

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'S DEMONSTRATIVE EXHIBITS
(EXHIBIT 2029)**

Netflix Inc., Hulu LLC v. DivX LLC

IPR2020-00558
U.S. Patent No. 10,225,588

Patent Owner DivX LLC
May 25, 2021

Nathan Lowenstein
Kenneth Weatherwax
Parham Hendifar
Lowenstein & Weatherwax LLP



Table Of Contents

1. Petitioner Fails To Show “Locating Encryption Information ... Within The Requested Portions Of The Selected Stream Of Protected Video.”
 - 1.A. In Contrast To Petitioner’s Attorney Arguments, Patent Owner’s Construction Is Supported By The Plain Meaning, Every Embodiment, And Unrebutted Expert Testimony.
 - 1.B. The Petition Does Not Argue The “Locating” Limitation Is Disclosed/Obvious Under Patent Owner’s Construction.
2. Petitioner Fails To Show That A POSITA Would Have Modified Chen To Implement Partial Frame Encryption.
3. Petitioner Fails To Show That A POSITA Would Have Encrypted Alternative Streams Of Protected Video With “A Set Of Common Keys Comprising At Least One Key.”

Table Of Contents

1. Petitioner Fails To Show “Locating Encryption Information ... Within The Requested Portions Of The Selected Stream Of Protected Video.”
 - 1.A. In Contrast To Petitioner’s Attorney Arguments, Patent Owner’s Construction Is Supported By The Plain Meaning, Every Embodiment, And Unrebutted Expert Testimony.**
 - 1.B. The Petition Does Not Argue The “Locating” Limitation Is Disclosed/Obvious Under Patent Owner’s Construction.
2. Petitioner Fails To Show That A POSITA Would Have Modified Chen To Implement Partial Frame Encryption.
3. Petitioner Fails To Show That A POSITA Would Have Encrypted Alternative Streams Of Protected Video With “A Set Of Common Keys Comprising At Least One Key.”

Claims Require “Locating Encryption Information ... Within The Requested Portions Of ... Video”

1. A playback device for playing protected content from a plurality of alternative streams, comprising:
 - 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:
 - 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;
 - obtaining a copy of the set of common keys;
 - detecting streaming conditions for the playback device;
 - selecting a stream from the plurality of alternative streams of protected video based on the detected streaming conditions;
 - receiving a container index that provides byte ranges for portions of the selected stream of protected video within an associated container file;
 - requesting portions of the selected stream of protected video based on the provided byte ranges;
 - locating encryption information that identifies encrypted portions of frames of video within the requested portions of the selected stream of protected video;
 - decrypting each encrypted portion of the frames of video identified within the located encryption information using the set of common keys; and
 - playing back the decrypted frames of video obtained from the requested portions of the selected stream of protected video.

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

- ① locating encryption information
- ② that identifies encrypted portions of frames of video
- ③ within the requested portions of the selected stream of protected video

Plain Meaning: “Encryption Information” Must Be “Locat[ed]” “Within The Requested Portions” Of Video



Prof. Seth Nielson
Univ. Texas at Austin

DECLARATION OF SETH NIELSON, PH.D.

87. A POSITA would understand that the first clause of the limitation requires “*locating* encryption information.” The next clause—“*that* identifies encrypted portions of frames of video”—informs a POSITA regarding the function of the “encrypted information.” The last clause—“*within* the requested portions of the selected stream of protected video”—informs a POSITA where the “*locat[ed]* encrypted information” is “located.” Therefore, a POSITA would interpret the limitation as requiring the “encryption information” to be “located” “within the requested portions of the selected stream of protected video.”

Every Embodiment Supports Patent Owner's Construction

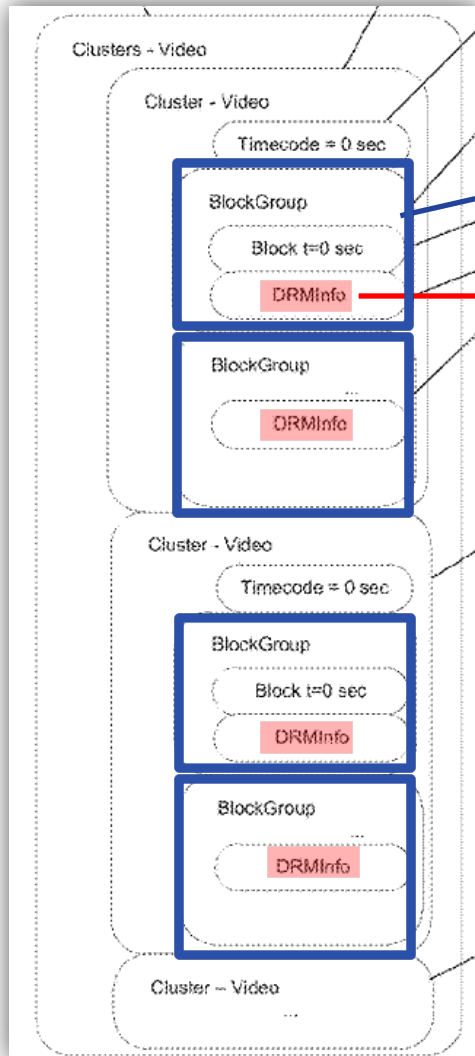


FIG. 4e

Requested Portion Of Video

Encryption Information

DECLARATION OF SETH NIELSON, PH.D.

88. This understanding of a POSITA from the claim language is also in accord with and is reinforced by every embodiment in the '588's specification. In every embodiment of the '588 Patent where a location for the encryption information is disclosed, "encryption information" is located within the "requested portion" of the video. Ex. 1001 ['588 Patent] 9:23-29; 13:57-63; 16:33-49; 22:14-17; 25:10-21.

Petitioner's Expert Agrees: Every Embodiment Supports Patent Owner's Construction

2 Q Yes, of course. In the embodiment of the
3 patent in Column 9, Line 23 through 29, the encryption
4 information is located within the requested portion of
5 the selected stream of the protected video, correct?

6 A It would appear so.

7 Q Okay. If I may refer you to Column 13,
8 Line 57 through 63.

9 A I am there.

10 Q In the embodiment of the patent in Column
11 13, Line 57 through 63, the encryption information is
12 located within the requested portion of the selected
13 stream of protected video, correct?

14 A In this -- in this embodiment.

15 Q Did you say, yes?

16 A In this embodiment, yes.

17 Q Now, if I may refer you to Column 16,
18 Line 33 through 49.

19 A Column 16?

20 Q Correct. Column 16, Lines 33 through 49.

21 A Okay. I am there.

22 Q Okay. In the embodiment of the patent in
23 Column 16, Line 33 through 49, the encryption
24 information is located within the requested portion of
25 the selected stream of protected video, correct?

4 THE WITNESS: In this embodiment, it would
5 appear that the encryption information is included.

6 BY MR. HENDIFAR:

7 Q Okay. If I may direct your attention now to
8 Column 22, Lines 14 through 17, please.

9 A Okay. I lost -- I was just reading my
10 report. Which Column? 22?

11 Q Sure. Column 22, Lines 14 through 17.

12 A 14 through 17, okay.

13 Q In the embodiment of the patent in Column
14 22, Lines 14 through 17, the encryption information is
15 located within the requested portion of the selected
16 stream of protected video, correct?

17 A Let me read this for context.

18 Q Sure.

19 A It would appear it was included. The DRM
20 element was included in the stream.

15 Q Sure. In the embodiment of the patent in
16 Column 25, Line 15 through 21, the encryption
17 information is located within the requested portion of
18 the selected stream of protected video, correct?

19 A It would appear so in this particular
20 embodiment.

Petitioner's Expert: Could Not Identify A Single Embodiment Contrary To Patent Owner's Construction

5 Is there any embodiment of the '588 patent
6 that is actually required in the '588 patent where the
7 encryption information of a given cluster is not
8 located within that cluster?

9 MR. LIANG: Same objection.

10 THE WITNESS: So -- so putting aside
11 somebody skilled -- how somebody skilled in the art
12 would interpret the '588, and putting aside the
13 embodiments that don't have an explicit description of
14 where the information lies, there is not an explicit
15 embodiment.

Claim Construction Is Guided By The Embodiments



- “We cannot look at the ordinary meaning of the term ... In a vacuum. Rather, **we must look at the ordinary meaning in the context of the written description** and the prosecution history.” - *Medrad, Inc. v. MRI Devices Corp.*, 401 F.3d 1313, 1319 (Fed. Cir. 2005)
- *Kinetic Concepts, Inc. v. Blue Sky Med. Grp., Inc.*, 554 F.3d 1010, 1018-19 (Fed. Cir. 2009) (limiting “wound” to “skin wounds” where **“[a]ll of the examples described in the specification** involve skin wounds”)
- *In re Abbott Diabetes Care Inc.*, 696 F.3d 1142, 1149-50 (Fed. Cir. 2012) (construing “electrochemical sensor” to exclude external cables or wires where **“every embodiment shows an electrochemical sensor without external cables or wires”**);
- *Wisconsin Alumni Res. Found. v. Apple Inc.*, 905 F.3d 1341, 1351-52 (Fed. Cir. 2018) (limiting “prediction” to dynamic prediction **where all embodiments** describe dynamic prediction and allowing the term to cover static prediction “would ‘expand the scope of the claims far beyond anything described in the specification’”)

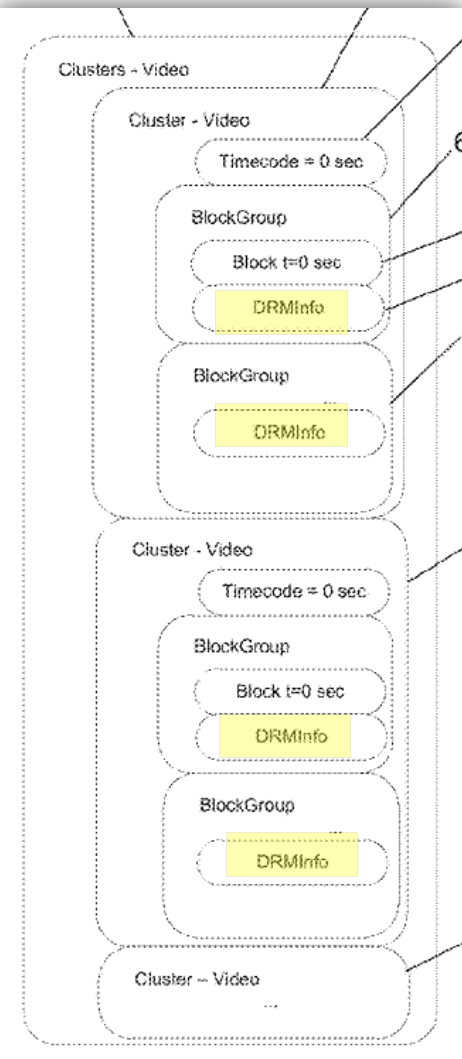
'588 Modified Industry Standard Container File To Locate Encryption Information Within Requested Portions

DECLARATION OF SETH NIELSON, PH.D.

90. A POSITA would further understand that locating encryption information within the requested portions of the stream is one of the central aspects of the '588's inventive system. For example, the inventors did not simply utilize the industry standard Matroska container file which was not able to contain the necessary encryption information, but, rather, modified the Matroska file format to add this aspect of the invention:

Patent No.: US 10,225,588 B2

mation. In many embodiments, the Matroska container files are specialized Matroska container files that include enhancements (i.e. elements that do not form part of the Matroska file format specification) that facilitate retrieval and decryption using common cryptographic information of specific portions of media during adaptive bitrate streaming.



Petitioner's And Dr. McDaniel's Analysis Concerning The Correct Claim Construction?



- **No** analysis in opening declaration
- **No** analysis in reply declaration
- **Do not** address Dr. Nielson's claim construction analysis
- **Neither** Petitioner **nor** Dr. McDaniel parse claim language
- **No** mention of "plain meaning" in Reply
- **No** specification support identified in Petitioner's briefing
- **No** caselaw support

Dr. Nielson's "Unrebutted Testimony" Should Be Dispositive



- “Dr. Sonka’s testimony is unrebutted by Petitioner’s expert ... His reply declaration does not address the meaning of the In Focus limitation ... nor whether that limitation is taught or suggested by the prior art.” - *3Shape A/S v. Align Tech.*, IPR2019-00163, Paper 37, 16-24 (PTAB Jun. 9, 2020)
- “Petitioner’s expert, Dr. Freedman, does not construe the ‘upload’ limitation and did not provide a declaration responsive to Dr. Burger’s testimony. Accordingly, Dr. Burger’s testimony is unrebutted.” - *Limelight Networks v. Akamai Techs.*, IPR2016-01894, Paper 30, 16 (PTAB Mar. 1, 2018)
- “...Patent Owner does not direct us to any evidence, such as expert testimony, negating Petitioner’s three other alternative meanings.” - *Volkswagen Grp. of Am., Inc. v. Michigan Motor Techs.*, IPR2019-01274, Paper 47, 64-65 (PTAB Dec. 21, 2020)
- “... rather than to explain with reasons, references to embodiments in the Specification, and supporting testimony from a technical witness, Patent Owner simply concludes that it is clear the language at issue carries a certain meaning. Such conclusory disagreement, without analysis and factual underpinning, is not sufficient to persuade. Petitioner correctly notes that Patent Owner’s arguments are merely ‘raw attorney argument, citing no evidence or expert testimony.’ Reply 30. Argument of counsel cannot take the place of evidence lacking in the record. - *Marvell Semiconductor, Inc. v. Uniloc 2017 LLC*, IPR2019-01350, Paper 24, 75-76 (PTAB Feb. 1, 2021)

Institution Decision: Relied On 24:63-25:2

Prelim. Resp. 29 (quoting Ex. 1001, 25:10–21). However, the portion just before the cited section recites more generally:

Depending upon the structure of the [Uniform Resource Identifiers] contained within the top level index file, the playback device can *either use information from the URIs or information from the headers of the Matroska container files* to request byte ranges from the server that contain at least a portion of the index from relevant Matroska container files.

Ex. 1001, 24:63–25:2 (emphases added). This suggests that information regarding ranges in the files need not come from the files themselves, at least in some embodiments. Patent Owner additionally cites to another

24:63-25:2 Is About Byte Ranges; Confirms Requested Portion (BlockGroup) Contains Encryption Information (DRMInfo)

Top Level Index File Contains Information To Request “Byte Ranges” Of Video

In many embodiments, the playback device does not retrieve the headers for all of the Matroska container files indexed in the top level index file. Instead, the playback device determines the stream(s) that will be utilized to initially commence playback and requests the headers from the corresponding Matroska container files. Depending upon the structure of the URIs contained within the top level index file, the playback device can either use information from the URIs or information from the headers of the Matroska container files to request byte ranges from the server that

Requested Portion Of Video (BlockGroup) Contains DRMInfo

25

contain at least a portion of the index from relevant Matroska container files. The byte ranges can correspond to the entire index or can correspond to the top level of a hierarchical index and a portion of a lower level index (i.e. a HierarchicalIndex element and one or more CuePoint elements). The server provides the relevant byte ranges containing the index information to the playback device, and the playback device can use the index information to request the byte ranges of Cluster elements containing encoded media using this information. When the Cluster elements are received, the playback device can extract encoded media from the BlockGroup elements within the Cluster element, and can decode and playback the media within the BlockGroup elements in accordance with their associated Timecode attributes. Prior to decoding the encoded media, the playback device can check for the presence of a DRMInfo element within each BlockGroup of a video stream to identify whether the encoded media is protected. The playback device can use the information within the DRMInfo element to decrypt encrypted portions of the video prior to decoding.

Dr. Nielson: 24:63-25:2 Is About The Location Of An Index Of Byte Ranges, Not “Encryption Information”

DECLARATION OF SETH NIELSON, PH.D.

91. As noted above, I therefore respectfully disagree with the Board’s preliminary construction of this limitation. In making its preliminary claim construction, the Board quotes the ‘588 at 24:63-25:2 for the proposition that the encryption information can be located anywhere and does not have to be located within the requested portions of the stream. Inst. Dec., 29-30. However, this cited sentence relates to an index of byte ranges of the streaming media that would allow the client to select which byte ranges of the streaming media to request for viewing. This sentence does not relate to the location of *encryption information* that identifies which portions of the frames within those requested byte ranges are encrypted. As discussed above, once the selected portions of video are actually received by the client, the encryption information is located within those selected portions. Thus, the specification does not support the Board’s preliminary construction.

Institution Decision Also Relied Upon Grammar

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

Grammatical Treatises Support Patent Owner's Construction

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

the ELEMENTS of STYLE
by
WILLIAM STRUNK JR.
and
E. B. WHITE

illustrated by
MAIRA KALMAN

“The lawn mower that is broken is in the garage. (Tells which one.)”



The Redbook
A Manual on Legal Style

Bryan A. Garner

“The meeting, which starts at 10 a.m., is about the Matthews case.”



Grammatical “Best Practices” Do Not Outweigh The Specification

Nestle’s Food Co. v. United States, 16 Ct. Cust. 451, 455 (1929 Ct. Cust. App.) (“While it is the general rule that a dependent or modifying clause relates to and modifies its nearest antecedent, such rule must yield, if to adhere to it would defeat the purpose of the Congress.”).

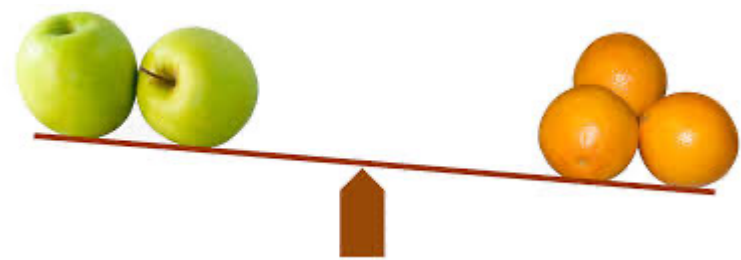
Quality Edge, Inc. v. Rollex Corp., 709 Fed. Appx. 1000, 1006-7 (Fed. Cir. 2017) (reversing claim construction where no “hard and fast” grammatical rule and specification mandated alternative construction to the one suggested by a general grammatical best practice).

Kingsley v. United States, 24 Ct. Cl. 219, 222-223 (1889 Ct. Cl.) (“The language of the section, grammatically considered, might justify that construction, but other considerations indicate that Congress did not so intend it.”)

Reordering Clauses Would Not Have Added Clarity

[1] *Locating encryption information* [3] *within* the requested portions of the selected stream of protected video [2] that identifies encrypted portions of frames of video

Petitioner Compares Apples And Oranges: Parent’s Claim Concerns Different Information Stored In A Different Place



'588 Patent, Claim 1	'522 Patent, Claim 1
“locating <i>encryption information that identifies encrypted portions of frames of video</i> within the requested portions of the selected stream of protected video ...”	“... wherein the top-level index file comprises ... a set of <i>DRM information</i> that identifies <i>protected portions of the alternative streams</i> of protected video”

	What?	Where is it located?
'588 claim 1	“ <i>encryption information</i> that identifies <i>encrypted portions of frames of video</i> ”	“within the requested portions of the selected stream of protected video”
'522 claim 1	“ <i>DRM information</i> that identifies <i>protected portions of the alternative streams</i> ”	“the top-level index file”

Claim 1 of the parent does not even require partial frame encryption

Different Claim Terms In '588 And Parent Presumed To Have Different Meanings



“the [parent] patent’s prosecution history is irrelevant to the meaning of this limitation because the two patents do not share the same claim language.”

-*Resqnet.com, Inc. v. Lansa, Inc.*, 346 F.3d 1374, 1383 (Fed. Cir. 2003)

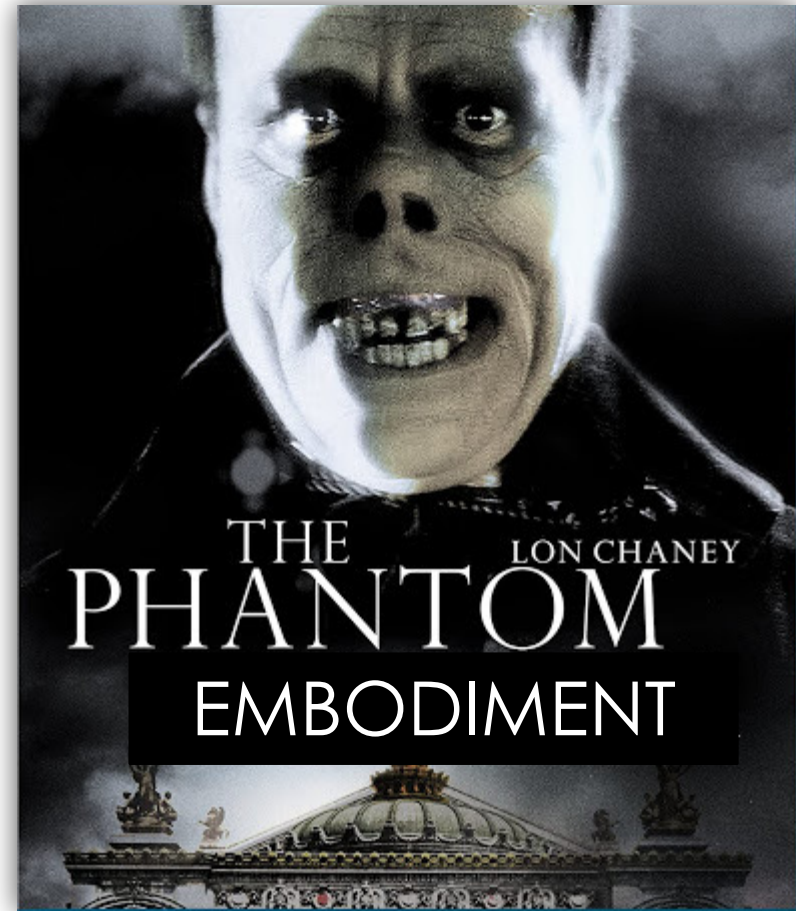
“In the absence of any evidence to the contrary, we must presume that the use of these different terms in the claims connotes different meanings.”

-*CAE Screenplates Inc. v. Heinrich Fiedler GmbH*, 224 F.3d 1308, 1317 (Fed. Cir. 2000)

Even If Some Unsubstantiated “Phantom” Embodiment Were Present, The Parent’s Claim Would Reinforce Patent Owner’s Construction

“The mere fact that there is an **alternative embodiment ... not encompassed by [our] claim construction does not outweigh the language of the claim**, especially when the court's construction is supported by the intrinsic evidence.” ... **This is especially true where, as here, other unasserted claims in the parent patent cover the excluded embodiments.** ...

August Tech. Corp. v. Camtek, Ltd., 655 F.3d 1278, 1285 (Fed. Cir. 2011) (citations omitted).



Petitioner Does Not Point To Any Actual Embodiment In Support Of Its Position

Petitioner's Minor Points Fail

- ❑ **Every** claim construction dispute could be resolved by clearer drafting
- ❑ Any uncertainty is best resolved by reference to the specification, not arbitrarily in Petitioner's favor. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1315-1316 (Fed. Cir. 2005) (en banc)
- ❑ Patent Owner does not seek to add the word "is" or import limitations into the claims
- ❑ Patent Owner's construction is entirely consistent with the plain meaning which requires "locating encryption information ... within the requested portions of the selected stream of the protected video"

All Evidence Supports Patent Owner's Construction

No Direct McDaniel Testimony	Every Embodiment
McDaniel's Admissions	Grammatical Treatises
Plain meaning	Caselaw
No rebuttal testimony	Unrebutted Expert Testimony



Parent Claim

24:63-25:2

Table Of Contents

1. Petitioner Fails To Show “Locating Encryption Information ... Within The Requested Portions Of The Selected Stream Of Protected Video.”
 - 1.A. In Contrast To Petitioner’s Attorney Arguments, Patent Owner’s Construction Is Supported By The Plain Meaning, Every Embodiment, And Unrebutted Expert Testimony.
 - 1.B. The Petition Does Not Argue The “Locating” Limitation Is Disclosed/Obvious Under Patent Owner’s Construction.**
2. Petitioner Fails To Show That A POSITA Would Have Modified Chen To Implement Partial Frame Encryption.
3. Petitioner Fails To Show That A POSITA Would Have Encrypted Alternative Streams Of Protected Video With “A Set Of Common Keys Comprising At Least One Key.”

Claim Construction Is Dispositive: Petitioner Presents No Argument Under Patent Owner's Construction



The Petition Relies Solely On Lindahl For The Disclosure Of “Locating” Limitation

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.*

Petitioner Does Not Argue That Lindahl Discloses Locating Encryption Information “Within Requested Portion” Of Video

“Retrieved” From Where?

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.*

Petitioner's Reply Does Not Dispute That The Petition Fails Under Patent Owner's Construction

PETITIONERS' REPLY

TABLE OF CONTENTS

I.	The Motivation to Combine	3
A.	DivX misrepresents the Petition's motivation to combine.	3
B.	The Petition relies on Chen's basic teachings of adaptive bitrate streaming, not its optional embodiments.	5
C.	Scalable layers, FEC, and fragment-level encryption are optional embodiments.	9
D.	DivX's incompatibility arguments are incorrect.	12
E.	A POSITA would have known how to modify standard file formats.	15
II.	Ground 1 teaches limitation [11]	20
A.	DivX is contradicted by the intrinsic record, including DivX's prior representations to the USPTO.	20
B.	The patentee could have drafted the claims as DivX now desires, but did not.	21
C.	Locating encryption information is not the focus of the '588 patent.	23
III.	The combination teaches "a set of common keys".	23
A.	A POSITA would have been motivated to apply Hurst's teachings.	24
B.	A POSITA would have been motivated to apply Lindahl's teachings.	27
IV.	Conclusion	29

Reply Only Challenges Patent Owner's Construction

Undisputed: Lindahl Does Not Disclose “Locating Encryption Information ... Within The Requested Portion Of The Selected Stream”

DECLARATION OF SETH NIELSON, PH.D.

96. Lindahl is not a streaming system in which “portions” of a “selected stream,” amongst a “plurality of alternative streams” is “requested.” Rather, Lindahl is a system in which the entire media, which is contained in a file, is downloaded for later play back. Ex. 1007 [Lindahl] ¶ 66 (“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.”). Additionally, Lindahl only permits decryption of media once the entire media has been downloaded.

97. Therefore, the concepts of “portions” of a video and “alternative streams” simply do not exist in Lindahl. Regardless of whether Lindahl locates any encryption information, it cannot locate any encryption information within the “requested portions” of the video because a user in Lindahl can never request a portion of a video, much less one from a “selected stream.”

In Lindahl, The Entire Media File Must Be Requested And Downloaded; *i.e.*, There Are No “Requested Portions”

[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 cryp-

Undisputed: Lindahl Does Not Disclose Requesting Any “Portion” Of Video

18 Is there any embodiment of Lindahl where the
19 user can request only parts of a media file?
20 A So I don't see one as I am looking here, but

Petitioner Has Not Provided Any Analysis Whatsoever To Modify Lindahl Beyond Its Teaching



“Petitioner has not presented an analysis sufficient to support modifying [the single reference] beyond the teachings of [the reference] itself.”

Microsoft Corp. v. IpLearn-Focus LLC,
IPR2015-00095, Paper 33, 29 (PTAB Apr. 11, 2016)

Table Of Contents

1. Petitioner Fails To Show “Locating Encryption Information ... Within The Requested Portions Of The Selected Stream Of Protected Video.”
 - 1.A. In Contrast To Petitioner’s Attorney Arguments, Patent Owner’s Construction Is Supported By The Plain Meaning, Every Embodiment, And Unrebutted Expert Testimony.
 - 1.B. The Petition Does Not Argue The “Locating” Limitation Is Disclosed/Obvious Under Patent Owner’s Construction.
2. **Petitioner Fails To Show That A POSITA Would Have Modified Chen To Implement Partial Frame Encryption.**
3. Petitioner Fails To Show That A POSITA Would Have Encrypted Alternative Streams Of Protected Video With “A Set Of Common Keys Comprising At Least One Key.”

“Video Includes Partially Encrypted Video Frames”

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

(10) **Patent No.:** US 10,225,588 B2
(45) **Date of Patent:** *Mar. 5, 2019

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

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;

obtaining a copy of the set of common keys;
detecting streaming conditions for the playback;
selecting a stream from the plurality of alternative streams of protected video based on the detected streaming conditions;

receiving a container index that provides byte ranges for portions of the selected stream of protected video within an associated container file;

requesting portions of the selected stream of protected video based on the provided byte ranges;

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

decrypting each encrypted portion of the frames of video identified within the located encryption information using the set of common keys; and
playing back the decrypted frames of video obtained from the requested portions of the selected stream of protected video.

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;

Petition Relies On Importing Partial Frame Encryption From Lindahl/Hurst Into Chen

PETITION FOR *INTER PARTES* REVIEW

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

A POSITA would have been motivated to apply Lindahl's teachings to Chen to address piracy concerns and improve efficiency, which Chen also raises as a goal. Ex. 1003, ¶¶115, 119-120. The teachings of Chen relied on here reflect

Petitioner's Combination Assumes Chen Permits Any Type Of Encryption, Including Partial Frame Encryption

PETITION FOR *INTER PARTES* REVIEW

OF U.S. PATENT NO. 10,225,588

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

FALSE

Pet., 18

Undisputed: Chen Requires A Modification Of The Standard File Formats To Implement Partial Frame Encryption

REMOTE DEPOSITION OF PATRICK MCDANIEL, Ph.D.

NOVEMBER 16, 2020

8:57 a.m.

25 Q Okay. Do any of the embodiments that you
1 rely on from Chen in your declaration require a
2 modification of a standard file format in order to
3 enable encryption?

4 MR. LIANG: Object to form.

5 THE WITNESS: Yeah, I think the
6 combination -- we are talking about Chen with, you
7 know, using things like partial encryption would
8 require some additional encryption information.

9 For example, to process the contents, so you
10 would probably have to make some modifications to 3GPP
11 to enable or to -- not enable -- to implement the
12 combination of Chen, Hurst and Lindahl.

Chen Discloses Encrypting Fragments, Not “Partial Frame Encryption”

United States
Patent Application Publication
Chen et al.

ENHANCED BLOCK-REQUEST STREAMING
USING SCALABLE ENCODING

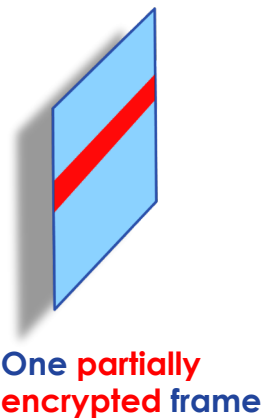
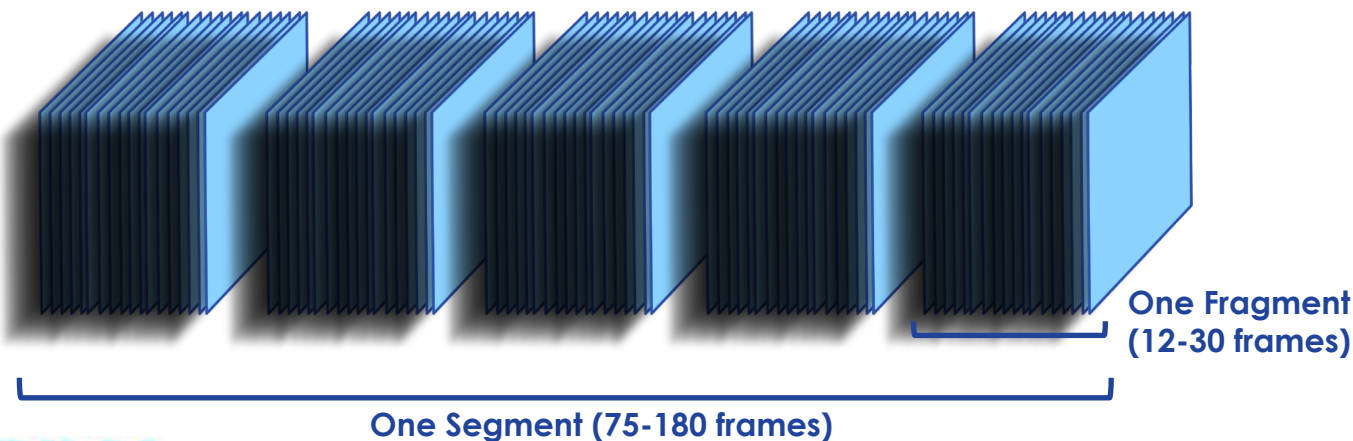
entire representation. Suppose further that the media data structure is such that playout of a block can be done when the entire block is available at the client, i.e., playout of a block can only start after the entire block is received, e.g., due to the structure of the underlying video encoding, or 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

This Is The Only Encryption Disclosure In Chen Cited By Petition (at 18).

Each Fragment Consists Of Multiple Frames

DECLARATION OF SETH NIELSON, PH.D.

51. In Chen, the media content is divided into “smaller pieces, perhaps on the order of a few seconds each, to form segments.” Ex. 1006 [Chen] ¶ 63; *see also id.*, ¶¶ 153, 200-205, 293. Each segment constitutes a separate file. *Id.* (“Each segment may then be stored on a web server or CDN as a separate file.”); *see also id.*, ¶ 72 (“The terms ‘file’ and ‘segment’ are used synonymously in this document unless otherwise specified.”). At the time of the invention, each second of a movie contains roughly 25-60 frames; therefore, a segment file of, e.g., three seconds would contain about 75-180 frames. Each segment in turn consists of one or more fragments of, e.g., a half-second. *See e.g.*, Ex. 1006 [Chen] ¶ 147 (“Multiple fragments may be concatenated into a single segment ...”); ¶ 141 (“with 500 [millisecond] movie fragments”).



Undisputed: Fragment Level Encryption Is Not Partial Frame Encryption

DECLARATION OF SETH NIELSON, PH.D.

50. Chen discusses encrypting Chen's video and highlights that "because encryption is being employed to encrypt each fragment or block separately, and thus the entire fragment or block¹ needs to be received before it can be decrypted." Ex. 1006 [Chen] ¶ 522. A POSITA would understand this statement to mean that the entire fragment or block is encrypted as a singular unit because the entire fragment has to be downloaded before it can be decrypted. I understand that Dr. McDaniel also agrees with my understanding of this aspect of Chen. Ex. 2013 [McDaniel Depo.] 108:5-9 ("encrypting a fragment could be performed at a larger granularity than a frame").

Other Chen Disclosures Teach Encryption Information For “Presentation” (i.e., Each Alternate Stream), Not Each Frame

DECLARATION OF SETH NIELSON, PH.D.

52. A POSITA interpreting Chen in its entirety would also recognize that there were other aspects of Chen that also confirm the understanding that Chen performs fragment level, not frame level, encryption. For example, Fig. 9(a) of Chen shows an example of Chen’s “metadata table 900,” which corresponds to the metadata provided in connection with each one of the one of plurality of “alternative streams.” Ex. 1006 [Chen] ¶ 218. As shown in Fig. 9(a), reproduced below with highlighted annotations added, DRM and encryption information are provided at a “presentation level” (i.e., for each of the alternative streams), and do not provide for any frame specific encryption information:

Chen et al.

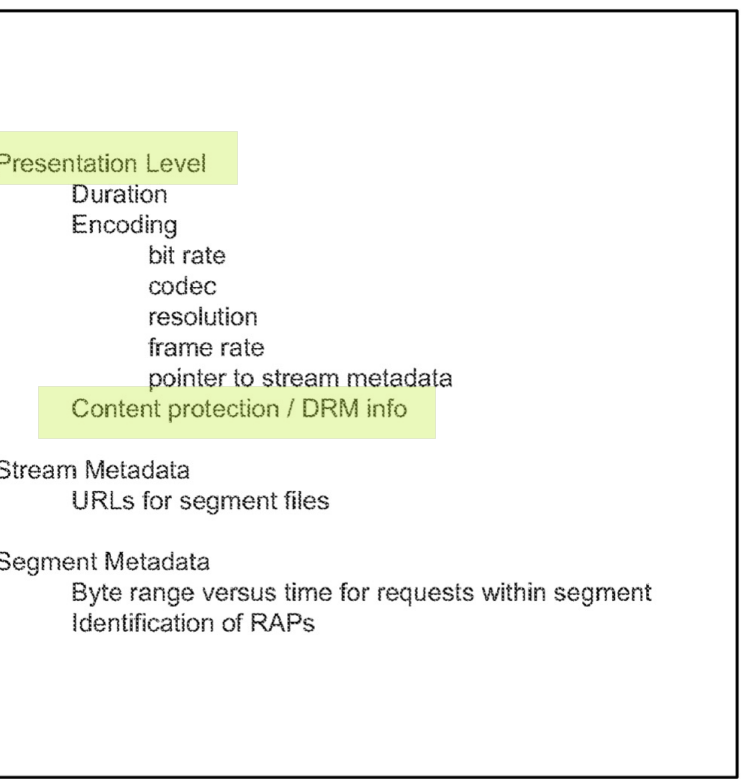


FIG. 9(a)

Chen's System Utilizes Segment-Level Encryption, Not Partial Frame Encryption.

Patent Owner's Expert Analysis

- ✓ Analysis of Chen's embodiments
- ✓ Analysis of other Chen statements and figures
- ✓ Analysis that partial frame encryption would require a modification of the standard file format in Chen

Petitioner's Expert Analysis

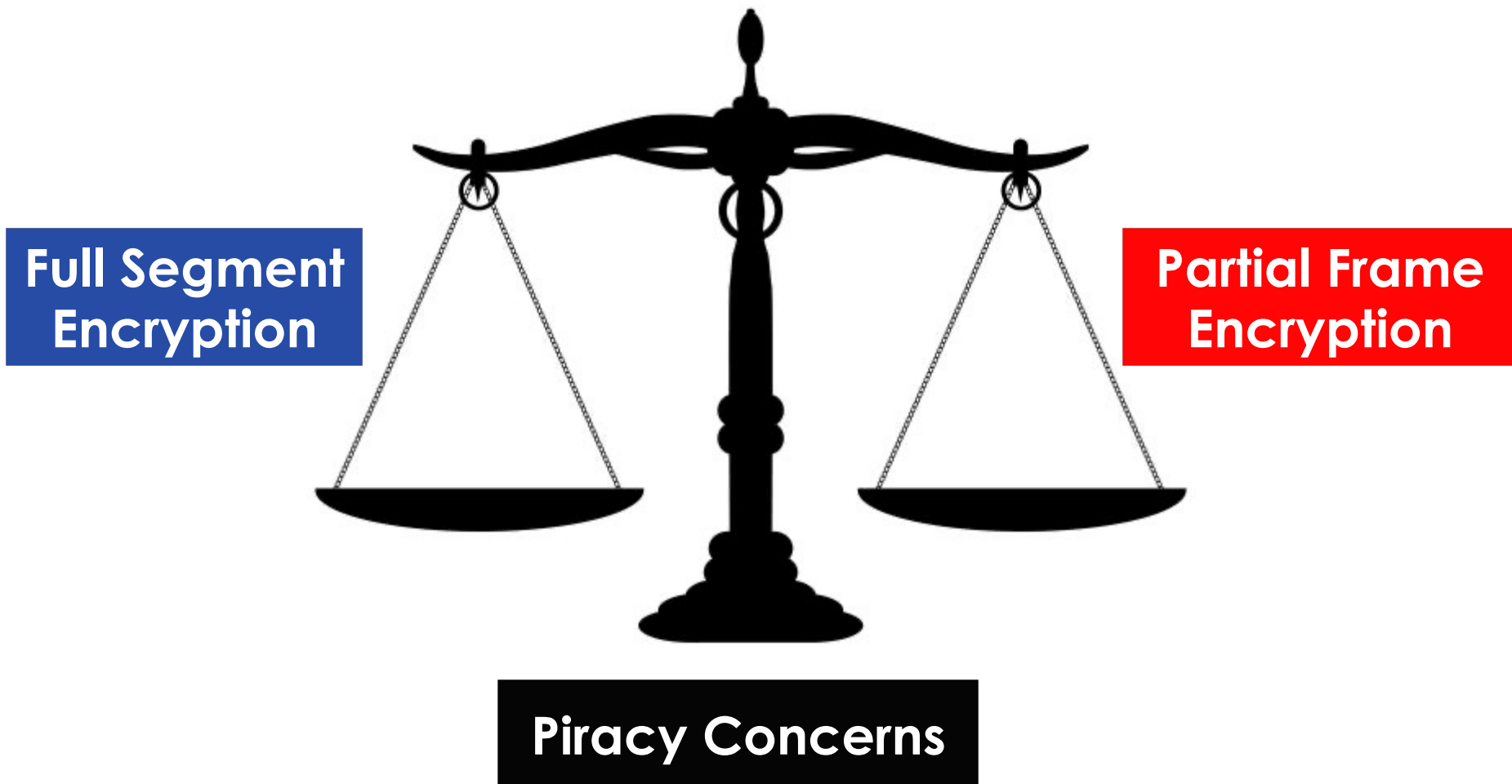


Petitioner Proposes Two Reasons To Modify Chen To Implement Partial Frame Encryption

PETITION FOR *INTER PARTES* REVIEW

① A POSITA would have been motivated to apply Lindahl's teachings to Chen to address piracy concerns and ② improve efficiency, which Chen also raises as a goal. Ex. 1003, ¶¶115, 119-120. The teachings of Chen relied on here reflect

1. No Evidence That Partial Frame Encryption Is Better Than Chen's Own Full Segment Encryption For "Piracy Concerns"



2. Partial Frame Encryption Will Not “Improve Efficiency” In Chen

Chen Without
Partial Frame
Encryption



Chen With Partial
Frame Encryption

Efficiency

A POSITA Would Have To Eliminate Integral Features Of Chen To Implement Partial Frame Encryption

DECLARATION OF SETH NIELSON, PH.D.

70. A POSITA would not have had a reasonable expectation of success in overcoming all of the obstacles identified above. Dr. McDaniel testifies that a POSITA has only one or two years of experience in “video streaming and media security.” Ex. 1003, ¶ 67. I do not believe that a person with this level of experience could implement partial frame encryption in the context of Chen’s system. As explained above, Chen’s layers could easily compromise the encrypted portions in a partially encrypted frame because unencrypted portions of a parallel layer could be used to fill-in encrypted portions. Similarly, Chen’s use of FEC could cause a similar problem of unencrypted portions revealing encrypted portions. Even if this issue could be overcome, there are also other additional challenges such as timing and manner of transmission of encryption parameters for packets that have not yet arrived, but are reconstructed using FEC. These are each significant hurdles that Petitioner and Dr. McDaniel do not address. I believe each of these problems is far beyond the level of skill of a POSITA because, *inter alia*, they involve complex mathematical, technical and system design aspects that well exceed the knowledge and experience of a POSITA.

a

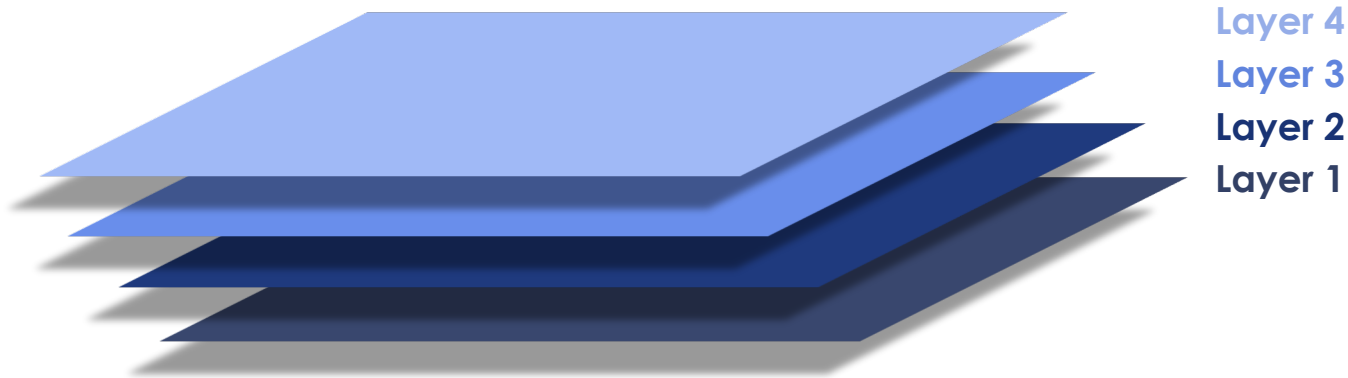
b

2a. Chen's "Layers" Implement Its Scalable Video Coding (SVC)

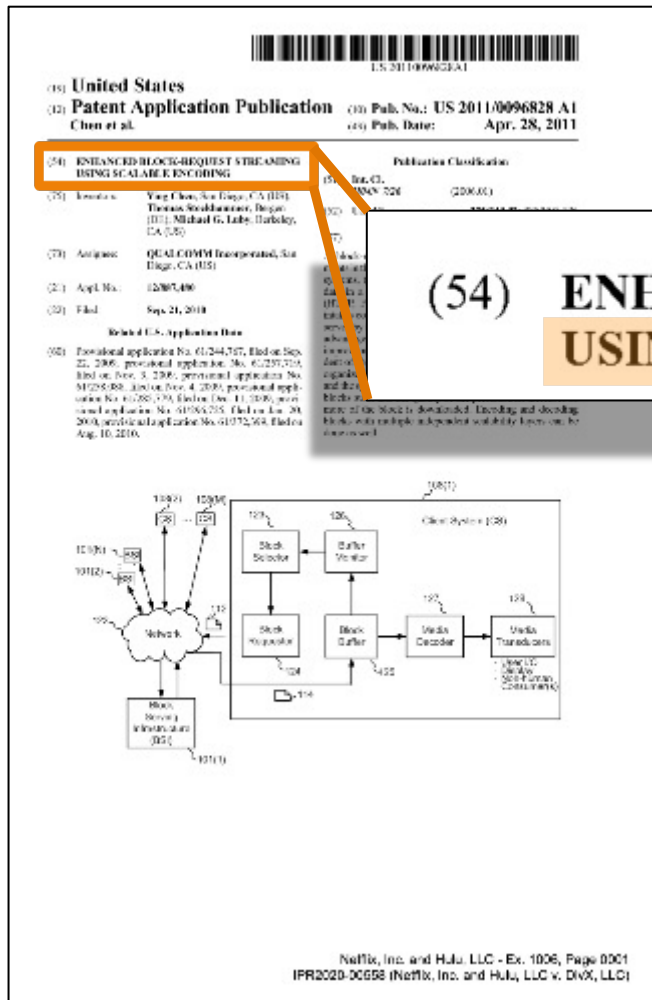
DECLARATION OF SETH NIELSON, PH.D.

58. Chen's "Scalable Layers" concept is related to a process known as "Scalable Video Coding" or SVC. This basic idea behind SVC is that a high-quality stream of media is coded such that packets can be lost (either dropped or delayed until unusable) without loss in quality. Higher quality video requires more data or information in order to create the higher quality pictures. In order to stream higher quality video over a network, the network must have the capacity for the greater quantities of data. SVC is designed to permit the quality to scale based on how much data is received. Instead of simply being unable to watch the high-quality video when network conditions worsen, the SVC coding permits the quality to degrade gracefully.

Scalable Video Coding (“SVC”) Encodes Video In Multiple Layers Of Quality



Scalable Video Coding Is Integral To Chen's System



(54) **ENHANCED BLOCK-REQUEST STREAMING
USING SCALABLE ENCODING**

Every Embodiment Of Chen Contains Scalable Blocks

**United States
Patent Application Publication**
Chen et al.

ENHANCED BLOCK-REQUEST STREAMING
USING SCALABLE ENCODING

ingestion process. The files or data elements are organized as blocks that are transmitted and decoded as a unit, and the system is configured to provide and consume scalable blocks such that the quality of the presentation increases as more of the block is downloaded. In some embodiments, novel improvements to methods for encoding and decoding blocks with multiple independent scalability layers are provided.

Petitioner Fails To Cite A Single Chen Embodiment Without Scalability

Every Embodiment Of Chen Contains Scalable Layers

United States Patent Application Publication Chen et al.

ENHANCED BLOCK-REQUEST STREAMING
USING SCALABLE ENCODING

Combinations

[0385] A number of embodiments are now described which may be advantageously employed by a block-request streaming client in order to achieve an improvement in the user experience and/or a reduction in serving infrastructure capacity requirements compared to existing techniques by use of media data partitioned into layers as described above.

[0388] In a third embodiment, the methods of the first and second embodiments may be combined such that there are provided multiple media representations each comprising a subset of the layers (as in the first embodiment) and such that the second embodiment is applied to a subset of the layers within a representation.

[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 to say that where an existing system might provide two dis-

[0387] In a second embodiment, a client in an enhanced block-request streaming system employing the method of layers now described may maintain a separate data buffer for each of several layers of the media encoding. As will be clear to those of skill in the art of data management within client

[0389] In a fourth embodiment the methods of the first, second and/or third embodiments may be combined with the embodiment in which multiple independent representations of the content are provided such that for example at least one of the independent representations comprises multiple layers to which the techniques of the first, second and/or third embodiments are applied.

Every Embodiment Of Chen Contains Scalable Layers; In Some Embodiments The Layers Are “Independent”

United States
Patent Application Publication
Chen et al.

ENHANCED BLOCK-REQUEST STREAMING
USING SCALABLE ENCODING

[0027]

ingestion process. The files or data elements are organized as blocks that are transmitted and decoded as a unit, and the system is configured to provide and consume scalable blocks such that the quality of the presentation increases as more of the block is downloaded. In some embodiments, novel improvements to methods for encoding and decoding blocks with multiple independent scalability layers are provided.

[0377]

One improvement detailed herein is an enhanced segment, a scalable segment map. The scalable segment map contains the locations of the different layers in the segment such that the client can access the parts of the segments accordingly and extract the layers. In another embodiment,

[0380]

To handle such situations, the block-streaming systems described herein might be configured to handle multiple scalability layers independently, such that a receiver can make layered requests and a transmitter can respond to layered requests.

Reply's Attorney Argument Incorrectly Implies That Chen's "Simplest Case" Does Not Include Scalability

What Petitioner's Reply Claims:

request streaming system" EX1006, ¶[0386]. And Chen teaches known, basic ABS: its "simplest case" stores "*Alternative* Representation[s]" as separate streams. EX1006, ¶[0070]. Chen's streams are *alternatives* to each other (*see id.*, Fig. 5), rather than enhancements of each other that are used together in scalable layers.

Reply, 9

What Chen Really Says:

[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

Irrelevant to whether Chen's Alternative Representations utilize scalability.

Efficiency: Chen's Scalability Method Allows Presentations To Continue Despite Bandwidth Changes

United States
Patent Application Publication
Chen et al.

(AVC). Advantageously, this method allows the presentation to continue based on the portion of a block that has been received even when reception of a block or blocks might be abandoned, for example due to changes in the available bandwidth. Another advantage is that a single data file may be used as the source for multiple different representations of the content. This is possible, for example, by making use of

Efficiency: Without Scalability, “Quality Is Necessarily Much Lower”

United States
Patent Application Publication
Chen et al.

creates a poor user experience. Stalls can be avoided, reduced or mitigated by restricting a data rate of the representations chosen to be much less than the available bandwidth, so that it becomes very unlikely that any given portion of the presentation would not be received in time, but this strategy has the disadvantage that the media quality is necessarily much lower than could in principle be supported by the available bandwidth. A lower quality presentation than is possible also can be interpreted as a poor user experience. Thus, the designer of

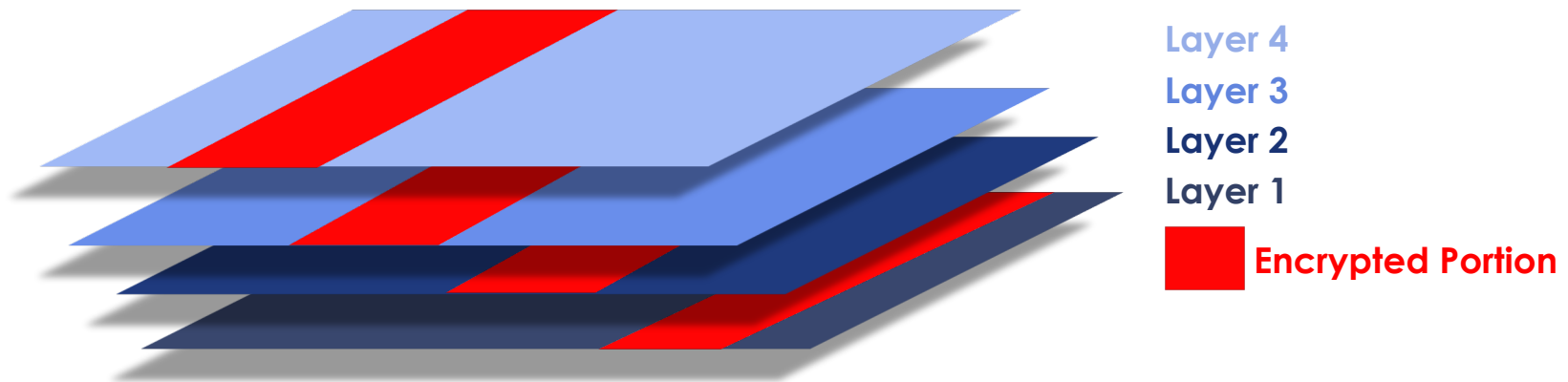
No Motivation/Reasonable Likelihood: Beyond A POSITA's Skill To Implement Partial Frame Encryption With Scalable Coding

DECLARATION OF SETH NIELSON, PH.D.

64. As I explained in the prior section, each fragment or segment in Chen is encoded as multiple parallel, scalable layers, and a user can reconstruct the requested video using only a subset of the layers. Ex. 1006 [Chen] ¶ 381. Chen's use of layers, however, is potentially incompatible with partial frame encryption because an unencrypted portion of one layer could be used to reconstruct the encrypted portion of a parallel layer, thus, compromising security. For example, as depicted below, an

70. A POSITA would not have had a reasonable expectation of success in overcoming all of the obstacles identified above. Dr. McDaniel testifies that a POSITA has only one or two years of experience in "video streaming and media security." Ex. 1003, ¶ 67. I do not believe that a person with this level of experience could implement partial frame encryption in the context of Chen's system. As

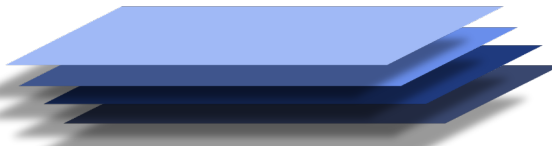
Dr. Nielson: Unencrypted Portion Of One Layer Could Be Used To Reconstruct Encrypted Portion Of Another Layer



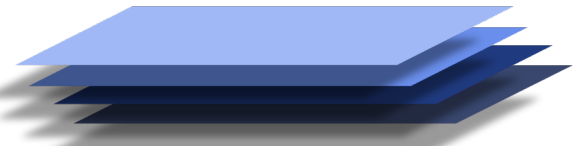
What If A POSITA Wanted To Reduce Encryption Burden Without Reducing Chen's Efficiency?



Frame 1 (Encrypted)



Frame 2 (Unencrypted)



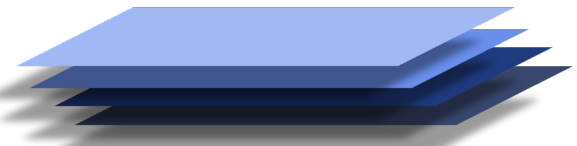
Frame 3 (Unencrypted)



Frame 4 (Unencrypted)



Frame 5 (Encrypted)



Frame 6 (Unencrypted)

DECLARATION OF SETH NIELSON, PH.D.

just to implement partial frame encryption. In fact, even if a POSITA desired to reduce the encryption burden in Chen, he or she would have likely implemented the much more routine and much simpler process of encrypting some, but not all, fragments, on a periodic basis. For example, a POSITA could have encrypted, *e.g.*,

A POSITA Would Not Have Eliminated Chen's Scalability Just To Implement Partial Frame Encryption

Patent Owner's Expert Analysis

- ✓ Analysis of Chen's system
- ✓ Analysis of scalability of Chen's system
- ✓ Analysis of compatibility of scalability with partial frame encryption
- ✓ Analysis of Chen with and without scalability
- ✓ Analysis of POSITA's skills in implementing partial frame encryption with scalability

Petitioner's Expert Analysis



Bruce Schneider, Leading Cryptography Expert: You Cannot Tack Cryptography On A System As An Afterthought

But the cryptography now on the market doesn't provide the level of security it advertises. Most systems are not designed and implemented in concert with cryptographers, but by engineers who thought of cryptography as just another component. It's not. You can't make systems secure by tacking on cryptography as an afterthought. You have to know what you are doing every step of the way, from conception through installation.

Billions of dollars are spent on computer security, and most of it is wasted on insecure products. After all, weak cryptography looks the same on the shelf as strong cryptography. Two e-mail encryption products may have almost the same user interface, yet one is secure while the other permits eavesdropping. A comparison chart may suggest that two programs have similar features, although one has gaping security holes that the other doesn't. An experienced cryptographer can tell the difference. So can a thief.



Petitioner Had The Burden To Show How And Why A POSITA Would Have Modified Chen As Proposed



“At the very least, Petitioner has not adequately supported its ‘good idea’ rationale for storing recovery information in the main memory database. We consider the added cost, limited capacity, and volatility of main memory databases at the time of the invention to be further reasons why an ordinarily skilled artisan would not have modified O’Neil’s databases as proposed by Petitioner.”

Hulu LLC v. Sound View Innovations LLC,
IPR2018- 00582, Paper 34 at 20-21 (PTAB Aug. 5, 2019) (informative)

Incompatibility of Chen's Scalability With Partial Frame Encryption Is Sufficient To Deny The Petition



POSITA Could Not Implement Yet Additional “Efficiency” Features Of Chen With Partial Frame Encryption

DECLARATION OF SETH NIELSON, PH.D.

used to fill-in encrypted portions. Similarly, Chen's use of FEC could cause a similar problem of unencrypted portions revealing encrypted portions. Even if this issue could be overcome, there are also other additional challenges such as timing and manner of transmission of encryption parameters for packets that have not yet arrived, but are reconstructed using FEC. These are each significant hurdles that Petitioner and Dr. McDaniel do not address. I believe each of these problems is far beyond the level of skill of a POSITA because, *inter alia*, they involve complex mathematical, technical and system design aspects that well exceed the knowledge and experience of a POSITA.

POSITA Could Not Implement Yet Additional “Efficiency” Features Of Chen With Partial Frame Encryption

DECLARATION OF SETH NIELSON, PH.D.

61. In addition to independent, scalable layers, another example of a technique used by Chen to improve its performance, latency, and efficiency is Forward Error Correction (FEC). FEC is a technique wherein each packet of data includes certain information about subsequent packets. Ex. 1006 [Chen] ¶ 88. Through FEC, the already received packets can supplement or correct other packets that may have parts corrupted during transmission. Chen, however, utilizes FEC as

Dr. Nielson Explains: It Was Beyond A POSITA's Skills To Implement FEC With Partial Frame Encryption

DECLARATION OF SETH NIELSON, PH.D.

68. A similar problem—unencrypted portions being used to decrypt encrypted portions—exists with attempting to implement partial frame encryption in connection with the FEC feature of Chen. As explained above, FEC provides correction information for packets in advance of the packets actually being received. If each packet is only partially encrypted, then the information from an unencrypted portion of an earlier packet may be used to decrypt the encrypted portion of a later packet without the need for the encryption key. For example, if packets 1-7 include FEC bits that allow for the reconstruction of packets 8-10, then the unencrypted portions of packets 1-7 could be used to determine the information contained in the encrypted portion of packets 8-10. This is a similar problem to the one I explained

Undisputed: Chen's Forward Error Correction (FEC) Improves Its Efficiency By Up To 70%

**United States
Patent Application Publication**
Chen et al.

ENHANCED BLOCK-REQUEST STREAMING
USING SCALABLE ENCODING

a channel zapping time of 1.7 seconds. Thus, in the example shown in FIG. 26, the No-FEC method is 70% worse in terms of channel zapping time than the FEC method. One of the reasons for the advantage shown by the FEC method in this example is that, for the FEC method, reception of any 80% of the requested data allows recovery of the fragment, whereas for the No-FEC method, reception of 100% of the requested data is required. Thus, the No-FEC method has to wait for the slowest TCP connection to finish delivery, and because of

Petitioner's Expert: Exhibit 1023 Proves That Partial Frame Encryption "Does No Harm" To FEC

Declaration of Patrick McDaniel, Ph.D.

12. Various prior art references (and known practices) teach the application of FEC-*after*-encryption, particularly for partial encryption, because “[a]pplying FEC to data which already has been partially encrypted ***does no harm*** with respect to the data security.” **EX1023, 217** (emphasis added). When used in

Ex. 1023: Partial Frame Encryption Not Harmful To FEC Only If FEC Is Not “Applied To The Application Layer Data”

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.

Chen Applies Its FEC Code To Its Application Layer Data

**United States
Patent Application Publication**
Chen et al.

ENHANCED BLOCK-REQUEST STREAMING
USING SCALABLE ENCODING

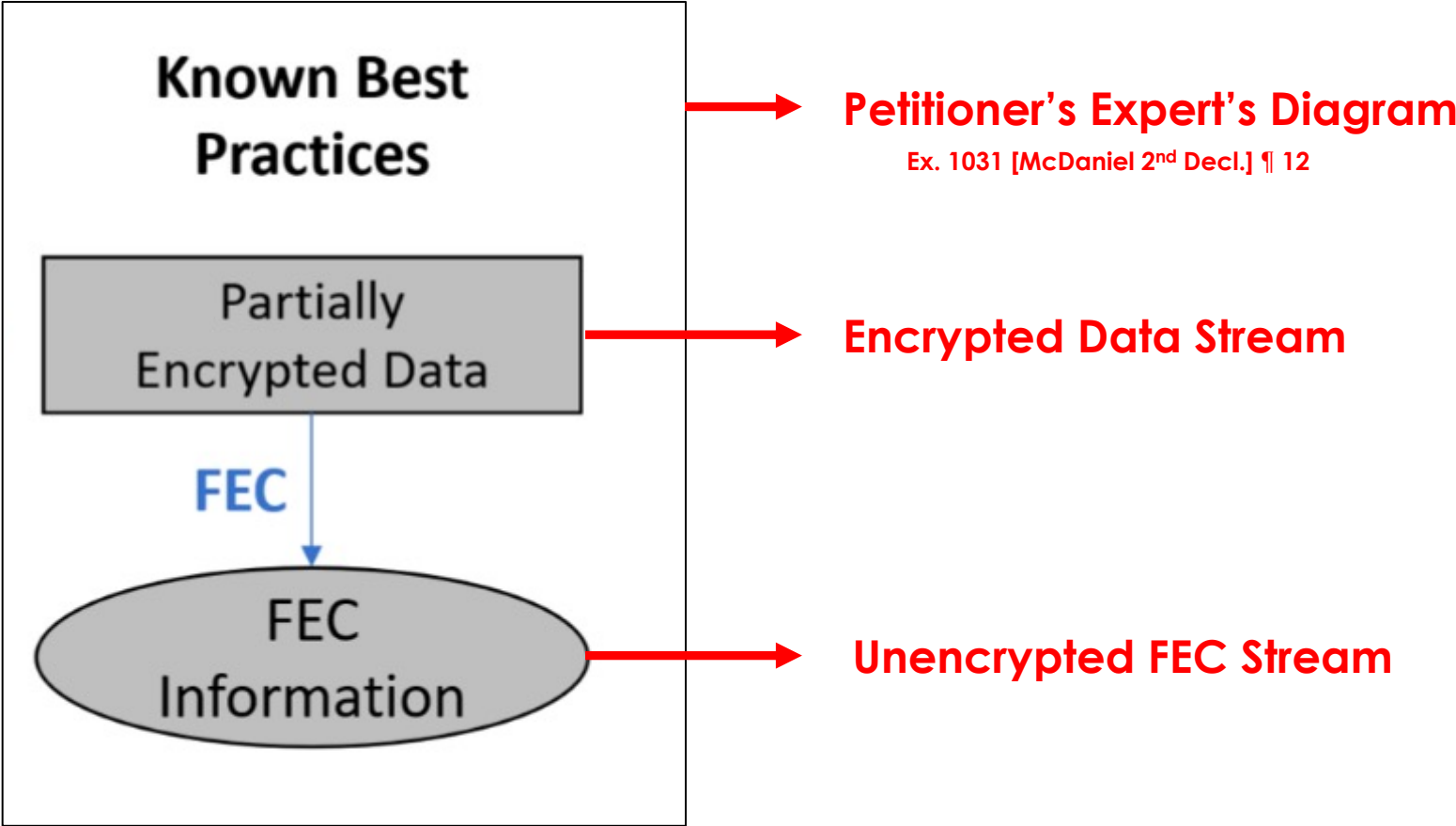
employed to advantage. In these embodiments, an erasure code is applied to each fragment to generate redundant versions of the data. Preferably, the source formatting is not

Ex. 1023 Confirms Dr. Nielson By Identifying “Redundancy Of The Transmitted Data” As A Threat With Partial Frame Encryption

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

Petitioner's Expert: Partial Encryption Is Safe If FEC Created After Partial Encryption As An Unencrypted FEC Stream

Declaration of Patrick McDaniel, Ph.D.



FEC Standard: Unencrypted FEC Stream With Encrypted Data Creates A “Layering Violation”

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.

Chen Discusses Non-FEC Method Only To Show Why A POSITA Should Use The FEC Method

United States
Patent Application Publication
Chen et al.

ENHANCED BLOCK-REQUEST STREAMING
USING SCALABLE ENCODING

zapping time could be large. Using the FEC method has the same advantages as the No-FEC method, and has the additional advantage that not all of the requested data needs to arrive before the fragment can be recovered, thus further reducing the channel zapping time and the variability in the channel zapping time. By making requests over different TCP connections, and over-requesting by also requesting FEC repair data on at least one of the connections, the amount of time it takes to deliver a sufficient amount of data to for example recover the first requested fragment that enables media playback to start, can be greatly reduced and made to be much more consistent than if cooperative TCP connections and FEC repair data was not used.

Chen Does Not Identify A Single Drawback For Its FEC Method

Petitioner Had To Present An Analysis Of Benefits And Drawbacks



"The Board must weigh the benefits and drawbacks of the modification against each other, to determine whether there would be a motivation to combine."

Arctic Cat Inc. v. Polaris Indus., Inc.,
795 F. App'x. 827, 833 (Fed. Cir. 2019)

Petitioner Chose To Place Improved “Efficiency” As A Motivation To Modify Chen



“Petitioner chose to argue that a [POSITA] implementing the teachings of Kim would have been motivated to consider Huang to obtain ‘better image quality’ (Pet. 39), and therefore retains the burden to prove the same. Had Petitioner not contended that combining Huang results in better image quality than Kim alone, we would not have needed to consider whether the combination results in ‘better image quality.’”

Unified Patents Inc. v. DivX LLC,
IPR2019-01379, Paper 52, 35 (PTAB Feb. 8, 2021) (Ahmed, J.)

Petitioner's Argument Against Claimed "Bodily Incorporation" Is Misplaced



“Rather than requiring Petitioner to demonstrate ‘bodily incorporation,’ Patent Owner’s arguments and evidence show that an ordinarily skilled artisan would not have expected to achieve Petitioner’s stated rationale in combining the references’ teachings in the way Petitioner proposes.”

Unified Patents Inc. v. DivX LLC,
IPR2019-01379, Paper 52, 36-39 (PTAB Feb. 8, 2021) (Ahmed, J.)

Yet More Reasons Against Modifying Chen: A POSITA Would Have To Modify The Standard File Format

DEPOSITION OF PATRICK MCDANIEL, Ph.D.

25 Q Okay. Do any of the embodiments that you
1 rely on from Chen in your declaration require a
2 modification of a standard file format in order to
3 enable encryption?

4 MR. LIANG: Object to form.

5 THE WITNESS: Yeah, I think the
6 combination -- we are talking about Chen with, you
7 know, using things like partial encryption would
8 require some additional encryption information.

9 For example, to process the contents, so you
10 would probably have to make some modifications to 3GPP
11 to enable or to -- not enable -- to implement the
12 combination of Chen, Hurst and Lindahl.

Petition's Showing That A POSITA Would Have Had A Reasonable Expectation Of Success In Modifying The Standard File Format



Reply's Change Of POSITA And New Evidence To Argue *Prima Facie* Case Of Reasonable Expectation Of Success Are Untimely

Petitioner In Petition

Did not recognize the need to modify the standard file format

Expert opined that POSITA could "use" standard file formats. Ex. 1003, ¶68

No expert opinion on the subject

No exhibits in support

Petitioner In Reply

Argues that a POSITA had a reasonable expectation of success in modifying the standard file format

Expert opines that a POSITA could modify standard file formats. Ex. 1031, ¶15

Five pages of new expert opinion to argue prima facie case

Five new exhibits to argue prima facie case (Exs. 1017-1018; 1020-1022)

Board Routinely Rejects Arguments On Reasonable Expectation Of Success Raised For The First Time In Petitioner's Reply



“[T]he expedited nature of IPRs bring with it an obligation for petitioner to make their case in their petition to institute.”

Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.,
821 F.3d 1359, 1369 (Fed. Cir. 2016)

A POSITA Would Consider The Need To Modify File Format As Yet Another “Disadvantage” Against Motivation To Modify Chen



“As further evidence against Petitioner’s proposed combination, Patent Owner argues that **an ordinarily skilled artisan would have considered other disadvantages** of main memory databases.

...

Thus, in the absence of other persuasive reasons to modify O’Neil, the record evidence of high cost and limited capacity associated with main memory databases **tends to undermine the implication that an ordinarily skilled artisan would have** used main memory instead of conventional disk-based memory.”

*Hulu LLC v. Sound View Innovations LLC,
IPR2018- 00582, Paper 34 at 19 (PTAB Aug. 5, 2019) (informative)*

Table Of Contents

1. Petitioner Fails To Show “Locating Encryption Information ... Within The Requested Portions Of The Selected Stream Of Protected Video.”
 - 1.A. In Contrast To Petitioner’s Attorney Arguments, Patent Owner’s Construction Is Supported By The Plain Meaning, Every Embodiment, And Unrebutted Expert Testimony.
 - 1.B. The Petition Does Not Argue The “Locating” Limitation Is Disclosed/Obvious Under Patent Owner’s Construction.
2. Petitioner Fails To Show That A POSITA Would Have Modified Chen To Implement Partial Frame Encryption.
3. **Petitioner Fails To Show That A POSITA Would Have Encrypted Alternative Streams Of Protected Video With “A Set Of Common Keys Comprising At Least One Key.”**

“[E]ach Of The Alternative Streams Of Protected Video ... Are Encrypted Using A Set Of Common Keys Comprising At Least One Key”

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

(10) Patent No.: US 10,225,588 B2
(45) Date of Patent: *Mar. 5, 2019

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

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;

obtaining a copy of the set of common keys;
detecting streaming conditions for the playback;
selecting a stream from the plurality of alternative streams of protected video based on the streaming conditions;

receiving a container index that provides byte ranges for portions of the selected stream of protected video within an associated container file;

requesting portions of the selected stream of protected video based on the provided byte ranges;

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

decrypting each encrypted portion of the frames of video identified within the located encryption information using the set of common keys; and

playing back the decrypted frames of video obtained from the requested portions of the selected stream of protected video.

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 Petition Relies On Lindahl And Hurst To Modify Chen To Encrypted Alternative Streams With A Common Set Of Keys

PETITION FOR *INTER PARTES* REVIEW

[1e] that are encrypted using a set of common keys comprising at least one key,

Lindahl and Hurst both teach or suggests this limitation, and either is sufficient by itself to render the limitation obvious. Ex. 1003, ¶¶143-151.

It Is Not Sufficient That Individual Claim Limitations May Have Been Separately Known



“We have observed that the prejudice of hindsight bias often overlooks that **the genius of invention is often a combination of known elements which in hindsight seems preordained.** We have also recognized that, when the art in question is relatively simple, as is the case here, the opportunity to judge by hindsight is particularly tempting.”

Polaris Indus. v. Arctic Cat, Inc.,
882 F.3d 1056, 1068 (Fed. Cir. 2018)

A POSITA Would Not Have Used A Set Of Common Keys In The Context Of A System With Claimed Features

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

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:

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;

obtaining a copy of the set of common keys;

detecting streaming conditions for the playback device;

selecting a stream from the plurality of alternative streams of protected video based on the detected streaming conditions;

receiving a container index that provides byte ranges for portions of the selected stream of protected video within an associated container file;

requesting portions of the selected stream of protected video based on the provided byte ranges;

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

decrypting each encrypted portion of the frames of video identified within the located encryption information using the set of common keys; and

playing back the decrypted frames of video obtained from the requested portions of the selected stream of protected video.

Sophisticated system that includes a top-level index file and video encoded in alternate streams

Partial frame encryption that requires modification of the standard file format and custom made decoders

Generally less secure

Sophisticated receiver that selects a stream and requests portions of video based on byte ranges

A POSITA Would Not Have Used A Set Of Common Keys In The Context Of A System With Claimed Features

DECLARATION OF SETH NIELSON, PH.D.

113. First, the Petition does not explain why, if media content were so unimportant that it would be consistent with Lindahl's teachings to encrypt it using a single global key, the content producer or server would invest the substantial effort of encoding that "not that sensitive" content with multiple alternative bitrates to create multiple alternative streams for it to be viewed by end-users, as opposed to simply utilizing a single stream for low-priority free content. Ex. 1007 [Lindahl] ¶

Protection System For DVDs Was Rendered Obsolete In The 90s For Using Too Few/Global Keys

THE ANONYMOUS DEVELOPERS of the decryption program that removes DVD copy protection had an easy time doing it, thanks to a gaffe by a software developer and the surprising weakness of the encryption technology. Essentially, the two European hackers who developed the DeCSS utility that copies a DVD movie disc were able to break the code because one of the product's licensees inadvertently neglected to encrypt the decryption key.

Industry experts were stunned by the hack because DVD as a movie-playing format is supposed to be copy-proof. In fact, DVD would not be on the market today without the permission of the motion picture industry which, sources say, is reeling from this development.

Breaking DVD's encryption was considered extremely difficult, but once the first key was discovered, the rest fell with ease, since the crackers were able to use their original, valid key as a launch point to find more valid decryption keys.

Even Free Broadcast Systems Did Not Use Global Keys

Commercial restrictions and targeting

The free-to-view system allows for restricting access based on location of the viewer. For example, in the UK prior to the launch of Astra 2D, UK channels broadcasting from the Astra 28.2°E satellites used a wide beam and could be received across Europe on small dishes. Those channels which were non-subscription but aimed at the UK only, or restricted from broadcasting outside the UK by way of programme rights (such as Channel 5) or governance (such as the BBC channels), were broadcast encrypted using Videoguard (as used by Sky (UK) for its pay-TV services) with viewing cards made available to UK residents only.^[3]

Petitioner's Expert Cites No Evidence That It Was “Well-Known” To Use The Same Key To Encrypt All Streams

§42.65 Expert testimony; tests and data.

(a) Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight. Testimony on United States patent law or patent examination practice will not be admitted.



Petitioner's Expert Only Presents Conclusory Assertions

Declaration of Patrick McDaniel, Ph.D.

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 using that set of keys. *See id.* Thus Hurst teaches the natural and obvious

Ex. 1003 [Reader Decl.] ¶ 116

Why?

What Is The Processing Gain?

How Does It Compare To Loss Of Security?

Lindahl Does Not Help Petitioner--Undisputed That It Has No Disclosure About Alternative Streams

6 Q Sure. Is there any embodiment in Lindahl
7 that discloses multiple alternative bitrates encoding
8 of media file?

9 A Again, that's not the purpose of Lindahl,

Lindahl Does Not Help Petitioner--Undisputed That Lindahl Is Not Even About Streaming

4 Is it your contention that reference to
5 streaming in Paragraph 65 of Lindahl, is referencing
6 streaming media and the fact that the user consumes
7 the media as it is received and before the entire file
8 is downloaded?

9 A No. But it is inviting the user as a means

Hurst Does Not Help Petitioner--Undisputed That It Gives No Particular Reason To Use A Set Of Common Keys

20 So I will ask the question again. If you
21 would please just answer the question, which is: Does
22 Hurst disclose any benefit or advantage for using the
23 same key to encrypt different bitrate of the same
24 video?

25 A While I don't see an explicit disclosure of
1 an advantage by Hurst, the whole point of Hurst is,
2 you know, particular, the processing of the adaptive
3 bitrates to improve performance.

Hurst Only States That A POSITA Could Use A Single Key, But Would “Beneficially” Use Different Keys

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. Alternatively, 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 authenticate a client device and accordingly communicate the appropriate decryption key.

Hurst Does Not Suggest Using The Same Key And Partial Frame Encryption Together

DECLARATION OF SETH NIELSON, PH.D.

acknowledges that such a configuration is possible. Even more to the point, there is no disclosure in Hurst to suggest to a POSITA that use of the same key to encrypt alternate streams of protected video provides adequate security in a system that *also* uses partial frame encryption as disclosed by Lindahl—as using both the same key and partial encryption could negatively impact security.

Petitioner Failed Its Burden To Show Why A POSITA Would Have Use A Single Key For All Alternative Streams In Chen



"It is not enough to say that...to do so would 'have been obvious to one of ordinary skill.' ***Such circular reasoning is not sufficient***—more is needed to sustain an obviousness rejection."

Kingston Tech. Co., Inc. v. Polaris Innovations Ltd.,
IPR2016-01622, Paper 7, 15- 16 (PTAB Feb. 15, 2017)
(citing *In re Chaganti*, 554 Fed. Appx. 917, 922 (Fed. Cir. 2014))



"[T]ak[ing] the ***inventor's disclosure as a blueprint*** for piecing together the prior art to defeat patentability" in this manner is ***"the essence of hindsight."***

In re Dembiczak, 175 F.3d 994, 999 (Fed. Cir. 1999)

Petition's Use Of Patent As A Roadmap Is Impermissible

PETITION

depending on channel bandwidth. Ex. 1003, ¶116. 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 using that set of keys. *See id.* Thus, Hurst teaches the natural and obvious

Pet., 19

'588 PATENT

putationally intensive process, the playback device can use the same cryptographic information to access content in any of the alternative streams of protected content within a single instance of a title.



Ex. 1001 ['588 Pat.] 13:11-21



Reserve

It Is Not Practical To Encrypt Only Overlapping Portions Of Layers In Scalable Video Coding

DECLARATION OF SETH NIELSON, PH.D.

evident. For example, it would be impractical to attempt to encrypt identical segments of parallel layers because range of bytes in one layer does not correspond to the range of bytes in another layer and, therefore, it would be very difficult to create a system wherein only overlapping portions of layers are encrypted. *See also* Ex. 1006 [Chen] ¶ 135 (“fragments are not aligned between the different rate streams.”).

The '588 Patent Teaches At Length How To Modify The Standard File Format

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

(10) **Patent No.:** **US 10,225,588 B2**
(45) **Date of Patent:** ***Mar. 5, 2019**

In many embodiments, the top level index file is a SMIL file and the media is stored in Matroska container files. As is discussed further below, the media can be stored within the Matroska container file in a way that facilitates the protection of the content using common cryptographic information. In many embodiments, the Matroska container files are specialized Matroska container files that include enhancements (i.e. elements that do not form part of the Matroska file format specification) that facilitate retrieval and decryption using common cryptographic information of specific portions of media during adaptive bitrate streaming.

Ex. 1001 ['588 Pat.] 11:45-50

Each Cluster element 48 includes a Timecode element 60 indicating the start time of the encoded video within the Cluster element and a plurality of BlockGroup elements. As noted above, the encoded video stored within the Cluster is constrained so that the encoded video can be played back without reference to the encoded video contained within any of the other Cluster elements in the container file. In many embodiments, encoding the video contained within the Cluster element as a GOP in which the first frame is an IDR frame enforces the constraint. In the illustrated embodiment, the first BlockGroup element 62 contains an IDR frame. Therefore, the first BlockGroup element 62 does not include a ReferenceBlock element. The first BlockGroup element 62 includes a Block element 64, which specifies the Timecode attribute of the frame encoded within the Block element 64 relative to the Timecode of the Cluster element 48 and a DRMInfo element 65 that identifies a portion of the frame that is encrypted and the cryptographic information that can be utilized to access the encrypted portion of the frame. In a number of embodiments, only a small portion of the video frame is encrypted and the DRMInfo includes a reference to the start of an encrypted block of data and the size of the encrypted block of data. As is discussed further below, the common cryptographic information utilized to protect alternative streams of video content is a set of frame keys in many embodiments of the invention and the DRMInfo element can also include an index to a specific frame key in the set of frame keys that can be utilized to access the encrypted block of data in the clear. In other embodiments, any of a variety of information appropriate to identifying encrypted data within a video frame and decrypting the encrypted data can be stored within a DRMInfo element.

Ex. 1001 ['588 Pat.] 16:21-52

Petitioner's Reliance On Ex. 1030 [Demos] To Argue Compatibility Of Scalable Coding With Partial Frame Encryption Is Misplaced

- ✗ Petitioner does not show that Demos utilizes scalable video coding and partial frame encryption **in the same embodiment**
- ✗ Demos states that partial frame encryption only works **in certain types of encryption**, e.g., where "GOPs are used as a unit of encryption."
- ✗ Demos has **no teaching about how** to implement scalable coding with partial frame encryption
- ✗ Demos does not show that **a POSITA, as opposed to an expert**, could implement scalable coding with partial frame encryption
- ✗ Not surprisingly, Petitioner does not provide **any expert support**

Petitioner Misrepresents Dr. Nielson's Testimony

Reply's Claim:

Dr. Nielson's scalable layer opinions are based on principles of "motion compensation" including "B and P" frame types. EX2012, ¶¶59, 66. But he did not know "[w]hat information is needed to perform motion compensation..." EX1029,

Reply, 12-13

Reality : Dr. Nielson Was Not Provided The MPEG Standard To Answer Questions About Details Of MPEG-4

15 Q. What information is needed to
16 perform motion compensation in MPEG-4?
17 MR. HENDIFAR: Objection, scope,
18 relevance, incomplete hypothetical.
19 A. And I would have the same answer,
20 which is: Without the standard, I can't do
21 those kind of details.

Ex. 1029 [Nielson 2nd Depo.] 91:15-21

Dr. Nielson: Professor And Researcher On Network Security; Industry Expert On Security And Data Breach

4 Q. Now, at Johns Hopkins, you taught
5 Advanced Network Security; is that right?
6 A. I did teach that class, yes.

Ex. 1029
24:4-6

18 Q. Okay. Do you teach network security
19 at UT?
20 A. The full name of the class is
21 Network Security and Privacy. That's one class
22 that I teach.

Ex. 1029
27:18-22

19 In my case in particular, as I was
20 the director of advanced research projects for
21 the institute, I was also tasked with trying to
22 bring in outside groups to collaborate on
23 these; and in this particular case, we were
24 collaborating with a group that was at the time
25 known as Onboard Security.

Ex. 1029
26:19-25

5 So this program was called M.S.S.I.,
6 Master's of Science and Security Informatics,
7 and it was a master's degree focused entirely
8 on computer security. The students had to take
9 a very wide range of courses in security topics
10 and had to complete a capstone project.

Ex. 1029
26:5-10

12 And so part of what I've been doing
13 is finding all the places people made mistakes.
14 I have been doing a deeper analysis than
15 they've done in the past about how critical the
16 data is and what an attacker might be able to
17 do with it and how, and, in some ways, helping
18 them to try and get those processes, even their
19 audit processes improved.

Ex. 1029
31:12-19

19 And the general themes are
20 cryptography/computer security, networking, and
21 software engineering; is that right?
22 A. That's a lot of my work, yes.

Ex. 1029
33:19-24

19 Q. So what do you spend the other 50
20 percent of your time on at Crimson Vista?
21 A. I work with a lot of different
22 clients on a number of computer security
23 issues: For example, I'm in Atlanta right now
24 working with a client post data breach. I

Ex. 1029
30:19-24

16 Q. At Johns Hopkins, did you work on a
17 research project regarding drones?
18 A. I did.

Ex. 1029
24:16-18

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the following documents were served by electronic service, by agreement between the parties, on the date signed below:

PATENT OWNER'S DEMONSTRATIVE EXHIBITS (EXHIBIT 2029)

The names and address of the parties being served are as follows:

Harper Batts	HBatts@sheppardmullin.com,
Chris Ponder	CPonder@sheppardmullin.com,
Jeffrey Liang	JLiang@sheppardmullin.com, and
	LegalTm-DivX-IPR@sheppardmullin.com

Respectfully submitted,

/Keith Moore/

Date: May 18, 2021