Análisis crítico de los sistemas de huella digital para multicast

Joaquim Camps, Antoni Martínez-Ballesté y Josep Domingo-Ferrer

Departament d'Enginyeria Informàtica i Matemàtiques

Universitat Rovira i Virgili

Av. Països Catalans, 26 – 43007 Tarragona

Contacto: jdomingo@etse.urv.es

Este artículo analiza varias propuestas de huella digital en entornos multicast. Con ellas se pretende, mediante técnicas de detección de copia, identificar quién es el responsable de la distribución ilegal de un contenido multimedia. El análisis revela que ninguna de las técnicas actuales es completamente satisfactoria, por lo que se apuntan posibles mejoras.

Palabras clave: Multicast, digital rights management, secure electronic commerce, fingerprinting.

1 Introducción

La aparición y despliegue de servicios relacionados con el disfrute de contenidos multimedia (por ejemplo, un vídeo) por parte de un número cada vez mayor de usuarios, justifica la adopción de nuevas estrategias para el transporte de dichos contenidos. La distribución de los contenidos a cambio de una transacción económica suele implicar que el contenido tenga una propiedad intelectual que debe protegerse. En este artículo nos centramos en la protección de la propiedad intelectual para servicios de transmisión de vídeo en tiempo real o casi-bajo demanda. El escenario en el cual nos centramos intervienen los siguientes elementos:

- Un flujo de vídeo, cuya propiedad intelectual debe estar protegida.
- Una red de distribución de contenido del proveedor a los usuarios.
- Un sistema de cifrado para acceso al contenido. En estos sistemas se impide, a nivel de aplicación y mediante el uso de criptografía simétrica, que los usuarios no autorizados accedan al contenido. En algunas de las propuestas recogidas, las claves de decodificación juegan un papel importante.
- Un número elevado de usuarios del sistema, que compran el contenido. Los usuarios pueden contar con un dispositivo que les permite obtener, sin pérdida de calidad, una copia digital del flujo al que están accediendo.
- Uno o varios clientes deshonestos, que pueden distribuir su copia a través de una red P2P, o bien obtener copias para ser vendidas en puestos ilegales.

1.1 Transmisión multicast

En la distribución de vídeo en tiempo real, la adopción de una política de distribución unicast (uno-a-uno) conlleva sobredimensionar el ancho de banda del canal de comunicaciones, y por lo tanto, no es rentable desde el punto de vista del operador que explota dicho servicio. La situación puede ser crítica en un entorno de redes inalámbricas con un ancho de banda limitado y un mercado potencial de miles o millones de usuarios finales.

En contraposición, el esquema multicast (uno-a-muchos) permite un aprovechamiento del ancho de banda del canal de comunicaciones mediante el envío de un único flujo multimedia que llega a un grupo final de usuarios, independientemente del número de estos. Las técnicas multicast precisan de unos nodos y protocolos capaces de organizar sesiones y distribuir el contenido sólo a aquellos clientes que estén suscritos a la recepción del contenido, impidiendo el acceso a usuarios no autorizados.

1.2 Detección de copias

La redistribución ilegal de contenidos multimedia por parte de usuarios deshonestos hace que la distribución comercial de estos contenidos se aleje de una situación idílica. La evitación en la copia fraudulenta es deseable, pero se ha demostrado que no es resistente frente al imparable fenómeno hacker. La detección en la distribución ilegal de contenidos es más realista y asumible en cuanto a implementación final.

La idea del proceso es que la copia de cada comprador incluye la identidad de éste: en caso de hallar una copia ilegal, recuperando la marca que esconde el contenido, se puede saber quién es el comprador que se ha convertido en distribuidor deshonesto. Marcar un contenido con la identidad el comprador recibe el nombre de huella digital o fingerprinting.

Las técnicas de marca de agua o watermaking permiten incluir esta identidad a base de esparcir una marca por el contenido a distribuir. El proceso usado debe marcar el contenido de forma imperceptible y evitando degradación del contenido multimedia. La robustez del proceso ha de evitar una detección fácil de la marca así como su modificación. Además, la marca debe resistir a una serie de transformaciones: en el caso de un vídeo interesa, por ejemplo, que la marca se conserve al pasar del formato MPEG-2 al formato DivX. Exceptuando el sistema descrito en la Sección 3.1, ninguna de las propuestas analizadas detalla el sistema de marca de agua utilizado para marcar el vídeo. De hecho, el diseño de un sistema de huella digital presupone su funcionamiento usando un esquema robusto de marca de agua.

1.2.1 Huella digital para sistemas multicast

Conceptualmente, la protección mediante huella digital basada en el envío de información diferenciada para cada usuario no casa bien con el esquema multicast que pretende un envío a todos por igual.

Algunos sistemas confían en la implicación de los nodos intermedios de la red para conciliar la transmisión multicast con la recepción de contenidos marcados de forma distinta para cada cliente. Otros sistemas se basan en que, a partir de una única copia cifrada transmitida por multicast, es el proceso de descifrado realizado por cada cliente el encargado de diferenciar la copia recibida de las copias recibidas por otros clientes; en este segundo tipo de soluciones, cada cliente tiene una clave de descifrado distinta.

1.3 Confabulaciones y códigos resistentes

El hecho de que todas las copias de un mismo contenido lleven marcas distintas hace posible los denominados ataques por confabulación. En estos ataques, dos o varios compradores deshonestos comparan bit a bit sus respectivas copias y utilizan la información sobre las diferencias encontradas entre ellas para componer una nueva copia cuya marca no les identifique.

Para evitar el éxito de este tipo de ataques, es preceptivo que la cadena de bits que identifica a un comprador sea una palabra de un código resistente a confabulaciones, como por ejemplo los propuestos por D. Boneh y J. Shaw [Boneh95]

La particularidad de estos códigos es que, mientras el número de confabulados no supere el límite permitido por el código, la copia generada en una confabulación contendrá una marca que identificará como mínimo a uno de ellos.

Otros códigos con igual propósito se describen en [Sebe03] y [Tardo03].

1.4 Contribución y contenido del artículo

Este artículo describe, compara y critica las distintas propuestas existentes para el marcado de contenido, distribuido y en tiempo real, para un número elevado de compradores en un entorno de distribución multicast.

La Sección 2 trata de sistemas que requieren la intervención de los nodos multicast. La Sección 3 analiza propuestas basadas en distribución de claves. La Sección 4 analiza la propuesta de Bao, basada en un dispositivo confiable asignado al cliente. Este documento finaliza en la Sección 5 con las conclusiones y las líneas maestras de una posible investigación futura en este campo.

2 Sistemas basados en la intervención de los nodos multicast

Las propuestas [Brown99] y [Judge00] implican la actuación de los nodos que conforman el árbol multicast. Se basan en sistemas de confianza distribuidos, cuya implementación no es tarea sencilla. Además, no contemplan el tema de los ataques por confabulación: los sistemas no tienen en cuenta, a la hora de marcar, si un par de compradores podrán eliminar fácilmente la marca.

2.1 Watercasting

En Watercasting [Brown99], se preparan varias versiones marcadas de un mismo paquete de contenido. Se mandan al canal multicast y los routers deben descartar algunos de estos paquetes. Al final, cada cliente contará con un flujo completo, pero marcado en forma particular. Durante el periodo en que los clientes pueden apuntarse al grupo multicast, estos mandan hacia la fuente la petición, juntamente con su identidad, en un mensaje cifrado.

De esta forma solamente la fuente puede reconstruir el árbol de la sesión multicast y, de paso, puede organizar el descarte de paquetes por parte de los routers.

Este sistema presenta una serie de inconvenientes. En primer lugar es muy dependiente del sistema de transmisión multicast utilizado, puesto que debe permitir, entre otras, herramientas de descarte de paquetes (en la propuesta se usa una modificación del PGM[1]). Por otra parte, la estructura del árbol que se forme tiene importancia en relación al rendimiento o complejidad de la propuesta para una sesión en concreto. Finalmente, se necesitan transmitir d versiones de cada paquete de contenido, siendo d la profundidad del árbol multicast. Así pues, en routers próximos a la fuente (que todavía

[1] Pragmatic General Multicast.

no han descartado muchos paquetes), el consumo de ancho de banda puede ser prohibitivo incluso para d moderada, puesto que se trata de vídeo en tiempo real.

En lo que concierne a una implementación real, Watercasting precisa que el distribuidor sea quien controle la red.

2.2 WHIM

En WHIM[2] [Judge00], la marca de agua se genera en función de la localización del cliente dentro de la red: el contenido se va marcando mientras va pasando por los distintos nodos del árbol multicast.

De hecho, el contenido es marcado mediante una red distribuida de intermediarios. Éste es el principal inconveniente: su implementación implica el despliegue de esta red de intermediarios. La principal ventaja respecto al anterior sistema está en la menor cantidad de datos transmitidos.

3 Sistemas basados en la distribución de claves

Los sistemas presentados en esta sección tienen en común que el marcaje del contenido tiene relación con las claves asignadas al comprador para poder acceder al contenido.

3.1 El cifrador de flujo Chameleon

Chameleon [Ander98] es un cifrador de flujo desarrollado a partir de PIKE [Ander94]. El objetivo primordial que persigue Chameleon es el de ofrecer un mecanismo que permita la remisión de una clave distinta a cada usuario de manera que todas ellas descifren un único contenido cifrado. Al tener claves diferentes, cada usuario descifrará de manera ligeramente diferente. El algoritmo subyacente a Chameleon permite reflejar en el texto cifrado los cambios producidos en la clave marcada de cifrado. Esta característica da nombre al cifrador en clara alusión al reptil que adapta su aspecto externo a las condiciones cambiantes de su entorno.

La Figura 1 ilustra el funcionamiento de Chameleon. En este esquema se denomina clave A a la clave que genera el cifrador PIKE como expansión de una clave inicial c.

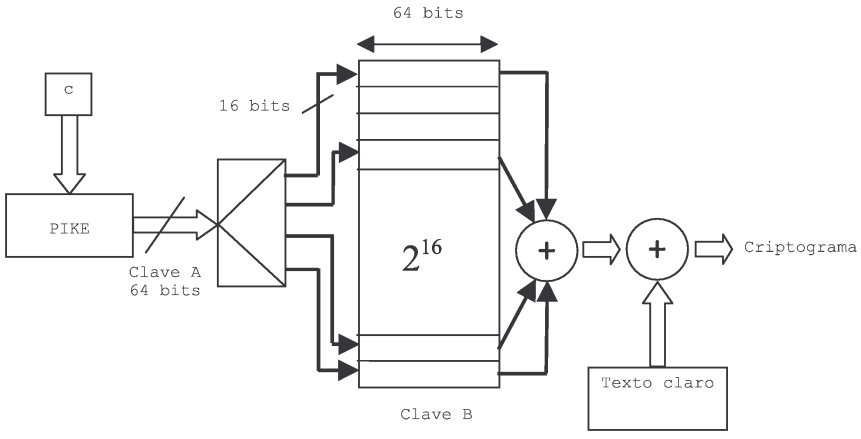

Figura 1. Cifrador de flujo con marcado de claves Chameleon

[2] Watermarking with a Hierarchy of InterMediaries.

Se dispone de una segunda clave B consistente en una tabla de 2^{16} palabras de 64 bits cada una: en total 512 KB. Una palabra de 64 bits a la salida del cifrador PIKE direcciona 4 palabras de 64 bits en B. La clave final es el resultado de realizar la operación OR-Exclusiva entre estas 4 palabras. Realizando de nuevo la operación OR-Exclusiva entre la clave obtenida y el contenido en claro se obtiene finalmente el criptograma.

El cambio de un único bit en B conlleva, en promedio, el cambio de 4 bits por cada 512 KB de clave final. Debido a la particular estructura del cifrador, estos cambios se reproducirán en las mismas posiciones en el criptograma resultante. En una aplicación de marcado de señales de audio de 16 bits, se podrá realizar dicho marcado en los bits de menor peso, minimizando la degradación del contenido a distribuir.

3.1.1 Ventajas e inconvenientes

La ventaja sustancial que ofrece esta aproximación es la transmisión de un único contenido cifrado, a diferencia de otros esquemas como pueden ser [Marti03] y [Parvi01], descritos más adelante. Ello supone un uso más eficiente del ancho de banda del canal de comunicaciones.

Al realizarse el proceso de marcado en el nodo emisor, no se hace necesaria en ningún momento la intervención de routers multicast en el proceso de distribución de contenidos multimedia: su operativa se limitará a encaminar los paquetes entre nodos.

Querer garantizar una cierta inmunidad frente a confabulaciones presupone en Chameleon hacer a priori una estimación del grado de coordinación de los atacantes. Una vez estimado el número de atacantes hay que establecer el número total de claves a disposición del emisor así como del subconjunto a distribuir a cada usuario final, pudiendo resultar un esquema no escalable.

La solución ideal podría pasar por encontrar una forma de marcar el contenido con un código resistente a confabulaciones (como un Boneh-Shaw, por ejemplo). De hecho, esto puede llevarse a cabo distribuyendo el código en las columnas de B referentes a las posiciones marcables del contenido. Pero, aun pudiendo insertar un código anti-confabulaciones, el problema estaría en que Chameleon marca directamente el contenido sin usar ningún método robusto de marca de agua. Así pues, un usuario puede eliminar arbitrariamente gran parte o la totalidad del código sencillamente haciendo un remuestreo o una compresión del contenido recibido.

Para finalizar, en la definición de Chameleon no se considera la existencia de una etapa de compresión/decompresión, muy importante en la transmisión de contenido digital. Incluir esta etapa en el proceso de codificación y decodificación de Chameleon impediría su buen funcionamiento.

3.2 La aproximación de Parviainen y Barnes

En el esquema de Parviainen y Barnes [Parvi01], cada nodo emisor envía dos copias cifradas diferentes de cada paquete de vídeo con marcas distintas. Este cifrado para el paquete i-ésimo se realiza mediante dos claves escogidas de manera aleatoria: k_i^0 y k_i^1. Los dos paquetes cifrados se envían a todos los miembros del grupo mediante multicast.

Cada cliente receptor dispone, para cada fracción del contenido, únicamente de una de las dos claves de encriptación, luego será capaz de descifrar sólo uno de los dos paquetes que le lleguen. La asignación de claves a cada usuario final por parte del emisor determina cual de los dos paquetes va a ser capaz de descifrar.

3.2.1 Ventajas e inconvenientes

Tal como sucede en Chameleon, no es necesaria la intervención de routers multicast en la distribución de los contenidos hacia los usuarios finales. Por lo tanto esta propuesta es válida tanto para entornos multicast como broadcast.

La estructura del esquema fuerza inevitablemente a transmitir dos veces un mismo contenido. Por consiguiente, es preceptivo el disponer del doble de ancho de banda que requieren otros esquemas como por ejemplo Chameleon. Aun así, se reduce considerablemente la cantidad de datos transmitida por el sistema Watercasting.

Asumiendo la robustez del algoritmo de inserción de marcas en el contenido a distribuir, el esquema de Parviainen y Barnes se muestra resistente frente a confabulaciones de dos compradores.

Sin embargo, no lo es cuando el número de éstos es igual o superior a tres, tal como se demuestra en [Marti03]. Desenmascarar al usuario deshonesto consiste en encontrar un usuario con huella digital cercana a la huella recuperada de la copia ilegal. La distancia con la huella recuperada vendrá determinada por la distancia de Hamming entre ambos. En una confabulación entre tres usuarios se seleccionan aquellos fragmentos de la trama que no son recibidos idénticamente por los tres. La estrategia para crear la copia pirata consiste en escoger siempre el fragmento que difiere de los otros dos. Siendo aleatoria la asignación de claves con k bits a cada usuario final, se espera que la huella de cualquier confabulante difiera en k/2 bits de la huella generada de manera fraudulenta. Al ser la distancia de Hamming esperada de un usuario honesto también de k/2 bits, queda patente la indefensión frente al ataque de tres confabulantes bien organizados.

3.3 El enfoque de Martínez et. al

A fin de solventar la debilidad de la propuesta de Parviainen y Barnes frente a confabulaciones de tres o más usuarios, proponemos en [Marti03] un esquema alternativo basado en los códigos de Boneh-Shaw. En este esquema:

- El distribuidor de los contenidos hace una estimación del número máximo de usuarios N y escoge los valores de c (número de confabulantes) y de ε, probabilidad de fallo en la reidentificación del confabulante).
- Se construye un código Boneh-Shaw de longitud de palabra L, de acuerdo con los parámetros de la sesión.
- El emisor divide el contenido multimedia en L paquetes y genera dos versiones cifradas para cada uno de ellos.
- Cada usuario recibe una palabra del código, que consiste en un conjunto de L claves para descifrar: considerando el paquete i-ésimo, si el bit i-ésimo en la palabra es 0, entonces el receptor recibirá k_i^0; en caso contrario recibe k_i^1.

3.3.1 Ventajas e inconvenientes

Tal como sucedía en la aproximación de Parviainen y Barnes, no se requiere de la intervención de routers multicast al realizarse el marcado en la fuente de la información, facilitando con ello el despliegue de un sistema con estas características.

En base a la utilización de códigos de Boneh-Shaw resistentes a confabulaciones, este esquema se muestra seguro frente a confabulaciones de tamaño arbitrario.

El inconveniente de esta propuesta es, como en la anterior, la necesidad de distribuir los contenidos por duplicado.

4 Marcaje mediante el dispositivo del usuario

Otra alternativa existente para marcar el contenido recibido por cada comprador, más simple pero no por eso menos válida, es usar un dispositivo resistente a manipulaciones (tamper-resistant hardware). Esta propuesta es válida tanto para entornos multicast como broadcast. En la propuesta expuesta en [Bao00], el usuario recibe datos digitales en su decodificador digital o D-STB[3], el cual decodifica el contenido gracias a una clave que se encuentra en un dispositivo resistente a manipulaciones, como por ejemplo una tarjeta inteligente. Una solución bastante habitual consiste en empotrar dicho dispositivo en el interior del decodificador, haciendo inviable el acceso al dispositivo.

El sistema descrito en [Bao00] consiste en:

- W(M,sn), un esquema robusto de marca de agua que empotra la cadena sn en el flujo multimedia M.
- Un dispositivo resistente a manipulaciones, que forma parte del D-STB. Este dispositivo se identifica por su número de serie sn. Internamente se guarda una clave secreta, SK_{sn}, que dispondrá de su correspondiente clave pública PK_{sn}.

Cuando el comprador se dispone a visualizar un contenido, la clave de decodificación del contenido se cifra con PK_{sn}, con lo cual se asegura que el comprador sea el único que puede acceder a dicho contenido. La misma tarjeta inteligente es quien marca el contenido con el valor de sn.

4.1.1 Ventajas e inconvenientes

Esta propuesta es fácilmente implementable y, según el artículo, ciertamente económica: unos 20 dólares. Sin embargo, marcar los contenidos a distribuir con el valor de sn es de poca utilidad: dos compradores confabulados (comparando sus copias), eliminarían fácilmente la marca o parte de ella, haciendo imposible su recuperación para hallar la identidad del pirata.

La solución podría consistir en utilizar códigos de Boneh-Shaw asociados a un sn determinado. Se podría mandar, conjuntamente con la clave de decodificación, el código asignado para el marcaje de aquella determinada copia.

5 Conclusiones

Este artículo ha analizado las propuestas existentes para huella digital en entornos multicast. La protección mediante huella digital (la copia del contenido que adquiere el comprador esconde una marca que lo identifica) no casa bien con el esquema multicast, que pretende un envío del mismo contenido a todos los compradores.

Se han descrito tres tipos de técnicas: propuestas que se basan en la participación de los nodos del árbol multicast, propuestas basadas en las claves de decodificación del contenido y una propuesta basada en la resistencia a manipulaciones del dispositivo reproductor.

---

[3] Digital Set Top Box.

Se concluye que ninguna de las técnicas actuales es completamente satisfactoria: por una parte, hay sistemas dependientes de los nodos o de la confianza hacia ellos; por otra parte, hay propuestas que precisan de la réplica de contenido para conseguir una marca distinta para cada usuario.

La línea actual de investigación se centra en hallar un sistema robusto frente confabulaciones que necesite el mínimo de intervención por parte de los nodos y que no precise de replicación de contenido.

Referencias

[Ander94] R. Anderson, “On Fibonacci Keystream Generators”, Fast Software Encryption, Springer LNCS vol. 1008, pp. 346-352, 1994.

[Ander98] R. Anderson y C. Manifavas, “Chameleon - A New Kind of Stream Cipher”, Fast Software Encryption, pp. 107-113, 1997.

[Bao00] F. Bao, “Multimedia Content Protection by Cryptography and Watermarking in Tamper-resistant Hardware”, Proceedings of the 2000 ACM workshops on Multimedia, pp. 139-142, 2000.

[Boneh95] D. Boneh y J. Shaw, “Collusion-secure fingerprinting for digital data", Advances in Cryptology - CRYPTO'95, LNCS 963, Springer-Verlag, pp. 452-465, 1995.

[Brown99] I. Brown, C. Perkins y J. Crowcroft, “Watercasting: Distributed Watermarking of Multicast Media”, Proceedings of the First International Workshop on Networked Group Communication, pp. 286-300, 1999.

[Judge00] P. Judge y M. Ammar, “WHIM: Watermarking multicast video with a hierarchy of intermediaries”, Proceedings of NOSSDAV 2000, 2000.

[Marti03] A. Martínez-Ballesté, J. Domingo-Ferrer y F. Sebé, “Fingerprinting schemes for multicast delivery”, International Conference on Information Technology: Research and Education - ITRE03, 2003.

[Parvi01] R. Parviainen y P. Barnes, “Large scale distributed watermarking of multicast media through encryption”, Proceedings of IFIP Communications and Multimedia Security, pp. 149-158, 2001.

[Sebe03] F. Sebé y J. Domingo-Ferrer, “Collusion-secure and cost-effective detection of unlawful multimedia redistribution”, *IEEE Transactions on Systems, Man and Cybernetics, Part C*, vol. 33, no. 3, pp. 382-389, 2003. ISSN 1094-6977

[Tardo03] G. Tardos, “Optimal probabilistic fingerprint codes”, Proceedings of the 35th Annual ACM Symposium on Theory of Computing, 2003.