de tales características pueda ser evaluado funcionando en un entorno GPRS o UMTS, se desarrolló un elemento de red capaz de introducir retardos en los paquetes y su pérdida según un modelo específico [Camp03]. De esta forma, se consigue evaluar el sistema como si se estuviera accediendo desde una red 2.5G o 3G. La inclusión de este elemento dentro de una red local inalámbrica permite usar el PDA tal como si estuviera conectado a Internet mediante una red GPRS.

Como se ha señalado anteriormente, se están realizando contactos para usar la red de pruebas UMTS de Vodafone a través del proyecto OPIUM.

Paralelamente, se está estudiando la viabilidad de la utilización de redes inalámbricas para el desarrollo de aplicaciones como las propuestas por el proyecto STREAMOBILE. Dichas redes inalámbricas, que utilizan estándares de comunicación como el IEEE 802.11 o el IEEE 802.15, tienen la ventaja que supone trabajar en un espectro de frecuencia no licenciado y por otro lado utilizar tecnologías disponibles ya en los productos de venta al público. En esta primera fase, la viabilidad del estudio se está centrando en la seguridad que pueden ofrecer dichas redes para aplicaciones de comercio electrónico [HP03, PHM03].

## 2.4 Resultados científico-tecnológicos relevantes

Patente internacional PCT ES02/00485 "Método para la obtención de un resultado imparcial de un juego a través de una red de comunicación y protocolos y programas asociados". En esta patente se describe un protocolo para póquer electrónico seguro sobre Internet, que usa transformaciones de cifrado homomórficas y permite que varios jugadores puedan sacar cartas de una baraja virtual de forma que se garantiza la imparcialidad del resultado obtenido. Dicha patente se halla en explotación por la empresa SCYTL Online World Security, con la que hemos firmado un convenio de colaboración.

Premio a la Investigación Más Destacada, dentro de la 8ª edición de los Premios Salvà i Campillo, concedidos por la Asociación Catalana de Ingenieros de Telecomunicación, que se entregaron a 20 de febrero de 2003 en Barcelona en un acto al que asistió el Ministro de Ciencia y Tecnología. Este premio nos fue concedido por nuestro trabajo sobre protección del copyright de la información multimedia, realizado en los proyectos TEL98-0699-C02-02, en STREAMOBILE y en el proyecto europeo CO-ORTHOAGONAL.

Coordinación (por parte del Prof. Domingo Ferrer) del proyecto europeo CO-ORTHOAGONAL (IST-2001-32012). Nuestro trabajo ha sido complementario al realizado en STREAMOBILE y ha consistido en el desarrollado en el desarrollo de huella digital resistente a confabulaciones.

Participación en los proyectos europeos CASC (IST-2000-25069) y AMRADS (IST-2000-26125). En estos proyectos se ha investigado en la preservación de la privacidad y el anonimato en las transacciones electrónicas.

Hemos participado en el proyecto europeo RESET (IST-2001-37936), en el que se han delineado las prioridades en la investigación sobre tarjetas inteligentes para el 6º PM de la Unión Europea.

Desde el inicio del proyecto STREAMOBILE, los integrantes del proyecto:

- Hemos publicado 22 artículos en revistas SCI, entre ellos artículos en *Electronics Letters*, *IEEE Transactions on Systems, Man and Cybernetics-Part C* e *IEEE Transactions on Knowledge and Data Engineering*.
- Hemos editado dos volúmenes internacionales: el volumen 2316 de *Lecture Notes in Computer Science* y un libro de Physica-Verlag.
- Hemos sido editores invitados de la revista SCI *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*.

Por último, se han leído 5 tesis doctorales relacionadas con el proyecto STREAMOBILE.

## 3. INDICADORES DE RESULTADOS (ENERO 2002-JULIO 2003)

### 3.1 Personal en formación

Tesis doctorales relacionadas con STREAMOBILE	
Terminadas	5
En desarrollo	2
Proyectos fin de carrera y tesis de Máster	
Proyectos Fin de Carrera	7
Tesis de Máster	1

### 3.2 Publicaciones realizadas

Tipo	Número
Libros como editor	2
Libros como autor	2
Artículos SCI	14
Artículos no SCI	3
Capítulos de libro y proc. con ISBN	25
	<b>46</b>

### 3.3 Transferencia tecnológica. Participación en Proyectos Nacionales y Extranjeros

Proyecto: **European Network of Excellence in Cryptology** – ECRYPT (Red de excelencia)

Organismo financiador: Comisión Europea – VI Programa Marco

Periodo: 2003 - 2008

Investigador principal: Bart Preneel

Proyecto: **Co-orthogonal Codes in Cryptography, Data Security, Watermarking and Entity Authentication** - CO-ORTHOGONAL IST-2001-32012

Organismo financiador: Comisión Europea – V Programa Marco

Periodo: 2001 - 2002

Coordinador e investigador principal: Josep Domingo-Ferrer

Proyecto: **Computational Aspects of Statistical Confidentiality** – CASC – IST-2000-25069

Organismo financiador: Comisión Europea – V Programa Marco

Periodo: 2000 – 2003

Investigador principal en la URV y miembro del *steering committee*: Josep Domingo-Ferrer

Proyecto: **Roadmaps for European research on Smartcard Technologies** – RESET IST-2001-37936

Organismo financiador: Comisión Europea – V Programa Marco

Periodo: 2002 – 2003

Investigador principal en la URV: Josep Domingo-Ferrer

Proyecto: **Plataforma de Protección de Imágenes Digitales** (PlaPID) FIT-070200-2002-120 (PROFIT)

Organismo financiador: Ministerio de Ciencia y Tecnología

Periodo: 2002

Investigador principal: Jordi Herrera Joancomartí

Proyecto: **Plataforma de Protección de Imágenes Digitales** (PlaPID-2) FIT-070200-2003-109 (PROFIT)

Organismo financiador: Ministerio de Ciencia y Tecnología

Periodo: 2002

Investigador principal: Jordi Herrera Joancomartí

Convenio de transferencia de tecnología: **SCYTL Online World Security SA**, para la explotación de la patente P9800608 por parte de la empresa

Fecha: septiembre de 2002

Investigador principal: Josep Domingo-Ferrer

Convenio de transferencia de tecnología: **SCYTL Online World Security SA**, para el desarrollo de patentes de juego electrónico

Fecha: septiembre de 2002

Investigador principal: Josep Domingo-Ferrer

### 3.4 Colaboración con Grupos de Investigación Nacionales y Extranjeros

Colaboración con el grupo Information Security Group de la Universidad Politècnica de Catalunya. Se han realizado sendos artículos sobre estado del arte y técnicas utilizadas, publicados en [FSDS02a] y [FSDS02b].

Colaboración con el grupo Signal Technologies Group de la Universidad de Vigo. Se participa con este grupo en la red de excelencia europea ECRYPT.

“Xarxa temàtica sobre control d’inferència” (Red temática sobre control de inferencia, 2002 XT 00111), financiada por la Generalitat de Catalunya. Esta red está coordinada por el Dr. Vicenç Torra (investigador principal del 3er subproyecto de STREAMOBILE) y participan en ella el IIIA-CSIC, la URV, la UPC y el Institut d’Estadística de Catalunya.

“Seguretat, codificació i transport de la informació” (2001 XT 00016), red temática financiada por la Generalitat de Catalunya. Está coordinada por el Prof. Josep Domingo (coordinador de

STREAMOBILE) y participan en ella la URV, la UPC, la UAB, la UOC, la UdL, la UIB y la Université de Bordeaux.

IFIP Working Group 8.8 sobre "Smart Cards". El Prof. Domingo (coordinador de STREAMOBILE) fue elegido en mayo de 2003 secretario de este grupo de trabajo de la *International Federation for Information Processing*.

Capítulo español de la *IEEE Information Theory Society*. El Prof. Domingo es el fundador y actual *chairman* de dicho capítulo.

Como consecuencia de la participación en los grupos anteriores, se han producido las siguientes estancias de investigación en el equipo de STREAMOBILE:

- **Cyril Maillet** (École Centrale de Nantes). Estancia de formación de cuatro meses en el grupo CRISES en Tarragona. Departamento de Ingeniería Informática y Matemáticas, Universidad Rovira i Virgili. Abril a junio 2003.
- **Michal Demyda** (Universidad de Bydgoszcz, Polonia). Estancia de formación para realizar una tesis de Master en el grupo de procesado de imagen del Departamento de Teoría de la Señal y Comunicaciones, Universidad Politècnica de Catalunya. Febrero a Junio 2002. Se realizó un estudio de adaptación de turbo códigos para la inserción de información en esquemas de watermarking.
- **Prof. Sadaaki Miyamoto** (Tsukuba University, Japón). El Prof. Miyamoto participa en la red temática sobre control de inferencia. En octubre de 2002, el Dr. Vicenç Torra realizó una estancia con él en la Universidad de Tsukuba para desarrollar métodos de clustering.
- **Prof. Yasuo Narukawa** (Instituto Toho Gakuen, Tokyo, Japón). En diciembre de 2002, el Prof. Narukawa realizó una estancia con el Dr. Torra (IIIA-CSIC) para desarrollar métodos de fusión de información, aplicables al incremento de la robustez de las marcas de agua y al testeo del anonimato de las huellas digitales para protección del copyright.
- **Prof. Hideyuki Imai** (Sapporo University, Japón). En marzo de 2003, el Prof. Imai realizó una estancia con el Dr. Torra (IIIA-CSIC) sobre la determinación de modelos para fusión de información. El Prof. Imai tiene previsto volver en verano de 2004.

## APÉNDICE

### Patentes

[Cast02] J. Castellà Roca, A. Riera Jorba, J. Borrell Viader, J. Domingo-Ferrer *Método para la obtención de un resultado imparcial de un juego a través de una red de comunicación y protocolos y programas asociados*. Patente internacional con número de solicitud PCT ES02/00485. Fecha de solicitud: 14 de octubre de 2002. Entidad titular: SCYTL Online World Security SA. Países de prioridad: todos.

### Tesis doctorales

**Marcel Fernández Muñoz**, *A Contribution to the Design and Efficient Decoding of Traceability Codes*. Universidad Politècnica de Catalunya, 2003.

**Francesc Sebé Feixas**, *Transparent Protection of Data*. Universidad Politècnica de Catalunya, 2003.

**Anna Oganian**, *Security and Information Loss in Statistical Database Protection*. Universidad Politècnica de Catalunya, 2003.

**Aïda Valls i Mateu**, *ClusDM: A multiple criteria decision making method for heterogeneous data sets*, Universitat Politècnica de Catalunya, 2002.

**David Nettleton**, *The use of complementary techniques of machine learning to discover knowledge in real complex domains*, Universitat Politècnica de Catalunya, 2002.

### Trabajos de investigación para la obtención del Diploma de Estudios Avanzados

**Josep Prieto Blázquez**, *Strong Personal Authentication Using Mobile Devices and Wireless Networks*. Universidad Oberta de Catalunya, Programa de doctorado Sociedad de la Información. Dirigido por el Dr. Jordi Herrera Joancomartí.

**Antoni Martínez Ballesté**, *Pay-per-view of Streamed Multicast Content Delivery*. Universidad Politècnica de Catalunya, Programa de doctorado Ingeniería Telemática.  
Dirigido por el Dr. Josep Domingo-Ferrer y el Dr. Miguel Soriano Ibáñez.

## Principales publicaciones científicas realizadas

### Capítulos de libro

- [DM02]** J. Domingo-Ferrer, A. Martínez-Ballesté, "STREAMOBILE: Pay-per-view video streaming to mobile devices over the Internet", en *Proceedings of the 13th International Workshop on Database and Expert Systems Applications (DEXA'2002)*, eds. A. Min Tjoa and R. R. Wagner, Los Alamitos CA: IEEE Computer Society, ISBN 0-7695-1668-8, pp. 418-422, 2002.
- [DMS02]** J. Domingo-Ferrer, A. Martínez-Ballesté, F. Sebé, "MICROCAST: Smart card based (micro)pay-per-view for multicast services", en *Proceedings of IFIP/USENIX 5th Smart Card Research and Advanced Application Conference-CARDIS'2002*, Berkeley CA: USENIX, ISBN 1-931971-04-8, pp. 125-134, 2002.
- [DOT02]** J. Domingo-Ferrer, A. Oganian, V. Torra, "Information-theoretic disclosure risk measures in statistical disclosure control of tabular data", en *Proceedings of the 14th International Conference on Scientific and Statistical Database Management*, Los Alamitos CA: IEEE Computer Society, ISBN 0-7695-1632-7, pp. 227-231, 2002.
- [DS02a]** J. Domingo-Ferrer, F. Sebé, "Enhancing watermark robustness through mixture of watermarked digital objects", en *IEEE Intl. Conf. on Information Technology: Coding and Computing-ITCC'2002*, Piscataway NJ: IEEE Computer Society, ISBN 0-7695-1506-1. pp. 85-89, 2002.
- [DS02b]** J. Domingo-Ferrer, F. Sebé, "Invertible spread-spectrum watermarking for image authentication and multilevel access to precision-critical watermarked images", en *IEEE Intl. Conf. on Information Technology: Coding and Computing-ITCC'2002*, Piscataway NJ: IEEE Computer Society, ISBN 0-7695-1506-1, pp. 152-157, 2002.
- [Domi03]** J. Domingo-Ferrer, "Networking in the New ICT curricula" en *IEEE Intl. Conf. on Information Technology: Coding and Computing-ITCC'2003*, Piscataway NJ: IEEE Computer Society, ISBN-0-7695-1916-4, pp.20-24, 2003.
- [HM03]** J. Herrera-Joancomartí, J. Minguillón, "Ataques a esquemas de watermarking de imágenes", en *VII- Reunión Española de Criptografía y Seguridad de la Información Oviedo*: Servicio de Publicaciones de la Universidad de Oviedo, Vol II, ISBN 84-699-8931-6, pp. 437-446, 2002.
- [HMM03]** J. Herrera-Joancomartí, J. Minguillón, D. Megías, "A Family of Image Watermarking Schemes Based on Lossy Compression", en *IEEE International Conference on Information Technology: Coding and Computing, ITCC'2003*, Piscataway NJ: IEEE Computer Society, ISBN-0-7695-1916-4, pp.559-563, 2003.
- [HP03]** J. Herrera-Joancomartí, J. Prieto Blázquez, "A Personal Authentication Scheme Using Mobile Technology", en *IEEE International Conference on Information Technology: Coding and Computing, ITCC'2003*, Piscataway NJ: IEEE Computer Society, ISBN-0-7695-1916-4, pp.253-257, 2003.
- [Imai03]** H. Imai, V. Torra, On a modeling of decision making with a twofold integral, in *EUSFLAT 2002*, Zittau, Germany, aceptado.
- [Lana03]** S. Lanau, V. Torra, S. Miyamoto, Fuzzy clustering for indexing in the GAMBAL information retrieval system, in *EUSFLAT 2002*, Zittau, Germany, aceptado.
- [MDS03a]** A. Martínez-Ballesté, J. Domingo-Ferrer, F. Sebé, "MINPAY: a Multi-device INternet PAY-as-you-watch system", en *IEEE Intl. Conf. on Information Technology: Coding and Computing-ITCC'2003*, Piscataway NJ: IEEE Computer Society, ISBN-0-7695-1916-4, pp.258-262, 2003.
- [MDS03b]** A. Martínez-Ballesté, J. Domingo-Ferrer, F. Sebé, "Fingerprinting schemes for multicast delivery", in *International Conference on Information Technology: Research and Education – ITRE'03* (en prensa).
- [MHM03a]** J. Minguillón, J. Herrera-Joancomartí, D. Megías, "Empirical Evaluation of a JPEG2000 standard Based Robust Watermarking Scheme", en *SPIE- 15th Annual Symposium Electronic Imaging 2003*.
- [MS04]** E. Martínez, E. Sayrol "Perceptual Masks in the Wavelet Domain", en revisión *SPIE Security and Watermarking of Multimedia Contents VI*.
- [MSD03]** A. Martínez-Ballesté, F. Sebé, J. Domingo-Ferrer, "Aspectos prácticos de la protección de la propiedad intelectual en contenidos multimedia", *Actas del II Simposio Español de Comercio Electrónico*, ISBN: 84-932902-0-3, Barcelona, pp. 219-228, 2003.
- [MSDS03]** A. Martínez-Ballesté, F. Sebé, J. Domingo-Ferrer, Miquel Soriano, "Practical Asymmetric Fingerprinting based on a TTP", *Trustbus'03* (en prensa).
- [MVS02]** M. Madueño, J. Vidal, E. Sayrol, "Color Image Watermarking Using Channel State Knowledge", en *SPIE Security and Watermarking of Multimedia Contents IV*.
- [NT03]** Y. Narukawa, V. Torra, Twofold integral and multi-step Choquet integral, in *International Summer School on Aggregation Operators and Their Applications*, Alcalá de Henares, Madrid, Spain, aceptado.
- [NT03b]** Y. Narukawa, V. Torra, Twofold integral: a graphical interpretation and its generalization to universal sets, in *EUSFLAT 2002*, Zittau, Germany, aceptado.

- [PHM03] J. Prieto Blázquez, J. Herrera Joancomartí, R. Martínez Peña, "Implementación de un sistema de autenticación personal basado en tecnología Bluetooth", in *Actas del II Simposio Español de Comercio Electrónico*, ISBN: 84-932902-0-3, Barcelona, pp. 13-24, 2003.
- [SD02c] F. Sebé, J. Domingo-Ferrer, "Códigos para huella digital seguros contra confabulaciones de hasta tres atacantes", en *Actas de la VII Reunión Española sobre Criptología y Seguridad de la Información*, eds. S. González y C. Martínez, Oviedo: Servicio de Publicaciones de la Universidad de Oviedo, ISBN 84-699-8931-6, pp. 779-792, 2002.
- [TD03] V. Torra, J. Domingo-Ferrer, "Record linkage methods for multidatabase data mining", en *Information Fusion in Data Mining* (ed. V. Torra), Berlin: Springer-Verlag, ISBN 3-540-00676-1, pp. 99-130, 2003.
- [VTD02] A. Valls, V. Torra, J. Domingo-Ferrer, "Aggregation methods to evaluate multiple protected versions of the same confidential data set", en *Soft methods in Probability, Statistics and Data Analysis*, Heidelberg: Physica-Verlag, ISBN 3-7908-1526-8, pp.289-294, 2002.
- [VSV03] S. Ventosa, E. Sayrol, J. Vidal, "Perceptual Mask Estimation from Watermarking Images", en *SPIE Security and Watermarking of Multimedia Contents V*.

#### Artículos SCI

- [DM02] J. Domingo-Ferrer, J. M. Mateo-Sanz, "Practical data-oriented microaggregation for statistical disclosure control", *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 1, pp. 189-201, ISSN 1041-4347, 2002.
- [Domi02] J. Domingo-Ferrer, "A provably secure additive and multiplicative privacy homomorphism", *Lecture Notes in Computer Science*, vol. 2433, ISSN 0302-9743, pp. 471-483, 2002.
- [DT02b] J. Domingo-Ferrer, V. Torra, "Validating distance-based record linkage with probabilistic record linkage", *Lecture Notes in Computer Science (subserie Lecture Notes in Artificial Intelligence)*, vol. 2504, pp. 207-215, ISSN 0302-9743, 2002.
- [DT03] J. Domingo-Ferrer, V. Torra, "Disclosure risk assessment in statistical disclosure control of microdata via advanced record linkage", *Statistics & Computing* (en prensa), ISSN 0960-3174.
- [DT03b] J. Domingo-Ferrer, V. Torra, "Selecting potentially relevant records using re-identification methods", *New Generation Computing* (en prensa), ISSN 0288-3635, 2003.
- [DT03c] J. Domingo-Ferrer, V. Torra, "Disclosure risk assessment in statistical data protection", *Journal of Computational and Applied Mathematics* (en prensa), ISSN 0377-427, 2003.
- [DT03d] J. Domingo-Ferrer, V. Torra, "On the connections between statistical disclosure control for microdata and some artificial intelligence tools", *Information Sciences*, vol. 151, ISSN 0020-0255, pp. 153-170, 2003.
- [DT03e] J. Domingo-Ferrer, V. Torra, "Median-based aggregation operators for prototype construction in ordinal scales", *International Journal of Intelligent Systems*, vol. 18, no. 6, pp. 633-655, ISSN 0884-8173, 2003.
- [DTV03] J. Domingo-Ferrer, V. Torra, A. Valls, "Semantic based aggregation for statistical disclosure control", *International Journal of Intelligent Systems* (en prensa, 2003), ISSN 0884-8173.
- [MHM03b] D. Megias, J. Herrera-Joancomartí, J. Minguillón "A robust audio watermarking scheme based on MPEG 1 layer 3 compression", en *Proceedings of the 7th. Conference on Communications and Multimedia Security*, Lecture Notes on Computer Science (en prensa).
- [SD02a] F. Sebé, J. Domingo-Ferrer, "Short 3-secure fingerprinting codes for copyright protection", *Lecture Notes in Computer Science*, vol. 2384, ISSN 0302-9743. Vol. *Information Security*, eds. L. Batten and J. Seberry, Berlin: Springer-Verlag, pp. 316-327, 2002.
- [SD02b] F. Sebé, J. Domingo-Ferrer, "Scattering codes to implement short 3-secure fingerprinting for copyright protection", *Electronics Letters*, vol. 38, no. 17, ISSN 0013-5194. pp. 958-959, 2002.
- [SD03] F. Sebé, J. Domingo-Ferrer, "Collusion-secure and cost-effective detection of unlawful multimedia redistribution", *IEEE Transactions on Systems, Man and Cybernetics, part C*, ISSN 1094-6977 (en prensa, 2003).
- [Torra02] V. Torra, "Learning weights for the quasi-weighted means", *IEEE Transactions on Fuzzy Systems*, vol. 10, no. 5, 2002.
- [Torra02a] V. Torra, Editor invitado de la revista *International Journal of Intelligent Systems, special issue on the Hierarchical Fuzzy Systems*, vol. 17, no. 5, 2002.
- [TDMN03] V. Torra, J. Domingo-Ferrer, J. M. Mateo-Sanz, Michael Ng, "Regression for ordinal variables without underlying continuous variables", *Information Sciences* (en prensa, 2003), ISSN 0020-0255.

## Artículos no SCI

- [DMS03b] J. Domingo-Ferrer, A. Martínez-Ballesté, F. Sebé, "Vídeos de pago en Internet", *Boletín de RedIRIS*, nos. 62-63, pp. 6-9, 2003.
- [FSDS02b] M. Fernández, M. Soriano, J. Domingo-Ferrer, F. Sebé, "Esquemas de fingerprinting para la protección de derechos de distribución", *Novática*, no. 160, ISSN 0211-2124, pp. 36-40, 2002.
- [FSDS02a] M. Fernández, M. Soriano, J. Domingo-Ferrer, F. Sebé, "Fingerprinting schemes for the protection of multimedia distribution rights", *Upgrade*, vol. III, no. 6, ISSN 1684-5285, pp. 36-40, 2002.

## Otros trabajos relacionados con el proyecto

- [Cama02] David Camarero, *Watermarking de Video*. Proyecto Fin de Carrera de Ingeniería Superior de Telecomunicaciones. Departamento de Teoría de la Señal y Comunicaciones. Universidad Politècnica de Catalunya. Septiembre 2002.
- [Camp03] Joaquim Camps Aragonès, *Servei WWW sobre GPRS*. Proyecto Final de Carrera de Ingeniería Informática. Departamento de Ingeniería Informática y Matemáticas, Universidad Rovira i Virgili. Junio 2003.
- [Mart02] Antoni Martínez Ballesté, *Pay-per-view en video streaming a Internet*. Proyecto Final de Carrera de Ingeniería Informática. Departamento de Ingeniería Informática y Matemáticas, Universidad Rovira i Virgili. Febrero 2002.
- [Mart03] Ramon Martínez Peña, *Implementació d'un sistema d'autenticació personal basat en Bluetooth*. Proyecto Final de Carrera de Ingeniería de telecomunicaciones. Escuela Técnica Superior de Telecomunicaciones de Barcelona, Universidad Politècnica de Catalunya.
- [Mart03b] Elena Martínez, *Watermarking de imágenes en color en el dominio wavelet*. Proyecto Fin de Carrera de Ingeniería Superior de Telecomunicaciones. Departamento de Teoría de la Señal y Comunicaciones. Universidad Politècnica de Catalunya. Junio 2003.
- [MMSD03] C. Mailet, A. Martínez-Ballesté, F. Sebé y J. Domingo-Ferrer, *Prototipos del proyecto STREAMOBILE*, Report técnico, Departamento de Ingeniería Informática y Matemáticas, Universidad Rovira i Virgili.
- [Vent02] Sergi Ventosa, *Técnicas de Watermarking Robustas a JPEG y a MPEG*. Proyecto Fin de Carrera de Ingeniería Superior de Telecomunicaciones. Departamento de Teoría de la Señal y Comunicaciones. Universidad Politècnica de Catalunya. Junio 2002.