ESQUEMAS DE *FINGERPRINTING* COMO PROTECCIÓN DE LOS DERECHOS DE AUTOR

SCHEMES OF FINGERPRINTING AS PROTECTION OF COPYRIGHT

Carolina Tripp-Barba, José Alfonso Aguilar Calderón, Carlos Eduardo Zurita
Facultad de Informática Mazatlán, Universidad Autónoma de Sinaloa, México.
E-mail: [ctripp, ja.aguilar, czurita]@uas.edu.mx

(Enviado Abril 25, 2018; Aceptado Junio 19, 2018)

Resumen
Una de las oportunidades que ofrece Internet es la facilidad para distribuir productos digitales; tal es así que una gran parte de los sectores productivos han utilizado la red como medio natural de intercambio de información. El uso de documentos digitales, además de facilitar su distribución y manejo, permite su transformación bien o malintencionada por la comunidad de usuarios del producto. En consecuencia, aparecen nuevos problemas relacionados con la implantación del *copyright* y derechos de distribución en contenidos digitales. En el presente documento se aborda un tema relacionado con la seguridad en los documentos digitales, los cuales en tiempo reciente han ido en aumento. Se explicará en que consiste el *fingerprinting* como ayuda a proteger los derechos de autor, así como sus técnicas más utilizadas y la necesidad de su implementación. El objetivo de este trabajo es el tomar conciencia sobre la manera en que se puede tratar de proteger dichos derechos haciendo énfasis en que en la actualidad no existe ningún método capaz de evitar la piratería.

Palabras clave: *Fingerprinting, Derechos de Autor, Seguridad.*

Abstract
One of the opportunities offered by the Internet is the ease of distributing digital products; such is the case that a large part of the productive sectors has used the network as a natural means of information exchange. The use of digital documents, in addition to facilitating their distribution and management, allows their transformation well or maliciously by the community of users of the product. As a result, new problems arise regarding the implementation of copyright and distribution rights in digital content. This research attempts to address the issue related to security in digital documents, which in recent times have been increasing. It will explain what is Fingerprinting regarding to help to protect copyright, as well as its most commonly used techniques. Going through the need of its implementation until reaching the explanation of these tools. All this to raise awareness about how you can try to protect these rights, but emphasizing that currently there is no 100% method capable of avoiding piracy.

Keywords: *Fingerprinting, Copyright, Security.*

1 INTRODUCCIÓN

Los requisitos de seguridad de la información dentro de una organización han sufrido dos cambios importantes en las últimas décadas. Antes del uso generalizado del equipo de procesamiento de datos, la seguridad de la información que se consideraba valiosa para una organización se proporcionaba principalmente por medios físicos y administrativos.

Con la introducción de la computadora, se hizo evidente la necesidad de herramientas automatizadas para proteger archivos y otra información almacenada en la computadora; principalmente en los sistemas a los que se puede acceder a través de una red telefónica pública, una red de datos o Internet. El nombre genérico para la colección de herramientas diseñadas para proteger los datos y frustrar los piratas informáticos es la seguridad informática.

Un ataque es cualquier acción que pueda comprometer la seguridad de la información que pertenece a una organización. En este sentido, un mecanismo de seguridad es un proceso (o dispositivo que incluya este proceso) diseñado para detectar, prevenir o recuperarse de algún ataque. Por lo cual, los servicios se seguridad están destinados a contrarrestar los ataques, y hacen uso de uno o más mecanismos de seguridad.

En el estándar de arquitectura de seguridad de la ISO 7498-2 se encuentra la definición de un servicio de seguridad, la cual se describe como el servicio proporcionado por un nivel de un sistema abierto que garantiza su seguridad o el de las transferencias de datos

en dichos sistemas. Estos servicios están divididos en cinco categorías [1], [2]:

1. Confidencialidad: Evita el acceso no autorizado a parte o a la totalidad de la información.
2. Autenticación: Ofrece la certeza de la identidad de una entidad. Puede ser simple o mutua. Cuando es simple, únicamente uno de los comunicantes tiene que demostrar su identidad. Cuando es mutua, ambos comunicantes se identifican el uno al otro.
3. Integridad: Protege contra la modificación, el borrado o la sustitución de la información durante la transmisión. Igual que ocurre con el servicio de confidencialidad, se puede aplicar a una cadena de mensajes, a un único mensaje, o a campos específicos del mensaje.
4. No repudio: Protege contra la negación de una entidad que participa en una comunicación, de haber enviado un mensaje (repudio de origen) o de haberlo recibido (repudio de entrega). Dicho servicio también es conocido como irrenunciabilidad.
5. Control de acceso: Evita el uso o la manipulación no autorizada de recursos. Se controla el acceso a los sistemas informáticos y a los enlaces de datos evitando las infiltraciones y el uso no autorizado de recursos [3].

2 ATAQUES Y AMENAZAS

Una amenaza puede considerarse como una potencial de violación de la seguridad, que existe cuando hay una circunstancia, capacidad, acción o evento que puede violar la seguridad y causar daño. Es decir, una amenaza es un posible peligro que podría explotar una vulnerabilidad. En cambio un ataque a la seguridad del sistema que se deriva de una amenaza inteligente; es decir, un acto que es un intento deliberado (especialmente en el sentido de un método o técnica) para evadir los servicios de seguridad y violar la política de seguridad de un sistema.

Tanto en la transmisión de datos como en el almacenamiento de éstos, se deben asegurar dos requisitos fundamentales: la confidencialidad y la autenticación, para prevenir el acceso a la información o su modificación de forma no autorizada.

Los ataques de los que pueden ser objetos los sistemas telemáticos se pueden dividir en dos categorías [4]:

- **Pasivos**: cuando el atacante o fisgón (*eavesdropper*) simplemente observa o escucha la información, pero no la manipula. En estos casos, no existen problemas de autenticidad. Los ataques pasivos son muy difíciles de detectar porque no implican ninguna alteración de los datos. Normalmente, el tráfico de mensajes se envía y recibe de una manera aparentemente normal y ni el remitente ni el receptor saben que un tercero ha leído los mensajes u observado el patrón de tráfico. Sin embargo, es factible evitar el éxito de estos ataques, generalmente mediante cifrado. Por lo tanto, el énfasis en lidiar con los ataques pasivos está en la prevención más que en la detección.
- **Activos**: implican algunas modificaciones de la secuencia de datos o la creación de una secuencia falsa. Los ataques activos presentan las características opuestas de los ataques pasivos. Mientras que los ataques pasivos son difíciles de detectar, existen medidas para evitar su éxito. Por otro lado, es bastante difícil evitar los ataques activos en forma absoluta, debido a la gran variedad de posibles vulnerabilidades físicas, de *software* y de red. En cambio, el objetivo es detectar ataques activos y recuperarse de cualquier interrupción o retraso causado por ellos. Si la detección tiene un efecto disuasorio, también puede contribuir a la prevención.

3 DERECHOS DE AUTOR

Las técnicas criptográficas no son suficientes para resolver la problemática de los derechos de autor, debido a que surgen dudas del comportamiento del receptor cuando posee un documento. La sentencia de un tribunal de apelaciones de California contra la empresa *Napster*, dada a conocer en febrero de 2001 puso de manifiesto que la distribución de contenidos multimedia sobre Internet sin respetar la propiedad intelectual de los propietarios de dichos contenidos constituye una actividad ilegítima.

A través de los años la importancia de proteger los derechos de autor ha crecido enormemente debido al incremento desmedido de la violación de los mismos. En realidad la defensa de los derechos de autor fue reconocida, de forma parcial, gracias a la revolución francesa. En la modernidad se reconoce como *copyright* según la convención de Berna en 1886 y le da al autor los siguientes derechos: Derecho de reproducción (crear copias del trabajo), Derecho derivativo (crear trabajos nuevos, que deriven o que sean adaptaciones del trabajo protegido), Derecho de distribución (vender o distribuir copias del trabajo al público), Derechos de muestra (mostrar su trabajo, como por ejemplo tocar una composición musical o realizar una exposición fotográfica en público).

El problema que se ha creado recientemente es la imposibilidad de garantizar el cumplimiento de estos derechos. En algunas legislaciones no se garantizaron totalmente, por ejemplo, en EUA se permitió el uso libre de grabadoras de casetes de video y de audio, lo que permite la distribución ilegal de música y video. Actualmente, un fenómeno muy perjudicial para los escritores es la distribución no autorizada (piratería) de libros, pues la inversión realizada del distribuidor pirata es mucho menor que la que la editorial original debe realizar y esto afecta de una manera realmente preocupante al autor, que es real poseedor de los derechos. Pero si la piratería de libros es un campo

preocupante, la industria de la música y el cine están siendo golpeadas por el fenómeno de la piratería de una manera alarmante. Otro de los escenarios en que se presentan violaciones graves en los derechos de autor es en Internet, gracias a las facilidades que existen hoy en día para acceder a la red con grandes anchos de banda a bajo costo, y la gran capacidad de procesamiento de los ordenadores actuales, los usuarios tienen la facilidad de transmitir, reproducir y guardar grandes cantidades de información en casi todos los formatos disponibles, en particular audio y vídeo, actualmente se permite utilizar algoritmos de compresión avanzados que reducen el ancho de banda y el tamaño requerido para que un usuario normal pueda disfrutar de una película o de una canción con una calidad muy aceptable.

Para evitar la violación de derechos de autor y sus consecuencias, se han desarrollado esquemas para evadir estos problemas en documentos de tipo digital [5]. La protección del *copyright* puede conseguirse mediante dos tipos de estrategias: protección a *priori* (impedimento de la copia) y protección a *posteriori* (detección de la copia). El fallo del mecanismo de impedimento de copia de DVD (*Digital Versatile Disk*) muestra la falta de efectividad de la protección a *priori*. Existe la convicción en la comunidad científica que la protección a *posteriori* es el único mecanismo con posibilidades de éxito. Esta realidad facilitó el desarrollo de nuevas técnicas que permitan dar validez real al *copyright* en el mundo de las nuevas tecnologías, tal es el caso de las marcas de agua (*watermarks*), las cuales se basan en la inserción de una marca consistente en un conjunto de *bits* en los contenidos que se desean proteger. Si la marca contiene información del autor, su extracción permite identificarlo, protegiendo la propiedad intelectual. En caso que la marca contenga información relativa al comprador la marca permitirá conocer que distribuidores han actuado de forma deshonesta en caso de copias ilegítimas. En tal caso, se denominan "huellas digitales" o *fingerprinting*.

4 *FINGERPRINTING*

Los *fingerprints* son característicos de un objeto que hacen que éste se pueda distinguir de otros objetos similares. *Fingerprinting* [6] se define como el proceso de agregar huellas digitales o marcas a un objeto o de identificar aquellos que ya han sido insertados dentro de un objeto. Los objetos a los que se les puede aplicar *fingerprinting* no tienen que ser objetos de tipo digital. Antes de la era digital este mecanismo era ya utilizado con otros fines. Los seres humanos son el ejemplo clásico, gracias a la huella dactilar (utilizada sobre todo para asuntos criminales), el iris de los ojos y la voz. Los números seriales de productos manufacturados son otro de los *fingerprints* que se usan para diferenciar productos. También en algunos explosivos se fabrican con partículas especiales que pueden recuperarse después de la explosión, con lo que se puede identificar, aún después datos como el fabricante de la bomba, el tiempo de manufactura de la misma y otros parámetros relevantes. En este sentido, es importante describir algunos conceptos que mejoran el entendimiento de estos mecanismos de identificación y su proceso, por ejemplo que, una marca es una porción de un objeto que tiene un número de posibles estados; un *fingerprint* es un grupo de marcas; un distribuidor es un proveedor autorizado de objetos ya marcados (con un *fingerprint*); un usuario acreditado es un individuo con acceso autorizado a un objeto marcado; un atacante es un individuo que obtiene acceso de manera no autorizada al objeto marcado; un traidor es un usuario autorizado que realiza copias y distribuye objetos marcados de manera ilegal, un objeto marcado es un objeto con su *fingerprint* insertado.

El proceso que se lleva a cabo en el *fingerprinting* comienza con la producción de los objetos, a los que se les añade posteriormente los *fingerprints* que los van a identificar, la inserción de los *fingerprints* es llevada a cabo por parte del distribuidor. Cuando el distribuidor vende los objetos ya marcados, uno o más compradores (usuarios autorizados) pueden distribuir de manera no autorizada copias del objeto marcado, pero cuando el distribuidor encuentre una copia ilegal, gracias al *fingerprint* que la copia tiene insertado se podrá descubrir cuál usuario es el traidor. En un modelo general de *fingerprinting* el objetivo del distribuidor es lograr identificar a los traidores mientras que el objetivo de un atacante es prevenir la identificación del traidor por parte del distribuidor.

5 ESQUEMAS DE *FINGERPRINTING*

Antes de que la era de la información basada en computadoras surgiera, sólo el *fingerprinting* físico era estudiado y aplicado. Pero debido al gran auge de los medios digitales en esta última era, existe una necesidad cada vez más amplia de proteger los derechos de autor de documentos que se pueden almacenar en formato digital. Algunos ejemplos de datos digitales que pueden ser marcados son documentos, imágenes, películas, archivos musicales, archivos ejecutables, etc.

En el caso de *fingerprinting* existe la posibilidad de realizar ataques de confabulación, es decir, distintos compradores se unen, comparan bit a bit sus copias y entre todos ellos eliminan o generan una nueva marca distinta a la que tienen cada uno de ellos. En consecuencia, un esquema de *fingerprinting* adecuado debe permitir identificar a los usuarios deshonestos que han participado en la confabulación. La detección de dichos usuarios se consigue mediante el uso de esquemas con propiedades de rastreo. Los esquemas de *fingerprinting* pueden clasificarse en simétricos, asimétricos y anónimos. A continuación se explicarán los principales esquemas existentes en nuestros días.

5.1 *Fingerprinting* simétrico

El *fingerprinting* simétrico [7] es aquel en el que tanto el distribuidor como el usuario autorizado tienen acceso al objeto marcado, además en la mayoría de los casos el distribuidor es el que introduce los *fingerprints* en ellos. Este tipo de *fingerprinting* tiene una gran objeción, por

ejemplo, cuando un usuario autorizado se ha convertido en un traidor debido a que ha copiado y distribuido el objeto marcado que le ha vendido el distribuidor de manera ilegal, si suponemos que el distribuidor encuentra una de las copias ilegalmente distribuidas y gracias al *fingerprint* encontrado en ella puede determinar quién es el traidor, no podrá culparlo de haber cometido el delito, puesto que el traidor fácilmente puede alegar que, dado que el distribuidor conocía perfectamente el *fingerprint* realizado al objeto, el mismo distribuidor puede estar distribuyendo las copias ilegalmente con el objetivo de inculparlo. Este problema se puede superar usando el esquema de *fingerprinting* asimétrico que será abordado posteriormente. El método más usado de *fingerprinting* de tipo simétrico es el seguro contra colusión [8].

5.2 *Fingerprinting* asimétrico

En los primeros sistemas de *fingerprinting*, llamados simétricos, es el vendedor quien marca el contenido. El problema de esto es que un vendedor deshonesto puede distribuir ilegalmente una copia que éste ha marcado para un determinado usuario. Si se encuentra la copia ilegal, se culparla al usuario. Por otra parte, un cliente fraudulento puede distribuir ilegalmente su copia y luego acusar al vendedor de la distribución.

Para evitar este problema es necesario que durante el proceso de marcado el vendedor no tenga acceso a la copia marcada. Los sistemas que cumplen con este requisito son los denominados asimétricos. En ellos, el proceso de marcaje consiste en un protocolo en el que intervienen vendedor y comprador.

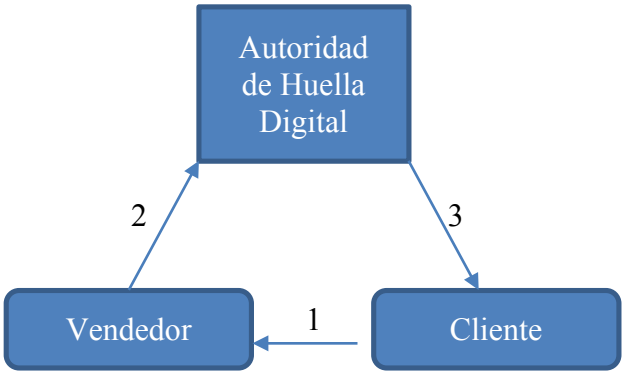

Figura 1 Esquema fingerprinting asimétrico.

El *fingerprinting* asimétrico fue introducido por Pfitzmann and Schunter [9], pretende solucionar el problema del *fingerprinting* simétrico impidiendo que el vendedor conozca la copia marcada que entrega al comprador, aunque puede identificarla. Para ello en el proceso de marcado deben intervenir tanto el vendedor como el comprador. El vendedor puede posteriormente identificar a partir de la marca al comprador, pero no puede generarla sin su presencia. Este esquema tiene el inconveniente del anonimato; el vendedor conoce la identidad del comprador. En la Figura 1 podemos ver un diagrama de su funcionamiento.

5.3 *Fingerprinting* anónimo

Hasta el momento se han descrito diferentes esquemas del *fingerprinting*, en el primer enfoque que se le dio al *fingerprinting* las marcas de las copias son realizadas solo por el vendedor, por lo que tanto el vendedor como el comprador conocen la copia marcada en cuanto se produce la compra, es así que habrá dos posibles culpables en caso de que se encuentre una copia con dichas marcas, y tanto el uno como el otro podrán negar responsabilidades. Con el fin de cubrir esas deficiencias en dicho esquema se presenta una mejora (*fingerprinting* asimétrico) en la cual el comprador es el único que conoce la copia marcada y en consecuencia cualquier redistribución posterior de la misma debe ser responsabilidad únicamente del comprador.

En el área de comercio electrónico (*e-commerce*) se buscar conservar el proceso de compra tradicional en donde el comprador acude a un establecimiento, elige sus productos y paga en efectivo, de tal manera que se resguarde el anonimato de las transacciones, no es deseable por los compradores que dicho anonimato se pierda solo por el caso del *fingerprinting* (sea este simétrico o asimétrico) preexistiendo que el proceso de marcaje revelaría la identificación del comprador, es así como se propone un nuevo esquema de *fingerprinting* en donde se parte del concepto del asimétrico pero enriquecido con la característica del anonimato, por lo que en el proceso de marcaje y la venta, el vendedor no conoce la copia marcada y tampoco conocerá la identidad del comprador ya que este realiza la compra mediante un pseudónimo, lo cual permitirá su identificación en caso de redistribución.

El esquema anónimo de *fingerprinting* [10, 11] sigue siendo sujeto de investigación porque sigue con deficiencias, tales como cuando el vendedor finalmente logra obtener la identidad y por otro lado el comprador tiene que contactar al centro de registro antes de cualquier compra, aquí solo presentamos el panorama general de funcionamiento así como también la evolución que cada uno de los esquemas representan entre ellos.

6 *TRAITOR TRACING* (RASTREO DEL TRAIDOR)

El *copyright* son los derechos que se le otorgan a los autores de obras intelectuales sobre estas. Esto es para evitar las copias de las ideas de otros. Esto primero se vio justificado bajo el pretexto de los pagos de editoriales e imprentas. Ahora en la llamada era digital, con el solo hecho de subir algún archivo digital a la red este puede darle la vuelta al mundo en segundos, esto desfavoreciendo los derechos del autor para difundir sus ideas. Por esto, los piratas están haciendo un negocio con el hecho de romper la seguridad de datos digitales para permitir que terceros puedan tener acceso a estos contenidos. Para tratar de evitar o minimizar en la medida

de lo posible la violación de estos privilegios o derechos de cada autor para que su obra no sea utilizada sin el pago correspondiente se ha desarrollado este esquema para tratar de localizar a la persona que al haber hecho el pago se siente con el derecho de distribuir la obra hacia terceros. Si existe un secreto que es conocido solo por una persona, y por alguna razón ese secreto es conocido por otra u otras personas el culpable es evidente. Pero cuando un grupo grande de personas comparten un secreto en común, es más complejo saber quién es el culpable en caso de ser descubierto, ya que si todos están compartiendo la misma información es demasiado improbable saber exactamente quien es culpable o inocente. Una posibilidad para poder encontrar al traidor es que a cada una de las partes que conocen el secreto se le dé a conocer la información pero con una leve modificación en los datos.

Tomando esto en cuenta, se aplicó la idea para combatir la piratería y prevenir la transferencia de información a los usuarios pirata pero sin dañar al usuario legítimo. Además, sirvió para proporcionar evidencia legal del usuario ilegitimo. El funcionamiento general de este esquema es el siguiente: el distribuidor genera un conjunto *R* con *r* llaves aleatorias y a cada usuario se le asigna *m* llaves fuera de *R*, estas formaran la llave personal del usuario.

Un mensaje del esquema *Traitor Tracing* [12, 13] consiste de múltiples pares, es decir, la información está dividida en *enabling block* (bloque permitido) y *cipher block* (bloque cifrado).

- El *cipher block* (bloque cifrado), es una cifra simétrica de la información actual, se podría decir que son unos segundo de un video bajo alguna llave secreta aleatoria S.

- El *enabling block* (bloque permitido) permite a los usuarios autorizados obtener *S*, y consiste en cifrar datos de video bajo alguna o todas las llaves r del distribuidor. Cada usuario puede utilizar S para cifrar y descifrar datos de video usando sus llaves, esto significa que, el conjunto de llaves de los usuarios y el *enabling block* (bloque permitido) se convierten en la entrada para generar la llave para descifrar el correspondiente bloque cifrado.

Los usuarios autorizados que permiten el uso de su información confidencial (traidores), pueden dar una copia no autorizada de sus llaves secretas a algún usuario no autorizado y de esta manera este también podrá descifrar el bloque cifrado. El punto principal de este esquema es asignar llaves a los usuarios de manera que cuando un usuario no autorizado o pirata obtiene la información es capturado y las llaves que tiene en su poder pueden ser examinadas, de esta manera es posible detectar al traidor. El esquema de la Figura 2 pretende aportar evidencia legal para las traiciones por parte de los usuarios legales.

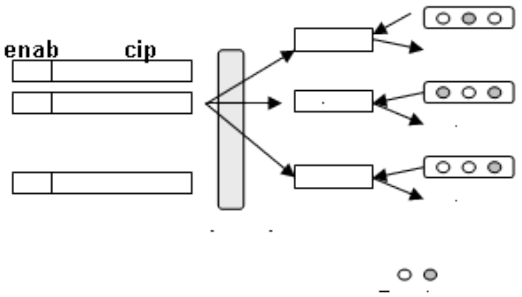

Figura 2 Esquema general de *Traitor Tracing.*

Este es el esquema general propuesto por Chor [14], pero a partir de ahí se ha seguido trabajando en diversas modificaciones a este, para obtener otros métodos como el *dynamic traitor tracing*, el *traitor tracing con black-box tracing*, *asymetric traitor tracing*, *public key, traitor tracing* usando RSA entre otros. Estas modificaciones o mejoras son encaminadas al mismo propósito que es maximizar la posibilidad de capturar al traidor y minimizar el hecho de poder acusar a personas inocentes. Cabe resaltar un caso muy conocido actualmente de la aplicación de este esquema que se da en la industria del cine, cuando los distribuidores de películas de Hollywood lo aplican al momento de enviar sus películas nuevas para que los miembros del comité del Oscar las revisen. Estas son etiquetadas para prevenir la fuga al mercado.

Resumiendo, el esquema *Traitor Tracing* ayuda en la prevención de tres aspectos de la piratería, disuadir a los que apoyan a las personas que utilizan la distribución ilegal de copias, identificarlos y permitir tomar medidas legales contra aquellos usuarios llamados piratas activos. Este esquema desaliente el apoyo a los traidores, ya que se puede identificar el origen de las fuentes de las llaves que utilizan los compradores de productos no legales.

7 CONCLUSIONES

Mediante el desarrollo de esta investigación se han tratado temas referentes a la detección de copias ilegales. Los sistemas de prevención de copia han dado lugar a multitud de publicaciones en la literatura científica. En este trabajo se han presentado los diferentes esquemas *fingerprinting*; simétrico, asimétrico y anónimo. Aunque se han realizado grandes esfuerzos en la construcción de mecanismos para construir una marca inmune a ataques, aún no existe forma de estar totalmente seguro de la culpabilidad de un usuario a pesar la detección de una copia no autorizada.

Una conclusión y recomendación derivada de este trabajo de investigación radica en el hecho de que las entidades que participan en el sistema tanto de autoridad de huella digital como de autoridad de registro deben contar con el consenso y la aceptación general similar a la que requieren las autoridades de certificación, dado que nadie puede dudar de la honestidad de una autoridad de certificación. Lo mismo ocurre con la honestidad de la

autoridad de huella digital. Grandes empresas de distribución audiovisual podrían llegar a desempeñar este papel. Pero sería preferible que la autoridad de huella digital fuese un organismo ajeno a la empresa y a los canales de distribución.

8 REFERENCIAS

[1] Casademont Serra, J. Redes, sistemas y servicios avanzados de telecomunicación. Apuntes de la asignatura. UPC, 2006.

[2] Mengual Galán, L. (s.a.). Arquitecturas de Seguridad. Recuperado de: http://www.personal.fi.upm.es/~lmengual/ARQ_REDES/Arquitecturas_Seguridad.pdf.

[3] Correa Haro, J. P. (2008). Estudios de los Aspectos Técnicos a Considerarse para la Implementación de Redes de Nueva Generación Next Generation Networks (NGN) Orientadas a la Telefonía Móvil. (Tesis Doctoral). Escuela Politécnica Nacional. Quito.

[4] Stalling, W. (2005). Cryptography and Network Security Principles and Practices. Prentice Hall, 4ta. Edición. USA.

[5] Michael, A.; Martin, S.; Wolthusen, S. D. Techniques and applications of digital watermarking and content protection. Artech House, Boston, 2003.

[6] Katzenbeisser, S.; Petitcolas F. A. P. Information hiding techniques for steganography and digital watermaking. Artech House, Boston, 2000.

[7] Yang, B.; Piyuan L.M Zhang W. An Efficient Anonymous Fingerprinting Protocol. IEEE International Conference on Computational Intelligence and Security, 2006, pp.1464-1469.

[8] Boneh, D.; Shaw, J. Collusion-Secure Fingerprinting for Digital Data. IEEE Transaction on Information Theory, vol. 44, 5 (1998), pp. 1897-1905.

[9] Pfitzmann B.; Schunter M. (1996). Asymmetric Fingerprinting. In: Maurer U. (eds) Advances in Cryptology — EUROCRYPT 1996. Lecture Notes in Computer Science, vol 1070. Springer, Berlin, Heidelberg.

[10] Pfitzmann, B.; Waidner, M. Collusion-Secure Fingerprinting for Digital Data. Advances in Cryptology, EUROCRYPT, LNCS 1233, SpringerVerlag, Berlin, 1997, pp. 88-102.

[11] Fernández, M.; Soriano, M.; Domínguez, J.; Sebé, F. Esquemas de fingerprinting para protección de derechos de distribución. Novática, no. 160, 2002

[12] Jianxin Yan, J.; Wu, Y. An attack on a traitor training scheme. 2001.

[13] Fiat, A.; Tassa, T. Dynamic Traitor Tracing. Journal of Cryptology, Israel, 2001.

[14] Chor, B., Fiat, A., Naor, M. (1995). Tracing Traitors. IEEE Trans Inf Theory. 46: 257-270. doi:10.1007/3-540-48658-5_25.

