Uso de códigos trazables para protección del copyright

Miguel Soriano Ibáñez

Dpto. Ingenieria Telemática
Universitat Politècnica Catalunya
Jordi Girona 1-3, 08034-Barcelona
soriano@mat.upc.es

La venta de contenidos digitales a través de redes informáticas constituye la forma más natural de comercio electrónico ya que incluso la distribución puede hacerse en el momento de la compra y a través de la red. Sin embargo, el volumen de negocio actual es muy inferior a las espectativas que se tenían hace unos años. Una de las causas que está frenando este mercado es la dificultad de proteger adecuadamente la propiedad intelectual y los derechos de distribución. La técnica que habitualmente se utiliza es la de fingerpriting, consistente en marcar de forma única y exclusiva del objeto a distribuir. Ante esta técnica, un posible ataque consiste en la confabulación de varios usuarios fraudulentos, creando así una copia pirata distinta a la de cada uno de ellos.

Los códigos trazables permiten rastrear e identificar a uno de los atacantes en el caso de un ataque de confabulación. Dichos códigos son un caso particular de los códigos correctores de errores. Las palabras código pueden ser usadas como "fingerprinting codewords". A cada distribución de la copia se le asigna una palabra código que será "empotrada" a lo largo del documento mediante el algoritmo de marcado.

El código ideal sería aquél que permitiese identificar a todos los participantes de una confabulación fraudulenta, independientemente del tamaño de dicha coalición. Se puede demostrar que no existe ningún código que pueda garantizar este objetivo deseable. Utilizando las técnicas habituales de control de errores, si el número de símbolos e en los que difiere la palabra recibida de la palabra código más cercana es inferior a la mitad de la distancia mínima del código, a la salida del decodificador se obtendría la única palabra código cuya distancia a la palabra recibida es e. Sin embargo, si el número de símbolos diferentes es mayor que la cota anterior, no se garantiza la condición de unicidad. En cualquier caso, no se puede asegurar que la palabra código más cercana esté asociada a un distribuidor ilegítimo. Por ello, puede ser necesario utilizar otro tipo de técnicas de decodificación.

A lo largo de este artículo se presentarán distintas alternativas para satisfacer los requisitos en distintos entornos. Por ello, en primer lugar se establece una clasificación de los tipos de códigos en base a sus propiedades de localización. Posteriormente se presentará esquemas de identificación sin incertidumbre, teniendo en cuenta tanto la codificación como la decodificación mediante técnicas soft-decision.