

Netflix, Inc. and Hulu, LLC
v.
DivX, LLC
IPR2020-00558
U.S. Patent No. 10,225,588

Petitioners' Demonstratives

Oral Argument
May 25, 2021

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Instituted Grounds

Grounds	Claims	Statutory Basis	Prior Art
1	1-24	§103	Chen in View of Lindahl and Hurst

Claim 1

- 1[a]. A playback device for playing protected content from a plurality of alternative streams, comprising:
- [b] a set of one or more processors; and
 - a non-volatile storage containing an application for causing the set of one or more processors to perform the steps of:
 - [c] obtaining a top level index file identifying a plurality of alternative streams of protected video,
 - [d] wherein each of the alternative streams of protected video includes partially encrypted video frames
 - [e] that are encrypted using a set of common keys comprising at least one key,
 - [f] and wherein the partially encrypted video frames contain encrypted portions and unencrypted portions of data;
 - [g] obtaining a copy of the set of common keys;
 - [h] detecting streaming conditions for the playback device;
 - [i] selecting a stream from the plurality of alternative streams of protected video based on the detected streaming conditions;
 - [j] receiving a container index that provides byte ranges for portions of the selected stream of protected video within an associated container file;
 - [k] requesting portions of the selected stream of protected video based on the provided byte ranges;
 - [l] locating encryption information that identifies encrypted portions of frames of video within the requested portions of the selected stream of protected video;
 - [m] decrypting each encrypted portion of the frames of video identified within the located encryption information using the set of common keys; and
 - [n] playing back the decrypted frames of video obtained from the requested portions of the selected stream of protected video.

DivX only disputes limitations [1e] and [1l]

- 1[a]. A playback device for playing protected content from a plurality of alternative streams, comprising:
- [b] a set of one or more processors; and
 - a non-volatile storage containing an application for causing the set of one or more processors to perform the steps of:
 - [c] obtaining a top level index file identifying a plurality of alternative streams of protected video,
 - [d] wherein each of the alternative streams of protected video includes partially encrypted video frames
 - [e] that are encrypted using a set of common keys comprising at least one key,**
 - [f] and wherein the partially encrypted video frames contain encrypted portions and unencrypted portions of data;
 - [g] obtaining a copy of the set of common keys;
 - [h] detecting streaming conditions for the playback device;
 - [i] selecting a stream from the plurality of alternative streams of protected video based on the detected streaming conditions;
 - [j] receiving a container index that provides byte ranges for portions of the selected stream of protected video within an associated container file;
 - [k] requesting portions of the selected stream of protected video based on the provided byte ranges;
 - [l] locating encryption information that identifies encrypted portions of frames of video within the requested portions of the selected stream of protected video;**
 - [m] decrypting each encrypted portion of the frames of video identified within the located encryption information using the set of common keys; and
 - [n] playing back the decrypted frames of video obtained from the requested portions of the selected stream of protected video.

PO does not dispute that Ground 1 teaches all other claim limitations

The title of the '588 patent identifies using a common set of keys

1[a]. A playback device for playing protected content from a plurality of alternative streams, comprising:

...

[d] wherein each of the alternative streams of protected video includes partially encrypted video frames

[e] that are encrypted using a **set of common keys comprising at least one key**,

...

'588 Patent:

(12) **United States Patent**
Kiefer et al.

(54) **PLAYBACK DEVICES AND METHODS FOR
PLAYING BACK ALTERNATIVE STREAMS
OF CONTENT PROTECTED USING A
COMMON SET OF CRYPTOGRAPHIC KEYS**

Hurst:

The DRM server **1204**, in one embodiment, is configured to maintain keys used to decrypt content, and determine whether a client device is allowed to access content. Content may be encrypted when the content is processed by the encoder module **406**, for example. **The streamlets 304 of different bitrates may be encrypted with the same key.** Alter-

Hurst discloses using a
common set of keys for the
alternative streams

Remaining Disputes

	Petitioner	Patent Owner
1. Whether Chen may be relied upon for its teaching of adaptive bitrate streaming (motivation to combine)	 Undisputed that Chen teaches adaptive bitrate streaming	 PO's arguments contradict Federal Circuit precedent
2. Whether the Board's construction from institution was correct for limitation [1l] ("locating encryption information that identifies encrypted portions of frames of video...")	 The Petition applied the natural reading of this limitation, which is supported by the specification	 PO attempts to rewrite the claim, contradicting the intrinsic evidence
3. Whether the combination teaches limitation [1e] ("encrypted using a set of common keys...")	 The prior art expressly discloses this limitation	 PO's arguments contradict Federal Circuit precedent

Ground 1 Overview

(Chen in view of Lindahl and Hurst)

It is undisputed that adaptive bitrate streaming was known in the art

'588 Patent:

BACKGROUND

The term streaming media describes the playback of media on a playback device, where the media is stored on a server and continuously sent to the playback device over a network during playback. Typically, the playback device stores a sufficient quantity of media in a buffer at any given time during playback to prevent disruption of playback due to the playback device completing playback of all the buffered media prior to receipt of the next portion of media. In many instances, content is divided into multiple streams. For example, content can be divided into audio, video, and subtitle streams and some streams can be encoded as alternative streams that are suitable for different network connection bandwidths or comply with specific geographic restrictions and/or other restrictions.

Adaptive bit rate streaming or adaptive streaming involves detecting the present streaming conditions (e.g. the user's network bandwidth and CPU capacity) in real time and adjusting the quality of the streamed media accordingly by selecting between different streams encoded for use at different network connection data rates. Typically, the source media is encoded at multiple bitrates and the playback device or client switches between streaming the different encodings depending on available resources.

Adaptive streaming solutions typically utilize either Hypertext Transfer Protocol (HTTP), published by the Internet Engineering Task Force and the World Wide Web Consortium as RFC 2616 to stream media between a server and a playback device. HTTP is a stateless protocol that enables a playback device to request a byte range within a file. HTTP is described as stateless, because the server is not required to record information concerning the state of the playback device requesting information or the byte ranges requested by the playback device in order to respond to requests received from the playback device.

In adaptive streaming systems, the source media is typically stored on a media server as a top level index file pointing to a number of alternate streams that contain the actual video and audio data. Each stream is typically stored in one or more container files. Different adaptive streaming solutions typically utilize different index and media containers. The Synchronized Multimedia Integration Language (SMIL) developed by the World Wide Web Consortium is utilized to create indexes in several adaptive streaming solutions including IIS Smooth Streaming developed by Microsoft Corporation of Redmond, Wash., and Flash Dynamic Streaming developed by Adobe Systems Incorporated of San Jose, Calif. HTTP Adaptive Bitrate Streaming developed by Apple Computer Incorporated of Cupertino, Calif. implements index files using an extended M3U playlist file (.M3U8), which is a text file containing a list of URIs that typically identify a media container file. The most commonly used media container formats are the MP4 container format specified in MPEG-4 Part 14 (i.e. ISO/IEC 14496-14) and the MPEG transport stream (TS) container specified in MPEG-2 Part 1 (i.e. ISO/IEC Standard 13818-1). The MP4 container format is utilized in IIS Smooth Streaming and Flash Dynamic Streaming. The TS container is used in HTTP Adaptive Bitrate Streaming.

Dr. Nielson admitted that adaptive bitrate streaming was known in the art

Dr. Nielson:

Q. Yeah. And I'm just referring to "adaptive bitrate streaming" as that term is used in the '588 patent.

So would you agree that before the '588 patent, adaptive bitrate streaming was known in the art?

A. Give me just a quick second. I just want to look at how the term is used in the '588 just before I give my answer. (Examined exhibit.) Yes, there were technologies in the art that were called that prior to the '588 patent.

PO cannot dispute that Chen teaches known adaptive bitrate streaming techniques with alternative streams of video

Chen:

HTTP Streaming

[0063] HTTP streaming is a specific type of streaming. With HTTP streaming, the sources might be standard web servers and content delivery networks (CDNs) and might use standard HTTP. This technique may involve stream segmentation and the use of multiple streams, all within the context of standardized HTTP requests. The media, such as video, may be encoded at multiple bitrates to form different versions, or representations. The terms “version” and “representation” are used synonymously in this document. Each version or representation may be broken into smaller pieces, perhaps on the order of a few seconds each, to form segments. Each segment may then be stored on a web server or CDN as a separate file.

[0064] On the client side, requests may then be made, using HTTP, for individual segments that are seamlessly spliced together by the client. The client may switch to different data rates based on available bandwidth. The client may also request multiple representations, each presenting a different media component, and may present the media in these representations jointly and synchronously. Triggers for switching may include buffer occupancy and network measurements, for example. When operating in the steady state, the client may pace requests to the server to maintain a target buffer occupancy.

Hurst teaches DRM for adaptive bitrate streaming

Adaptive streaming

DRM

Hurst:

(57)

ABSTRACT

An apparatus, system, and method for maintaining a programming lineup of adaptive-bitrate content streaming is provided. The apparatus includes a timeline module configured to maintain a programming lineup of media content available over a network. The media content may comprise a plurality of streamlets. The apparatus also includes at least one data

The CMS 1202 is configured to manage content stored in the streamlet database 408. The CMS 1202, in one embodiment, provides a user interface for a person to build virtual timelines as described above. The CMS 1202 will be discussed in greater detail below with reference to FIG. 13. The DRM server 1204 is configured to provide digital rights management capability to the system 1200. The DRM server 1204 is further configured to supply encryption keys to the end user upon authenticating the end user.

Hurst teaches using the same key for encrypting alternative streams for ABS

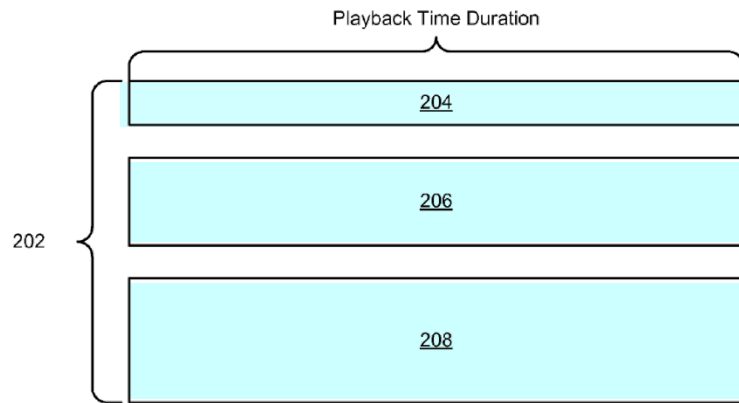


FIG. 2b

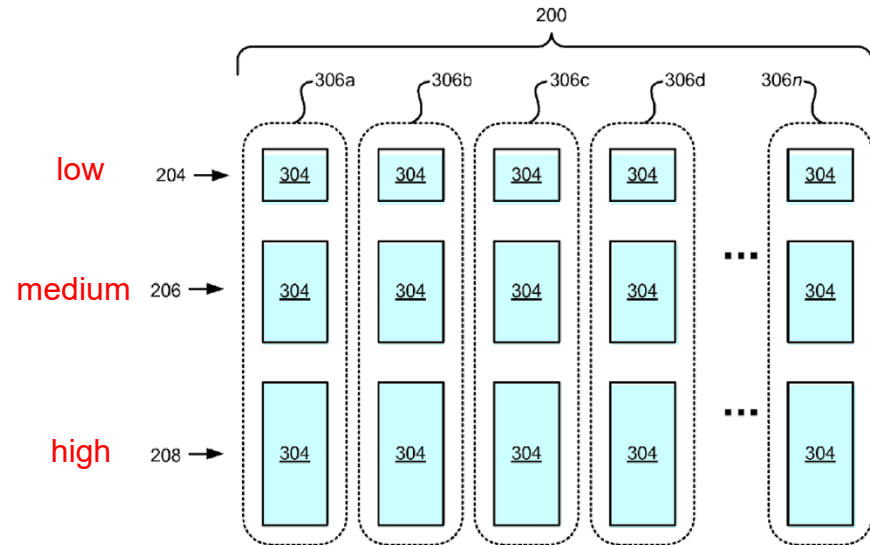


FIG. 3b

encoder module 406, for example. The streamlets 304 of different bitrates may be encrypted with the same key. Alter-

It is undisputed that partial encryption was known in the art

'588 Patent:

BACKGROUND

* * *

The term Digital Rights Management (DRM) is utilized to describe access control technologies that are used to control access to and/or copying of digital content. DRM systems typically involve the use of cryptographic information to control access to or protect a piece of content. Content protection is typically achieved using cryptographic information such as (but not limited to) one or more encryption keys to encrypt some or all of the content. An important component of most DRM systems is a mechanism for securely providing cryptographic information to authorized playback devices for use in accessing protected content. The protected content cannot be accessed without the cryptographic data and ideally the cryptographic data is bound to specific playback devices and cannot be readily used by unauthorized playback devices or is securely provided to the playback devices (often on a session basis).

Dr. Nielson:

- Q. So would you agree that partial frame encryption was known in the art for video before 2011?
- A. There have been different approaches to doing what you could call partial frame encryption prior to 2011.

Lindahl teaches partial encryption

Lindahl:

SUMMARY OF THE INVENTION

[0010] The invention pertains to improved techniques to partially encrypt media files. The encryption serves to cryptographically secure only a portion of the media data within a media file, while the remaining portion of the media data is not cryptographically secured. Although only partial encryption is used, the portion being encrypted serves to substantially disrupt usefulness of other parts of the media file which are not encrypted. In other words, the partial encryption renders the media file substantially unusable by unauthorized users.

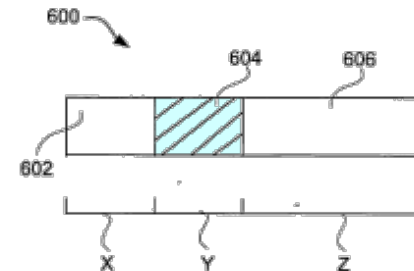


FIG. 6A

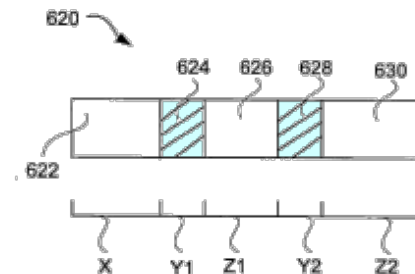


FIG. 6B

The Petition combines known adaptive bitrate streaming with known partial encryption techniques

PO fails to address the prior art's express teaching, suggestion, and motivation for the combination

Chen-924:

(57)

ABSTRACT

Various embodiments are directed towards employing a container and communication protocol proxy component within a client device to receive securely real-time streamed, progressively downloaded, or adaptively streamed container over a network using one container and communication protocol, and to securely decrypt the container and provide it to a media player using a different container and communications protocol. In one embodiment, the container is in Flash Video (FLV) file format. A browser or the media player on the client device may be used to request the container. The requested container is sent over one communication protocol and intercepted by the container and communication protocol proxy component. The container may be received as selectively encrypted container. The container and communication protocol proxy component then may enable decryption of the container and providing of it to the media player using another container and communication protocol combination.

Adaptive bitrate streaming and partial encryption had widely known advantages

Bitrate adaptation for bandwidth variability

Chen:

[0065] Advantages of HTTP streaming may include bitrate adaptation, fast startup and seek, and minimal unnecessary delivery. These advantages come from controlling the delivery to be only a short time ahead of the playout, making maximum use of available bandwidth (through variable bit rate media), and optimizing stream segmentation and intelligent client procedures.

Address piracy with power-efficient computational burden

Lindahl:

[0095] The advantages of the invention are numerous. Different aspects, embodiments or implementations may yield one or more of the following advantages. One advantage of the invention is that digital media data can be protected from unauthorized usage through encryption of only parts of the digital media data. Another advantage of the invention is that portable, battery-powered media devices can perform decryption in a power efficient manner since the computational burden to decrypt encrypted media files is substantially decreased through use of partial encryption. Still another advantage of the invention is that portable media devices can yield higher quality media output.

Lindahl combines its DRM teachings with streaming media

Lindahl:

[0065] Next, the media file is downloaded 708 to the user. In one embodiment, the download 708 of the media file can be performed by streaming the media file through the data network to the user, namely, to the user's client machine. Here, the downloading 708 of the media file can be efficient because the manner in which the media file can be stored facilitates its immediate download without the need for processing-intensive conversion.

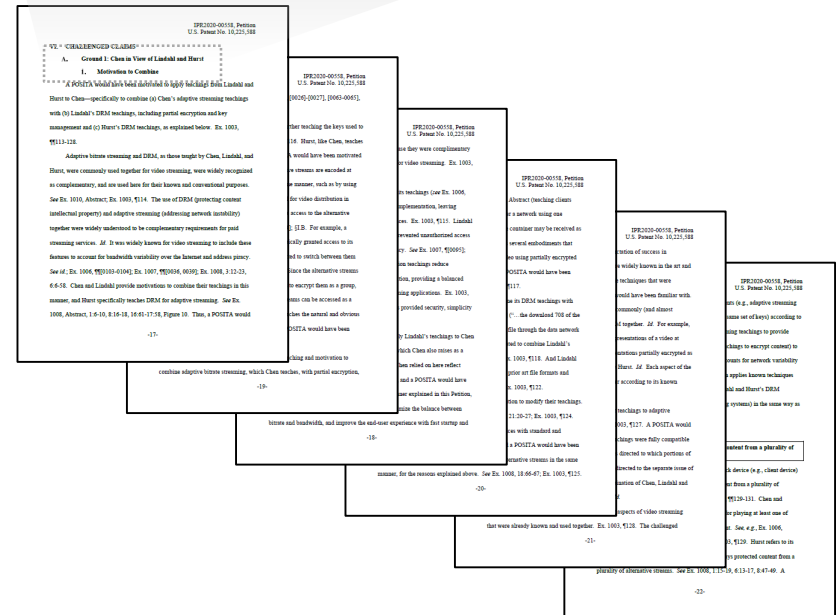
PO argues there is “just one sentence” for the motivation to combine; the Petition included 6 pages

POR:

partial encryption and key management.” Pet., 17. Petitioner argues that a POSITA would have been motivated to apply Lindahl’s partial frame encryption to Chen to “address piracy concerns and improve efficiency,” directing just one sentence to establish to the goals animating its proffered motivation:

Petition:

A. Ground 1: Chen in View of Lindahl and Hurst 1. Motivation to Combine





PO argues there is no motivation to apply Lindahl's partial encryption to Chen's file format

Chen teaches the MP4 file format.



Chen:

[0119] The 3GPP File Format or any other file based on the ISO base media file format, such as the MP4 file format or the 3GPP2 file format, may be used as the container format for HTTP streaming with the following features. A segment

Lindahl applies its partial encryption to the MP4 file format.



Lindahl:

[0067] The media file, whether encrypted or not, can have a file format (i.e., encoding) that varies. The file format is typically dependent on the type of media. For example, when the type of media is video, one suitable file format is a H.264 format. Other suitable formats include QuickTime movies, MPEG-1 format, MPEG-2 format and MPEG-4 format.

The Petition cited Chen-924 for express teaching, suggestion, and motivation to combine Chen with Lindahl

Chen-924 teaches partial frame encryption for the MP4 and 3GP file formats

Chen-924 (Ex. 1010):

In one embodiment, the containers are encrypted. In one embodiment, the containers may be selectively encrypted. That is, the some portions of the containers may be encrypted using one or more encryption keys, while another portion of the container stream may be unencrypted or left in the clear. Moreover, encryption may be selectively applied to at least a portion of a video elementary stream (ES) of the real-time streamed, progressively, or adaptively downloaded container, a portion of the audio ES, a portion of the digital data ES, and/or any combination and any portion of video, audio, data elementary streams that comprise container stream. Selective encryption may further include selectively encrypting at least a portion of an I-frame, P-frame, B-frame, and any combination of P, B, and I frames within the container stream.

As used herein, the term “content” includes any digital data that may be communicated over a network to be used by a computing device. Non-exhaustive examples of content include but is not limited to multimedia data, including movies, videos, music, Pay Per View (PPV), Video On Demand (VoD), interactive media, audios, still images, text, graphics, scripts, applications, and other digital content useable by a computing device. Content is often described by its format, or container, in which the content is provided. Thus, as used here, the term “container” refers to a computer file or stream format in which content may be presented. Containers often disclose how the digital content is encoded, interleaved, and/or compressed. A non-limiting and non-exhaustive list of examples of a container is: MPEG2-TS, FLV, H.264, MOV, MP4, 3GP, and ASF.

An express teaching, suggestion, and motivation is one of the classic foundations for the motivation to combine

“Here, because a person of skill in the art reading Grab would readily envisage the combination of ruthenium binders and PVD coatings, it would have been obvious to that person that these two could be combined with a reasonable expectation of success.”



Kennametal, Inc. v. Ingersoll Cutting Tool Co., 780 F.3d 1376, 1385 (Fed. Cir. 2015)

“Furthermore, the references in this case go beyond just illuminating a known problem; they also expressly propose the claimed solution... Accordingly, the prior art's direct recommendations to use 24/4 and 23/5 dosing regimens to minimize the risks of escape ovulation would have motivated one of ordinary skill in the art to implement such a shortened pill-free interval for use with known low-dose COCs, as recited in the asserted claims.”

Bayer Healthcare v. Watson Pharmaceuticals, Inc., 713 F.3d 1369, 1375-1376 (Fed. Cir. 2013)

PO does not dispute that a POSITA would have knowledge and skills necessary to build systems with DRM and adaptive streaming

Dr. McDaniel (Ex. 1003):

68. Given this level of skill in the 2011 time frame, a POSITA would have had the knowledge and skills necessary to program and build systems that meet all limitations of the challenged claims, including the following:

* * *

- Using known communication protocols for streaming, including Hypertext Transfer Protocol (HTTP). *See, e.g.,* Ex. 1009, 1:38-3:3; Ex. 1010, 3:7-22. The '588 patent admits this was known in the art. *See* Ex. 1001, 2:1-10.
- Using known adaptive streaming technologies to stream video over the Internet, including MPEG Dynamic Adaptive Streaming over HTTP (DASH) and adaptive bitrate streaming solutions from companies such as Microsoft, Adobe, and Apple. *See, e.g.,* Ex. 1009, 2:1-3:3. The '588 patent admits this was known in the art. *See* Ex. 1001, 2:12-34.

- Encrypting and decrypting data, including by using common symmetric key algorithms (e.g., Blowfish, AES, DES) and asymmetric key algorithms. *See, e.g.,* Ex. 1007, ¶[0008]; Ex. 1010, 7:34-42. The '588 patent admits this was known in the art. *See* Ex. 1001, 2:47-62.
- Using DRM for video security, including for authentication, key management (such as the assignment and identification of keys), and partial encryption of video streams. *See, e.g.,* Ex. 1011, 1:49-63, 2:1-8, 8:23-32; Ex. 1013, 6:15-56, 7:15-8:42.

PO does not dispute that a POSITA would have been able to use the MP4 and 3GP file formats

Dr. McDaniel (Ex. 1003):

68. Given this level of skill in the 2011 time frame, a POSITA would have had the knowledge and skills necessary to program and build systems that meet all limitations of the challenged claims, including the following:

* * *

- Using known video container file formats for streaming, such as the ISO base media file format, sometimes referred to as the MP4 container format, and 3GPP extensions to the ISO base media file format. *See, e.g.*, Ex. 1009, 1:15-37; Ex. 1010, 2:59-3:6. The '588 patent admits this was known in the art. *See* Ex. 1001, 2:27-41.

Dr. McDaniel (Ex. 1031):

5. In my opening declaration, I noted that a POSITA would have been able to use known file formats including the MPEG-4 file format and 3GPP extensions. EX1003, ¶68. Dr. Nielson argues that I did not include the word “modify” in my description. EX2012, ¶80. However, the use of 3GPP and MPEG-4 file formats encompasses the ability to extend those formats because their architectures were extensible by design. A key aspect of these file formats was their extensibility—a fact that Dr. Nielson did not consider. Indeed, 3GPP and MP4 are both derived from the ISO base media file format.¹ EX1006, ¶[0119]

PO does not dispute that the MP4 and 3GP file formats were extensible by design

A POSITA would have known how to modify the MP4 file format to add information for partial frame encryption

Dr. McDaniel (Ex. 1031):

6. Multiple references teach modifying standard file formats to implement partial encryption, confirming that a POSITA would have known how to do so. For example, Shamoon teaches partially encrypting video frames in an MPEG-4 file and modifying the MPEG-4 file format by adding an Initial Object Descriptor that contains a DigiBox. EX1018, 22:26-38, 2:5-9 (“The digital bit stream includes content, which is encrypted at least in part...”), 23:50-56

Adding encryption information to MP4 files was known in the art

Ex. 1018:

FIG. 21 illustrates one manner in which a protected MPEG-4 file may be created. In this figure, CreateBox 2101 represents a DigiBox creation utility, which accepts keys and rules. In one embodiment, CreateBox 2101 may pass these keys and rules to IRP 2102 and receive DigiBox 2103 from IRP 2102. In another embodiment, IRP 2102 may be incorporated into CreateBox 2101, which accepts keys and rules and outputs DigiBox 2103.

DigiBox 2103 contains governance rules, initialization vectors and keys. DigiBox 2103 is passed from CreateBox

* * *

If DigiBox 2103 contains all keys and rules necessary to render all of the content, it may be unnecessary for Mux 2105 to create any IPMP streams. If additional keys or rules may be necessary for at least a portion of the content, Mux 2105 may incorporate those rules and keys into one or more additional DigiBoxes, and incorporate those DigiBoxes either in the IPMP stream or in the OD update stream.

Dispute #1

Chen teaches adaptive bitrate streaming.

PO attacks Chen's optional embodiments, which is improper as a matter of law.

The Petition relies on Chen's basic teachings of adaptive bitrate streaming—its “simplest case”

Chen:

[0070] In a simplest case, each Alternative Representation may be stored in a single 3GP file, i.e., a file conforming as defined in 3GPP TS26.244, or any other file that conforms to the ISO base media file format as defined in ISO/IEC 14496-12 or derived specifications (such as the 3GP file format described in 3GPP Technical Specification 26.244). In the remainder of this document, when referring to a 3GP file, it should be understood that ISO/IEC 14496-12 and derived specifications can map all described features to the more general ISO base media file format as defined in ISO/IEC 14496-12 or any derived specifications. The client may then request an initial portion of the file to learn the media meta-data (which typically is stored in the Movie header box, also referred to as “moov” box) together with movie fragment times and byte offsets. The client may then issue HTTP partial get requests to obtain movie fragments as required.

PO does not dispute that Chen teaches adaptive bitrate streaming, but argues that other features must also be included in the combination

POR:

Second, Petitioner does not establish that partial frame encryption would be superior to “address piracy concerns and improve efficiency” in the context of Chen’s adaptive streaming system. In fact, Chen has various features, such as independent layers and Forward Error Correction (FEC), that are integral to Chen’s system, but are incompatible with partial frame encryption, or at least would be beyond the capability of the POSITA to implement with partial frame encryption.

Chen cannot be limited to other embodiments, even if allegedly preferred

“A reference must be considered for everything that it teaches, not simply the described invention or a preferred embodiment.”

CRFD Research, Inc. v. Matal, 876 F.3d 1330, 1348-49 (Fed. Cir. 2017).



“A reference must be considered for everything it teaches by way of technology and is not limited to the particular invention it is describing and attempting to protect. On the issue of obviousness, the combined teachings of the prior art as a whole must be considered.”

EWP Corp. v. Reliance Universal Inc., 755 F.2d 898, 907 (Fed. Cir. 1985).

PO's arguments regarding FEC and scalable video layers contradict
Federal Circuit precedent

Chen's other features do not preclude a POSITA from utilizing Chen's basic teaching of adaptive bitrate streaming



“One of ordinary skill in the art is not foreclosed from combining the Breivogel dimensions with the Weling cross-sectional shape merely because Breivogel discloses triangular grooves. A reference must be considered for everything that it teaches, not simply the described invention or a preferred embodiment. ***Even though Breivogel describes grooves with a particular cross-sectional shape, this does not preclude one of ordinary skill in the art from utilizing Breivogel's other teachings*** on the width, depth, and pitch in combination with other features of the Weling pad. One of ordinary skill in the art is not an ‘automaton.’ KSR, 550 U.S. at 421, 127 S.Ct. 1727.”

In re Applied Materials, 692 F.3d 1289, 1298 (Fed. Cir. 2012) (citations omitted)

The challenged claims do not require FEC or scalable video layers



“But *an unclaimed and undisclosed feature such as the ‘specialized screw’ cannot be the basis for finding Synthes’s patent to be non-obvious* over the prior art. See *E.I. Du Pont de Nemours & Co. v. Phillips Petroleum Co.*, 849 F.2d 1430, 1433 (Fed. Cir. 1988), quoting *McCarty v. Lehigh Valley R. Co.*, 160 U.S. 110, 116, 16 S.Ct. 240, 40 L.Ed. 358 (1895) (‘[N]o principle of law ... would authorize us to read into a claim an element which is not present, for the purpose of making out a case of novelty....’).”

Smith & Nephew, Inc. v. Rea, 721 F.3d 1371, 1381 (Fed. Cir. 2013)

The Federal Circuit has rejected alleged incompatibilities that are not required by the claims



“Baker Hughes next argues that ... [the prior art’s] cup packers would be unsuitable for use in an open-hole bore. We disagree. As noted above, ***the claims do not require a particular type of packer. Moreover, obviousness does not require the bodily incorporation of the teachings of one reference to another reference***—an ordinary artisan has the capacity for ordinary creativity when combining references.”

Packers Plus Energy Services Inc. v. Baker Hughes Oilfield Operations, LLC, 2019 WL 2420139, *4 (Fed. Cir. 2019) (nonprecedential) (emphasis added).

Whether Lindahl is compatible with Chen's optional embodiments is irrelevant to obviousness



“Any alleged nonequivalence in the type of circuit is irrelevant to the Board's determination since the examiner did not rely on art-recognized equivalence in substituting the crossbar arrays. **It is well-established that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of elements.** *In re Etter*, 756 F.2d 852, 859 (Fed. Cir. 1985) (en banc) (‘Etter's assertions that Azure cannot be incorporated in Ambrosio are basically irrelevant, the criterion being not whether the references could be physically combined but whether the claimed inventions are rendered obvious by the teachings of the prior art as a whole.’); *In re Sneed*, 710 F.2d 1544, 1550 (Fed. Cir. 1983) (‘[I]t is not necessary that the inventions of the references be physically combinable to render obvious the invention under review.’); *In re Keller*, 642 F.2d 413, 425 (CCPA 1981) (‘**The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference....**’).”

In re Mouttet, 686 F.3d 1322, 1332 (Fed. Cir. 2012)

Whether Lindahl is compatible with Chen's optional embodiments is irrelevant to obviousness



“Contrary to Allied's position, **‘it is not necessary that [Caterpillar and Ogawa] be physically combinable to render obvious the ['489 patent].’** *In re Sneed*, 710 F.2d 1544, 1550 (Fed. Cir. 1983); *see also In re Etter*, 756 F.2d 852, 859 (Fed. Cir. 1985) (en banc) (**‘Etter’s assertions that Azure cannot be incorporated in Ambrosio are basically irrelevant**, the criterion being not whether the references could be physically combined but whether the claimed inventions are rendered obvious by the teachings of the prior art as a whole.’). **‘The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference,’** *In re Keller*, 642 F.2d 413, 425 (CCPA 1981). *See also In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012) (citing *In re Keller*, 642 F.2d at 425), but rather whether ‘a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention,’ *Pfizer, Inc. v. Apotex, Inc.*, 480 F.3d 1348, 1361 (Fed. Cir. 2007).”

Allied Erecting and Dismantling Co, Inc. v. Genesis Attachments, LLC. 825 F.3d 1373, 1381. (Fed. Cir. 2016)

PO's counsel once again relies on improper bodily incorporation— a mistake the PTAB has explained previously



“Patent Owner attempts to defeat the teachings of Blake through bodily incorporation of those teachings into Bernstein; however, the Court of Appeals for the Federal Circuit has consistently held . . . that “[t]he test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art.”

Hulu, LLC v. Sound View Innovations, LLC, IPR2018-00366, Paper 41 at 23-24, 31 (PTAB Apr. 9, 2019)

Chen states that viable systems “need not include all of” its features

Chen:

[0062] A block-request streaming system according to embodiments described herein provides many benefits. It should be understood that a viable system need not include all of the features described herein, as some applications might provide a suitably satisfying experience with less than all of the features described herein.

PO's allegedly integral features are optional

Some embodiments modify “known” adaptive streaming techniques with scalable layers

Chen:

[0376] However, it might be wasteful to have the receiver entirely discard the data already received from the abandoned representation. In an embodiment of a block-streaming system described herein, the data within each block can be encoded and arranged in such a way that certain prefixes of the data within the block can be used to continue the presentation without the remainder of the block having been received. For example, the well-known techniques of scalable video encoding may be used. Examples of such video encod-

[0386] In a first embodiment, the known techniques of a block request streaming system may be applied with the modification that different versions of the content are in some cases replaced by different combinations of the layers. That is

FEC is not required

Chen:

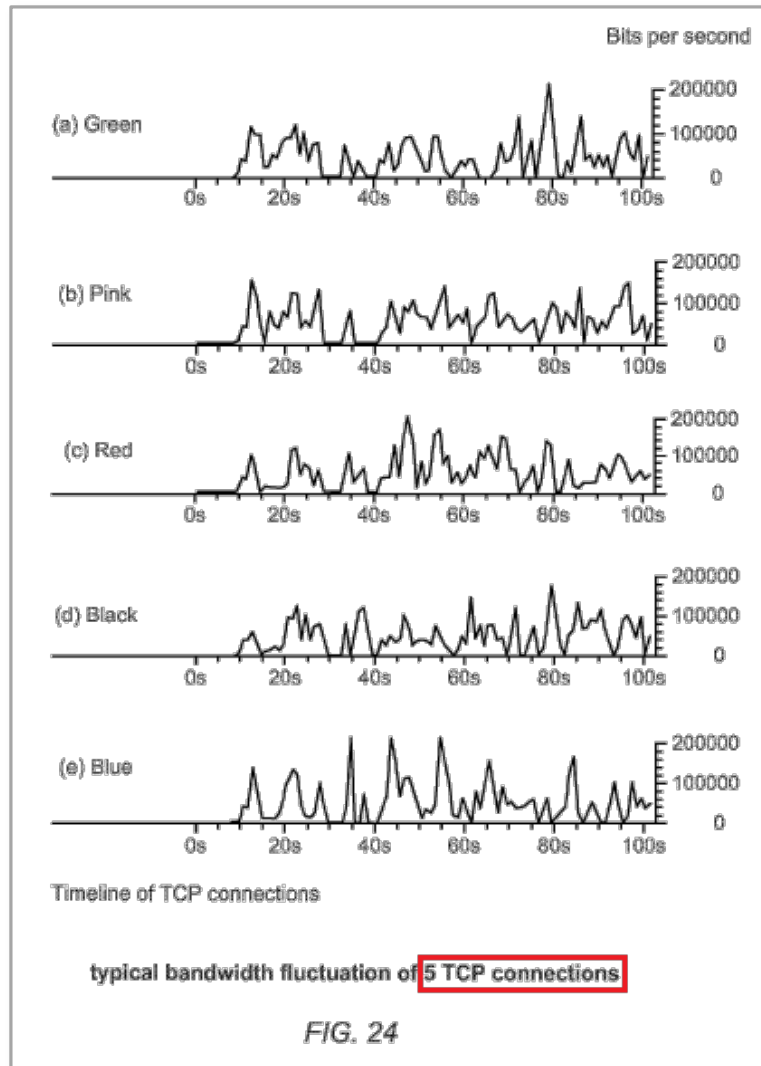
Cooperative HTTP/TCP Requesting

[0527] We now describe methods for using concurrent HTTP/TCP requests in a cooperative fashion. A receiver may employ multiple concurrent cooperative HTTP/TCP requests, for example using a plurality of HTTP byte-range requests, wherein each such request is for a portion of a fragment in a source segment, or all of a fragment of a source segment, or a portion or a repair fragment of a repair segment, or for all of a repair fragment of a repair segment.

[0534] There are many variations of the No-FEC method and the FEC method described above. For example, the cooperative HTTP/TCP requests may be used for only the first few fragments after a channel zap has occurred, and thereafter only a single HTTP/TCP request is used to download further fragments, multiple fragments, or entire segments. As another example, the number of cooperative HTTP/TCP connections used can be a function of both the urgency of the fragments being requested, i.e., how imminent is the playout time of these fragments, and of the current network conditions.

For FEC, PO relies on an optional embodiment with 5 concurrent TCP connections

Chen:



Chen explains that FEC with multiple TCP connections has drawbacks

Chen:

**25% overhead from
additional HTTP
connection for FEC**



[0532] FIG. 25 shows a possible request structure for a fragment that is 250,000 bits in size (approximately 31.25 kilobytes), where there are 4 HTTP byte range requests made in parallel for different parts of the fragment, i.e., the first HTTP connection requests the first 50,000 bits, the second HTTP connection requests the next 50,000 bits, the third HTTP connection requests the next 50,000 bits, and the fourth HTTP connection requests the next 50,000 bits. If FEC is not used, i.e., the No-FEC method, then these are the only 4 requests for the fragment in this example. If FEC is used, i.e., the FEC method, then in this example there is one additional HTTP connection that requests an additional 50,000 bits of FEC repair data of a repair segment generated from the fragment.

PO argues that Chen requires both scalable layers and FEC, but fails to identify a single embodiment with both features

Scalable layer embodiment

POR cites Exhibit 1006, ¶¶[0379-0384]:

[0381] In such embodiments, the encoded media data for each block may be partitioned into multiple disjoint pieces, referred to herein as “layers”, such that a combination of layers comprises the whole of the media data for a block and such that a client that has received certain subsets of the layers may perform decoding and presentation of a representation of the content. In this approach, the ordering of the data in the stream is such that contiguous ranges are increasing in the quality and the metadata reflects this.

No overlap

FEC embodiment

POR cites Exhibit 1006, ¶¶[0529-0534]:

[0534] There are many variations of the No-FEC method and the FEC method described above. For example, the cooperative HTTP/TCP requests may be used for only the first few fragments after a channel zap has occurred, and thereafter only a single HTTP/TCP request is used to download further fragments, multiple fragments, or entire segments. As another example, the number of cooperative HTTP/TCP connections used can be a function of both the urgency of the fragments being requested, i.e., how imminent is the playout time of these fragments, and of the current network conditions.

The Sur-Reply had no answer

PO argues that Chen requires fragment-level encryption

PO relies on a mention of fragment-level encryption in a **hypothetical discussion**

Chen:

[0522] As is known to those of skill in the art, there is a large variation in the data rate of TCP connections. However, to simplify this discussion, suppose ideally that all connections are proceeding in parallel such that the first block will be completely received at about the same time as the other $n-1$ blocks requested. To simplify the discussion further, assume that the aggregate bandwidth utilized by the n download connections is fixed to a value B for the entire duration of the download, and that the streaming rate S is constant over the entire representation. Suppose further that the media data structure is such that playout of a block can be done when the entire block is available at the client, i.e., playout of a block can only start after the entire block is received, e.g., due to the structure of the underlying video encoding, or because encryption is being employed to encrypt each fragment or block separately, and thus the entire fragment or block needs to be received before it can be decrypted. Thus, to simplify the discussion below, we assume that an entire block needs to be received before any of the block can be played out. Then, the time required before the first block has arrived and can be played out is approximately $n \cdot t \cdot S/B$.



Chen uses a hypothetical to “simplify this discussion” of bandwidth calculations



The hypothetical “suppose[s]” various conditions



Fragment-level encryption is one possible supposition, offered as an example

According to PO, Petitioner must prove that Lindahl's partial encryption was "better" than fragment-level encryption, scalable layers, and FEC

POR:

encryption" in Chen to "address piracy concerns" is misplaced. Chen already discloses fragment level encryption which addresses piracy concerns. Petitioner makes no showing whatsoever that Lindahl's system, which only partially encrypts a frame, provides better protection or that Chen's own fragment level encryption does not provide sufficient "piracy" protection. Rather, and as discussed in the preceding section, implementing partial frame encryption in Chen's system (assuming such a thing could be done) would likely undermine security in view of Chen's scalable layers and FEC method, both of which could allow unencrypted portions decrypt encrypted portions when combined with partial frame encryption. *See also* Ex. 2012 [Nielson Decl.] ¶ 72.

The Federal Circuit has held PO's arguments to be "improper"



“[O]ur case law does not require that a particular combination must be the preferred, or the most desirable, combination described in the prior art in order to provide motivation for the current invention.’ In re Fulton, 391 F.3d 1195, 1200 (Fed. Cir. 2004); see also Bayer Healthcare Pharm., Inc. v. Watson Pharm., Inc., 713 F.3d 1369, 1376 (Fed. Cir. 2013). It is thus improper to require West-Ward to prove that a person of ordinary skill would have selected everolimus over other prior art treatment methods.”

Novartis Pharm. Corp. v. W.-Ward Pharm. Int’l Ltd., 923 F.3d 1051, 1059 (Fed. Cir. 2019)

Even if Chen's optional features were better, it would not make the combination inapt for obviousness



“This court has further explained that ***just because better alternatives exist in the prior art does not mean that an inferior combination is inapt for obviousness purposes.*** Gurley, 27 F.3d at 553.”

In re Mouttet, 686 F.3d 1322, 1334 (Fed. Cir. 2012);

For unclaimed features, it is irrelevant whether the prior art combination would be less effective than one reference alone



“We agree with the Board, however, that the ’483 patent claims do not require absorption of specific resonances at specific frequencies, nor any specific threshold with respect to signal loss. ... ***It is irrelevant whether Tomonori and Sadaie together would be less effective than Sadaie alone at avoiding the absorption of certain low frequencies.***”

Slot Speaker Technologies, Inc. v. Apple Inc., 680 Fed.Appx. 932, 940 (Fed. Cir. 2017).

FEC and scalable video layers are not required by the challenged claims.

Even if Chen's optional embodiments offered benefits, they do not undercut Chen's teaching of adaptive bitrate streaming



“While acknowledging that Irie's principal focus is on the addition of antimony in conjunction with hot-band annealing, the Board found that Irie nonetheless teaches that ‘the addition of antimony to a steel composition improves the magnetic properties of the steel, even in the absence of a hot band annealing step.’... Thus, ***Irie's recitation of the benefits of the preferred procedure***, which includes annealing, ***does not undercut Irie's teaching that adding antimony is useful even in the absence of annealing.***”

In re Inland Steel Co., 265 F.3d 1354 (Fed. Cir. 2001)

Alleged disadvantages do not obviate the motivation to combine



“Although modification of the movable blades may impede the quick change functionality disclosed by Caterpillar, ‘[a] given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine.’”

Allied Erecting and Dismantling Co, Inc. v. Genesis Attachments, LLC. 825 F.3d 1373, 1381. (Fed. Cir. 2016) (citations omitted)

PO does not address the Petition's explanation that Lindahl's partial encryption reduces computational/load

PO argues against generic “efficiency” for the reason to modify Chen with Lindahl's partial encryption

But the Petition specifically explained *computational* efficiency (reduced computational load) as the motivation to apply Lindahl's partial encryption to Chen

PO does not dispute that partial encryption reduces computational load

Sur-Reply:

Here, Petitioner relied on improved “efficiency” as the reason to modify Chen. Pet., 18. That the proposed modification would in fact reduce efficiency



Pet., 18:

While Chen accounted for the use of DRM in its teachings (*see* Ex. 1006, ¶[0522]), Chen did not require any particular DRM implementation, leaving particulars to the POSITA's knowledge and preferences. Ex. 1003, ¶115. Lindahl and Hurst provided such DRM teachings. Lindahl prevented unauthorized access to media while improving the **computational efficiency**. *See* Ex. 1007, ¶[0095]; Ex. 1003, ¶¶115, 121-122. Lindahl's partial encryption teachings **reduce computational load** while maintaining content protection, providing a balanced level of security that was well-suited for video streaming applications. Ex. 1003,

Evidence confirms that a POSITA would have known how to implement FEC with partial encryption

Kunkelmann:

Forward Error Correction. Generally, *forward error correction* (FEC) mechanisms should not be applied to the application layer data of streams which are transmitted via partial encryption or a distinct-route approach. The reason is that an FEC coder increases the redundancy of the transmitted data so that an attacker gets access to more information, and hence the security of the stream is reduced. Applying FEC to data which already has been partially encrypted does no harm with respect to the data security.

PO assumes FEC is applied before partial encryption, contrary to known best practices

Dispute #2

PO's construction for limitation [11] is contradicted by the intrinsic record

[11] locating encryption information that identifies encrypted portions of frames of video within the requested portions of the selected stream of protected video;

The Petition explained limitation [1l] under its plain and ordinary meaning

Petition:

V. CLAIM CONSTRUCTION

For all grounds, the challenged claims are invalid under their plain and ordinary meaning. Ex. 1003, ¶¶100-101. Petitioner's arguments are not a

Institution Decision:

Petitioner does not present any specific claim terms for construction. Petitioner contends that “the challenged claims are invalid under their plain and ordinary meaning.” Pet. 16 (citing Ex. 1003 ¶¶ 100–101). Patent Owner, likewise, does not proffer any specific constructions for claim terms. *See generally* Prelim. Resp. As such, we apply the plain and ordinary meaning of each claim term in the analysis below. We remind the parties

The plain and ordinary meaning is the claim limitation, read in the order it is written

[11] locating encryption information that identifies encrypted portions of frames of video within the requested portions of the selected stream of protected video;

Institution Decision:

More natural to the language of claim 1, the “frames of video” are denoted as coming from those “within the requested portions,” where those requested portions are parts “of the selected stream of protected video.” A common treatise on grammar teaches that “[t]he position of words in a sentence is the principle means for showing their relationship,” and “[t]he writer must, therefore, bring together the words and groups of words that are related in thought and keep apart those that are not so related.” William Strunk, Jr. & E.B. White, *The Elements of Style* 36 (4th ed. 2000). The

The Petition addressed the natural, plain and ordinary meaning

[11] locating encryption information that identifies encrypted portions of frames of video within the requested portions of the selected stream of protected video;

Petition:

The combination teaches or suggests locating encryption information (e.g., encryption parameters) that identifies encrypted portions of frames of video within the requested portions of the selected stream (e.g., representation) of protected (e.g., partially encrypted) video. Ex. 1003, ¶¶182-187. Lindahl teaches using encryption parameters to identify encrypted portions. See Ex. 1007, ¶¶[0056]

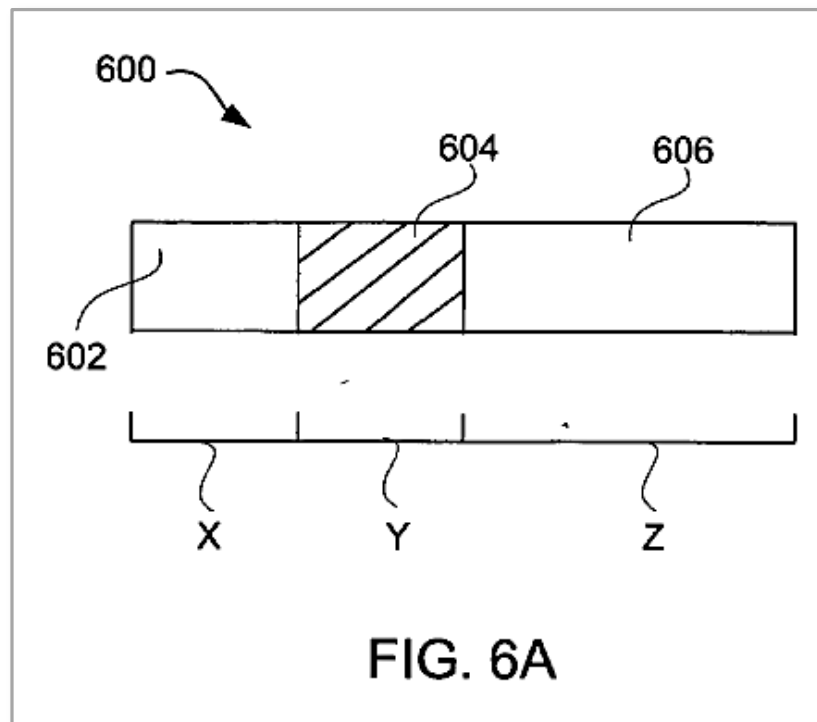
Lindahl teaches that the encryption parameters are “retrieved” to decrypt the media. See Ex. 1007, ¶[0072] (“After a media file to be decrypted has been identified 902, encryption parameters associated with the media file are retrieved 904....”); Ex. 1003, ¶187. It would have been obvious to retrieve the encryption parameters to identify the encrypted portions of the content so that they may be decrypted efficiently. *Id.*

PO does not dispute that the combination teaches limitation [11] under the plain and ordinary explained in the Institution Decision

Lindahl:

[0057] FIG. 6A is a diagram of a partially encrypted block 600 according to one embodiment. The partially encrypted block 600 has an initial unencrypted portion 602, followed by an encrypted portion 604, and followed by an unencrypted portion 606. The size of the unencrypted portion 602 is denoted by the variable X, the size of the encrypted portion 604 is denoted by the variable Y, and the size of the unencrypted portion 606 is denoted by the variable Z. The size of the partially encrypted block 600 is the sum of the variables X, Y and Z. Although the encrypted portion 604 has a length or size of Y, prior to the encryption, the size of this same portion can also be denoted by the variable Y, or the size can be different than its size once encrypted. Although the length of the variables can vary widely with implementation, in one representative embodiment, the variables X, Y and Z can be sized as 16 bytes, 64 bytes and 512 bytes, respectively.

[0072] The media file decryption process 900 initially identifies 902 a media file to be decrypted. Typically, a media file would be decrypted when a user or device has requested to play the media file, such as noted in FIG. 8. After a media file to be decrypted has been identified 902, encryption parameters associated with the media file are retrieved 904. The encryption parameters can be the same parameters that were utilized with respect to the media file encryption process 400 illustrated in FIG. 4. The encryption parameters are again utilized to decrypt the media file that was previously encrypted. These encryption parameters can also be referred to as decryption parameters. In other words, the parameters for encryption and decryption are the same.



PO attempts to rewrite the claim

[11] locating encryption information that identifies encrypted portions of frames of video **within the requested portions of the selected stream of protected video.**

POR:

As discussed above, the “locating” limitation of claims 1 and 12 requires, *inter alia*, “locating encryption information” “within the requested portions of the selected stream of protected video.” The Petition contends that this limitation is disclosed

PO's supposed plain meaning adds new verbs to the claim and changes its sentence structure

[11] locating encryption information that identifies encrypted portions of frames of video within the requested portions of the selected stream of protected video.

^
and is

POR:

selected stream of protected video.” The “located encryption information” (a) identifies encrypted portions of frames of video and (b) is within the requested portions of the selected stream of protected video.

PO attempts to rewrite the claim based on non-existent language

POR:

For instance, in one embodiment, the specification explains that once the requested portion of the video (referred to as a “BlockGroup”) is received, it is “parsed” for the DRMInfo (*i.e.*, “encryption information”) that identifies the encrypted portions of the frame (*i.e.*, “locating the encryption information within the requested portions of the video”):

[E]ach of the Matroska container files containing an alternative stream of protected video includes *a DRMInfo element in a BlockGroup element containing a protected frame of video, where the DRMInfo element indicates at least a portion of the protected frames of video that is encrypted* ..., and the client application configures the processor



This purported quote appears *nowhere* in the '588 patent.

- Not in the claims
- Not in the specification

Embodiments cited by PO also support the plain and ordinary meaning that was applied by the Petition

ID:

a relationship. Likewise, although embodiments disclosed in the Specification of the '588 Patent support Patent Owner's more restrictive construction, the same embodiments also support the more grammatically correct construction as well.

POR:

For instance, in one embodiment, the specification explains that once the requested portion of the video (referred to as a "BlockGroup") is received, it is "parsed" for the DRMInfo (i.e., "encryption information") that identifies the encrypted portions of the frame (i.e., "locating the encryption information within the requested portions of the video"):

[E]ach of the Matroska container files containing an alternative stream of protected video includes a *DRMInfo element in a BlockGroup* element containing a protected frame of video, where *the DRMInfo element indicates at least a portion of the protected frames of video that is encrypted* ..., and the client application configures the processor to access video frames in a stream of protected video using the common cryptographic information by configuring the processor to: obtain a BlockGroup containing a protected frame of video; *parse the BlockGroup element to obtain a DRMInfo element indicating at least a portion of the protected frame of video that is encrypted* using an encryption key from the set of encryption keys ...

DRMInfo identifies encrypted portions of frames of video within the requested portions of the selected stream of protected video

'588 Patent:

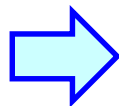
at least a portion of an index from the container file; identify the portion of the container file containing a specific portion of content using the index; and request the identified portion of the container file.

According to PO, the specification requires encryption information to be *inside* the requested portions of the selected stream

Based on an identical specification, the '588 parent recites encryption (DRM) information *outside* the requested portions of the selected stream.

The top level index file is outside of the streams (it identifies the alternative streams).

The encryption information ("DRM information") is in the top level index file, not the video container files.



US 9,621,522 (parent of the '588 patent):

obtain a top level index file from the content distribution server, wherein the top level index file identifies a plurality of alternative streams of protected video that have been protected by a common set of frame keys generated by a source encoder, and wherein the top level index file comprises (i) an encrypted copy of a first key from the common set of frame keys and (ii) a set of DRM information that identifies protected portions of the alternative streams of protected video and frame keys to utilize in accessing the protected portions of the alternative streams;

PO argues that “encryption information” and “DRM information” are two different things

Sur-Reply:

inconsistent with DivX’s construction. In fact, the two claims concern *different* types of information. As can be seen below, claim 1 of the ’588 concerns “*encryption information* that identifies *encrypted portions of frames of video*” whereas claim 1 of the parent concerns “*DRM information* that identifies *protected portions of the alternative streams* of protected video.”

But PO and its expert admitted that the “DRM information” in the specification is the “encryption information” recited in the claims

POR:

For instance, in one embodiment, the specification explains that once the requested portion of the video (referred to as a “BlockGroup”) is received, it is “parsed” for the **DRMInfo (i.e., “encryption information”)** that identifies the encrypted portions of the frame (i.e., “locating the encryption information within the requested portions of the video”):

Dr. Nielson:

Q: Is the **DRM information** described here in column 5 the **encryption information** that's recited in the challenged claims?

...

Q: Column 5, lines 4 through 11.

A: (Examined exhibit.) Let's see. So it says that the DRM information indicates portions of frames of videos that are encrypted.

...

Yes, I would say that that is encryption information that indicates portions of frames of video that are encrypted.

In the parents of the '588 patent, PO included the limitation it now seeks to insert—
but omitted that limitation from the '588 patent

US 8,909,922 (Claim 1):

obtain a top level index file identifying a plurality of separate container files each containing one of a plurality of alternative streams of protected video, wherein each of the alternative streams of protected video includes video frames that are encrypted using a common set of frame keys comprising a plurality of different frame keys, wherein each of the container files containing the alternative streams of protected video comprises (i) an encrypted copy of the common set of frame keys and (ii) a set of DRM information that identifies encrypted portions of the video frames and frame keys to utilize in accessing the encrypted portions of the video frames, and wherein the set of DRM information in each of the plurality of alternative streams of protected video references the same common set of frame keys;

US 9,247,311 (Claim 1):

after encrypting the portions of encoded video frames, (1) write the encoded video frames of each alternative stream to a separate container file from a plurality of container files and (2) write DRM information to each separate container file that identifies the encrypted portions of several encoded video frames written to the separate container file;

PO argues that locating encryption information is “central” to the alleged invention—but did not mention this feature in district court

POR:

Indeed, locating encryption information within the requested portions of the stream is one of the central aspects of the '588's inventive system.

UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETFLIX INC. AND HULU, LLC,
Petitioners,

v.
DIVX, LLC,
Patent Owner.

Case IPR2020-00558
Patent 10,225,588

PATENT OWNER DIVX LLC'S RESPONSE
TO PETITION FOR INTER PARTES REVIEW
OF UNITED STATES PATENT NO. 10,225,588

PO's District Court Complaint :

224. The '588 claims are directed to “perform[ing] adaptive bitrate streaming using alternative streams of protected content.” ’588 patent, 2:66-3:1. The '588 invention reduces the complexity of the cryptographic information needed to ensure content security for multiple, alternative video streams so that a user performing ABS experiences fewer stalls, delays, or errors caused by processing of the cryptographic information on the playback device. The '588 patent is directed to a new encryption architecture for digital video streams that uses common frame encryption keys to encode alternate video streams, reducing playback stalls and improving performance during ABS. The inventions recited in the '588 patent enable Netflix to offer its users an improved experience for ABS while maintaining the content security that it and other content providers require to make video content available over the internet.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Re: DIVX, LLC v. Netflix, Inc. and Hulu, LLC, et al.
Case No. 2:19-cv-08279-DWM

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

Plaintiff:
DIVX, LLC, a Delaware limited liability company.

v.

Defendant:
NETFLIX, INC., a Delaware corporation.

FIRST AMENDED COMPLAINT
FOR PATENT INFRINGEMENT
DEMAND FOR JURY TRIAL

— 1 —
FIRST AMENDED COMPLAINT
Netflix, Inc. and Hulu, LLC, et al. v. DivX, LLC
IPR2020-00558 (DivX, Inc. and Hulu, LLC v. DivX, LLC)

Dispute 3

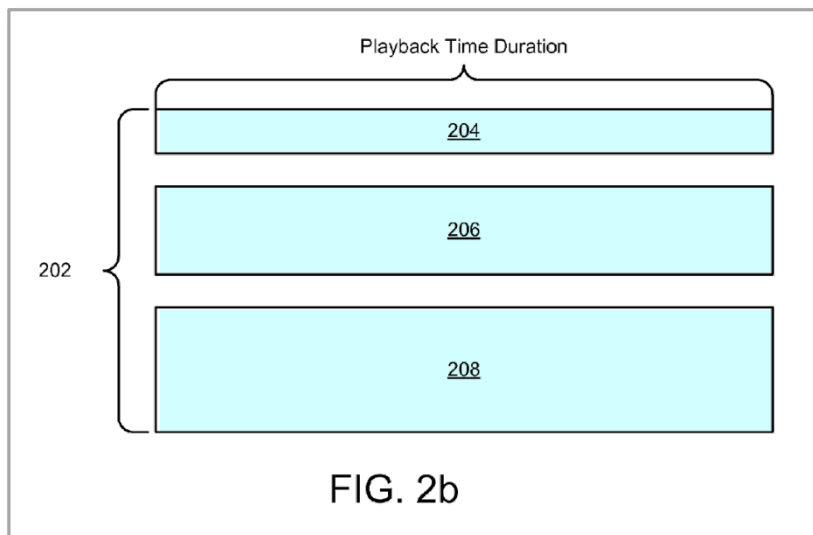
The combination teaches limitation [1e] (“... encrypted using a set of common keys ...”)

[1e] obtaining a top level index file identifying a plurality of alternative streams of protected video, wherein each of the alternative streams of protected video includes partially encrypted video frames that are encrypted using a set of common keys comprising at least one key, and wherein the partially encrypted video frames contain encrypted portions and unencrypted portions of data;

The Combination teaches Limitation [1e] two alternative ways

Hurst

encoder module 406, for example. The streamlets 304 of different bitrates may be encrypted with the same key. Alter-



Lindhahl's Global Key

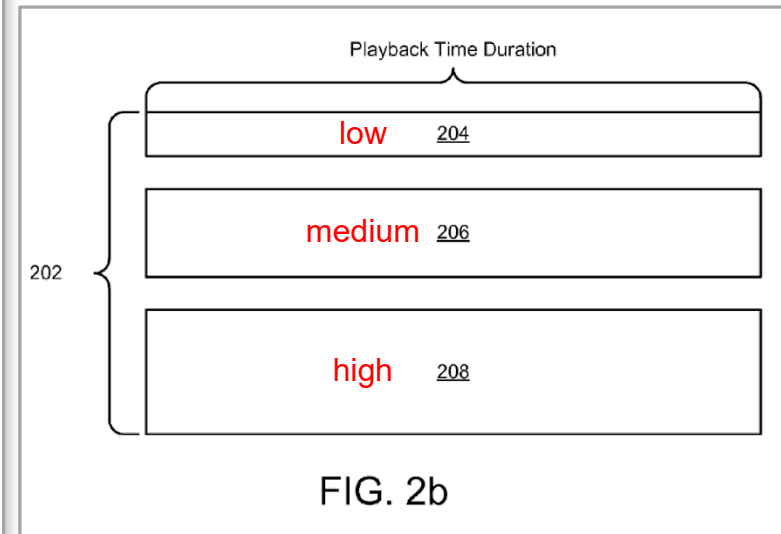
Petition:

First, Lindahl teaches or suggests that media files may be encrypted (and therefore decrypted²) with a global key. *See* Ex. 1007, ¶[0066] (“Once the media file is downloaded 708, the media file can then be decrypted 710 at the user's local machine using the cryptographic key. The global key or other cryptographic key may also be used.”); Ex. 1003, ¶144. Here, Lindahl teaches an embodiment where a “global” key is used to encrypt and decrypt all of the media files on the server. *See id.*

Hurst teaches adaptive bitrate streaming

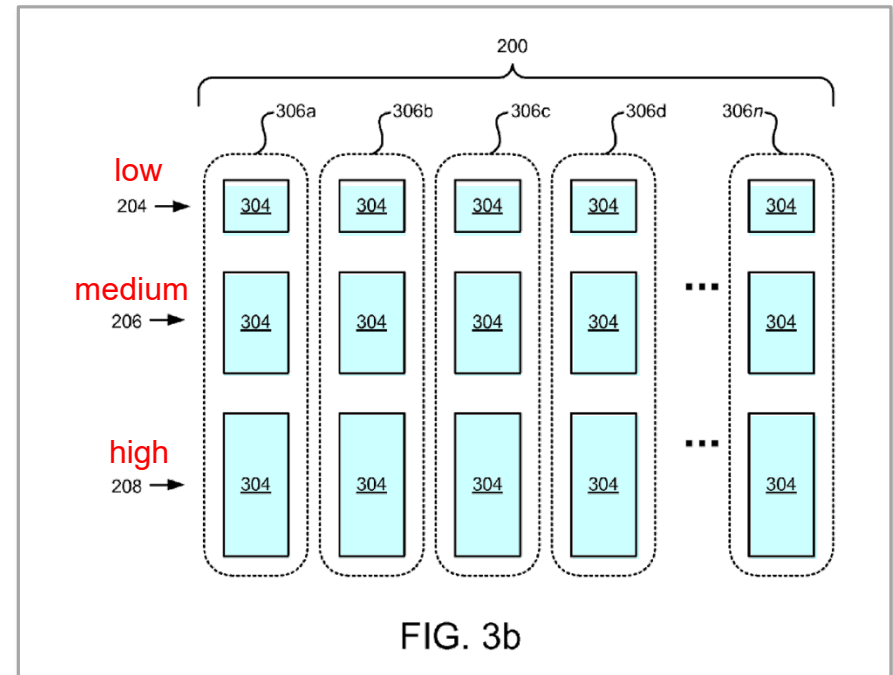
Hurst:

FIG. 2b is a schematic block diagram illustrating one embodiment of a plurality of streams **202** having varying degrees of quality and bandwidth. In one embodiment, the plurality of streams **202** comprises a low quality stream **204**, a medium quality stream **206**, and a high quality stream **208**. Each of the streams **204**, **206**, **208** contains an encoded representation of the content file **200** encoded and compressed to varying bit rates. For example, the low quality stream **204** may be encoded and compressed to a bit rate of 100 kilobits per second (kbps), the medium quality stream **206** may be encoded and compressed to a bit rate of 200 kbps, and the high quality stream **208** may be encoded and compressed to 600 kbps.



Hurst teaches encrypting the alternative streams using the same key

encoder module 406, for example. The streamlets 304 of different bitrates may be encrypted with the same key. Alter-



Annotations added

Using the same key was a natural approach for adaptive streaming

Chen explains that client devices switch between alternative streams.

Chen:

standard HTTP. This technique may involve stream segmentation and the use of multiple streams, all within the context of standardized HTTP requests. The media, such as video, may be encoded at multiple bitrates to form different versions, or representations. The terms “version” and “representation” are used synonymously in this document. Each version or representation may be broken into smaller pieces, perhaps on the order of a few seconds each, to form segments. Each segment may then be stored on a web server or CDN as a separate file. [0064] On the client side, requests may then be made, using HTTP, for individual segments that are seamlessly spliced together by the client. The client may switch to different data rates based on available bandwidth. The client may also request multiple representations, each presenting a different media component, and may present the media in these representations jointly and synchronously. Triggers for switching may include buffer occupancy and network measurements, for example. When operating in the steady state, the client may pace requests to the server to maintain a target buffer occupancy.

Since the alternative streams are accessed as a group, it was obvious to encrypt them as a group, as Hurst teaches.

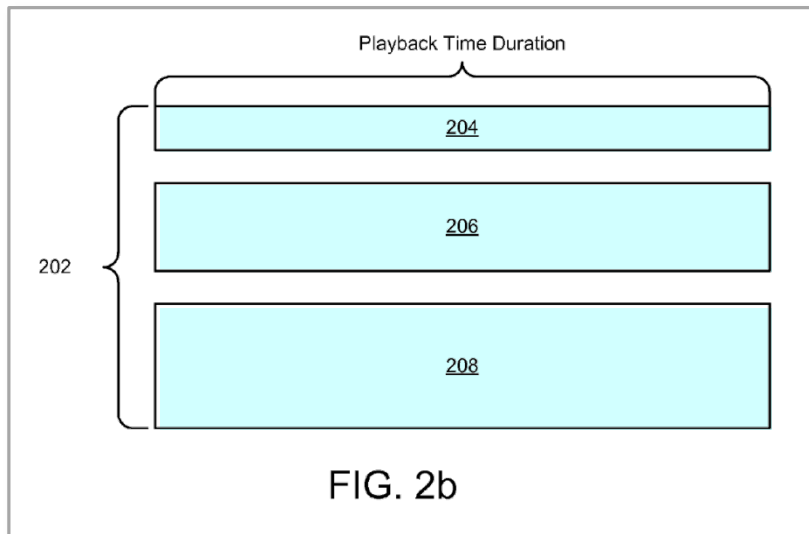
Dr. McDaniel (Ex. 1003):

Hurst’s teachings, e.g., where the alternative streams are encoded at different bitrates and encrypted as a group in the same manner, such as by using the same key, because they follow the usage model for video distribution in adaptive streaming, where the playback device gains access to the alternative streams as a group. See Ex. 1006, ¶¶[0063-0064]; *supra* Section IV.B; VIII.A.2[1e]. For example, a playback device adaptively streaming a movie is typically granted access to its alternative streams for the movie because it is expected to switch between them depending on channel bandwidth. Since the alternative streams are accessed as a group, it would have been obvious to encrypt them as a group, using the same set of keys, so that the alternative streams can be accessed as a group

Hurst teaches using the same key as one of two possibilities

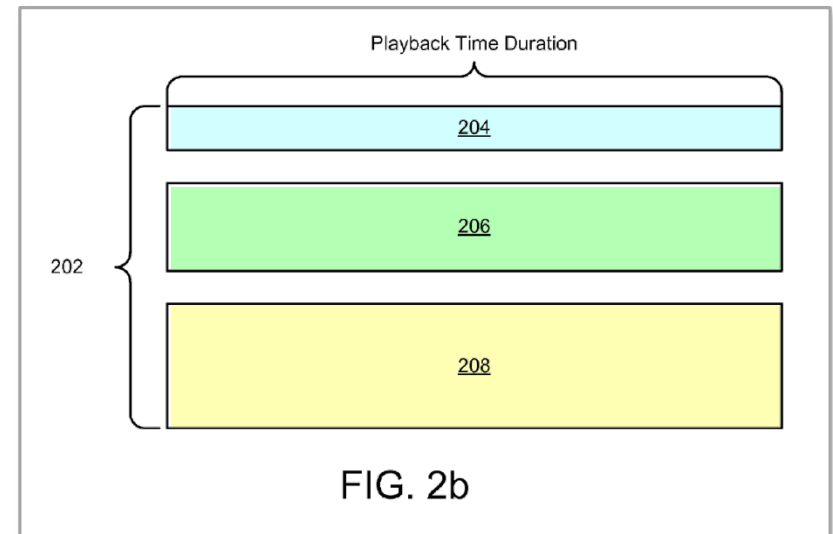
EX1008, 18:66-67:

“The streamlets 304 of different bitrates may be **encrypted with the same key.**”



EX1008, 18:67-19:2:

“***Alternatively***, the encoder module 406 may be configured to encrypt each bit rate with a different set of encryption keys.”



There is no dispute that Hurst discloses limitation [1e]

POR:

The Petition alternatively relies on Hurst for the disclosure of encrypting video frames in alternative streams of content using “a set of common keys.” Pet., 32-33. Hurst, however, only references in passing the fact that the same key *can* be used for all streams, a point that was not in dispute. The question is whether Hurst teaches doing so for alternative streams of protected content, and Hurst teaches against doing such a thing—for Hurst follows its entirely noncommittal mention that it is *possible* to use a single key followed by a prolonged discussion of why it is better to *not* use a single key and to instead use a different specialized

Hurst suggests using different keys for an “alternative[]” usage model with standard and premium versions of content

Hurst:

natively, the encoder module **406** may be configured to encrypt each bit rate with a different set of encryption keys. This, beneficially, allows for a publisher to allow a “standard” user to view the movie at a lower resolution while a “premium” user is allowed to watch the movie at a higher resolution or bitrate. The DRM server **1204** is configured to authen-

Petition:

While Hurst discloses other embodiments, e.g., services with standard and premium streams, those are not relied upon here, and a POSITA would have been motivated to apply Hurst’s teaching of encrypting alternative streams in the same manner, for the reasons explained above. See Ex. 1008, 18:66-67; Ex. 1003, ¶125.

The Petition did not rely on this alternative usage model

PO argues teach-away based on a benefit of using different keys—
but a benefit for one of two possibilities “does not amount to a teaching away”

POR:

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETFLIX INC. AND HULU, LLC,
Petitioners,

v.

DIVX, LLC,
Patent Owner.

Case IPR2020-00558
Patent 10,225,588

PATENT OWNER DIVX LLC'S RESPONSE
TO PETITION FOR INTER PARTES REVIEW
OF UNITED STATES PATENT NO. 10,225,588

That sentence is immediately followed by an explanation of why it would be
“beneficial” to instead “encrypt each bit rate with a different set of encryption keys”:

Federal Circuit:



“But the teaching away inquiry does not focus on whether a person of ordinary skill in the art would have merely *avored* one disclosed option over another disclosed option. In assessing whether prior art teaches away, that ‘better alternatives exist in the prior art does not mean that an inferior combination is inapt for obviousness purposes.’ *In re Mouttet*, 686 F.3d 1322, 1334 (Fed. Cir. 2012). **When there are only two possible formulations and both are known in the art at the time, the fact that there may be reasons a skilled artisan would prefer one over the other does not amount to a teaching away from the lesser preferred but still workable option.**”

Bayer Pharma AG v. Watson Laboratories, Inc., 874 F.3d 1316, 1327 (Fed. Cir. 2017)

Known techniques do not become patentable simply because supposedly better options are known



“A known or obvious composition does not become patentable simply because it has been described as somewhat inferior to some other product for the same use.”

In re Gurley, 27 F.3d 551, 552–53 (Fed. Cir. 1994)

PO argues teach-away based on an alleged benefit of using different keys

Hurst:

Reference throughout this specification to features, advantages, or similar language does not imply that all of the features and advantages that may be realized with the present invention should be or are in any single embodiment of the invention. Rather, language referring to the features and

PO contradicts Hurst's express teachings

When there is a motivation to pursue one of multiple potential options, there is a motivation to combine



“After reviewing the prior art, the district court found that a person of ordinary skill ‘would have been motivated to pursue everolimus as ***one of several potential treatment options*** for advanced solid tumors, including advanced RCC.’ *Decision*, 287 F. Supp. 3d at 516. ***This finding should have affirmatively answered whether there would have been a motivation to combine.***”

Novartis Pharm. Corp. v. W.-Ward Pharm. Int’l Ltd., 923 F.3d 1051, 1059-1060 (Fed. Cir. 2019)

The combination of Lindahl and Chen leaves only a finite number of possibilities

Petition:

Second, the application of Lindahl to Chen leaves only a finite number of possibilities: either (1) use the same set of keys for all representations of a video, or (2) use different sets of keys. Ex. 1003, ¶146. A POSITA would have found it obvious to use the same set of keys as one of those two possibilities; recognized the design need to apply encryption to adaptive streaming because it was widely known that adaptive video streaming would require DRM; and recognized the market pressure to do so given the growth of popular commercial streaming services. *Id.*

Lindahl teaches using a global key to encrypt media files

Lindahl:

[0066] Once the media file is downloaded 708, the media file can then be decrypted 710 at the user's local machine using the cryptographic key. The global key or other cryptographic key may also be used. If the metadata of the media file itself is encrypted, the metadata can also be decrypted using the global key which has previously been provided to the user who has purchased the access rights to the media file. Also, if decrypted 710, the media file can optionally be encrypted 710 again in accordance with another cryptographic key. This optional encryption 710 can be used to re-encrypt the media file for restricted usage by the user.

PO argues that Lindahl “never” discloses encrypting *media files* with the global key

POR:

may be encrypted...with a global key.” Pet., 31. But Lindahl never discloses that media files may be encrypted with a global key. Rather, Lindahl only teaches that *metadata* associated with a media file, but *not* the media data within the file, may be encrypted with a global key—and even for metadata, Lindahl teaches the use of

Lindahl:

[0066] Once the media file is downloaded 708, the media file can then be decrypted 710 at the user’s local machine using the cryptographic key. The global key or other cryptographic key may also be used. If the metadata of the media file itself is encrypted, the metadata can also be decrypted using the global key which has previously been provided to the user who has purchased the access rights to the media file. Also, if decrypted 710, the media file can optionally be encrypted 710 again in accordance with another cryptographic key. This optional encryption 710 can be used to re-encrypt the media file for restricted usage by the user.

Lindahl expressly teaches using the global key for media files



PO argues that Lindahl “only teaches” encrypting metadata with the global key

POR:

may be encrypted...with a global key.” Pet., 31. But Lindahl never discloses that *media files* may be encrypted with a global key. Rather, Lindahl only teaches that metadata associated with a media file, but *not* the media data within the file, may be encrypted with a global key—and even for metadata, Lindahl teaches the use of

Lindahl:

[0066] Once the media file is downloaded 708, the media file can then be decrypted 710 at the user’s local machine using the cryptographic key. The global key or other cryptographic key may also be used. If the metadata of the media file itself is encrypted, the metadata can also be decrypted using the global key which has previously been provided to the user who has purchased the access rights to the media file. Also, if decrypted 710, the media file can optionally be encrypted 710 again in accordance with another cryptographic key. This optional encryption 710 can be used to re-encrypt the media file for restricted usage by the user.



Metadata is discussed in the next sentence.

The media file and metadata are both decrypted using the global key.

A global key is sufficiently secure for many applications

Shi:

Previous studies of cryptography have focused on text data. The encryption algorithms developed to secure text data, such as DES[17] and RSA[17], may not be suitable to multimedia applications because of large data size, low value and real-time constraint. Security is a trade-off between the cost of the data being protected and the cost it takes an attacker to get that data. Protecting data worth only several dollars with a security system that costs a million dollars to break is obviously a bad investment. The trade-off is to find the balance between the cost to an attacker and the value of the data to its owner. The cost to break a security system can be measured in many ways, which include the amount of computer time necessary to perform the security break, the amount of time and money spent by attackers. The costs of a multimedia security system include the amount of investment by data provider and the payment required for customer service. In multimedia applications, data providers, such as VOD providers, do not want to spend too much money on their security equipments; data receivers do not want to buy extra devices(hardware boxes, or co-processors). Multimedia applications appeal those encryption algorithms which require less computation and low implementation cost. For multimedia data, we only need to provide sufficient security level such that the cost to break the security system is much more expensive than to buy the program. Hence, light-weight and cost-effective multimedia data encryption algorithms should be developed.

PO's new Sur-Reply evidence

PO's Sur-Reply evidence is prohibited



“All arguments for the relief requested in a motion must be made in the motion. A reply may only respond to arguments raised in the corresponding opposition, patent owner preliminary response, patent owner response, or decision on institution. A sur-reply may only respond to arguments raised in the corresponding reply and **may not be accompanied by new evidence other than deposition transcripts** of the cross-examination of any reply witness.”

37 CFR § 42.23(b)

DivX's new evidence is irrelevant

No mention of RTP until Sur-Reply

An RTP Payload Format for Generic Forward Error Correction

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

PO misunderstands its new evidence

12 Security Considerations

The use of FEC has implications on the usage and changing of keys for encryption. As the FEC packets do consist of a separate stream, there are a number of permutations on the usage of encryption. In particular:

- o The FEC stream may be encrypted, while the media stream is not.
- o The media stream may be encrypted, while the FEC stream is not.
- o The media stream and FEC stream are both encrypted, but using different keys.
- o The media stream and FEC stream are both encrypted, but using the same key.

The first three of these would require any application level signaling protocols to be aware of the usage of FEC, and to thus exchange keys for it and negotiate its usage on the media and FEC streams separately. In the final case, no such additional mechanisms are needed. The first two cases present a layering violation, as FEC packets should really be treated no differently than other RTP packets. Encrypting just one may also make certain known-plaintext attacks possible. For these reasons, applications utilizing encryption SHOULD encrypt both streams.

PO mischaracterizes Kunkelmann

Second, Dr. McDaniel cites Exhibit 1023, 217, for the proposition that “[a]pplying FEC to data which already has been partially encrypted does no harm with respect to the data security.” Ex. 1031 [McDaniel-Reply-Decl.] ¶12. But the same exhibit explains that partial frame encryption cannot be applied to systems where FEC is created at the application level, for some of the same reasons identified by Dr. Nielson:

Generally, forward error correction (FEC) mechanisms should not be applied to the application layer data of streams which are transmitted via partial encryption or a distinct-route approach. The reason is that an FEC coder increases the redundancy of the transmitted data so that an attacker gets access to more information, and hence the security of the stream is reduced.